ESTAFAS Y FRAUDES RELACIONADOS CON CRIPTOACTIVOS

NO BAJES LA GUARDIA: PROTÉGETE

El rápido crecimiento de los criptoactivos, unido a sus características específicas —accesibilidad global, rapidez, anonimato y, a menudo, irreversibilidad de las transacciones—, te convierten en un blanco fácil para los ciberdelincuentes. Los defraudadores y estafadores utilizan tácticas sofisticadas para engañarte, como los «esquemas Ponzi», oportunidades falsas de inversión, ofertas gratuitas en redes sociales y mensajes fraudulentos. También recurren a estafas amorosas o afectivas o a direcciones falsas para «contaminar» tu monedero. 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 posibles estafas y fraudes relacionados con criptoactivos:
Infórmate sobre los diferentes tipos de estafas y fraudes
(consulta las páginas 5, 6, 7 y 8).

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

Protégete y protege tus activos:
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 oferta no solicitada.

Una garantía de alta rentabilidad en poco tiempo.

Necesidad de actuación urgente (por ejemplo, ofertas por tiempo limitado que te presionan para actuar de inmediato).

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

Una invitación para hacer clic en un enlace, escanear un código QR o descargar una aplicación.

Una solicitud para enviar o compartir claves privadas y frases semilla (conjunto de palabras para acceder a tu monedero de criptoactivos y recuperarlo).

Una URL sospechosa o incorrecta.

Un logotipo con ligeras modificaciones, un sitio web que copia el aspecto de la web de una empresa real o que parece profesional, pero que no incluye datos de contacto verificados, información registral, historial o cuya existencia no sea comprobable.

Una plataforma de intercambio desconocida.

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

Pasos para protegerte

1 Para un instante y piensa antes de actuar

No te precipites al invertir, compartir información o hacer clic en enlaces: los estafadores crean deliberadamente una sensación de urgencia. En caso de duda, por pequeña que sea, no actúes ni inviertas y verifica cuidadosamente la fuente.

2 Verifica la autenticidad de la fuente

- 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. 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 el sitio web 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.
- Aunque una oferta parezca oficial, contrástala siempre en el sitio web de la empresa o comprueba que la cuenta en las redes sociales sea oficial y esté verificada (por ejemplo, con marcas de verificación oficiales).
- 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 o utiliza directorios empresariales verificados). Los estafadores pueden afirmar que están autorizados o falsificar el sitio web de una empresa autorizada. Puedes verificar si el proveedor de criptoactivos está autorizado en la UE consultando el registro de la Autoridad Europea de Valores y Mercados (AEVM) (). También puedes consultar el sitio web de la autoridad financiera de tu país () para ver si ha emitido alguna advertencia o publicado listas negras, o si está incluido en la lista I-SCAN ().

3 Nunca compartas contraseñas, claves privadas ni frases semilla

Si alguien accede a ellas podrá controlar tus activos. Las empresas legítimas nunca te pedirán tus contraseñas o códigos de seguridad por correo electrónico, mensaje de texto ni por teléfono.

4 Mantén seguros tus dispositivos y claves privadas

Utiliza contraseñas robustas y únicas para cada una de tus cuentas de criptoactivos, mantén tu contraseña 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.

5 Ten cuidado con las ofertas de inversión que surgen de forma imprevista

Desconfía de las inversiones que prometen grandes beneficios. Si parece demasiado buena para ser cierta, probablemente lo es.

6 Piensa antes de compartir información en las 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.

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.

Desconecta y revoca el acceso:

Revoca los permisos de acceso sospechosos a tu monedero realizados a través de contratos inteligentes (acuerdos digitales que se ejecutan automáticamente en la cadena de bloques) para evitar que los estafadores gasten tus *tokens* sin tu consentimiento. Muchos monederos y exploradores de *blockchain* ofrecen herramientas que te permiten ver qué contratos inteligentes tienen acceso a tu monedero para gastar tus *tokens*. Para ello puedes:

- utilizar un «comprobador de permisos» de confianza, que verifica si un usuario o una dirección de cadena de bloques están autorizados a ejecutar una operación,
- revisar la lista de permisos y
- utilizar el botón «revocar» directamente desde la plataforma.

Transfiere tus fondos:

Si tu monedero está comprometido, transfiere inmediatamente los activos que te queden a un nuevo monedero seguro.

Ponte en contacto con tu proveedor de criptoactivos:

Informa a tu proveedor de criptoactivos lo antes posible a través de los canales oficiales con el fin de valorar las opciones disponibles. Aun cuando en la mayoría de los casos no sea posible revertir la transacción de la cadena de bloques, el proveedor podría congelar la cuenta del estafador (si está en su plataforma) y poner la dirección del monedero en una lista de advertencias.

Denuncia y da la señal de alarma:

Denuncia el incidente a la policía o a la autoridad de supervisión 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 no impide que te vuelvan a estafar.

La advertencia conjunta de las Autoridades Europeas de Supervisión contiene más información sobre los riesgos relacionados con los criptoactivos (↖) y la ficha informativa «Los criptoactivos explicados: Qué significa el Reglamento MiCA para ti como consumidor» (↖).

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 978-92-9407-257-3 doi:10.2853/5382497 DZ-01-25-145-ES-N

TIPOS DE ESTAFAS RELACIONADAS CON CRIPTOACTIVOS

Esquema de inflar y desinflar («pump and dump») o estafa de salida («rug pull»)

Ves un anuncio en las redes sociales o en un sitio web que promociona una «oportunidad de inversión en criptoactivos por tiempo limitado», recomendando invertir en un nuevo *token* o proyecto de criptoactivos. Tras mostrar interés, se ponen en contacto contigo y te redirigen a una plataforma de intercambio de criptoactivos o a un canal de mensajería (por ejemplo, Telegram, Viber o WhatsApp). Un contacto aparentemente de confianza promete beneficios rápidos o altos rendimientos si inviertes de inmediato. Te animan a invertir una pequeña cantidad y luego te presionan para que inviertas cantidades mayores.

¿Qué podría ocurrir?:

Descubres que el token en el que has invertido no vale nada y la persona con la que has estado en contacto deja de responder. Cuando intentas retirar tu dinero, el sitio web ya no existe y la empresa está ilocalizable. Los estafadores inflaron o sobrevaloraron artificialmente un criptoactivo de bajo valor para aumentar su precio («pump») y luego vendieron todos sus activos («dump»), haciendo que el valor cayera y provocando pérdidas a los inversores. Alternativamente, podrían cerrar el proyecto y desaparecer con los fondos («rug pull»).

Estafa de suplantación de identidad

Después de publicar una pregunta en una plataforma de redes sociales o un sitio web sobre un problema con el monedero de criptoactivos, recibes un mensaje directo inesperado (DM) o un correo electrónico de alguien que finge ser un contacto de confianza (por ejemplo, una plataforma de intercambio de criptoactivos, un proveedor de monederos, un servicio de soporte informático o incluso un amigo). La persona te pide tu frase semilla (es decir, la secuencia de palabras que sirve como clave para acceder a tu monedero digital), tus contraseñas o tus claves privadas (un código criptográfico generado automáticamente que demuestra la propiedad de los activos digitales).

¿Qué podría ocurrir?:

Una vez que compartes tu frase semilla, tus contraseñas o tus claves privadas, el estafador las usa para robar tus criptoactivos u otros fondos. Ten en cuenta que la pérdida de claves privadas supone la pérdida permanente e irreversible del acceso y de la propiedad de tus criptoactivos. A diferencia de las transacciones bancarias, en el caso de las transferencias de criptoactivos, una vez que tus fondos se transfieren, la recuperación es casi imposible.

Phishing

Recibes un mensaje inesperado por correo electrónico, teléfono, ventana emergente o redes sociales de alguien que se presenta como un conocido proveedor de criptoactivos. El mensaje te invita a iniciar sesión o a descargar una nueva aplicación. También podrías recibir un correo electrónico que parece proceder de tu aplicación de monedero de criptoactivos, en el que se te urge a resolver un problema de seguridad haciendo clic en un enlace procedente de una fuente no oficial o actualizando la aplicación.

¿Qué podría ocurrir?:

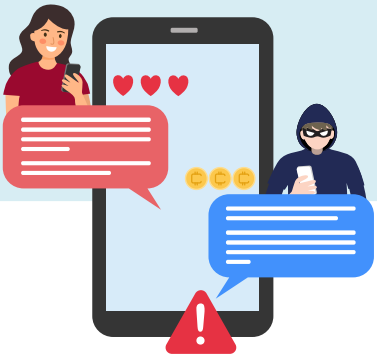
Al hacer clic en el enlace, descargar la aplicación o escanear un código QR, instalas un malware que permite al estafador acceder a tu información y usarla para robar tus criptoactivos o tus fondos.

Estafa del regalo («giveaway»)

Te encuentras con un anuncio en las redes sociales que afirma que las empresas están regalando criptoactivos tras realizar una pequeña inversión en estos instrumentos. Incluyen un vídeo o una publicación con fotos de una persona famosa o una marca —generalmente falsas u obtenidas sin autorización— que prometen «duplicar tus criptoactivos» si envías dinero primero. El logotipo, el diseño, los testimonios y el lenguaje utilizado tienen apariencia profesional y oficial, al igual que el sitio web al que se te redirige.

¿Qué podría ocurrir?:

Después de enviar tus criptoactivos, no recibes nada a cambio y pierdes el dinero enviado. El regalo era una trampa y la publicación o retransmisión en directo en la que se suplantaba la identidad de personas famosas o empresas estaba diseñada para engañarte.



Estafa amorosa o afectiva de inversión

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 hacia oportunidades financieras; la persona asegura que ha obtenido grandes beneficios invirtiendo en criptoactivos y te anima a invertir, prometiendo grandes beneficios y bajos riesgos. Te guía para que crees una cuenta y hagas un pequeño depósito inicial con el fin de que el esquema parezca legítimo.

Los estafadores crean perfiles falsos y usan imágenes robadas o generadas con inteligencia artificial para acercarse a ti.

¿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. En algunos casos, los estafadores pueden utilizar la información obtenida para estafar a tus amigos y familiares y suplantar tu identidad, con posibles consecuencias económicas o legales para ti (por ejemplo, el estafador podría verificar tus carteras robadas y hacer que se te considere responsable de deudas o delitos hasta que se demuestre lo contrario).

«Esquema Ponzi»

Te invitan a participar en un proyecto que promete rendimientos altos y constantes en inversiones en criptoactivos, a menudo respaldados por testimonios o historias de éxito falsas. El esquema puede presentarse como una oportunidad comercial de tipo piramidal, donde obtienes beneficios no solo por tu propia inversión, sino también por reclutar a otros inversores. Los primeros inversores parecen recibir pagos, lo que incentiva la incorporación de nuevos participantes y la promoción del esquema.

En realidad, no hay un verdadero negocio ni se generan beneficios. De hecho, el dinero proviene únicamente de las aportaciones de los inversores más recientes, que se destinan a pagar rendimientos a los organizadores del esquema y a los primeros participantes.

¿Qué podría ocurrir?:

Una vez que las nuevas inversiones se ralentizan, el esquema se derrumba y tú, como la mayoría de los participantes, pierdes tu dinero. Los organizadores desaparecen sin que haya manera de recuperar los fondos. La estructura piramidal facilita la rápida expansión de la estafa, a medida que las víctimas, sin saberlo, se convierten en promotores.

Una dirección falsa, parecida a una dirección de monedero real, que está contaminando tu monedero

Después de realizar una transacción de criptoactivos, observas que aparece una nueva dirección en el historial de tu monedero. Esta dirección es similar a otra con la que has interactuado previamente. Los estafadores pueden hacer que aparezcan direcciones de monedero falsas en tu historial de transacciones enviando una pequeña cantidad de criptoactivos desde una dirección muy parecida a otra dirección con la que has operado previamente. Al final, terminas almacenando en la actividad reciente o en autosugerencias de tu monedero la dirección falsa creada por el estafador. Los estafadores crean deliberadamente direcciones parecidas cambiando solo unos pocos caracteres, a menudo en el medio de la dirección, para evitar ser detectados.

¿Qué podría ocurrir?:

Cuando intentas enviar criptomonedas y copias la dirección equivocada del historial de tu monedero, envías fondos sin saberlo al monedero del estafador. Dado que las transacciones de criptoactivos suelen ser irreversibles, tus fondos se pierden en la mayoría de los casos de forma permanente. Esta estafa, que se basa en el engaño visual y el error del usuario, explota el hábito de copiar y pegar direcciones de monedero sin fijarse detenidamente en ellas.