



Europol desmanteló una red de fraude de criptomonedas de 540 mdd,
arrestando a 5 personas

Europol anunció el lunes el desmantelamiento de una red de fraude de inversiones en criptomonedas que lavó 460 millones de euros (540 millones de dólares) de más de 5,000 víctimas en todo el mundo.

La operación, según la agencia, fue ejecutada por la Guardia Civil española con el apoyo de autoridades policiales de Estonia, Francia y Estados Unidos. Europol indicó que la investigación sobre este grupo criminal comenzó en 2023.

Además, cinco presuntos responsables del esquema fraudulento fueron arrestados el 25 de junio de 2025. Tres de las detenciones ocurrieron en las Islas Canarias y las otras dos en Madrid.

«Para llevar a cabo sus actividades fraudulentas, los cabecillas de la red criminal supuestamente utilizaron una red de colaboradores distribuidos por todo el mundo para recaudar fondos mediante retiros de efectivo, transferencias bancarias y transacciones en criptomonedas», [señaló Europol](#).

Este tipo de estafas siguen con frecuencia un patrón conocido como fraude de confianza o “romance crypto” (antes llamado «pig butchering»), en el que los estafadores ganan la confianza de las víctimas durante semanas o meses—usualmente a través de apps de citas o conversaciones amigables—antes de persuadirlas para invertir en plataformas falsas de criptomonedas. Detrás de escena, los delincuentes usan ingeniería social, como paneles de trading falsos y diálogos preestablecidos, para mantener la ilusión. Una vez depositado el dinero, se transfiere entre múltiples cuentas en un proceso conocido como “layering”, dificultando su rastreo por las autoridades.

Se cree que los ciberdelincuentes establecieron una red bancaria y corporativa en Hong Kong, a través de la cual canalizaron los fondos ilícitos utilizando un laberinto de pasarelas de pago y cuentas a nombre de diversas personas y en distintos intercambios.

Este acontecimiento llega poco después de que el Departamento de Justicia de EE.UU. presentara una demanda de decomiso civil para recuperar más de 225 millones de dólares



Europol dismanteló una red de fraude de criptomonedas de 540 mdd, arresando a 5 personas

en criptomonedas vinculadas a fraudes de confianza que operaban desde Vietnam y Filipinas.

Europol describió la “*escala, variedad, sofisticación y alcance*” de estos fraudes en línea como “*sin precedentes*”, y advirtió que podrían superar al crimen organizado tradicional debido al uso creciente de tecnologías de inteligencia artificial.

«*La integración de inteligencia artificial generativa por parte de grupos criminales transnacionales dedicados al fraude digital es una tendencia compleja y preocupante observada en el sudeste asiático, y representa un multiplicador de poder para las actividades delictivas*», afirmó John Wojcik, analista regional de la UNODC, a finales del año pasado.

Según un informe de INTERPOL de la semana pasada, los delitos cibernéticos representan más del 30% de todos los crímenes reportados en África Occidental y Oriental. Esto incluye estafas en línea, ransomware, suplantación de correos empresariales (BEC) y extorsión sexual digital.

«*El cibercrimen continúa superando a los sistemas legales diseñados para detenerlo*», [declaró](#) INTERPOL, agregando que «*el 75% de los países encuestados dijeron que sus marcos legales y capacidad de enjuiciamiento necesitaban mejoras*».

Una de las razones por las que este tipo de fraude es tan difícil de combatir es porque los criminales se aprovechan de vacíos legales y leyes internacionales fragmentadas. Muchos estafadores ahora usan identidades sintéticas—personas ficticias creadas con datos robados o generados por IA—para registrar cuentas o alquilar acceso a bancos. También reclutan «*mulas financieras*» que transfieren dinero, muchas veces sin saber que participan en un crimen.

Para ejecutar este tipo de estafas de inversión, personas desprevenidas de Asia y África son atraídas al sudeste asiático con promesas de empleos lucrativos, pero luego son retenidas



Europol desmanteló una red de fraude de criptomonedas de 540 mdd, arresando a 5 personas

contra su voluntad en «centros de estafa» operados por grupos del crimen organizado transnacional provenientes de China.

Amnistía Internacional ha [identificado](#) al menos 53 de estos centros en Camboya, donde, según la organización, *“han ocurrido o siguen ocurriendo violaciones a los derechos humanos, incluyendo trata de personas, tortura, trabajos forzados, trabajo infantil, privación de libertad y esclavitud»*.

Muchas de las personas reclutadas fueron inicialmente engañadas con ofertas de empleo en tecnología o ventas. Una vez en el lugar, les confiscan los pasaportes y las obligan a estafar a otros bajo amenazas de violencia o endeudamiento.

El año pasado, el Instituto de Paz de EE.UU. [reveló](#) que las ganancias del fraude digital en Camboya superan los 12,500 millones de dólares al año, lo cual equivale a la mitad del producto interno bruto (PIB) formal del país.

La operación ilegal ha tenido tanto impacto que la Embajada de la India en Camboya mantiene una advertencia destacada en su sitio web, exhortando a los ciudadanos a estar alertas para no caer en manos de traficantes de personas que ofrecen falsos empleos bien remunerados. La advertencia señala que los solicitantes de empleo son obligados a realizar estafas financieras en línea y otras actividades ilegales.

Agregando más contexto a esta actividad criminal, un reciente [informe](#) de ProPublica indicó que canales de Telegram en idioma chino están promocionando entre estafadores la posibilidad de alquilar cuentas bancarias estadounidenses en Bank of America, Chase, Citibank y PNC, las cuales luego se usan para lavar dinero. Telegram ha comenzado a tomar medidas contra algunos de estos canales.

Meta, por su parte, dijo haber detectado y eliminado al menos siete millones de cuentas de Facebook vinculadas a centros de estafa en Asia y Medio Oriente desde principios de 2024, según declaró la compañía al medio de periodismo de investigación.