INTERPOL

EVALUACIÓN MUNDIAL DE INTERPOL SOBRE LA AMENAZA QUE PLANTEAN LAS ESTAFAS

MAYO DE 2024

Descargo de responsabilidad

Secretaría General de INTERPOL
200 quai Charles de Gaulle
69006 Lyon
Francia
Teléfono: + 33 4 72 44 70 00
Fax: + 33 4 72 44 71 63
Sitio web: www.interpol.int
Correo electrónico: info@interpol.int

Índice

Resumen y conclusiones principales

Las estafas han aumentado y se han diversificado considerablemente, tanto en lo que respecta a su volumen como a los métodos utilizados para cometerlas. En la actualidad, estos fraudes representan una amenaza omnipresente y generalizada.

Comprendidas como una categoría general que abarca las actividades "destinadas a obtener un lucro a través de acciones deliberadas y engañosas contra personas y en su detrimento", las estafas no solo provocan grandes pérdidas económicas a las personas y las empresas, además socavan las economías nacionales y mundiales al reducir la confianza y debilitar la integridad de los sistemas financieros.

La Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas constituye un análisis en profundidad de los acervos de datos de INTERPOL sobre delitos y delincuentes relacionados con estafas perpetradas contra personas o empresas. Dichos acervos de datos incluyen las notificaciones y difusiones de INTERPOL que tratan de delitos de estafa. Entre las conclusiones principales de esta evaluación cabe señalar las siguientes:

- Los tipos más frecuentes en todo el mundo de fraudes por ánimo de lucro son las estafas de inversión, las de pago por anticipado, las sentimentales por Internet y las estafas a empresas por e-mail mediante suplantación de identidad (también denominadas estafas BEC).
- Los delincuentes utilizan cada vez más las tecnologías de la información y la comunicación, que son de por sí globalizadas, para cometer las estafas. Estas adquieren un carácter transnacional y, a menudo, transcontinental.
- Los estafadores utilizan tecnologías emergentes, en particular la inteligencia artificial (como los deepfakes o contenido ultrafalso), para engañar a sus víctimas y ocultar su identidad.
- Según los datos de los que se disponen, la utilización de "centros de estafas" es cada vez más frecuente, y algunos de estos fuerzan a víctimas de la trata de personas a perpetrar estafas. Esta tendencia se ha detectado en el Sudeste Asiático, Europa del Este, América Latina y África Occidental, Oriental y Austral.
- La estafa de inversión en criptomonedas, cada vez más usual y en expansión, es difícil de denunciar para las víctimas. Se trata de un modelo híbrido que combina las estafas que provocan un perjuicio patrimonial con las sentimentales, y en el que con frecuencia se utilizan criptomonedas.
- Por lo general, las estafas suelen ser cometidas por una red de coautores cuya organización varía de grupos muy estructurados a grupos delictivos poco organizados.
- En los delitos de estafa suele darse una convergencia de otros delitos, debido a que los estafadores, ya sea actuando solos o en grupo, también utilizan los ciberdelitos y el blanqueo de capitales como servicio para sus actividades delictivas.
- Si bien se conoce el modus operandi de las estafas, se sabe menos sobre cómo están organizadas y quiénes son los estafadores. Así pues, existe una necesidad urgente de fortalecer la recopilación y el análisis de datos relacionados con las estafas para poder preparar unas estrategias de lucha más fundamentadas y que den mejores resultados.

Las estafas son un tipo de delito predatorio cometido en el anonimato y a través de las fronteras. INTERPOL trabaja sin cesar para brindar asistencia a los países miembros en la lucha mundial contra este tipo de fraudes, ya sea recopilando datos, analizando información o prestando apoyo operativo.

Las conclusiones presentadas en este documento forman parte de una iniciativa analítica en curso que pretende estudiar la situación de la delincuencia actual y la emergente a fin de elaborar la Evaluación de INTERPOL sobre las amenazas planteadas por la delincuencia a escala mundial, que los organismos encargados de la aplicación de la ley tendrán a su disposición en noviembre de 2024.

Introducción

En un mundo cada vez más digitalizado e interconectado, las estafas se han convertido en una amenaza generalizada y costosa tanto para las personas como para las empresas. Sus repercusiones económicas son escalofriantes. A medida que la tecnología evoluciona, igual lo hace el modus operandi utilizado por los estafadores, que no tardan en explotar nuevas vulnerabilidades y adaptar sus tácticas para eludir las medidas de seguridad, de modo que puedan quedar un paso por delante de los organismos encargados de la aplicación de la ley.

Los diferentes tipos de estafas se cometen de diferentes formas y conllevan diferentes peligros que deben detectarse y evaluarse, junto con los factores que impulsan su crecimiento y los perpetradores, a fin de contrarrestarlos. Sin embargo, debido a la reticencia de las víctimas para denunciar los engaños, las fuerzas del orden ignoran muchos de ellos, por lo que casi no es posible apreciar plenamente su verdadero alcance y efecto.

A menudo, los datos e investigaciones existentes sobre las estafas se centran en la forma de proceder y se sabe mucho menos acerca de los diferentes perfiles de los estafadores y, lo que es más importante, de la forma en que se organizan estos delitos. Es evidente que estos requieren distintos grados de colaboración entre sus coautores, pero es necesario comprender mejor la naturaleza y el alcance de la convergencia de los delitos.

A través de un examen de la información de que dispone INTERPOL, este informe pretende presentar una evaluación de las tendencias mundiales de las estafas, la forma en que se perpetran a escala regional y mundial y el perfil de los perpetradores, a fin de elaborar estrategias bien fundamentadas y eficaces para llevar a cabo actuaciones colectivas contra las personas y los grupos delictivos organizados que cometen este tipo de delitos.

Metodología

La Evaluación mundial de INTERPOL sobre la amenaza que plantean las estafas es producto del empleo de una metodología en la que se recabó información procedente de todas las fuentes. La mayor parte de los datos analizados se extrajo de los acervos de datos de INTERPOL y provino, en parte, de las notificaciones y las difusiones de la Organización acerca de los delitos relacionados con las estafas, las aportaciones directas de los países miembros de INTERPOL y sus socios, los mensajes con respecto de las operaciones de los países miembros y las respuestas a los cuestionarios de 2022 y 2024 sobre las tendencias de la delincuencia a escala mundial. Estos datos se complementaron, cuando fue apropiado, con documentación de fuentes públicas elaborada por socios internacionales en los sectores público y privado.

Marco analítico

La conceptualización del delito de estafa que se hace en este informe emana de una perspectiva operativa y de aplicación de la ley. Por consiguiente, "estafa" se emplea aquí como un término general que abarca una amplia variedad de "actividades ilícitas destinadas a obtener un lucro a través de acciones engañosas contra personas o empresas[1], y en su detrimento".

Desde este punto de vista, la estafa es fundamentalmente una interacción de dos elementos: el motivo (el lucro) y los medios (el engaño en diversas formas) que da lugar a una ventaja o beneficio injusto perjudicial para una persona. En consecuencia, los tipos de estafa a los que se enfrentan las fuerzas del orden son dinámicos y evolucionan a medida que se producen cambios en el entorno social, económico, tecnológico y jurídico.

1 La presente evaluación se centra en la comisión de estafas contra personas y entidades privadas, y excluye las estafas cometidas contra gobiernos o administraciones públicas.

Tipos de estafas y modus operandi

Estafa de suplantación de identidad

La estafa de suplantación de identidad es llevada a cabo por un estafador que se hace pasar por una persona o un trabajador de una empresa con la que la víctima tiene o podría haber tenido algún tipo de relación real, tanto personal como oficial o de negocios (como un pariente lejano, un empleado de la administración fiscal, un policía o un proveedor de algún servicio que la víctima utilice). En este tipo de estafa se suele provocar miedo o preocupación a la víctima para engañarla.

Estafas a empresas por e-mail mediante suplantación de identidad o estafas BEC

Las estafas a empresas por e-mail mediante suplantación de identidad o estafas BEC[2], también conocidas como fraudes del CEO, son una forma cada vez más frecuente de usurpación de identidad. En este caso, los estafadores utilizan técnicas de ingeniería social para atacar a las empresas interceptando sus cuentas de correo electrónico y haciéndose pasar por ejecutivos y abogados de negocios para engañar a los empleados y que estos transfieran fondos a cuentas bancarias de los estafadores, quienes después blanquean rápidamente los fondos. Los delincuentes, que a veces operan desde centros de estafas, son capaces de poner en marcha estafas de suplantación de identidad a gran escala dirigidas a millones de empresas y personas a través de correos electrónicos, mensajes de texto, medios sociales y llamadas automáticas.

Estafa de inversión

La estafa de inversión consiste en engañar a las personas para que inviertan dinero en empresas fraudulentas, ocasionando importantes pérdidas financieras a las víctimas. Este modus operandi representa una amenaza prolífica puesto que las víctimas suelen sufrir mayores pérdidas en esta estafa que en otros tipos de defraudaciones. Los perpetradores utilizan diversas tácticas engañosas, como presentar unos rendimientos elevados prometedores, deformar las inversiones y crear una falsa sensación de urgencia. Los esquemas de las estafas de inversión se suelen basar en modelos operativos utilizados en las estafas piramidales y Ponzi, que proporcionan a los estafadores una base más amplia de víctimas y les permiten mantener el flujo de inversiones y aumentar las ganancias ilícitas. Los perpetradores suelen dirigirse a posibles víctimas o inversores a través de los medios sociales, aplicaciones o sitios web fraudulentos, campañas de venta telefónica (la mayoría de ellas realizadas desde centros de llamadas u oficinas clandestinas) y en persona, sirviéndose de cada una de estas técnicas de comunicación en etapas precisas de la estafa. Los grupos delictivos o las redes que participan en ella suelen adoptar las formas de una entidad comercial legítima para cometer su delito. El aumento del uso de las criptomonedas ha creado nuevas oportunidades para las estafas de inversión, y la manipulación de los mercados o la "seducción financiera" son algunas de las técnicas utilizadas para cometer fraudes con estas criptodivisas. Los estafadores utilizan plataformas fraudulentas de inversión en criptomonedas y el método rug pull para persuadir a los inversores a los que posteriormente defraudan.

RUG PULL

EN EL 2023, INTERPOL IDENTIFICÓ LA ESTAFA RUG PULL COMO UNA DE LAS ESTAFAS DE INVERSIÓN DIGITALES EN CRECIMIENTO. ESTA CONSISTE EN EL ABANDONO REPENTINO DE PROYECTOS CON CRIPTOMONEDAS POR PARTE DE LOS DESARROLLADORES, HACIENDO QUE LAS PERSONAS QUE INVIRTIERON EN ELLOS PIERDAN SU DINERO.[3]

2 Si bien se trata de un subtipo de estafa de suplantación de identidad, las estafas BEC han sido tratadas de forma independiente en este informe por su alta presencia y la frecuencia con la que se llevan a cabo en diferentes regiones.

3 INTERPOL. (19 de diciembre de 2023). 300 millones de dólares incautados y 3 500 sospechosos detenidos en una operación internacional contra la delincuencia financiera. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2023/300-millones-de-dolares-incautados-y-3-500-sospechosos-detenidos-en-una-operacion-internacional-contra-la-delincuencia-financiera

Entre los diferentes modus operandi utilizados para cometer fraudes con ánimo de lucro, INTERPOL ha detectado que la suplantación de identidad, la estafa de inversión, la sentimental y la de pago por anticipado son los más generalizados a escala mundial.

Estafa sentimental por Internet

La estafa sentimental por Internet es un tipo de engaño en el que los estafadores, cuya motivación es lucrarse, desarrollan una "relación" íntima o de confianza con las víctimas que suele comenzar a través de medios sociales, aplicaciones de citas y plataformas de mensajería. En ella, los delincuentes manipulan a la persona, a menudo varias veces, y le causan daño emocional y económico.

Estafa de pago por anticipado

La estafa de pago por anticipado, uno de los tipos de fraude más frecuentes, consiste en llevar a cabo una transacción financiera a fin de obtener productos o servicios fraudulentos. Los perpetradores pueden servirse de sitios web comerciales, plataformas de medios sociales u otros medios para promover la venta, a precios inferiores a los del mercado, de bienes y servicios para los que existe una demanda. El pago se solicita por adelantado, antes de la recepción de todo producto o servicio, que puede no existir o ser de una calidad muy inferior a la anunciada.

Usurpación de identidad

La usurpación de identidad consiste en la adquisición y el uso no autorizados de datos personales (nombre de usuario y contraseña, datos de la tarjeta de crédito, datos biométricos…) a fin de obtener ganancias ilícitas. Los usurpadores pueden acceder a la información personal mediante el robo físico, la ingeniería social (utilizando métodos como el phishing, smishing, vishing, spoofing y otros) o la intrusión en sistemas informáticos (utilizando software malicioso o técnicas de piratería). Esta estafa se compone de dos elementos: la facilitación (es decir, la técnica empleada para la adquisición de datos personales con ánimo de lucro) y el uso de estos datos para dicho fin[4]. Los estafadores pueden usurpar identidades sin la participación directa de las víctimas y, además de robarles dinero, suelen vender en los mercados delictivos en línea la información personal confidencial, que puede ser utilizada por los delincuentes para usurpar identidades, revictimizar a las personas y facilitar las técnicas engañosas utilizadas en otros tipos de fraude (como las estafas sentimentales por Internet).

4 A continuación, el estudio de la estafa de usurpación de identidad se centrará en la amenaza que representa el phishing, así como otras técnicas de ingeniería social y de intrusión.

Datos de INTERPOL sobre las estafas y tendencias

Según el Informe sobre las tendencias de la delincuencia a escala mundial - INTERPOL 2022, las estafas constituyen una de las mayores amenazas para los países miembros de la Organización. En las encuestas, la mayoría de los participantes, provenientes de todas las regiones del mundo, indicaron que consideraban que la delincuencia financiera, incluidas las estafas, iba a "aumentar" o a "aumentar considerablemente" en los próximos tres a cinco años.

Entre 2022 y 2023, el 85 % de las notificaciones y difusiones rojas publicadas por los países miembros tenían relación con las estafas. Las notificaciones y difusiones provinieron en su mayoría de países europeos, seguidos por países de las regiones de Asia y las Américas.

Según la información comunicada por los países miembros de INTERPOL, en la mayoría de los casos, la comisión de estafas tiene un componente transnacional y las víctimas más frecuentes son las personas físicas, por delante de las empresas del sector privado. Solo en 2023, el Centro de INTERPOL contra la Delincuencia Financiera y la Corrupción ayudó a tratar más de 700 casos de estafa investigados por sus países miembros, que sumaban unas pérdidas de alrededor de 1 200millones de dólares estadounidenses. A escala mundial, las estafas BEC y de inversión constituyeron los tipos más frecuentes de fraude notificados a INTERPOL, seguidos de las estafas sentimentales por Internet, las de usurpación de identidad, las de pago por anticipado y del phishing.

A pesar de que la estafa es un delito omnipresente en todo el mundo, se pueden distinguir diferentes tendencias en cada región. En la región de **Asia**[5], las estafas de usurpación de identidad, las sentimentales por Internet y el phishing son las más frecuentes. Si bien la mitad de los casos notificados en 2023 por países asiáticos se originaron en la región, estos engaños no son una amenaza endógena, debido a que INTERPOL ya ha identificado casos de estafas BEC cometidas desde Europa y América, así como estafas sentimentales por Internet cometidas desde África, todas ellas dirigidas a países asiáticos.

En cuanto a **África**[6], las estafas de pago por anticipado constituyen la forma más preocupante de fraude, seguidas por las estafas de inversión, las BEC y las sentimentales. Los casos de estafa comunicados por los países miembros de África en 2023 se cometieron en Asia, África y Europa. No obstante, África (especialmente los países de África Occidental) sigue siendo una importante fuente de timos dentro y fuera del continente según confirmaron recientemente las operaciones Contender y Killerbee dirigidas por INTERPOL.

Las estafas de inversión son las más preocupantes en la **región europea,** por delante de las estafas por medios de telecomunicación, las BEC y las sentimentales. En lo que respecta a la **región de las Américas,** se observa un aumento preocupante del phishing y las estafas BEC y de pago por anticipado, si bien siguen existiendo importantes vacíos de inteligencia que impiden una evaluación exhaustiva de la amenaza en esta región.

5 En la presente evaluación , la región de Asia incluye países de Oriente Próximo y el Pacífico, a menos que se indique lo contrario.

6 Del mismo modo, la región de África incluye países en el Norte de África, a menos que se indique lo contrario.

Nuevas tendencias en las estafas

Capitalización de los avances tecnológicos

En el marco de las estafas, la tecnología se ha convertido en el factor más importante para los grupos delictivos. El uso de la inteligencia artificial (IA), los grandes modelos de lenguaje (LLM) y las criptomonedas puede mejorar exponencialmente ciertos tipos de estafas sin realizar costosas inversiones.

El uso de contenido sintético generado a través de la IA (también denominado deepfake o contenido ultrafalso) a fin de cometer estafas en línea es una tendencia emergente y una preocupación creciente para los países miembros. Las barreras para acceder al uso de la inteligencia artificial generativa y los contenidos ultrafalsos van cayendo, ya que la tecnología es cada vez más accesible y fácil de usar.

Los modelos de negocio (como la delincuencia como servicio, el phishing como servicio y el ransomware como servicio) posibilitan además la entrada de ciberdelincuentes nuevos y menos eficientes desde el punto de vista tecnológico, con lo que facilitan el aumento de las estafas en línea y la realización de campañas de fraude más sofisticadas sin necesidad de que los perpetradores posean conocimientos técnicos avanzados. Estos modelos permiten el intercambio de habilidades y la distribución en la red oscura o en la Internet profunda de software delictivo complejo o datos personales robados, donde las partes de confianza comercian abiertamente con datos, servicios de alojamiento y software. El modelo de delincuencia como servicio también ayuda a los grupos de delincuencia organizada a reclutar y ampliar su red de mulas bancarias. En combinación con estos elementos, el rápido crecimiento de los usuarios en línea en todo el mundo crea un terreno propicio para una rápida expansión de las estafas en todas las regiones.

Los datos de los que dispone INTERPOL confirman que las criptomonedas y los proveedores de servicios de criptomonedas se utilizan ampliamente en las estafas de inversión y en las sentimentales y, en menor medida, en las de pago por anticipado y las estafas por medios de telecomunicación. Aunque el uso de bitcoines en las estafas es común en todo el mundo, determinados países miembros han informado de la circulación de otras criptomonedas, como las tether (también denominada USDT), altcoin (en África, Asia Oriental, el Sudeste Asiático y el Pacífico) o ether (en Europa). Asimismo, han advertido de que los estafadores utilizan proveedores de servicios de activos virtuales (como Binance) y sistemas virtuales de pago e inversión (como Skrill, Perfect Money, Netteller, Altcoin Trader y Luno Trading) para facilitar las estafas con criptomonedas, en particular en África, Asia y Europa. En algunos casos, los delincuentes crean su propia aplicación de inversión falsa como parte de sus estrategias de engaño o subcontratan su instalación. Según la información disponible, también clonan plataformas de inversión especulativas que imitan a empresas o servicios de inversión de renombre. Los estafadores manipulan las transacciones y muestran unas ganancias excepcionales en estas plataformas clonadas, con lo cual crean una ilusión de triunfo y alientan a las víctimas A invertir más dinero en los planes fraudulentos.

El uso habitual de las ultrafalsificaciones y de los grandes modelos de lenguaje beneficia aún más a las redes delictivas. Ha habido casos recientes en los países miembros en que se han creado fotografías ultrafalsas para abrir cuentas en bancos en línea con el fin de expandir las redes de mulas bancarias y en que se han utilizado grandes modelos de lenguaje para cometer estafas de inversión y de ofertas de empleo en aplicaciones de mensajería (como WhatsApp o Telegram). Cabe señalar que en estos casos la tecnología ha sido relativamente rudimentaria en lo que respecta a su aplicación, a pesar de haber tenido un inmenso potencial de complejidad.

Estafas y delincuencia forzada

La investigación y el análisis llevados a cabo por los funcionarios de INTERPOL pusieron de manifiesto una tendencia consistente en el recurso a la trata de personas con miras a la perpetración forzada de estafas en línea[7], cuyo modus operandi incluye, por una parte, a las víctimas de la trata (A), obligadas a cometer estafas en línea en así denominados "centros de llamadas" y, por otra parte, a las víctimas de la estafa (B), a las que las víctimas de la trata defraudan grandes sumas de dinero. En el marco de las operaciones STORM MAKERS I y II, la unidad de Trata de Personas y Tráfico Ilícito de Migrantes descubrió que unos grupos delictivos asiáticos perpetraban operaciones de trata de personas a gran escala facilitadas por Internet con el fin de forzar a las víctimas A cometer fraudes en línea en diferentes países del Sudeste Asiático[8]. Si bien al principio las víctimas de la trata de personas eran en su mayoría de habla china, la tendencia se ha ido extendiendo y las estrategias tanto de reclutamiento como de engaño se dirigen ahora a víctimas de todo el mundo[9].

OPERACIÓNES STORM MAKERS I Y II

Con ocasión de la operación STORM MAKERS llevada a cabo en 2022, la unidad INTERPOL de Trata de Personas y Tráfico Ilícito de Migrantes empezó a recibir información acerca de víctimas de trata obligadas a trabajar en centros de estafas situados en el Sudeste Asiático. En 2023 tuvo lugar la operación STORM MAKERS II, que tenía por objeto detectar y desmantelar organizaciones delictivas dedicadas a la trata de personas y al tráfico ilícito de migrantes y estaba dedicada exclusivamente a la tendencia de la trata de personas para la perpetración de estafas en línea en el Sudeste Asiático y en otras regiones afectadas.

Si bien es importante señalar que no todos los centros de estafas coaccionan a las personas que trabajan en ellos, la información que los países miembros han puesto en conocimiento de INTERPOL recientemente sugiere que han comenzado a surgir por todo el mundo centros que sí utilizan a víctimas de la trata de personas. Los países miembros de INTERPOL en América Latina han informado de la detección de un modus operandi similar en el que las víctimas A, que normalmente proceden de la región, son reclutadas mediante anuncios de empleo falsos, y a veces en espacios públicos. Una vez dentro de las instalaciones, son despojadas de sus documentos de identidad y obligadas a cometer estafas en línea, principalmente estafas de pago por anticipado, por medios de telecomunicación y de usurpación de identidad que, si bien no proporcionan mucho dinero (entre 100 y 500 dólares estadounidenses), se llevan a cabo a gran escala a través de plataformas de medios sociales y mercados en línea. El hecho de que las sumas de dinero sean pequeñas con frecuencia disuade a las víctimas de denunciar los fraudes, lo que impide identificar a las organizaciones delictivas que están detrás de ellos.

Además, se ha notificado a INTERPOL la existencia de centros de estafas similares en diversos países africanos, cuyas víctimas potenciales son personas y empresas de la región africana y de otras partes del mundo.

Con respecto a Europa, y sobre la base de los casos comunicados a INTERPOL, desde la segunda década del siglo XXI se viene informando de la existencia de centros de estafas en diversos países europeos[10]. Por otro lado, y a pesar de que persisten ciertos vacíos en materia de información, nos ha sido comunicada la existencia de centros de llamadas facilitados por la trata de personas en países de Europa del Este, en los que se cree que grupos locales trabajan con organizaciones delictivas extranjeras. En estos casos, según la información disponible, las víctimas A provienen de Oriente Próximo.

A medida que este modus operandi se expande y los perfiles de las víctimas A se diversifican (haciendo que existan víctimas de Asia, África y América Latina retenidas en centros de estafas), es altamente probable que el número de posibles víctimas B también aumente. Asimismo, es probable que el surgimiento de contenido generado mediante inteligencia artificial aumente el alcance, la sofisticación y la capacidad de los fraudes cometidos a través de centros de estafas que utilizan a víctimas de la trata de personas y hagan que estos afecten a personas en cualquier lugar del mundo.

7 INTERPOL. (2 de mayo de 2023). Notificación naranja de INTERPOL: Trata de personas para cometer estafas en línea, 2021 – 2023. N° de control: O-668/3-2023.

8 INTERPOL. (25 de octubre de 2022). Estafas en línea y trata de seres humanos en el Sudeste Asiático, Versión pública. INTERPOL – Exclusivamente para uso oficial. 2022/1626/OEC/VOC/HTSM/SBA.

9 INTERPOL. (6 de julio de 2023). Estafas en línea y trata de seres humanos en el Sudeste Asiático / Actualización 2 - De amenaza regional a amenaza mundial (versión pública). INTERPOL – Exclusivamente para uso oficial. 2023/923/OEC/VCO/HTSM/SBA.

10 INTERPOL. (6 de julio de 2023). Estafas en línea y trata de seres humanos en el Sudeste Asiático / Actualización 2 - De amenaza regional a amenaza mundial (versión pública). INTERPOL – Exclusivamente para uso oficial. 2023/923/OEC/VCO/HTSM/SBA.

Estafas híbridas: escalada de la estafa de inversión en criptomonedas

Desde 2022, INTERPOL ha observado una notable escalada de casos y una complejidad y sofisticación crecientes de las estafas en línea. Una tendencia, en ocasiones denominada en inglés pig butchering (el despiece del cerdo), se ha convertido rápidamente en una de las principales preocupaciones de las fuerzas del orden, ya que produce víctimas en todo el mundo que pierden millones a manos de hábiles estafadores[11]. Se trata de una estafa híbrida que combina elementos de las estafas sentimentales por Internet y de las estafas de inversión con criptomonedas, en las que los delincuentes manipulan el mercado de las criptodivisas y muestran unas grandes ganancias falsas para animar así a las víctimas A invertir más dinero en entramados fraudulentos.

La estafa de inversión en criptomonedas suele empezar como un tipo de estafa sentimental en la que estafadores expertos se dirigen a las víctimas a través de plataformas de redes sociales, aplicaciones de citas e incluso enviando mensajes directos a números de teléfono. Un aspecto destacado de este tipo de fraude es la revictimización de las personas afectadas por él. El fenómeno de revictimización aumenta el perjuicio económico y agrava el trauma psicológico y emocional que sufren las víctimas. Más allá de las repercusiones financieras inmediatas, este modus operandi supone unos desafíos importantes por su alcance internacional y el uso de criptomonedas.

Fases de la estafa de la inversión en criptomonedas (fuente: IGCR 2023)[12]

Las recientes investigaciones de INTERPOL ponen de manifiesto las huellas de la expansión geográfica de esta tendencia. Existen pruebas de que este tipo de fraude está traspasando los límites geográficos del núcleo inicial, el Sudeste Asiático, y está siendo replicado en otras regiones, como África y América Latina, en las que han surgido centros de llamadas similares a los de la región de origen. Los datos de INTERPOL confirman que algunos grupos delictivos asiáticos han captado a jóvenes, principalmente estudiantes, para que cometan fraudes en línea desde centros de llamadas situados en África Austral. Los delincuentes atraen a sus víctimas, concentradas principalmente en Norteamérica, para que inviertan en estafas con criptomonedas. INTERPOL prevé que las estafas en línea, incluidas las estafas sentimentales por Internet y las de inversión con criptomonedas, aumentarán en un futuro próximo a medida que este modus operandi híbrido vaya creciendo y añadiendo nuevas complejidades a estos tipos de fraude.

11 Centro de INTERPOL contra la Delincuencia Financiera y la Corrupción (IFCACC). (25 de mayo de 2023). Pig Butchering Scam: An Emerging and Sophisticated Romance Fraud Involving Crypto Currency Investment Schemes, 2023/521/IFCACC/OPS/CNI. INTERPOL – Exclusivamente para uso oficial.

12 INTERPOL. (Noviembre de 2023). Informe sobre las tendencias de la delincuencia a escala mundial - INTERPOL 2023, página 19.

Tendencias regionales de las estafas

OPERACIONES DELILAH, FALCON II, AFRICA CYBER SURGE I & II, CONTENDER

ENTRE 2022 Y 2023, INTERPOL CONDUJO VARIAS OPERACIONES EN EL CONTINENTE AFRICANO (DELILAH, FALCON II, AFRICA CYBER SURGE I Y II Y CONTENDER), DIRIGIDAS CONTRA GRUPOS DELICTIVOS Y DELINCUENTES DEDICADOS A LA COMISIÓN DE ESTAFAS DE TIPO BEC, SENTIMENTALES, CON CRIPTOMONEDAS, PHISHING Y OTROS CIBERDELITOS.[13]

África

El sector financiero africano se ha digitalizado con rapidez. La región se cuenta entre los principales usuarios mundiales de la banca móvil y las transacciones monetarias, lo cual ha brindado numerosas oportunidades a los delincuentes para cometer fraudes financieros.

Según el informe de evaluación de las ciberamenazas en África en 2023 preparado por INTERPOL, las estafas BEC, el phishing y otras estafas en línea son un problema creciente en África debido a la rápida transición hacia una economía cada vez más digitalizada[14]. La ampliación del acceso a Internet, junto con los bajos niveles de alfabetización digital, hacen que muchos africanos sean blancos fáciles para los estafadores y los ciberdelincuentes.

Las estafas BEC siguen siendo una de las tendencias con mayor prevalencia en África, y causan importantes pérdidas financieras a personas y empresas. Se ha comprobado que muchos de los perpetradores de estafas BEC están ubicados en África Occidental, si bien sus víctimas suelen encontrarse en otros lugares. A menudo, estos delincuentes tienen conexiones con redes delictivas más amplias de todo el mundo, lo que les permite atacar a un gran número de víctimas a escala global.

Las estafas en línea incluyen una amplia variedad de actividades fraudulentas en el entorno digital. Las estafas de pago por anticipado y de pedidos que no se entregan, las relacionadas con el comercio electrónico, las sentimentales por Internet, las de asistencia técnica y las de inversión con criptodivisas son cada vez más frecuentes en la región africana.

También es motivo de preocupación la comisión creciente de estafas de inversión en criptomonedas. Se han detectado casos de este tipo de fraude en África Occidental y Austral dirigidos a víctimas de otros continentes.

El crimeware como servicio se está volviendo una tendencia cada vez más extendida en África. Ha permitido la entrada de nuevos ciberdelincuentes que tienen menos conocimientos tecnológicos ya que, al permitir realizar complejos ataques sin necesidad de conocimientos técnicos avanzados, facilita las actividades maliciosas de los ciberdelincuentes.

La operación Jackal de INTERPOL, iniciada en mayo de 2023, estaba dirigida contra grupos delictivos de África Occidental que actúan en 21 países. Se saldó con más de 100 detenciones y el bloqueo de más de 200 cuentas vinculadas a los beneficios ilícitos de las estafas en línea.

La información de la que dispone INTERPOL sugiere que algunos grupos delictivos de África Occidental están ganando en transnacionalidad y están asentados en países y regiones de todo el mundo. Se sabe que estos grupos de África Occidental dedicados a la multidelincuencia son grandes conocedores de las estafas en línea, como las sentimentales, las de inversión, las de pago por anticipado y las de criptomonedas, y las practican[15].

13 INTERPOL - Dirección de Ciberdelincuencia: Operaciones Conjuntas contra la Ciberdelincuencia en África (AFJOC). (2023). https://www.interpol.int/es/Delitos/Ciberdelincuencia/Operaciones-contra-la-ciberdelincuencia/Operaciones-Conjuntas-contra-la-Ciberdelincuencia-en-la-Region-Africana-AFJO.

14 INTERPOL - Dirección de Ciberdelincuencia. (Marzo de 2023). Informe de evaluación de las ciberamenazas en África - 2023: Tendencias de las ciberamenazas.

15 Centro de INTERPOL contra la Delincuencia Financiera y la Corrupción. (3 de octubre de 2023). Las fraternidades Supreme Eiye y Airlords, 2023/742/IFCACC/OPS/PP. INTERPOL - USO RESTRINGIDO.

OPERACIÓN JACKAL

La operación Jackal de INTERPOL, iniciada en mayo de 2023, estaba dirigida contra grupos delictivos de África Occidental que actúan en 21 países. Se saldó con más de

100 DETENCIONES

Y EL BLOQUEO DE MÁS DE 200 CUENTAS VINCULADAS A LOS BENEFICIOS ILÍCITOS DE LAS ESTAFAS EN LÍNEA.

América

En consonancia con las tendencias mundiales, en la región de las Américas los fraudes en línea con ánimo de lucro aumentaron considerablemente, muchos de ellos aprovechando la creciente demanda de suministros médicos y otras vulnerabilidades intensificadas por la pandemia, en particular los dirigidos contra particulares y empresas de América del Norte. En el Informe sobre las tendencias de la delincuencia a escala mundial - INTERPOL 2022 se señalaba que algunas de las estafas más comunes eran las de usurpación de identidad, las sentimentales, las de asistencia técnica, las de pago por anticipado y las estafas por medios de telecomunicación[16].

Las empresas y los habitantes de esta región han sufrido enormes pérdidas económicas a causa de las estafas en línea. Según la información recibida, estas provienen principalmente de África (y más concretamente de África Occidental, donde operan las fraternidades delictivas) y de Asia (donde se encuentran las organizaciones delictivas asiáticas). El aumento de los perjuicios patrimoniales provocados por las estafas trae consigo un incremento del problema del blanqueo de capitales.

Las estafas cometidas por víctimas de la trata de personas son un fenómeno delictivo que crece sin cesar. La operación Turquesa V coordinada por INTERPOL reveló que cientos de víctimas eran transportadas a otras regiones después de haber sido atraídas a través de aplicaciones de mensajería y plataformas de medios sociales, y que a continuación se las obligaba a cometer estafas, como las de inversiones, en centros telefónicos del Sudeste Asiático dirigidos por grupos delictivos[17].

Se ha comenzado a tener pruebas de que diversos grupos delictivos latinoamericanos también se dedican a cometer estafas siguiendo una tendencia que despegó con fuerza después del brote de COVID-19[18]. Estos grupos han estado tradicionalmente vinculados con el tráfico de drogas, el tráfico de armas, el blanqueo de capitales, secuestros y episodios de violencia intensificada a escala nacional y regional[19].

Los proveedores de servicios de delincuencia están transformando los fraudes en actividades relativamente fáciles de llevar a cabo, lucrativas y de bajo riesgo. Las herramientas digitales y la tecnología aumentan los efectos de las operaciones, aseguran el anonimato de los delincuentes y facilitan el blanqueo de los fondos ilícitos. Por ello, es altamente probable que más organizaciones delictivas se entreguen a actividades ilícitas de este tipo.

16 INTERPOL. (Octubre de 2022). Informe de INTERPOL sobre las tendencias de la delincuencia a escala mundial.

17 INTERPOL. (11 de diciembre de 2023). Américas: Detención de 257 sospechosos de tráfico de migrantes y trata de personas. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2023/Americas-detencion-de-257-sospechosos-de-trafico-de-migrantes-y-trata-de-personas

18 Datos de INTERPOL (21 de octubre de 2023); Meegan-Vickers, J. (2023), Scam call centres in Ukraine (Centros de llamadas para cometer estafas en Ucrania), The Global Initiative Against Transnational Organized Crime (GI-TOC). https://globalinitiative.net/analysis/scam-call-centres-in-ukraine/ (consultado el 22 de febrero de 2024).

19 El País México. (30 de noviembre de 2023). EE UU sanciona a 12 empresas vinculadas al Cartel Jalisco Nueva Generación en Puerto Vallarta. https://elpais.com/mexico/2023-11-30/ee-uu-sanciona-a-12-empresas-vinculadas-al-cartel-jalisco-nueva-generacion-en-puerto-vallarta.html (consultado el 15 de febrero de 2024).

OPERACIÓN HAECHI IV

En diciembre de 2023, INTERPOL ejecutó una operación policial en varios continentes contra las estafas facilitadas por Internet y otros ciberdelitos (como las estafas sentimentales, de inversión, BEC, relacionadas con el comercio electrónico, phishing telefónico, sextorsión y blanqueo de capitales relacionado con las apuestas en línea). Esta operación dio lugar a casi 3 500 arrestos y la incautación de activos por valor de 30 millones de dólares estadounidenses en 34 países de África, América, Asia, Europa y Oceanía.
Esta operación permitió alertar a los países miembros sobre una técnica emergente utilizada en los fraudes con criptomonedas (también denominada rug pull) mediante la cual un equipo de desarrolladores crea una criptomoneda, la promociona entre los inversores y después abandona repentinamente el proyecto para causar que los inversores pierdan su dinero.
Además, puso de manifiesto el uso cada vez más frecuente de la inteligencia artificial y de la tecnología de ultrafalsificación para estafar, acosar y extorsionar en estafas sentimentales por Internet, de usurpación de identidad y de inversión.

3 500 ARRESTOS

MILLONES DE DÓLARE

34 COUNTRIES

Asia

Las estafas son una amenaza que evoluciona con rapidez en esta zona geográfica. Los países miembros de la región se han convertido en los principales blancos de las estafas, dado que se encuentran entre las economías digitales de más rápido crecimiento del mundo. La pandemia de COVID-19 aceleró la digitalización de los servicios y los comportamientos de la ciudadanía y las empresas de la región asiática. A resultas de ello, las estafas, ampliamente facilitadas por Internet, se han intensificado y seguirán haciéndolo. Frecuentemente, los países miembros de la región asiática indican que las estafas representan una amenaza muy elevada.

INTERPOL detectó recientemente la estafa de inversión en criptomonedas, una variante de la tradicional estafa sentimental por Internet con el elemento añadido de la inversión con criptomonedas. Este tipo de fraude surgió por primera vez en Asia en 2019 y se expandió durante la pandemia de COVID-19. Con el paso del tiempo, Asia ha ido convirtiéndose en un centro de coordinación en el que organizaciones delictivas de los países más pobres de la región emplean estructuras gestionadas como empresas y, en algunos casos, explotan a las víctimas de la trata de personas para llevar a cabo las actividades fraudulentas. Las investigaciones indican que este modus operandi se está extendiendo rápidamente a otras regiones fuera de Asia.

Otras estafas que han experimentado un aumento en los últimos años en Asia son las cometidas por medios de telecomunicación en las que, desde los centros de operaciones de ciertos países de la región, los perpetradores se hacen pasar por agentes de las fuerzas del orden o empleados de banca y contactan a través de líneas locales o internacionales a las víctimas con el fin de engañarlas y que estas les proporcionen los datos de sus cuentas o tarjetas bancarias o les envíen grandes sumas de dinero.

Según la evaluación de las ciberamenazas llevada a cabo en 2021 por INTERPOL y la ASEAN, las estafas de tipo BEC, las relacionadas con el comercio electrónico y el phishing son algunas de las tendencias delictivas que siguen suponiendo una amenaza muy alta para los países en la región. INTERPOL prevé que estas tendencias seguirán aumentando en los próximos años[20]. Las pruebas procedentes del Sudeste Asiático indican que en 2023 un país miembro perdió más de 500 millones de dólares estadounidenses a causa de este tipo de estafas, y más del 30 % de esa cantidad por estafas de inversión[21].

Si bien los datos de que dispone INTERPOL indican que todos los grupos de edad son vulnerables frente al fraude, la mayoría de las víctimas de la región de Asia tienen entre 30 y 49 años. Estas son escogidas principalmente a través de medios sociales y plataformas de mensajería. El uso cada vez más recurrente de la tecnología por parte de los estafadores y ciberdelincuentes hace que los delitos de estafa en la región no muestren señales de desaceleración o disminución.

20 INTERPOL - Dirección de Ciberdelincuencia. (21 de enero de 2021). ASEAN Cyberthreat Assessment 2021: Key Cyberthreat Trends Outlook From the ASEAN Cybercrime Operations Desk' (Evaluación de INTERPOL y la ASEAN sobre ciberamenazas 2021: Perspectiva sobre las principales tendencias de las ciberamenazas, por la Oficina de Operaciones contra la Ciberdelincuencia en la región de la ASEAN). https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2021/INTERPOL-describe-en-un-informe-las-principales-ciberamenazas-en-el-Sudeste-Asiatico (consultado el 13 de febrero de 2024).

21 Policía de Singapur. (18 de febrero de 2014). Annual Scams and Cybercrime Brief 2023 [Informe Anual sobre Estafas y Ciberdelincuencia, página 8.

Europa

Los países europeos indican que en esta región las estafas representan una amenaza muy elevada para las personas, las empresas y las entidades públicas. Al igual que en otras regiones, el uso de herramientas en línea por parte de los delincuentes para perpetrar estos delitos se ha expandido desde la pandemia. Existen pruebas de que las estafas facilitadas por Internet constituyen más del 80 % de las estafas denunciadas en algunos países de la región. Predomina el blanqueo de capitales, que se vale probablemente de modus operandi sometidos a controles financieros menos estrictos, incluido el uso de criptomonedas para blanquear las ganancias ilícitas.

Las estafas de inversión en línea, el phishing y otras estafas financieras por Internet se dirigen de forma creciente contra objetivos seleccionados cuidadosamente para maximizar los beneficios. Las aplicaciones de telefonía móvil también están en el punto de mira de los ciberdelincuentes. Según la información disponible, las estafas de inversión y las BEC son los tipos de fraude más prolíficos y los que causan las mayores pérdidas económicas en la región[22]. Las estafas en línea representan una amenaza cada vez mayor, dado que la variedad de víctimas a las que se dirigen los estafadores es cada vez más amplia e incluye a personas, empresas y organismos públicos de toda Europa. Las redes delictivas que llevan a cabo estos engaños suelen utilizar modus operandi sofisticados y complejos que por lo general combinan diferentes tipos de estafas.

En los últimos años, se han detectado cada vez más fraudes que explotan grandes crisis o situaciones de emergencia, como el conflicto en Ucrania y el terremoto mortífero de Türkiye. En estos casos, los estafadores se hacen pasar por organizaciones legítimas o celebridades y fingen recaudar fondos para actividades humanitarias, engañando así a las víctimas para que les entreguen dinero, a menudo en forma de criptomonedas.

Otra estafa en aumento es la de inversión en criptomonedas, casi siempre llevada a cabo desde centros telefónicos ilegales del Sudeste Asiático. Según los datos disponibles, se han identificado en Europa centros de llamadas como los dirigidos por los grupos de delincuencia organizada del Sudeste Asiático, aunque son casos aislados. En los análisis de INTERPOL también se ha detectado la existencia de grupos de delincuencia organizada cuyos cabecillas proceden de Oriente Próximo, especializados en estafas por medios de comunicación, sentimentales por Internet, de usurpación de identidad (o fraudes del CEO) y de divisas (Forex), con frecuencia cometidas desde centros de llamadas. Si bien se empieza a hacer patente la cooperación entre los grupos de delincuencia organizada europeos y estos grupos delictivos para la comisión de estafas en diferentes formas, se cree que dichos centros se encuentran, al menos, en Europa del Este y, presumiblemente, en algunos países africanos.

Sin embargo, las estafas en línea (como las estafas de inversiones, de suplantación de identidad y sentimentales por Internet) se apoyan en gran parte en delincuentes solitarios y grupos delictivos que operan desde África Occidental, comúnmente con conexiones en Europa y una amplia red de cómplices, quienes facilitan tramos del fraude a escala internacional. Las estafas cometidas en esta región tienen vínculos demostrados con una fraternidad delictiva de África Occidental.

Los estafadores conocen bien los protocolos bancarios y disponen de acceso a una sofisticada y compleja red de mulas bancarias, lo que dificulta seguir el rastro de las ganancias ilícitas. El uso de los bancos en línea en lugar de bancos convencionales, las criptomonedas, las aplicaciones de transferencia de dinero y las tarjetas de regalo para blanquear las ganancias ilícitas hace que sea difícil identificar su origen. Sin embargo, algunos países han indicado que estos fondos blanqueados a veces terminan en otras zonas de África Occidental y el Sudeste Asiático.

Las pruebas de las que se dispone indican que los estafadores y los ciberdelincuentes suelen utilizar los medios sociales y las aplicaciones de mensajería para dirigirse a personas de cualquier género, de países europeos y de entre 30 y 80 años. Las víctimas de las estafas, especialmente las de estafas sentimentales por Internet, suelen ser personas vulnerables.

La creciente presencia de facilitadores tales como paquetes de phishing, herramientas de administración remota, violaciones de datos de tarjetas bancarias, bases de datos de datos personales y manuales sobre métodos de fraude en foros de la web oscura está facilitando la comisión de delitos.

Se prevé que las estafas en línea sigan aumentando en un futuro próximo puesto que los estafadores y los ciberdelincuentes seguirán probablemente integrando en su haber nuevas tecnologías y herramientas, como los deepfakes y otras variantes de inteligencia artificial generativa, para atraer a más víctimas. El aumento de las nuevas tecnologías hará que las amenazas en constante evolución sean cada vez más complejas.

22 EUROPOL. (19 de diciembre de 2023). Online Fraud Schemes: A Web of Deceit (IOCTA 2023) [Estafas en línea: una red de engaños (IOCTA 2023)], https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023

Estafas organizadas

Los grupos delictivos organizados son los principales perpetradores de fraudes con ánimo de lucro en el mundo. Sus recursos y estructuras, así como su naturaleza predatoria, los hacen particularmente peligrosos. A pesar de la falta de información acerca de los grupos delictivos organizados que cometen estafas transnacionales, los datos de INTERPOL sugieren que la tecnología utilizada y las asociaciones creadas refuerzan las capacidades de estas redes de delincuentes y les dan gran poder en el ecosistema de las estafas y más allá. A este respecto, INTERPOL ha observado que los delitos de este tipo y el blanqueo de las ganancias ilícitas obtenidas con ellos suelen converger con otras actividades delictivas además de la trata de personas, como el tráfico de drogas, de productos falsificados y de otros productos ilícitos. Es probable que esta convergencia o efecto de creación de redes estén relacionados con la creación de los lazos indicados de colaboración entre delincuentes.

A menudo, los grupos de delincuentes involucrados en las estafas crean redes que traspasan las fronteras nacionales, las regionales y las continentales. Estas colaboraciones con otros coautores de los delitos les permite controlar diferentes áreas de las operaciones delictivas. Algunos ejemplos de las tareas que pueden realizar los colaboradores de las estafas son los siguientes:

- **Captación de cómplices con conocimientos o competencias particulares:** Búsqueda de proveedores de servicios delictivos y otras personas que posean competencias adecuadas (como especialistas en tecnología o asesores financieros), para llevar a cabo tareas clave en las operaciones; por ejemplo, para desarrollar tramas de inversión complejas.
- **Identificación de objetivos y víctimas:** Búsqueda y determinación de grupos de población u objetivos fáciles de manipular o, en función del método de estafa que se utilice, compra de listas de datos a personas con acceso a información sobre objetivos potenciales.
- **Blanqueo de ganancias ilícitas:** La transferencia y el blanqueo de los fondos obtenidos mediante las estafas es imprescindible para que los grupos delictivos que participan en ellas mantengan su actividad. Para blanquear los capitales, los delincuentes pueden colaborar con propietarios de negocios legítimos o encontrar a personas o a redes que propongan el blanqueo de capitales como servicio. Con frecuencia creciente las redes delictivas mueven los fondos ilícitos provenientes de las estafas a través de fronteras físicas y virtuales siguiendo tramas complejas de blanqueo de capitales. INTERPOL ha puesto en marcha un mecanismo de bloqueo de pagos para limitar el blanqueo de millones de dólares generados por las estafas (ver tabla a continuación).

CASO CONCRETO DE USO DEL SISTEMA I-GRIP

Una empresa radicada en el país A fue objeto de una estafa de usurpación de identidad en la que los delincuentes se hicieron pasar por el banco central del país. La víctima transfirió 1,2 millones de euros a una cuenta domiciliada en el país B y 2 millones a otra cuenta domiciliada en el país C.

La OCN del país A alertó al banco de la víctima para solicitar el bloqueo del pago, si era posible, y se puso en contacto con el Centro de INTERPOL contra la Delincuencia Financiera y la Corrupción (IFCACC) para mejorar la coordinación con los países B y C con el fin de bloquear los pagos y poner fin a la dispersión de los fondos. En estrecha colaboración con el IFCACC, las OCN de los países B y C solicitaron que los bancos beneficiarios presentes en sus respectivos territorios bloquearan los pagos. La suma total, 3,2 millones de euros, fue recuperada en un día y restituida a la víctima.

Los grupos de delincuencia organizada invierten cuanto es necesario en la creación de sitios web y perfiles de medios sociales falsos, así como en correos electrónicos de phishing que parecen auténticos. También son capaces de desarrollar herramientas automatizadas que permiten preparar ciberataques a gran escala. La emergencia del crimeware como servicio ha ampliado enormemente las oportunidades de colaboración y venta e intercambio de recursos entre los grupos de delincuencia organizada. Tal y como se ha mencionado, este nuevo servicio es una empresa lucrativa para los empresarios delincuentes y les facilita la tarea a los grupos delictivos con competencias técnicas menos desarrolladas.

Estructura de los grupos delictivos organizados

Según el método utilizado para delinquir, el fraude con ánimo de lucro no requiere necesariamente que los delincuentes colaboren entre sí. Sin embargo, es más probable que algunos tipos de estafa a gran escala facilitada por Internet sean cometidos por grupos delictivos organizados transnacionales. Si bien puede resultar laborioso investigarlos, se advierte que los grupos conocidos tienen tanto estructuras jerárquicas como células descentralizadas.

INTERPOL ha observado que los grupos o fraternidades de delincuencia organizada de África Occidental siguen en general un modelo jerárquico en el que cada miembro cumple una función específica y tiene asignada una responsabilidad concreta. No obstante, otras fuentes han comunicado a INTERPOL que los integrantes de estos grupos a menudo tratan intencionalmente de poner trabas a las investigaciones policiales utilizando cargos engañosos para nombrar a sus líderes. En el caso de las fraternidades de África Occidental, la estructura jerárquica puede variar igualmente entre países.

Existen, además, otros grupos de delincuencia organizada dedicados a las estafas que operan de una manera más descentralizada ofreciendo el crimeware como servicio. Los que así lo hacen son menos rígidos y sus relaciones con otros grupos delictivos pueden ser más efímeras. Según un informe coescrito por INTERPOL y sus socios, se observó que un grupo delictivo operaba siguiendo este modelo y ofrecía servicios de blanqueo de capitales a estafadores que actuaban por Internet[24].

En la preparación de este informe, INTERPOL y sus socios identificaron varias organizaciones delictivas que cometen estafas y operan en diferentes regiones. Los datos disponibles indican que hay organizaciones delictivas de Asia Oriental, Latinoamérica, África Occidental y Europa implicadas en diferentes tipos de fraude con ánimo de lucro y blanqueo de capitales. El uso de tecnologías de la información y la comunicación globalizadas para cometer estafas facilitadas por Internet hacen que estos grupos delictivos sean capaces de engañar a víctimas de cualquier lugar del mundo.

SISTEMA DE INTERPOL DE INTERVENCIÓN RÁPIDA DE PAGOS A ESCALA MUNDIAL (I-GRIP)

INTERPOL creó un mecanismo mundial de bloqueo de pagos para facilitar la comunicación entre los países miembros a fin de interceptar el movimiento de dinero ilícito y ayudar a las víctimas A recuperar los fondos robados por grupos delictivos a través de delitos financieros facilitados por Internet. La coordinación entre los organismos aumenta las probabilidades de que se tomen rápidamente las medidas oportunas dentro de los límites que las leyes nacionales autoricen y antes de que se efectúen los pagos ilícitos, se retire dinero en efectivo o los activos sean transferidos hacia otros lugares. Desde la puesta en marcha en 2022 del sistema I-GRIP, INTERPOL ha ayudado a los países miembros a interceptar más de 500 millones de dólares estadounidenses obtenidos en gran medida mediante estafas facilitadas por Internet.

23 FATF, INTERPOL, GRUPO EGMONT. (Noviembre de 2023). Illicit Financial Flows from Cyber-Enabled Fraud]Flujos Financieros Ilícitos Obtenidos a partir del Fraude Facilitado por Internet.

Conclusiones

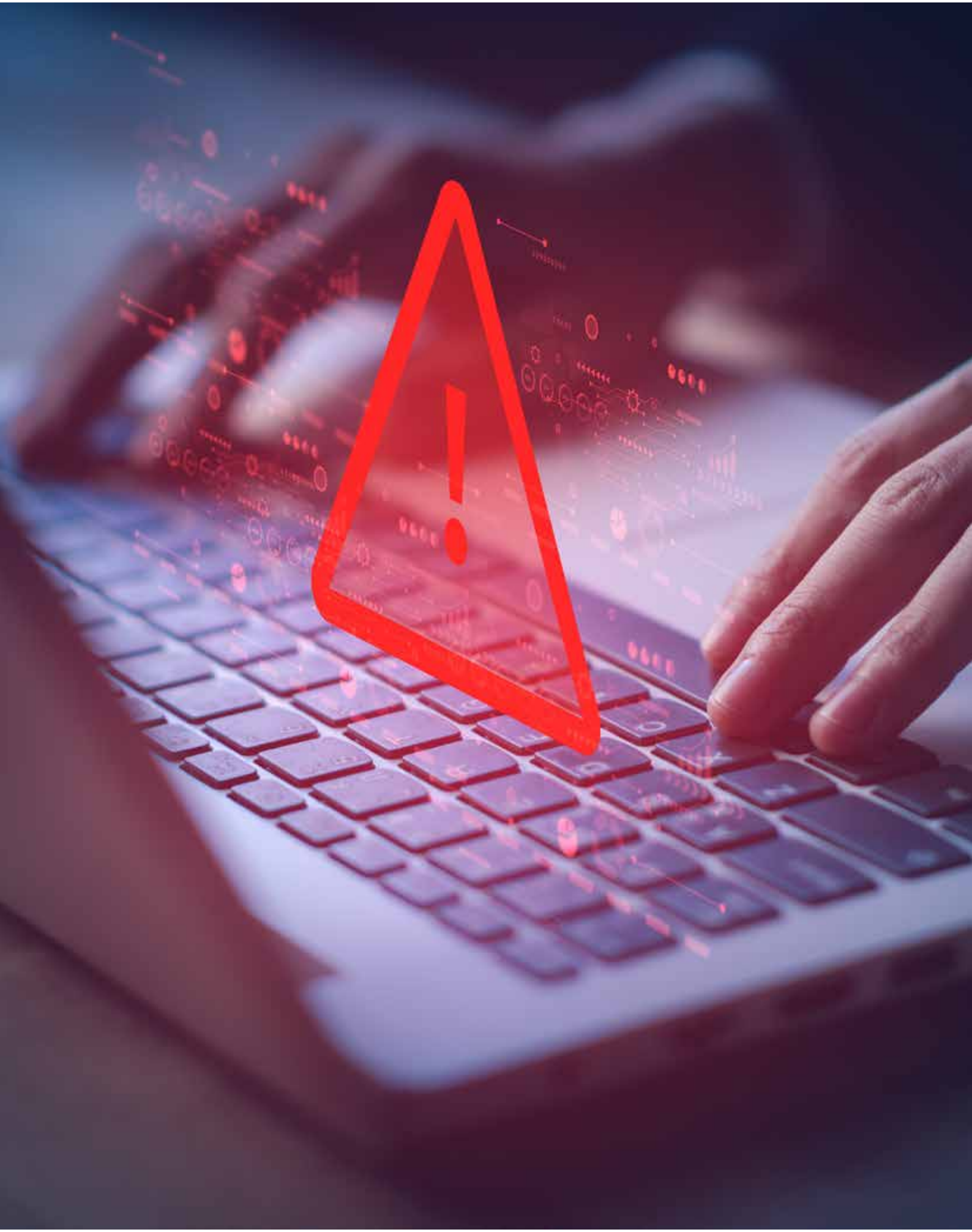
El presente informe tiene por objeto analizar los datos de INTERPOL a fin de comprender la evolución de las tendencias de las estafas y determinar cuáles de ellas plantean las mayores amenazas para las personas y las empresas en cada región y en todo el mundo. Además, se examina la convergencia de las estafas con otros delitos, en particular la trata de personas y el blanqueo de capitales, y la dinámica de los grupos delictivos organizados que participan en ellas.

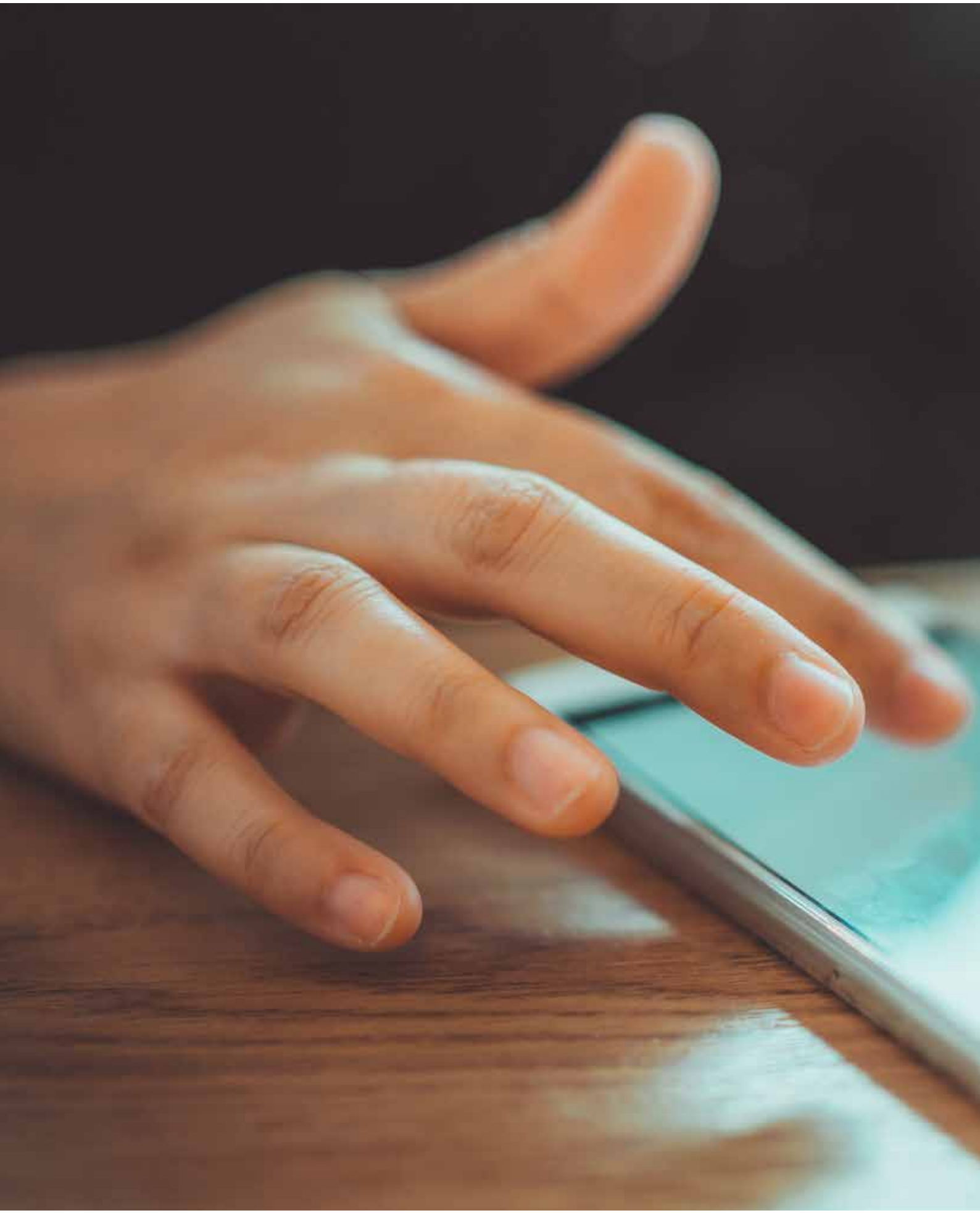
Según los datos de los que dispone INTERPOL, las estafas de inversión y las BEC siguen siendo el principal modus operandi a escala mundial. Aunque las estafas se cometen en todo el mundo, sus tendencias varían de una región a otra. Los tipos más frecuentes de fraude en Asia son las estafas de suplantación de identidad y las sentimentales por Internet; en África, las de pago por anticipado, seguidas por las sentimentales por Internet y las BEC; en Europa, las cometidas por medios de telecomunicaciones, las BEC y las sentimentales por Internet; y en la región de las Américas, las más comunes son el phishing, las BEC y de pago por anticipado.

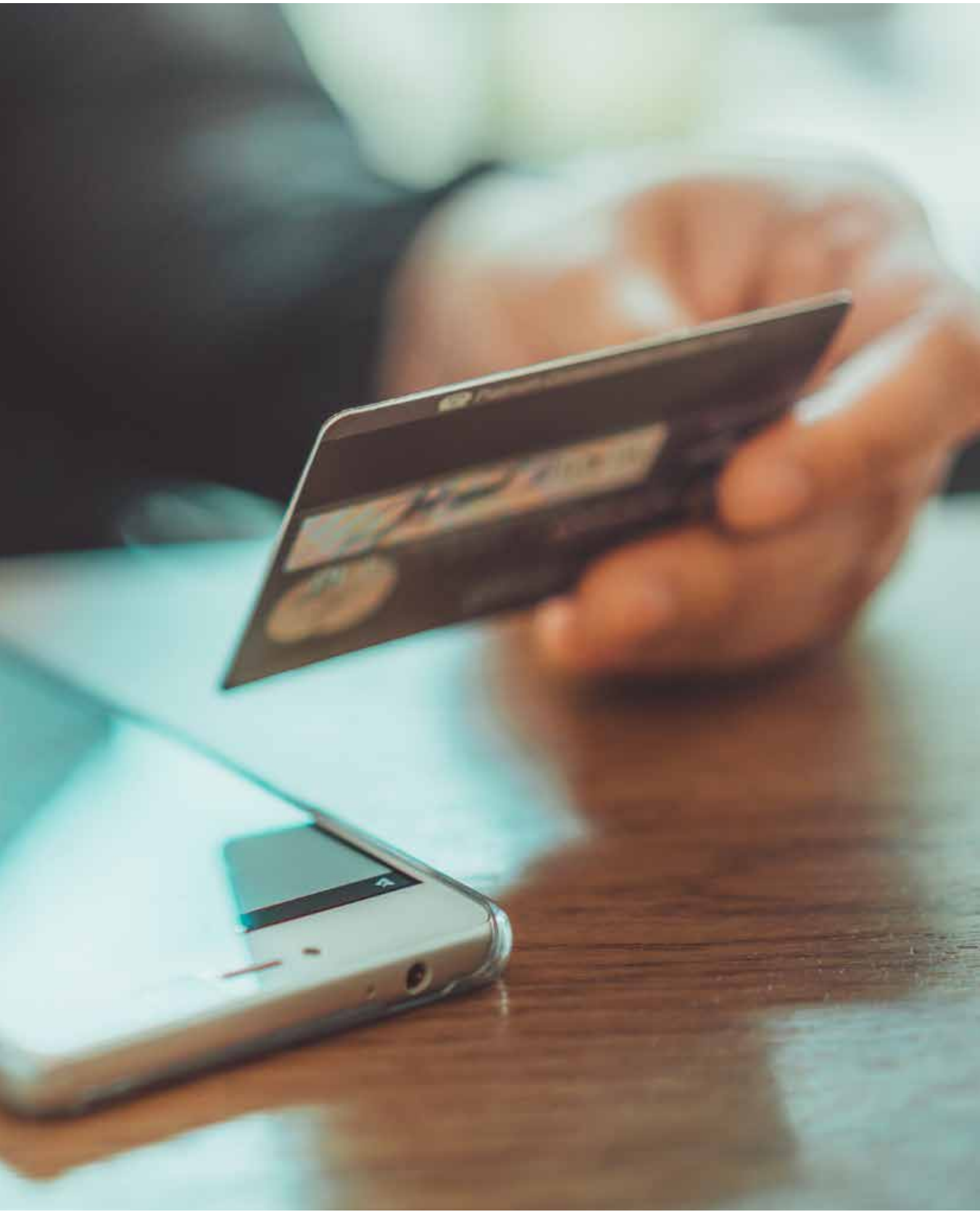
Los países miembros prevén que el alcance y la magnitud de las estafas aumenten a la par que los avances tecnológicos y la expansión de los servicios virtuales en todo el mundo. De hecho, ya han surgido nuevas tendencias que utilizan las criptomonedas y la inteligencia artificial, y los estafadores también están utilizando técnicas híbridas que combinan estafas sentimentales por Internet con fraudes de inversión. Sin embargo, la sofisticación de las nuevas técnicas de fraude no es una barrera para los delincuentes menos expertos en el uso de las tecnologías. Los proveedores de servicios de delincuencia se han convertido en importantes facilitadores de estafas a gran escala, en particular de la ciberdelincuencia como servicio y del blanqueo de capitales como servicio.

Las estafas, y en particular las facilitadas por Internet, que por defecto son mundializadas y anónimas, suele ser perpetradas por grupos delictivos organizados transnacionales. Si bien es necesario recabar más datos para comprender mejor la dinámica y el grado en que los grupos delictivos organizados las cometen, la información disponible con respecto de los grupos señalados en el presente informe indica que los delincuentes operan a escala mundial, parecen compartir experiencias delictivas y conocimientos especializados y muy probablemente colaboran para optimizar las oportunidades de la delincuencia y las ganancias que genera.

INTERPOL sigue realizando esfuerzos para evaluar el grado de amenaza que representan las estafas perpetradas tanto por personas como por grupos a escala regional y mundial, y los datos que proporcionan los 196 países miembros de la Organización siguen siendo fundamentales para realizar evaluaciones precisas. Las conclusiones de este informe servirán de base a la estrategia de la Organización para apoyar a los países miembros en la lucha contra las estafas y serán incluidas en la Evaluación de INTERPOL sobre las amenazas planteadas por la delincuencia a escala mundial, que se publicará en noviembre de 2024.







INTERPOL

ACERCA DE INTERPOL

La función de INTERPOL es permitir que las policías de nuestros 196 países miembros colaboren para combatir la delincuencia transnacional y hacer del mundo un lugar más seguro. Mantenemos bases de datos mundiales con información policial sobre delincuentes y delitos, y proporcionamos a los países miembros apoyo operativo y forense, servicios de análisis y formación. Estas capacidades policiales se prestan en todo el mundo y sustentan cuatro programas mundiales: delincuencia financiera y corrupción, lucha contra el terrorismo, ciberdelincuencia, y delincuencia organizada y nuevas tendencias delictivas.

NUESTRA META: "MAYOR COMUNICACIÓN POLICIAL PARA UN MUNDO MÁS SEGURO"

Nuestra meta es lograr un mundo en el que todos los profesionales de los organismos encargados de la aplicación de la ley sean capaces, a través de INTERPOL, de transmitir, intercambiar y consultar de forma segura información policial vital cuando y donde lo necesiten, garantizando así la seguridad de los ciudadanos de todo el planeta. Constantemente proporcionamos y promovemos soluciones avanzadas e innovadoras para hacer frente a los desafíos en el ámbito del trabajo policial y la seguridad que se plantean a escala mundial.

www.interpol.int | INTERPOL | @INTERPOL_HQ | INTERPOL_HQ | INTERPOL HQ | INTERPOL