

Cómo no perder sus criptomonedas

Una lista de verificación: qué no hacer nunca, cómo protegerse y qué hacer si ya ha ocurrido.

Nunca haga esto

- 1 **Nunca revele a nadie su frase de recuperación (12-24 palabras) ni su clave privada.** Ningún exchange, servicio de soporte ni policía se la pedirá. Quien se la pida quiere robarle.
- 2 **Nunca invierta a través de alguien que conoció en internet:** en una aplicación de citas, Telegram, WhatsApp o Facebook. Así empiezan la mayoría de las estafas, incluso tras meses de conversación.
- 3 **Nunca crea en ganancias garantizadas.** «2 % al día», «sin riesgo», «solo hoy» siempre significan estafa.
- 4 **Nunca pague para retirar su propio dinero.** Si le exigen una «comisión», un «impuesto» o un «seguro» antes de una retirada, el dinero ya se ha perdido.
- 5 **Nunca instale aplicaciones de acceso remoto** (AnyDesk, TeamViewer y similares) porque alguien se lo pida.
- 6 **Nunca responda a un «soporte» que le escribió primero.** Los administradores y empleados reales de un exchange no escriben primero.
- 7 **¿Le llama su «banco», su «exchange» o «la policía»?** Cuelgue y llame usted mismo al número oficial.
- 8 **Nunca apruebe en su billetera nada que no entienda.** Un solo «Approve» o «Sign» en un sitio falso puede vaciar toda la billetera.
- 9 **Compruebe la dirección de destino completa, no solo el principio y el final.** No copie direcciones de su historial de transacciones: los estafadores introducen allí direcciones casi idénticas.
- 10 **Nunca confíe en servicios de «recuperación»** que garantizan la devolución de su dinero o piden criptomonedas por adelantado. Es la segunda estafa después de la primera.

Cómo protegerse

- Escriba usted mismo la dirección del exchange o ábrala desde un marcador. En los resultados y anuncios de Google aparecen sitios falsos.
- Use un exchange autorizado para operar en su país o región. Active la verificación en dos pasos con una aplicación de autenticación, no por SMS.
- Active en su exchange la lista de direcciones de retirada permitidas, para que el dinero solo pueda ir a direcciones que usted haya aprobado.
- Guarde las cantidades grandes en una billetera física (hardware) comprada solo al fabricante.
- De vez en cuando, revise a qué sitios ha dado permisos su billetera y revoque los que no necesite (por ejemplo, con revoke.cash).

Si ya ha ocurrido

- 1 **No pague nada más** y deje de hablar con los estafadores.
- 2 **Guarde las pruebas:** ID de transacción (TxID), direcciones, importes, horas y capturas de pantalla de los chats y del sitio web.
- 3 **Comuníquelo de inmediato** a su exchange y denúncielo a la policía. Las primeras horas son las más importantes: mientras el dinero siga en un exchange, se puede congelar.
- 4 **Si necesita rastrear adónde fue el dinero** y preparar pruebas para la policía y el exchange: trailforensics.com.

Trail Forensics nunca pide frases de recuperación, contraseñas ni acceso a billeteras, y no garantiza que el dinero vaya a ser devuelto.