ESTAFAS Y FRAUDES FINANCIEROS EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

NO BAJES LA GUARDIA: PROTÉGETE

Las estafas y fraudes financieros en entornos digitales no son nuevos, pero la inteligencia artificial (IA) ha hecho que sean más sofisticados y difíciles de detectar. Para proceder al engaño, los delincuentes ahora recurren a mensajes y sitios web ficticios, perfiles falsos de personas famosas e incluso a voces o vídeos generados por IA que imitan a empleados de tu banco, a tus amigos o a familiares.

Suelen ponerse en contacto contigo a través de las redes sociales, aplicaciones de mensajería, por correo electrónico y mediante llamadas inesperadas que parecen reales.

Los riesgos van desde pérdidas económicas hasta la suplantación de identidad y el estrés emocional. Ten cuidado y sigue estos consejos básicos para proteger tu seguridad:

Cuidado con las estafas y fraudes financieros en entornos digitales que emplean IA
por ejemplo, la suplantación de identidad, el *phishing*, las estafas de inversión y de seguros, e incluso las estafas y fraudes amorosos o afectivos. Infórmate sobre los diferentes tipos de estafas y fraudes (consulta las páginas 5, 6, y 7).

Y sobre estafas y fraudes específicos relacionados con criptoactivos (consulta el folleto específico sobre estafas y fraudes relacionados con criptoactivos).

Identifica las señales de alerta:
Aprende a reconocer comportamientos, mensajes u ofertas sospechosos (consulta la página 2).

Protégete:
Protege tu información personal (consulta la página 3).

Conoce cómo actuar si eres víctima de estafas o fraudes
(consulta la página 4).

Señales de alerta

Una promesa que parece demasiado buena para ser cierta.

Una llamada inesperada de un número desconocido.

Una solicitud de dinero urgente o de información personal, incluso de alguien que parece ser un familiar, un amigo o hasta de una figura pública.

Una solicitud para acceder a tu dispositivo, descargar una aplicación, escanear un código QR o hacer clic en un enlace.

Una solicitud de información personal o de datos bancarios (por ejemplo, contraseñas, números de tarjetas de crédito, claves de acceso a la banca electrónica o códigos de seguridad).

Una solicitud de pago a través de métodos no rastreables (por ejemplo, criptoactivos, tarjetas de regalo, envío de dinero o tarjetas prepago).

Una dirección de correo electrónico o un enlace sospechoso o incorrecto (por ejemplo, errores ortográficos en la URL o direcciones web inusuales).

Un archivo adjunto de una fuente desconocida, especialmente .exe, .scr, .zip o un archivo de Office habilitado para macros (.docm, .xlsm).

Errores gramaticales o de formato en un documento de aspecto oficial, aunque cada vez son más difíciles de detectar gracias a la IA.

Un sitio web que parece profesional, pero que no incluye datos de contacto verificados ni información del registro de la empresa.

Una entonación que suena poco natural, sin pausas y parece excesivamente fluida o robótica. Cuidado con la «clonación de voz», aunque el habla generada por IA también puede sonar muy natural.

Videos en los que la voz puede sonar robótica o demasiado fluida, en los que los movimientos de los labios y las expresiones faciales pueden ir desacompasados con la voz, o donde el fondo, la iluminación y las sombras pueden ser incoherentes. A menudo se trata de videos generados por IA (*deepfakes*).

Pasos para protegerte

1 **Nunca compartas información personal ni datos bancarios:**

Las empresas legítimas nunca te pedirán tus PIN, contraseñas, claves de acceso a la banca electrónica ni códigos de seguridad por correo electrónico, mensajes de texto, redes sociales ni por teléfono.

2 **Para un instante y piensa antes de actuar:**

No te precipites al enviar dinero, compartir información o hacer clic en enlaces: los estafadores crean deliberadamente una sensación de urgencia (por ejemplo, problemas informáticos con tu banco, llamadas de emergencia relacionadas con amigos o familiares, lenguaje amenazante, etc.). En caso de duda, por pequeña que sea, no actúes; termina la llamada y verifica la autenticidad de la fuente o su identidad.

3 **Verifica la autenticidad de la fuente/su identidad:**

- Verifica siempre la procedencia de los mensajes, llamadas, correos electrónicos y enlaces, incluso si aparentan ser oficiales o parecen provenir de un amigo o familiar, o incluso de una figura pública. Por ejemplo, llama o envía un mensaje de texto a tus familiares y amigos utilizando un número conocido y a través de un canal de confianza; revisa si hay errores ortográficos, URL extrañas o faltan indicadores de seguridad (por ejemplo, verifica que el enlace del sitio web incluya una «s» en «https» para asegurarte de que es seguro y comprueba si hay letras de más o de menos en el nombre de la empresa).

- No abras enlaces de mensajes no solicitados, instala solo aplicaciones oficiales de tiendas de aplicaciones de confianza y no escanees códigos QR desconocidos.

- Elige con tu familia una «palabra de seguridad»: una frase secreta que puedas usar para confirmar la identidad de alguien con voz familiar que llama con una petición urgente de dinero y afirma ser un miembro de la familia (por ejemplo, padre o madre, hermano, hijo).

- Usa datos de contacto verificados para ponerte en contacto directamente con la empresa o la persona y nunca confíes en la información proporcionada por el presunto estafador (por ejemplo, busca el nombre de la empresa por tu cuenta, utiliza directorios empresariales verificados o métodos de contacto previamente confirmados). Los estafadores pueden afirmar que están autorizados o falsificar el sitio web de una empresa autorizada. Verifica si la autoridad financiera de tu país ha emitido alguna advertencia o está incluido en la lista I-SCAN (↖). En el caso de los proveedores de criptoactivos, comprueba si están autorizados en la UE (por ejemplo, consulta el registro de la Autoridad Europea de Valores y Mercados (AEVM) (↖).

4 **Mantente alerta ante posibles engaños con IA:**

A medida que la tecnología avanza, las estafas son cada vez más difíciles de detectar, incluso siguiendo todas las recomendaciones de seguridad. Si algo te parece extraño o detectas alguna de las señales de alerta descritas anteriormente, para un instante y vuelve a evaluar la situación.

5 **Nunca instales *software* de acceso remoto ni compartas tu pantalla:**

Ni los bancos ni las entidades financieras te pedirán que lo hagas.

6 **Mantén seguros tus dispositivos y cuentas:**

Utiliza contraseñas robustas y únicas, mantenlas en secreto y evita reutilizar las mismas credenciales en diferentes plataformas. Activa un segundo factor de autenticación siempre que sea posible. En este enlace se ofrecen algunos consejos sobre contraseñas (↖). Mantén tu *software* y protección antivirus actualizados y activados.

7 **Ten cuidado con las oportunidades de inversión que surgen de forma imprevista y por tiempo limitado:**

Si parece demasiado buena para ser cierta, probablemente lo es.

8 **Piensa antes de compartir información en redes sociales:**

Los grupos de chat, foros, publicaciones en redes sociales y fotos pueden ser valiosas fuentes de información para los estafadores. Si revelas demasiada información sobre ti o tus inversiones puedes convertirte en un blanco fácil.

Qué debo hacer si he sido víctima de una estafa o fraude

Cancela de inmediato cualquier transacción:

Para impedir nuevas transferencias a cuentas sospechosas y evitar pérdidas adicionales. Corta todo contacto con los estafadores: ignora sus llamadas y correos electrónicos y bloquea al remitente.

Ponte en contacto con tu banco o entidad financiera:

Infórmales de inmediato a través de los canales oficiales para valorar si hay posibilidad de bloquear o revertir las transacciones.

Cambia las contraseñas en todos tus dispositivos y aplicaciones/sitios web:

Los estafadores compran contraseñas filtradas por internet y las prueban en varias cuentas. No basta con cambiar solo una contraseña; asegúrate de cambiarlas todas para que los estafadores no puedan reutilizarlas.

Denuncia y da la señal de alarma:

Denuncia el incidente a la policía o a la autoridad financiera de tu país ( ) e informa a tu entorno (por ejemplo, amigos y familiares) para que estén al tanto. Estas acciones pueden ayudar a protegerte a ti mismo y a los demás.

Ten cuidado con el fraude de recuperación de fondos «recovery room»:

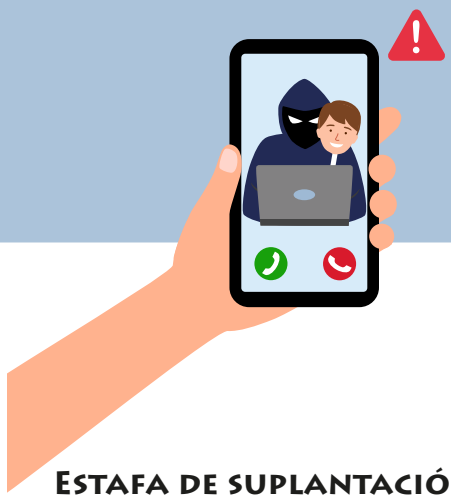
El estafador puede comunicarse contigo a sabiendas de que has sido víctima de una estafa anterior, afirmando ser una autoridad pública (por ejemplo, la policía, la autoridad fiscal o financiera, etc.) y ofrecerte recuperar el dinero que has perdido a cambio de una comisión. Suele ser otro intento de estafa. Recuerda: haber sido estafado una vez no impide que te vuelvan a estafar.

Autoridad Bancaria Europea, Autoridad Europea de Seguros y Pensiones de Jubilación, Autoridad Europea de Valores y Mercados, 2025

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2025

PDF ISBN 978-92-9407-222-1 doi:10.2853/3933360 DZ-01-25-110-ES-N

TIPOS DE ESTAFAS Y FRAUDES FINANCIEROS QUE EMPLEAN IA



Estafa de suplantación de identidad y uso de *deep fake*

Recibes una llamada inesperada de alguien que afirma ser tu banco, una autoridad pública (por ejemplo, la policía, la autoridad fiscal o financiera, etc.), un distribuidor de seguros, una empresa de telecomunicaciones o incluso un familiar. La persona que llama te puede urgir a transferir fondos para mantenerlos a salvo, alegando que ha habido actividades sospechosas en tu cuenta o en tu póliza de seguros. También pueden pedirte que facilites tus datos bancarios (por ejemplo, el número de la tarjeta, claves de acceso a la banca electrónica o contraseñas), que hagas clic en un enlace o que instales un *software*, haciéndote creer que puede resolver el problema rápidamente. El número desde el que llama puede estar falsificado, y, en muchos casos, puede coincidir con el número de tu banco para dar apariencia de legitimidad («spoofing»).

Los estafadores pueden usar IA para crear vídeos, imágenes o audios falsos que replican voces (por ejemplo, de la persona de contacto en tu banco o de un familiar), caras (por ejemplo, de una persona famosa) o movimientos. **Esto se conoce como «Deepfake».**

¿Qué podría ocurrir?:

Al mencionar datos personales y crear una sensación de urgencia, el estafador te induce a tomar decisiones que no contemplabas, como transferir dinero a su cuenta, hacer clic en un enlace malicioso o instalar un malware en tu dispositivo. Esto, a su vez, podría darle acceso a tus credenciales bancarias. Con esta información, el estafador puede cambiar tu contraseña, acceder a tu cuenta bancaria y robar tu dinero. Recuerda: el hecho de que la persona que te llama conozca tus datos personales no significa que sea digna de tu confianza.

Phishing y técnicas de ingeniería social

Recibes un correo electrónico o un mensaje que aparenta ser enviado por tu banco o una entidad financiera, advirtiéndote de cierta «actividad sospechosa» en tu cuenta. El logotipo, el diseño y el lenguaje tienen apariencia profesional, y el mensaje puede aparecer en el mismo hilo que otras conversaciones de tu banco. El mensaje te urge a hacer clic en un enlace para verificar tu cuenta o restablecer tu contraseña. El enlace conduce a un sitio web falso que parece idéntico al de tu banca electrónica. Sin darte cuenta, introduces tus datos en una página diseñada para robar tu información personal.

Los estafadores utilizan la IA para crear mensajes de *phishing* convincentes analizando información de las redes sociales para identificar a sus víctimas y adaptar el contenido a cada una de ellas.

¿Qué podría ocurrir?:

El estafador accede a tu cuenta bancaria y roba tu dinero o crea un perfil falso con tus datos personales para cometer fraude.

Estafa de inversión o de seguros

Ves un anuncio en las redes sociales o en un sitio web que promociona una «oportunidad de inversión por tiempo limitado y de bajo riesgo» o un «descuento por tiempo limitado» en un seguro de una compañía reconocida. El anuncio incluye la foto de una persona famosa y recomendaciones que a menudo son falsas. Tras mostrar interés haciendo clic en un enlace o rellenando un formulario, se ponen en contacto contigo y te redirigen a una plataforma o canal de mensajería donde recibes asesoramiento y documentos de aspecto profesional. Te animan a invertir una pequeña cantidad, seguida de sumas más grandes, o a pagar una prima en lo que parece ser una cuenta segura.

Los estafadores utilizan herramientas de IA para hacer que estas propuestas o correos electrónicos falsos sean altamente convincentes y difíciles de detectar. También utilizan *bots* de redes sociales impulsados por IA para crear cuentas falsas que interactúan contigo, difunden información engañosa y simulan comportamientos reales con el fin de ganarse tu confianza e influir en tus decisiones.

¿Qué podría ocurrir?:

Cuando intentas retirar tu dinero o notificar un siniestro, la persona de contacto deja de responder. Descubres que la entidad no existe o que el riesgo asegurado no está cubierto. Entonces te das cuenta de que has enviado dinero directamente a un estafador como parte de un esquema fraudulento. Lamentablemente, no puedes recuperar tu dinero y tus datos personales y financieros podrían utilizarse para cometer más fraudes (por ejemplo, firmar contratos en tu nombre, lo que podría ocasionarte pérdidas aún mayores).

Estafa y fraude amoroso o afectivo

Alguien a quien no conoces en la vida real se pone en contacto contigo a través de las redes sociales, aplicaciones de citas o por teléfono/mensaje de texto. Esta persona entabla conversaciones frecuentes, personales y afectivas para ganarse tu confianza utilizando perfiles falsos. Con el tiempo, la conversación deriva a cuestiones económicas o supuestas oportunidades financieras, como inversiones en criptoactivos que prometen altos beneficios y bajos riesgos. La persona te pide que transfieras dinero a una cuenta o te guía para que crees una cuenta y hagas un pequeño depósito inicial con el fin de que el esquema parezca legítimo, antes de convencerte para invertir una cantidad mayor.

Los estafadores emplean la IA para generar perfiles falsos, identificar a sus víctimas en redes sociales o aplicaciones de citas a partir de los datos que ellas mismas comparten, o para crear mensajes mediante *chatbots*.

¿Qué podría ocurrir?:

El estafador sustrae la mayor cantidad de dinero posible, luego corta toda comunicación y desaparece. El sitio web o la aplicación de inversión fraudulentos se desactivan, dejándote sin acceso a las supuestas inversiones. Además de la pérdida económica, la información personal que compartiste podría utilizarse para estafar a tus amigos y familiares o para suplantar tu identidad, con posibles consecuencias económicas o legales para ti (por ejemplo, el estafador podría realizar compras, contratar préstamos en tu nombre o hacer que se te considere responsable de deudas o delitos hasta que se demuestre lo contrario).

Estafa de compra

Descubres una oportunidad de compra a un precio atractivo en una plataforma digital (*marketplace*). La empresa que realiza la oferta solicita un pago fuera de la plataforma oficial, afirmando que utiliza un «sistema de pago seguro» y te envía un enlace para completar la compra. El enlace te redirige a una página fraudulenta de autenticación bancaria que imita el sitio web oficial del banco y utiliza su logotipo y diseño, por lo que introduces tus credenciales para efectuar el pago.

Los estafadores usan la IA para crear sitios web falsos de bancos, así como confirmaciones de pedidos y facturas que parecen auténticas. La IA les ayuda a replicar el tono, la imagen corporativa y el estilo de empresas reales. En algunos casos, utilizan *chatbots* de IA para responder preguntas y hacer que la oferta parezca más creíble.

¿Qué podría ocurrir?:

El pago a través de un enlace de terceros elude las garantías de la plataforma. El estafador obtiene tus credenciales para iniciar una sesión en tu cuenta bancaria y roba tu dinero.