INTERPOL

RAPPORT INTERPOL ÉVALUATION DES ESCROQUERIES FINANCIÈRES AU NIVEAU MONDIAL

MAI 2024

Avertissement

Secrétariat général d'INTERPOL
200, quai Charles de Gaulle
69006 Lyon
France
Téléphone : + 33 4 72 44 70 00
Fax : + 33 4 72 44 71 63
Site Internet : www.interpol.int
Courriel : info@interpol.int

Table des matières

Résumé des principales conclusions

Les escroqueries financières se sont multipliées et diversifiées, tant en matière de volume que de méthodes employées pour les commettre. Aujourd'hui, elles représentent une menace mondiale et généralisée.

Considérée comme une catégorie générale englobant les activités qui « visent à l'obtention d'un gain financier par le biais d'actions délibérées et trompeuses à l'encontre de personnes et à leur détriment », l'escroquerie ne fait pas seulement perdre des sommes colossales à des particuliers et à des entreprises, elle ébranle également les économies nationales et mondiales en sapant la confiance et en affaiblissant les systèmes financiers.

L'évaluation des escroqueries financières au niveau mondial constitue une analyse approfondie des données d'INTERPOL sur les infractions liées aux escroqueries financières et leurs auteurs, qui s'en prennent autant à des particuliers qu'à des entreprises. Elle s'appuie sur les notices et diffusions INTERPOL en lien avec des faits d'escroquerie financière. Les principales conclusions de l'évaluation sont les suivantes :

- Les escroqueries aux placements, à l'avance de frais, aux sentiments et aux faux ordres de virement sont les plus répandues au niveau mondial.
- Les escroqueries financières sont intrinsèquement liées aux technologies de l'information et de la communication, qui sont par nature mondialisées, ce qui signifie que les activités d'escroquerie sont transnationales et souvent transcontinentales.
- Les malfaiteurs se servent des nouvelles technologies, notamment de l'intelligence artificielle (IA) avec des techniques telles que l'hypertrucage (deep fake), pour tromper leurs victimes et dissimuler leur identité.
- Les données indiquent un recours croissant à des centres ou même des camps d'arnaques, qui sont tributaires de la traite d'êtres humains aux fins de criminalité forcée. Cette tendance a été observée en Asie du Sud-Est, en Afrique australe, en Afrique de l'Est et de l'Ouest, en Europe de l'Est et en Amérique latine.
- Le système d'escroquerie aux placements dans les cryptomonnaies, un mode opératoire hybride combinant escroquerie aux sentiments et escroquerie aux placements, progresse et prend de l'ampleur. Les victimes sont quant à elles souvent réticentes à se manifester.
- Les escroqueries financières sont souvent commises par un réseau de malfaiteurs, dont le degré d'organisation varie grandement, allant de groupes criminels organisés informels à des groupes hautement structurés.
- Les escroqueries financières font converger différents types de criminalité. La cybercriminalité en tant que service et le blanchiment d'argent en tant que service sont des facteurs essentiels à l'autonomisation des escrocs, qui peuvent être des malfaiteurs isolés comme des groupes criminels.
- Si les modes opératoires sont clairs, il est beaucoup plus difficile d'obtenir des informations sur les malfaiteurs ou sur l'organisation des escroqueries. Il est donc urgent de renforcer la collecte et l'analyse de données sur les escroqueries financières afin d'élaborer des stratégies de lutte plus efficaces et solidement étayées.

Les escroqueries financières sont des infractions prédatrices perpétrées dans l'anonymat et qui dépassent les frontières. INTERPOL s'engage à continuer de soutenir les pays membres dans la lutte mondiale contre ce type d'escroquerie, grâce à la collecte de données, à l'analyse criminelle et à l'appui opérationnel.

Les conclusions de ce rapport font partie intégrante du travail d'analyse actuellement mené pour évaluer les menaces criminelles existantes et nouvelles afin de rédiger le rapport d'INTERPOL intitulé « Évaluation des menaces criminelles au niveau mondial », qui sera mis à la disposition des services chargés de l'application de la loi des pays membres de l'Organisation en novembre 2024.

Introduction

Dans un monde de plus en plus dominé par le numérique et interconnecté, les escroqueries financières sont devenues une menace omniprésente et coûteuse tant pour les particuliers que pour les entreprises. Les répercussions économiques des escroqueries sont faramineuses. Plus la technologie évolue, plus les modes opératoires utilisés par les escrocs sont innovants. Ces derniers s'empressent d'exploiter toute nouvelle faille et d'adapter leurs stratégies pour contourner les mesures de sécurité et toujours avoir une longueur d'avance sur les services chargés de l'application de la loi.

Pour lutter contre cette menace à multiples facettes, il est essentiel d'identifier et d'évaluer la menace que représentent les différents types d'escroquerie (c'est-à-dire les méthodes d'infraction), mais aussi les facteurs favorisant leur développement et les acteurs de ces infractions. Néanmoins, les victimes étant souvent réticentes à se manifester, les escroqueries financières ne font pas l'objet de signalements suffisants auprès des services chargés de l'application de la loi. Par conséquent, l'étendue réelle et les répercussions de ce type de criminalité sont très certainement sous-estimées.

Par ailleurs, quand des informations et travaux de recherche sur les escroqueries financières existent, ils se concentrent souvent sur les modes opératoires et s'intéressent beaucoup moins aux différents profils des auteurs d'escroqueries ou, plus important encore, à l'organisation des escroqueries. Il est évident que les escroqueries financières font appel à différents degrés de collaboration entre malfaiteurs. Ainsi, la nature et l'ampleur de la convergence entre différents types de criminalité mériteraient d'être mieux compris.

L'objectif du présent rapport, qui analyse les données dont INTERPOL dispose, est de présenter une évaluation des tendances mondiales en matière d'escroqueries financières afin d'élaborer des stratégies étayées et efficaces pour prendre des mesures collectives contre les personnes et les groupes criminels organisés se livrant à des escroqueries financières. Deux questions majeures se posent ici : comment ces tendances se manifestent-elles aux niveaux régional et mondial ? Qui sont les acteurs de la menace ?

Méthodologie

L'évaluation des escroqueries financières au niveau mondial est le résultat d'une méthodologie intégrant toutes les sources disponibles. La plupart des données analysées proviennent des données d'INTERPOL, y compris de notices et diffusions portant sur des infractions liées à des escroqueries financières, de contributions directes des partenaires et pays membres d'INTERPOL, de messages opérationnels de la part des pays membres et des réponses aux questionnaires INTERPOL 2022 et 2024 sur les tendances criminelles mondiales en matière d'escroqueries financières. Le cas échéant, ces données ont été complétées avec des documents de sources publiques élaborés par des partenaires des secteurs public et privé.

Démarche d'analyse

Dans le présent rapport, le concept d'escroquerie financière est compris sous l'angle opérationnel et du point de vue des services chargés de l'application de la loi. Ainsi, ce rapport considère l'escroquerie financière comme un terme général englobant un large éventail d'« activités illégales visant à l'obtention d'un gain financier par le biais d'actions délibérées et trompeuses à l'encontre et au détriment de personnes ou d'entités[1] ».

De ce point de vue, l'escroquerie financière conjugue efficacement deux éléments : la motivation (obtention d'un gain financier) et les moyens (tromperie sous plusieurs formes), et débouche sur un avantage ou bénéfice indu portant atteinte à la victime. Par conséquent, les types d'escroquerie rencontrés par les services chargés de l'application de la loi sont dynamiques et évoluent en même temps que le contexte social, économique, technologique et juridique.

1 Cette évaluation se concentre sur les escroqueries financières contre des personnes et des entités privées. Elle exclut dont les escroqueries commises à l'encontre des gouvernements et de l'administration publique.

Modes opératoires de l'escroquerie financière

Usurpation d'identité

Un malfaiteur se fait passer pour une personne ou une institution avec laquelle la victime a, ou pourrait avoir, une relation réelle et préexistante, qu'elle soit personnelle, officielle ou commerciale. Le malfaiteur peut par exemple se faire passer pour une autorité fiscale ou policière, un prestataire de services auquel la victime fait appel, ou encore une connaissance lointaine. L'usurpation d'identité fonctionne quand le malfaiteur suscite de la peur ou de l'inquiétude chez la victime, et ce pour mieux la tromper.

Escroquerie aux faux ordres de virement (FOVI)[2]

C'est une forme d'usurpation d'identité de plus en plus courante dans laquelle les escrocs ciblent des entreprises en ayant recours à des techniques de manipulation psychologique. Ces escrocs piratent des comptes de messagerie et se font passer pour des cadres ou des avocats d'affaires afin de pousser des employés à transférer des fonds sur des comptes qu'ils détiennent, et détournent ensuite rapidement les fonds. Les malfaiteurs, qui opèrent parfois depuis des centres d'escroquerie, sont capables de réaliser des usurpations d'identité à grande échelle et de cibler des millions d'entreprises et de particuliers par le biais de courriels, de SMS, des réseaux sociaux et d'appels automatiques.

Escroqueries aux placements

Elles consistent à pousser des personnes à placer de l'argent dans des entreprises fausses ou trompeuses, entraînant des pertes financières considérables pour les victimes. Ce mode opératoire représente une menace rampante faisant perdre plus d'argent aux victimes qu'avec d'autres types d'escroquerie individuelle. Les escrocs utilisent diverses tactiques trompeuses, notamment en promettant des rendements très élevés, en mentant sur les investissements et en créant un sentiment d'urgence. Les systèmes d'escroquerie aux placements fonctionnent souvent comme des pyramides de Ponzi qui permettent aux malfaiteurs de se doter d'une base plus large de victimes pour maintenir le flux d'investissement et augmenter ainsi leurs gains illicites. Les malfaiteurs ciblent souvent des victimes ou investisseurs potentiels via les réseaux sociaux, des applications ou sites Internet frauduleux, des campagnes de télémarketing (généralement menées depuis des centres d'appels ou des locaux de vente sous pression) ou encore en personne. Les escrocs déploient efficacement toutes ces techniques de communication au cours des différentes étapes du système d'escroquerie aux placements. Les groupes et réseaux criminels impliqués dans les escroqueries aux placements adoptent en général les habitudes d'une entreprise légitime pour perpétrer leurs méfaits. L'essor des cryptomonnaies a offert à ce type d'escroquerie de nouvelles possibilités. La manipulation des marchés et la manipulation psychologique à des fins de gains financiers sont certaines des techniques utilisées pour commettre des escroqueries aux placements en cryptomonnaies. Les escrocs utilisent des plateformes frauduleuses et des projets d'investissements fantômes dans les cryptomonnaies pour convaincre puis escroquer les investisseurs

RUG PULL

EN 2023, INTERPOL A CONSTATÉ QUE L'ESCROQUERIE APPELÉE « RUG PULL » (OU « PROJET FANTÔME ») ÉTAIT UN TYPE D'ESCROQUERIE AUX PLACEMENTS NUMÉRIQUES EN PLEIN ESSOR. LE MODE OPÉRATOIRE CONSISTE EN L'ABANDON SOUDAIN, PAR LES AUTEURS DE L'ESCROQUERIE, D'UN PROJET LIÉ AUX CRYPTOMONNAIES, FAISANT PERDRE AUX INVESTISSEURS TOUT LEUR ARGENT.[3]

2 Bien qu'il s'agisse d'un sous-type d'usurpation d'identité, les FOVI sont évalués indépendamment dans ce rapport compte tenu du volume et de la fréquence de cette méthode d'escroquerie financière dans toutes les régions.

3 « 300 millions d'USD saisis et 3 500 suspects arrêtés dans le cadre d'une opération internationale contre la criminalité financière », INTERPOL, 19 décembre 2023, https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2023/300-millions-d-USD-saisis-et-3-500-suspects-arretes-dans-le-cadre-d-une-operation-internationale-contre-la-criminalite-financiere.

Parmi les nombreux modes opératoires employés pour commettre une escroquerie financière, INTERPOL a remarqué que les usurpations d'identité, les escroqueries aux placements, les escroqueries aux sentiments, les escroqueries à l'avance de frais et les fraudes à l'identité sont les plus répandues au niveau mondial.

Escroquerie aux sentiments

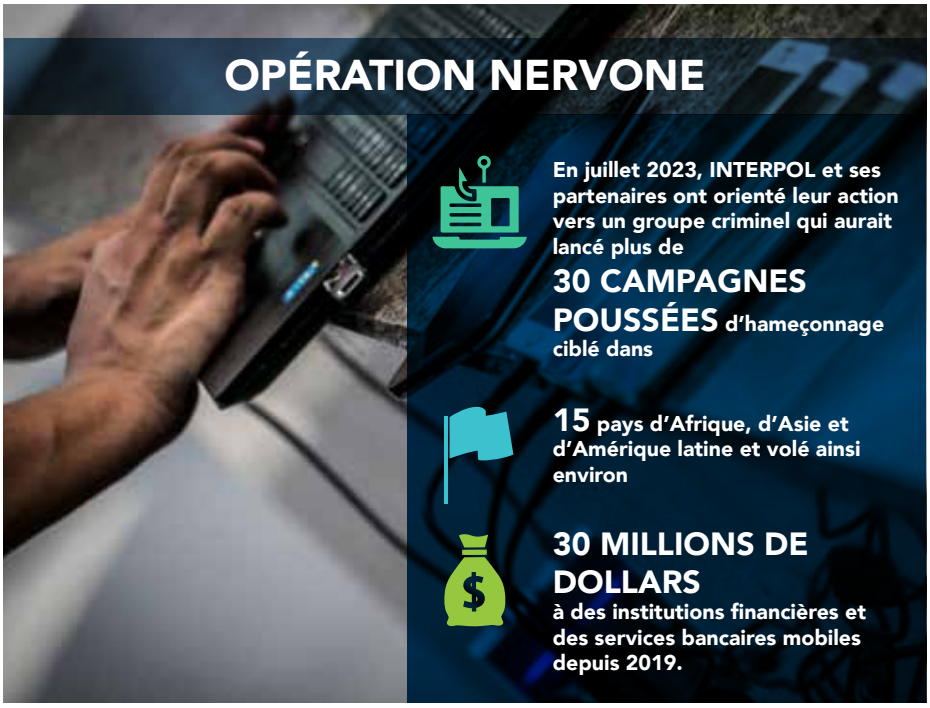
Les malfaiteurs prennent contact avec leurs cibles sur les réseaux sociaux, les applications de rencontres ou les plateformes de messagerie et instaurent avec elles une « relation » de confiance ou d'intimité. Motivés par l'appât du gain, les malfaiteurs finissent par manipuler les victimes, souvent à plusieurs reprises, leur causant un préjudice à la fois financier et émotionnel.

Escroquerie à l'avance de frais

C'est l'un des types d'escroquerie les plus répandus. Il consiste en une transaction financière portant sur des services ou produits frauduleux. Les malfaiteurs utilisent des sites marchands en ligne, des plateformes de réseaux sociaux ou d'autres moyens pour promouvoir la vente de biens et services très demandés, en dessous des prix du marché. Un paiement anticipé est requis, avant même la réception du produit ou du service, qui sera soit inexistant soit de bien moins bonne qualité que l'indiquait la publicité.

Fraude à l'identité

Elle se réfère à l'acquisition et l'utilisation non autorisées des informations personnelles d'une personne (identifiants et mots de passe, numéros de carte de crédit, données biométriques, etc.) en vue d'obtenir un gain financier de nature illicite. Les malfaiteurs peuvent avoir accès à ces informations personnelles grâce à des techniques de manipulation psychologique (hameçonnage, hameçonnage par SMS, hameçonnage par téléphone, usurpation d'identité électronique, etc.), d'intrusion dans les systèmes (via des logiciels malveillants ou du piratage informatique) ou de vols physiques. Les fraudes à l'identité comprennent donc deux éléments : d'un côté un outil, c'est-à-dire la technique employée pour acquérir des données à caractère personnel, et de l'autre, l'utilisation de ces données en vue de l'obtention de gains financiers illicites[4]. Les escrocs peuvent commettre une fraude à l'identité sans participation directe de la victime, dont l'identité a été volée. En plus de voler des fonds, les malfaiteurs vendent souvent les informations personnelles compromises sur des marchés criminels en ligne. Elles peuvent ensuite être exploitées par des criminels pour commettre une fraude à l'identité, victimiser à nouveau des cibles et utiliser facilement les techniques trompeuses associées à d'autres types d'escroquerie comme les escroqueries aux sentiments.



4 Dorénavant, l'évaluation des fraudes à l'identité se concentrera sur la menace que représentent l'hameçonnage et d'autres techniques de manipulation psychologique et d'intrusion.

Données d'INTERPOL et tendances en matière d'escroquerie financière

Selon le Rapport d'INTERPOL sur les tendances mondiales de la criminalité en 2022, les escroqueries financières constituent l'une des menaces les plus inquiétantes pour les pays membres d'INTERPOL. Dans toutes les régions du monde, la plupart des personnes interrogées ont indiqué s'attendre à voir la criminalité financière, notamment les escroqueries financières, augmenter voire monter en flèche au cours des trois à cinq prochaines années.

Entre 2022 et 2023, 85 % des notices et diffusions rouges émises par les pays membres d'INTERPOL étaient en lien avec des escroqueries. La majorité de ces notices et diffusions provenaient des pays membres européens, suivis par les pays d'Asie et des Amériques.

Selon les pays membres d'INTERPOL, la plupart des escroqueries financières comportent une composante transnationale, et les victimes sont plus souvent des personnes que des entités du secteur privé. Pour la seule année 2023, le Centre INTERPOL de lutte contre la criminalité financière et la corruption (IFCACC) a apporté son soutien aux pays membres dans plus de 700 affaires d'escroquerie financière, portant sur environ 1,2 milliard de dollars. À l'échelle mondiale, les escroqueries aux faux ordres de virement (FOVI) et les escroqueries aux placements constituaient les types d'escroquerie financière les plus signalés à INTERPOL, suivies par les usurpations d'identité, les escroqueries à l'avance de frais, les escroqueries aux sentiments et l'hameçonnage. Bien que les escroqueries financières soient omniprésentes dans le monde entier, les tendances varient d'une région à une autre.

Dans la région **Asie**[5], les usurpations d'identité, les escroqueries aux sentiments et l'hameçonnage sont les formes d'escroquerie les plus fréquentes. S'il est vrai que la moitié des cas signalés en 2023 par des pays d'Asie provenait de la région, l'escroquerie financière n'est pas une menace endogène. En effet, INTERPOL a aussi détecté des cas d'escroqueries aux FOVI commises depuis l'Europe et les Amériques, et des cas d'escroqueries aux sentiments commises depuis l'Afrique. Toutes ciblaient des pays d'Asie.

Dans le cas de **l'Afrique**[6], les escroqueries à l'avance de frais représentent la forme la plus inquiétante d'escroquerie financière, suivie par les escroqueries aux placements, les escroqueries aux FOVI et les escroqueries aux sentiments. Les cas d'escroquerie signalés par des pays membres africains en 2023 ont été commis depuis l'Asie, l'Afrique et l'Europe. L'Afrique (et notamment les pays ouest-africains) reste toutefois une source importante d'escroqueries financières sur le continent et au-delà. Cela a récemment été confirmé par les opérations Contender et Killerbee, pilotées par INTERPOL.

Les escroqueries aux placements représentent la forme la plus inquiétante d'escroquerie financière dans la région **Europe**, suivies des escroqueries aux FOVI, des escroqueries aux sentiments et des fraudes aux télécommunications. En ce qui concerne les **Amériques**, les systèmes d'hameçonnage, les escroqueries aux FOVI et celles à l'avance de frais sont de plus en plus source d'inquiétude, mais le manque de renseignements fait obstacle à une réelle évaluation de la menace dans cette région.

5 Dans cette évaluation, la région Asie comprend les pays du Moyen-Orient et les pays du Pacifique, sauf mention contraire.

6 De la même manière, la région Afrique comprend les pays d'Afrique du Nord, sauf mention contraire.

Nouvelles tendances en matière d'escroqueries financières

Tirer parti des progrès technologiques

Pour les groupes criminels, les technologies représentent un facteur propice à la réalisation d'escroqueries financières. L'utilisation de l'IA, des grands modèles de langage (LLM) et des cryptomonnaies peut amplifier certains types d'escroquerie financière, qui ne nécessitent donc pas de mise de départ très importante.

L'utilisation de contenu synthétique généré par l'IA – aussi connu sous le nom d'« hypertrucage » – à des fins d'escroquerie en ligne est une nouvelle tendance suscitant une inquiétude croissante parmi les pays membres. Les barrières à l'utilisation de l'IA générative et de l'hypertrucage sont de moins en moins élevées étant donné que la technologie devient toujours plus facile à utiliser et accessible.

Les modèles commerciaux de la criminalité en tant que service (CaaS), de l'hameçonnage en tant que service (PaaS) et du rançongiciel en tant que service (Raas) permettent à de nouveaux cybermalfaiteurs sans compétences techniques particulières de commettre des escroqueries en ligne de plus en plus élaborées. Ces modèles favorisent le partage des compétences et la distribution de logiciels criminels complexes ou de données à caractère personnel volées sur le darknet (Internet clandestin) ou le Web profond, où des partenaires de confiance échangent ouvertement des données, des services d'hébergement et des logiciels. Le modèle de CaaS permet également aux groupes criminels organisés de recruter et d'étendre leur réseau de mules financières. Par ailleurs, la croissance rapide du nombre d'utilisateurs en ligne dans le monde entier constitue un terreau propice à la propagation des escroqueries financières dans toutes les régions.

Selon les données d'INTERPOL, les cryptomonnaies et les fournisseurs de services de cryptomonnaies font partie intégrante des escroqueries aux sentiments et aux placements, et dans une moindre mesure, des fraudes aux télécommunications et à l'avance de frais. Si le Bitcoin est souvent utilisé dans les escroqueries financières à travers le monde, les pays membres d'Afrique, d'Asie du Sud-Est et de l'Est et du Pacifique ont également signalé l'utilisation du Tether (aussi connu sous l'acronyme USDT) et des Altcoins (les cryptomonnaies alternatives). En Europe, il s'agit plutôt de l'Ethereum. Les services proposés par les prestataires de services d'actifs virtuels comme Binance, et les systèmes d'investissement et de paiement virtuels comme Skrill, Perfect Money, Netteller, Altcoin Trader et Luno Trading, seraient utilisés par des escrocs pour commettre des escroqueries financières aux cryptomonnaies, surtout en Afrique, en Asie et en Europe. Dans certains cas, dans le cadre de leurs manœuvres trompeuses, les malfaiteurs mettent en place ou sous-traitent la mise en place d'une fausse application d'investissement. Ils vont parfois jusqu'à cloner des plateformes d'investissement de services ou d'entreprises réputés. Sur ces fausses plateformes, les malfaiteurs manipulent les transactions et affichent des bénéfices enflés, créant ainsi l'illusion du succès et encourageant les victimes à investir encore plus d'argent dans des mécanismes frauduleux.

Les réseaux criminels tirent grandement profit de l'hypertrucage et des grands modèles de langage. Lors d'affaires récentes dans les pays membres, des photographies hypertruquées ont été créées pour ouvrir des comptes bancaires en ligne et étendre ainsi les réseaux de mules financières. Les LLM sont quant à eux utilisés pour des arnaques aux placements ou à l'emploi sur des plateformes en ligne ou des applications de messagerie instantanée largement disponibles. Il convient de noter que dans chacun de ces cas, la technologie mise en œuvre était assez grossière, mais avait un grand potentiel d'amélioration.

Escroquerie financière et criminalité forcée

Les recherches et analyses d'INTERPOL ont révélé une tendance portant sur la traite d'êtres humains aux fins d'escroquerie en ligne forcée. Le mode opératoire en question met en jeu d'un côté les victimes (A), celles qui font l'objet de la traite d'êtres humains et qui sont forcées à commettre des escroqueries en ligne depuis des camps ou centres d'appels, et d'un autre côté les victimes (B), qui sont escroquées par les victimes (A) et qui perdent d'énormes sommes d'argent. Dans le cadre de l'opération STORM MAKERS I et II, l'Unité Traite d'êtres humains et Trafic de migrants (HTSM) d'INTERPOL a détecté des activités de traite d'êtres humains à grande échelle commises à l'aide d'Internet par des groupes criminels asiatiques à des fins d'escroquerie en ligne forcée dans plusieurs pays d'Asie du Sud-Est[7]. Si à l'origine, les victimes du trafic étaient généralement sinophones, à mesure que la tendance se propage, le recrutement et les stratégies d'escroquerie évoluent et font des victimes dans le monde entier[8].

OPÉRATIONS STORM MAKERS I ET II

En 2022, lors de l'opération STORM MAKERS, l'unité HTSM d'INTERPOL a commencé à recevoir des signalements de victimes de la traite d'êtres humains enfermées dans des centres d'escroquerie en Asie du Sud-Est. En 2023, l'opération STORM MAKERS II, qui avait pour but d'identifier et de démanteler les organisations criminelles se livrant à la traite d'êtres humains et au trafic de migrants, a été consacrée exclusivement à la tendance que constitue la traite d'êtres humains aux fins d'escroquerie en ligne en Asie du Sud-Est et dans les autres régions touchées par ce phénomène.

S'il est important de noter que tous les centres d'escroquerie ne dépendent pas de la criminalité forcée pour fonctionner, les pays membres ont récemment partagé des informations avec INTERPOL indiquant que ces centres – ou camps – de cyberescroqueries exploitant des victimes de la traite d'êtres humains commencent à se répandre partout dans le monde. En Amérique latine, les pays membres d'INTERPOL ont détecté un mode opératoire semblable, où les victimes (A), qui sont souvent originaires de la région, sont recrutées par le biais de fausses offres d'emploi, parfois dans l'espace public. Une fois dans les camps, on leur confisque leurs documents d'identité et on les force à commettre des escroqueries financières en ligne, principalement des escroqueries à l'avance de frais, des fraudes aux télécommunications et des usurpations d'identité. Ces systèmes mettent en jeu des sommes d'argent relativement faibles (entre 100 et 500 dollars), mais ils sont répliqués à grande échelle via les plateformes de réseaux sociaux et les places de marché en ligne. Les sommes engagées étant peu élevées, les victimes sont souvent découragées de signaler les faits, ce qui entrave l'identification des structures criminelles derrière ces mécanismes d'escroquerie.

En outre, INTERPOL a été informé de l'existence de tels centres d'escroquerie dans des pays africains. Ces centres ciblent des particuliers et des entreprises dans la région africaine, mais aussi dans le monde entier.

En Europe, d'après les informations partagées avec INTERPOL, des centres d'escroquerie semblent être actifs depuis les années 2010[9]. Bien que les renseignements fassent toujours défaut, certains centres d'escroquerie dans les pays d'Europe de l'Est semblent fonctionner grâce au travail forcé de victimes de la traite d'êtres humains. Dans les pays en question, les groupes criminels locaux collaboreraient avec des organisations criminelles étrangères. Dans ces centres, les victimes (A) semblent venir du Moyen-Orient.

À mesure que ce mode opératoire se propage et que les profils des victimes (A) se diversifient, avec des victimes venant d'Asie, d'Afrique et d'Amérique latine retenues dans des centres d'escroquerie, il est fort probable que le nombre de victimes (B) ciblées augmente également. Par ailleurs, l'émergence de contenu généré par l'IA risque d'accroître la portée, la complexité et la capacité des escroqueries commises depuis des centres opérant grâce au travail forcé, ce qui contribuera à l'essor des escroqueries dans le monde.

7 INTERPOL. Escroqueries en ligne et traite d'êtres humains en Asie du Sud-Est. 25 octobre 2022. Version publique. À usage officiel INTERPOL uniquement.

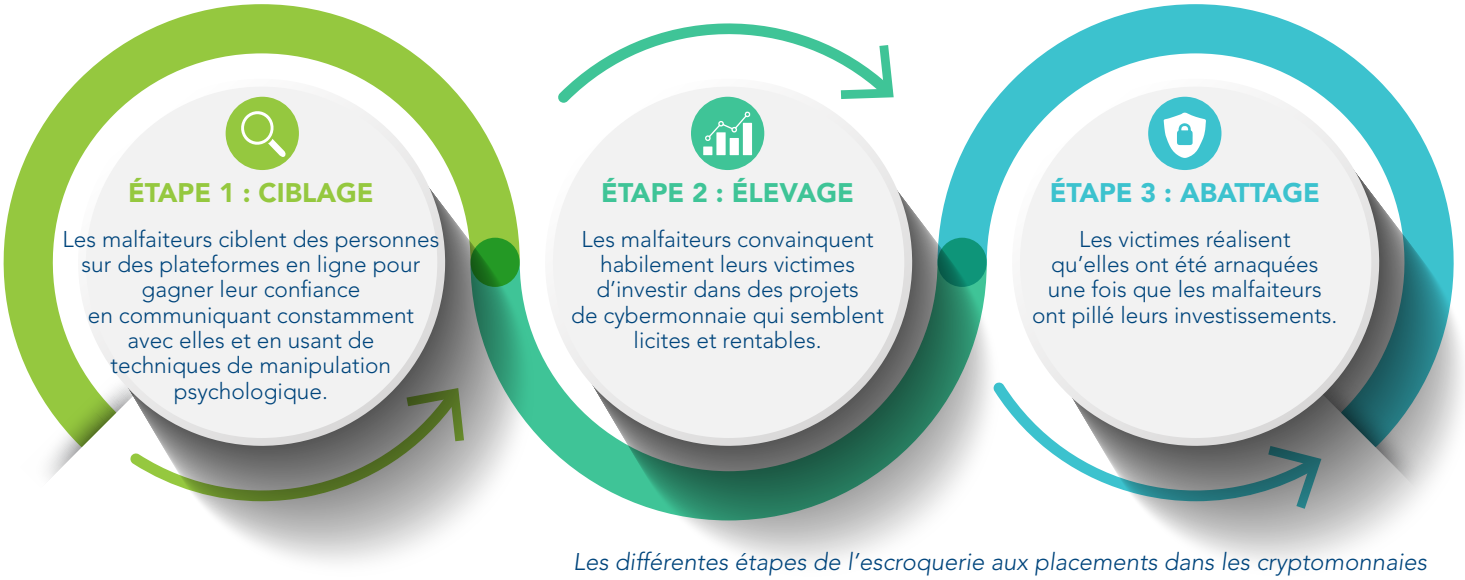
8 INTERPOL. Escroqueries en ligne et traite d'êtres humains en Asie du Sud-Est / Mise à jour 2 – D'une menace régionale à une menace mondiale (version publique). 6 juillet 2023. À usage officiel INTERPOL uniquement.

9 INTERPOL. Escroqueries en ligne et traite d'êtres humains en Asie du Sud-Est / Mise à jour 2 – D'une menace régionale à une menace mondiale (version publique). 6 juillet 2023. À usage officiel INTERPOL uniquement.

Méthodes hybrides d'escroquerie financière – l'essor de l'escroquerie aux placements dans les cryptomonnaies

Depuis 2022, INTERPOL a non seulement observé une multiplication des cas mais également une augmentation de la complexité et du niveau d'élaboration des escroqueries financières en ligne. Une tendance en particulier, parfois appelée « pig butchering », ou arnaque de type « dépeçage de cochon »[10], est rapidement devenue source d'inquiétude pour les services chargés de l'application de la loi : elle a fait perdre plusieurs millions de dollars à ses victimes dans le monde entier au profit des arnaqueurs. Il s'agit d'une méthode hybride qui conjugue des éléments de l'escroquerie aux sentiments et de l'escroquerie aux placements dans les cryptomonnaies. En effet, les malfaiteurs manipulent les transactions de cryptomonnaies pour afficher des bénéfices gonflés et pousser leurs victimes à investir plus d'argent dans des mécanismes frauduleux.

L'escroquerie aux placements dans les cryptomonnaies commence souvent comme une escroquerie aux sentiments. Des escrocs expérimentés ciblent des personnes sur les réseaux sociaux et les applications de rencontre, et même en envoyant des messages directement à des numéros de téléphone. Le phénomène de revictimisation est un élément central de ce type de criminalité. La revictimisation aggrave non seulement le préjudice financier, mais aussi les traumatismes psychologiques et émotionnels subis par les victimes. Au-delà des implications financières immédiates, la portée internationale de ce mode opératoire et l'utilisation des cryptomonnaies représentent un défi de taille.



Les différentes étapes de l'escroquerie aux placements dans les cryptomonnaies (Source : Rapport 2023 sur les tendances mondiales de la criminalité)[11]

Dans des recherches récentes, INTERPOL a démontré l'expansion géographique de cette forme de criminalité. Des éléments de preuve indiquent que cette tendance se propage au-delà de l'Asie du Sud-Est, son centre originel, pour se reproduire dans d'autres régions comme l'Afrique ou l'Amérique latine, où des centres similaires ont été détectés. Les informations dont dispose INTERPOL confirment que les groupes criminels organisés asiatiques recrutent des jeunes, principalement des étudiants, pour commettre des escroqueries en ligne depuis des centres d'appels en Afrique australe. Ces malfaiteurs poussent leurs victimes, dont la plupart résident en Amérique du Nord, à investir dans des mécanismes de cryptomonnaies frauduleux. INTERPOL s'attend à un essor des escroqueries en ligne, notamment des escroqueries aux sentiments et des escroqueries aux placements en lien avec les cryptomonnaies, et l'émergence de ce mode opératoire hybride ne fera qu'ajouter une couche de complexité à ces types d'escroquerie.

10 Par respect pour les victimes, et pour ne heurter personne, INTERPOL préfère ne pas utiliser cette terminologie en référence à ce mode opératoire d'escroquerie financière.

11 INTERPOL, Rapport 2023 sur les tendances mondiales de la criminalité, novembre 2023, page 12 de la version anglaise.

Tendances régionales en matière d'escroqueries financières

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

ENTRE 2022 ET 2023, INTERPOL A PILOTÉ PLUSIEURS OPÉRATIONS, DONT L'OPÉRATION DELILAH, L'OPÉRATION FALCON II, LES OPÉRATIONS CYBER SURGE AFRIQUE I ET II ET L'OPÉRATION CONTENDER, SUR LE CONTINENT AFRICAIN POUR CIBLER LES GROUPES CRIMINELS ET LES MALFAITEURS SE LIVRANT À DES ESCROQUERIES AUX FAUX ORDRES DE VIREMENT, DES ESCROQUERIES AUX SENTIMENTS, DES ESCROQUERIES AUX CRYPTOMONNAIES, DE L'HAMEÇONNAGE ET D'AUTRES TYPES DE CYBERINFRACTIONS[12].

Afrique

Le secteur financier en Afrique a rapidement migré vers le numérique, et la région se classe parmi les leaders mondiaux de la banque mobile et des transactions financières en ligne. Cela a créé pour les malfaiteurs une multitude d'opportunités de commettre des escroqueries financières.

Selon le Rapport INTERPOL d'évaluation des cybermenaces en Afrique publié en 2023, les escroqueries aux FOVI, l'hameçonnage et d'autres types d'escroquerie en ligne suscitent de plus en plus d'inquiétude en Afrique compte tenu de la rapide transition vers une économie de plus en plus dominée par le numérique[13]. L'élargissement de l'accès à Internet associé à de faibles niveaux d'habileté numérique font de nombreux Africains des cibles faciles pour les escrocs et les cybermalfaiteurs.

Les escroqueries aux FOVI sont l'une des tendances les plus répandues en Afrique. Elles entraînent des pertes financières majeures pour les particuliers et les entreprises. La plupart des auteurs d'escroqueries aux FOVI sont implantés en Afrique de l'Ouest, mais leurs victimes se trouvent souvent dans d'autres pays. Ces criminels sont généralement en lien avec de plus vastes réseaux criminels à l'échelle mondiale, ce qui leur permet de cibler un grand nombre de victimes aux quatre coins du monde.

Les escroqueries en ligne comprennent un vaste éventail d'activités frauduleuses dans la sphère numérique. Les escroqueries par défaut de livraison avec paiement anticipé, les escroqueries commerciales en ligne, les escroqueries aux sentiments, les escroqueries à l'assistance technique et les escroqueries aux cryptomonnaies (placements) figurent parmi les escroqueries en ligne les plus courantes et gagnent du terrain dans la région africaine.

L'escroquerie aux placements dans les cryptomonnaies progresse également de manière inquiétante en Afrique. Des cas ont été détectés en Afrique de l'Ouest et en Afrique australe, ciblant des victimes dans d'autres pays, au-delà du continent.

La cybercriminalité en tant que service, ou CaaS, est de plus en plus courante en Afrique. Globalement, la CaaS a assoupli les barrières à l'entrée pour les cybercriminels en herbe, qui peuvent mener des attaques complexes sans même disposer de compétences techniques poussées.

D'après les informations dont dispose INTERPOL, certains groupes criminels ouest-africains continuent de s'internationaliser et de bien s'établir dans des pays et régions du monde entier. Ces groupes criminels organisés ouest-africains, qui se livrent à des activités criminelles diverses, sont connus pour commettre des escroqueries financières avec beaucoup d'agilité, comme les escroqueries aux sentiments, les escroqueries aux placements, les escroqueries à l'avance de frais et les escroqueries aux cryptomonnaies.

12 INTERPOL (Direction de la Cybercriminalité), Opération conjointe de lutte contre la cybercriminalité en Afrique (AFJOC), 2023, https://www.interpol.int/fr/Infractions/Cybercriminalite/Operations-en-matiere-de-cybercriminalite/Operation-conjointe-de-lutte-contre-la-cybercriminalite-en-Afrique-AFJOC (consulté le 13 février 2024).

13 Direction de la Cybercriminalité d'INTERPOL, Rapport d'évaluation des cybermenaces en Afrique (2023) : tendances en matière de cybermenaces, mars 2023 (consulté le 12 février 2023).

OPÉRATION JACKAL

L'opération Jackal d'INTERPOL, lancée en mai 2023, a permis de cibler des groupes criminels ouest-africains dans 21 pays à travers le monde et d'arrêter plus de

100 INDIVIDUS.

L'OPÉRATION A MENÉ AU GEL DE PLUS DE 200 COMPTES BANCAIRES LIÉS AU PRODUIT D'ACTIVITÉS RELEVANT DE LA CRIMINALITÉ FINANCIÈRE EN LIGNE.

Amériques

Conformément aux tendances mondiales, les escroqueries financières en ligne – dont beaucoup visent à tirer profit de la demande accrue de fournitures médicales ou d'autres vulnérabilités accentuées par la pandémie de COVID-19 – ont pris beaucoup d'ampleur dans la région Amériques et ciblent principalement des particuliers et des entreprises établis en Amérique du Nord. Selon le Rapport d'INTERPOL sur les tendances mondiales de la criminalité en 2022, les types d'escroquerie les plus fréquents sur ce continent étaient les usurpations d'identité ainsi que les escroqueries aux sentiments, à l'assistance technique ou à l'avance de frais et les fraudes aux télécommunications[14].

Les entreprises et les particuliers de cette région ont subi d'immenses pertes financières à cause de ces escroqueries financières en ligne. Ces menaces proviendraient en grande partie d'Afrique et d'Asie où des groupes criminels organisés, comme les confréries criminelles ouest-africaines et les groupes criminels asiatiques, opèrent. La hausse des pertes financières causées par les escroqueries financières pose un problème croissant de blanchiment d'argent.

Les escroqueries reposant sur la traite d'êtres humains représentent toujours un phénomène criminel en pleine croissance. L'opération Turquesa V, coordonnée par INTERPOL, a révélé que des centaines de victimes avaient fait l'objet de trafic en étant attirées en dehors de la région via des applications de messagerie et des plateformes de réseaux sociaux puis forcées à commettre des escroqueries, notamment des escroqueries aux placements, et ce depuis des locaux de vente sous pression gérés par des groupes criminels en Asie du Sud-Est[15].

Par ailleurs, il semble de plus en plus évident que les groupes criminels latino-américains commettent aussi des escroqueries financières. Une tendance qui s'est vraisemblablement accentuée après l'apparition du COVID-19, alors que ces groupes sont historiquement liés au trafic de drogue, au trafic d'armes, au blanchiment d'argent, aux enlèvements et à des épisodes de violence criminelle accrue tant au niveau national que régional.

Des prestataires de services criminels rendent les escroqueries financières relativement simples, peu risquées et lucratives. Par ailleurs, les technologies et les outils numériques augmentent l'échelle de ces opérations, garantissent l'anonymat des malfaiteurs et facilitent le blanchiment du produit d'activités illicites. Pour ces raisons, il est fort probable que de plus en plus d'organisations criminelles se lancent dans des escroqueries financières.

14 INTERPOL, Rapport d'INTERPOL sur les tendances mondiales de la criminalité en 2022, octobre 2022.

15 INTERPOL, Amériques : Arrestation de 257 personnes soupçonnées de trafic de migrants et de traite d'êtres humains, 11 décembre 2023, https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2023/Americas-257-suspected-migrant-smugglers-and-human-traffickers-arrested.

OPÉRATION HAECHI IV

En décembre 2023, INTERPOL a piloté une opération de police transcontinentale contre des escroqueries commises au moyen d'Internet et d'autres cyberinfractions (escroquerie aux sentiments, escroquerie aux placements, FOVI, escroquerie liée au commerce électronique, hameçonnage par téléphone, sextorsion en ligne et blanchiment d'argent lié aux jeux en ligne illégaux), aboutissant à 3 500 arrestations et à des saisies d'avoirs d'un montant de 300 millions de dollars dans 34 pays en Afrique, dans les Amériques, en Asie, en Europe et en Océanie.
L'opération a également permis de mettre en garde les pays membres contre une nouvelle escroquerie aux cryptomonnaies appelée « projet fantôme », dans laquelle les auteurs de l'escroquerie créent un nouveau jeton et le promeuvent auprès d'investisseurs, puis abandonnent soudainement le projet, ce qui entraîne des pertes financières pour les investisseurs. HAECHI IV a aussi mis en lumière l'utilisation croissante de l'IA et de la technologie d'hypertrucage pour tromper, harceler et escroquer les victimes, notamment par le biais d'usurpations d'identité ou bien d'escroqueries aux sentiments ou aux placements.

3 500 ARRESTATIONS

300 MILLIONS DE DOLLARS

34 PAYS

Asie

Les escroqueries financières évoluent rapidement dans la région. Compte tenu de leur position parmi les économies numériques à la croissance la plus rapide au monde, les pays membres de la région sont devenus des cibles de choix pour les escroqueries financières. La pandémie de COVID-19 a accéléré la migration numérique des services et des usages des particuliers, des gouvernements et des entreprises de la région Asie. De ce fait, les escroqueries financières, grandement facilitées par Internet, ont augmenté et cette tendance devrait se poursuivre. Les pays membres de la région Asie la perçoivent comme une menace très importante.

INTERPOL a récemment détecté une variante de l'escroquerie aux sentiments traditionnelle intégrant des placements dans les cryptomonnaies. Cette escroquerie est apparue pour la première fois en 2019 en Asie et s'est répandue durant la pandémie de COVID-19. Par la suite, l'Asie est devenue un centre de liaison où les organisations criminelles ont commencé à installer des structures quasi commerciales dans les pays les plus pauvres de la région, en exploitant parfois des victimes de la traite d'êtres humains pour réaliser ces activités frauduleuses. Des recherches indiquent que ce mode opératoire se propage à toute vitesse dans d'autres pays, au-delà du continent.

Ces dernières années, un autre type de fraude a également gagné du terrain en Asie : la fraude aux télécommunications. Les malfaiteurs utilisent des lignes nationales et internationales depuis des centres situés dans certains pays de la région, et usurpent l'identité d'agents chargés des services chargés de l'application de la loi ou d'employés de banque pour piéger les victimes et les pousser à divulguer leurs numéros de cartes de crédit ou de compte bancaire, ou à transférer d'importantes sommes d'argent.

D'après le rapport INTERPOL d'évaluation des cybermenaces dans la région de l'ASEAN en 2021, les escroqueries aux FOVI, l'hameçonnage et les escroqueries liées au commerce électronique continuent de représenter une très grande menace pour les pays membres de la région. INTERPOL estime que ces tendances criminelles continueront de croître dans les années qui viennent[16]. Des données provenant d'Asie du Sud-Est indiquent qu'en 2023, les escroqueries auraient causé un préjudice supérieur à 500 millions de dollars dans l'un des pays membres, 30 % de ce montant étant le résultat d'escroqueries financières[17].

Les données dont dispose INTERPOL révèlent que tous les groupes d'âge peuvent être victimes d'escroqueries, même si la plupart des victimes dans la région Asie sont âgées de 30 à 49 ans. Les victimes sont principalement prises pour cible via les réseaux sociaux et les plateformes de messagerie. Les escroqueries financières dans la région ne montrent aucun signe de faiblesse. Au contraire, les escrocs et cybermalfaiteurs s'adaptent toujours plus à la technologie.

16 Direction de la Cybercriminalité d'INTERPOL, Rapport d'évaluation des cybermenaces dans la région de l'ASEAN en 2021 : panorama des principales tendances en matière de cybermenaces dressé par le Desk pour les opérations de lutte contre la cybercriminalité dans la région de l'ASEAN, 21 janvier 2021, https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2021/Un-rapport-d-INTERPOL-dresse-la-liste-des-principales-cybermenaces-en-Asie-du-Sud-Est (consulté le 13 février 2024).

17 Police de Singapour, Rapport annuel 2023 sur les escroqueries et la cybercriminalité, 18 février 2024, page 8 de la version anglaise.

Europe

Selon les pays européens, les escroqueries financières représentent une très grande menace pour les particuliers, les entreprise et les institutions publiques de la région. Comme dans d'autres régions du monde, les malfaiteurs utilisent de plus en plus d'outils en ligne pour commettre des escroqueries financières et ce, depuis la pandémie. Dans certains pays de la région, les escroqueries commises à l'aide d'Internet représenteraient 80 % des escroqueries signalées. Le blanchiment d'argent lié aux escroqueries est très répandu, et les modes opératoires faisant l'objet de contrôles financiers moins stricts sont susceptibles d'être exploités (notamment l'utilisation des cryptomonnaies pour blanchir le produit des activités criminelles).

Les escroqueries aux placements en ligne, l'hameçonnage et d'autres infractions financières sur Internet se sont multipliées en s'attaquant à des cibles soigneusement sélectionnées, de manière à en tirer le plus de bénéfices possible. Les applications mobiles sont également ciblées par les cybermalfaiteurs. Les informations disponibles indiquent que les escroqueries aux placements et aux FOVI sont les types d'escroquerie qui progressent le plus rapidement et qui engendrent le plus de pertes financières dans la région[18]. Les escroqueries en ligne représentent une menace croissante, les escrocs s'attaquant de plus en plus à des particuliers, des entreprises mais aussi des institutions publiques dans toute l'Europe. Les réseaux criminels qui se livrent à ces escroqueries en ligne s'appuient souvent sur des modes opératoires complexes et élaborés, combinant généralement différents types d'escroquerie.

Ces dernières années, de plus en plus de malfaiteurs ont tiré profit de crises majeures ou de situations d'urgence, comme le conflit en Ukraine ou le tremblement de terre mortel en Türkiye, pour commettre des escroqueries[19]. En effet, ils se font passer pour de véritables organisations ou célébrités en prétendant lever des fonds pour l'aide humanitaire et poussent les victimes à réaliser des paiements, souvent au moyen de cryptomonnaies.

Les escroqueries aux placements dans les cryptomonnaies, principalement commises depuis des locaux de vente sous pression en Asie du Sud-Est, sont aussi en hausse. D'après les données disponibles, des centres d'appels comme ceux gérés par des groupes criminels organisés en Asie du Sud-Est ont été détectés en Europe, même si cela reste rare. Les analyses d'INTERPOL ont également révélé l'existence de groupes criminels organisés dirigés par des ressortissants de pays du Moyen-Orient et spécialisés dans l'usurpation d'identité (escroquerie au président), les escroqueries sur le marché des changes (Forex), les fraudes aux télécommunications et les escroqueries aux sentiments, souvent depuis des centres d'appels. De nouveaux éléments de preuve indiquent que les groupes criminels organisés européens coopèrent avec ces groupes criminels pour commettre des escroqueries financières sous différentes formes. Ces centres seraient situés en Europe de l'Est et selon toute vraisemblance, dans certains pays africains.

Toutefois, la principale menace en matière d'escroquerie en ligne – escroquerie aux sentiments ou aux placements, usurpation d'identité – provient de criminels isolés et de groupes criminels opérant depuis l'Afrique de l'Ouest, souvent avec une composante européenne et un vaste réseau de complices, qui permettent les escroqueries au niveau international. Des liens sont avérés entre les escroqueries perpétrées dans la région et les confréries criminelles ouest-africaines.

Les escrocs connaissent les ficelles des protocoles bancaires et ont accès à un réseau complexe et élaboré de mules financières. Il est donc difficile de suivre la trace du produit des escroqueries. L'abandon des banques traditionnelles au profit des banques en ligne, des cryptomonnaies, des applications de transfert d'argent et des cartes cadeaux pour blanchir le produit des escroqueries complique la détection de l'origine de l'escroquerie. Certains pays ont néanmoins indiqué que les fonds blanchis finissaient parfois dans d'autres pays d'Afrique de l'Ouest ou d'Asie du Sud-Est.

D'après les données disponibles, les escrocs et cybermalfaiteurs passent généralement par les réseaux sociaux ou les applications de messagerie pour cibler des femmes ou hommes âgés de 30 à 80 ans, issus de pays européens. Les victimes, surtout dans le cas des escroqueries aux sentiments, sont souvent vulnérables.

Par ailleurs, les facteurs facilitant les activités des malfaiteurs se multiplient. Ce sont par exemple des kits d'hameçonnage, des outils d'administration à distance, des logiciels pour cloner les cartes de crédit, des bases de données d'informations personnelles et des manuels de méthodes d'escroquerie sur les forums du darknet (Internet clandestin).

Les escrocs et les cybermalfaiteurs vont probablement continuer à s'adapter aux nouvelles technologies et aux nouveaux outils, comme l'hypertrucage et d'autres variantes de l'intelligence artificielle générative, pour leurrer plus de victimes, ce qui signifie que les escroqueries en ligne risquent de prendre de l'ampleur dans un avenir proche. Le développement des nouvelles technologies ne fera qu'ajouter de la complexité à cette menace en constante évolution.

18 EUROPOL, Les escroqueries en ligne : la tromperie est présente partout sur le Web (iOCTA 2023), 19 décembre 2023, https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023.

19 EUROPOL, Les escroqueries en ligne : la tromperie est présente partout sur le Web (iOCTA 2023), 19 décembre 2023, https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023.

Escroquerie financière organisée

Les groupes criminels organisés sont des acteurs majeurs de la menace dans le monde de l'escroquerie financière. Leurs ressources, leur structure et leur nature prédatrice les rendent particulièrement dangereux. Bien que les données manquent sur les groupes criminels organisés transnationaux se livrant à des escroqueries financières, les informations d'INTERPOL à ce sujet indiquent que ces réseaux de malfaiteurs sont renforcés par la technologie et les partenariats, qui font d'eux des menaces majeures dans l'écosystème des escroqueries financières et au-delà. De fait, INTERPOL a observé que les escroqueries financières et le blanchiment du produit de celles-ci étaient non seulement liés à la traite d'êtres humains, mais aussi à d'autres activités criminelles comme le trafic de drogue, les produits contrefaits et d'autres marchandises illicites. Cette convergence ou effet de réseau est probablement liée à la mise en place de collaborations entre les acteurs de la criminalité.

Les groupes criminels qui commettent des escroqueries financières créent souvent des réseaux qui transcendent non seulement les frontières nationales, mais aussi régionales et continentales. Cette collaboration avec d'autres malfaiteurs permet de couvrir les différents aspects de ces activités criminelles. Dans le cadre d'une escroquerie financière, la collaboration se fait à différents niveaux :

- **Recrutement de complices experts et compétents :** identifier des personnes, y compris des prestataires de services criminels ayant des compétences spécifiques (techniques, financières, etc.) qui pourront jouer un rôle essentiel dans leurs activités, en développant des mécanismes d'investissement complexes par exemple.
- **Identification des cibles et des victimes :** effectuer des recherches et déterminer quel public cible sera le plus facilement manipulable ou, en fonction de la méthode d'infraction utilisée, acheter des listes de victimes potentielles à des personnes qui ont accès à des informations sur des cibles.
- **Blanchiment du produit d'activités illicites :** le transfert et le blanchiment du produit d'activités illicites sont fondamentaux pour la participation durable des groupes criminels aux escroqueries financières. Cela peut se faire en collaborant avec des chefs d'entreprises légitimes ou en faisant appel à d'autres individus ou réseaux proposant le blanchiment d'argent en tant que service. Les réseaux criminels transfèrent le produit des escroqueries de plus en plus rapidement au-delà des frontières physiques et virtuelles en ayant recours à des mécanismes complexes de blanchiment d'argent. INTERPOL a mis en place un mécanisme mondial de blocage des paiements pour entraver le blanchiment de millions de dollars issus de l'escroquerie financière (voir tableau ci-après).

ÉTUDE DE CAS I-GRIP

Une société établie dans un pays A a été victime d'une usurpation d'identité commise par des malfaiteurs qui se sont fait passer pour la Banque nationale. Elle a transféré 1,2 million d'EUR vers un compte dans un pays B et 2 millions d'EUR vers un autre compte dans un pays C.

Le B.C.N. du pays A a alerté la banque de la société victime et lui a demandé de bloquer le paiement, si possible. Il a également contacté le Centre INTERPOL de lutte contre la criminalité financière et la corruption (IFCACC) afin d'assurer la coordination avec les pays B et C pour bloquer les paiements et éviter toute dispersion supplémentaire des fonds. Agissant en étroite coopération avec l'IFCACC, les B.C.N. des pays B et C ont demandé aux banques bénéficiaires sur leurs territoires respectifs de bloquer les paiements. Le montant total de la perte, 3,2 millions d'EUR, a été recouvré et restitué à la société victime en l'espace d'une journée.

Les groupes criminels organisés investissent sans compter dans les technologies pour créer de faux sites Internet, de faux profils sur les réseaux sociaux et des courriels d'hameçonnage qui semblent authentiques. Ils sont également capables de mettre au point des outils automatisés pour lancer des cyberattaques à grande échelle. L'émergence du modèle CaaS (cybercriminalité en tant que service) a élargi l'éventail des possibilités des groupes criminels organisés pour collaborer, vendre et partager des ressources. Comme cela a été mentionné plus haut dans ce rapport, ce modèle criminel, outre qu'il est une entreprise rentable pour les entrepreneurs criminels, permet également à des groupes criminels ayant peu de compétences techniques de se livrer à ce genre d'activités.

Structure des groupes criminels organisés

Selon la méthode utilisée, l'escroquerie financière ne nécessite pas forcément de collaboration criminelle. Toutefois, certains types d'escroqueries à grande échelle commises à l'aide d'Internet ont de grandes chances d'être perpétrées par des groupes criminels organisés transnationaux. Bien qu'il soit difficile d'enquêter à leur sujet, les groupes connus semblent fonctionner selon une structure hiérarchique et grâce à des cellules décentralisées.

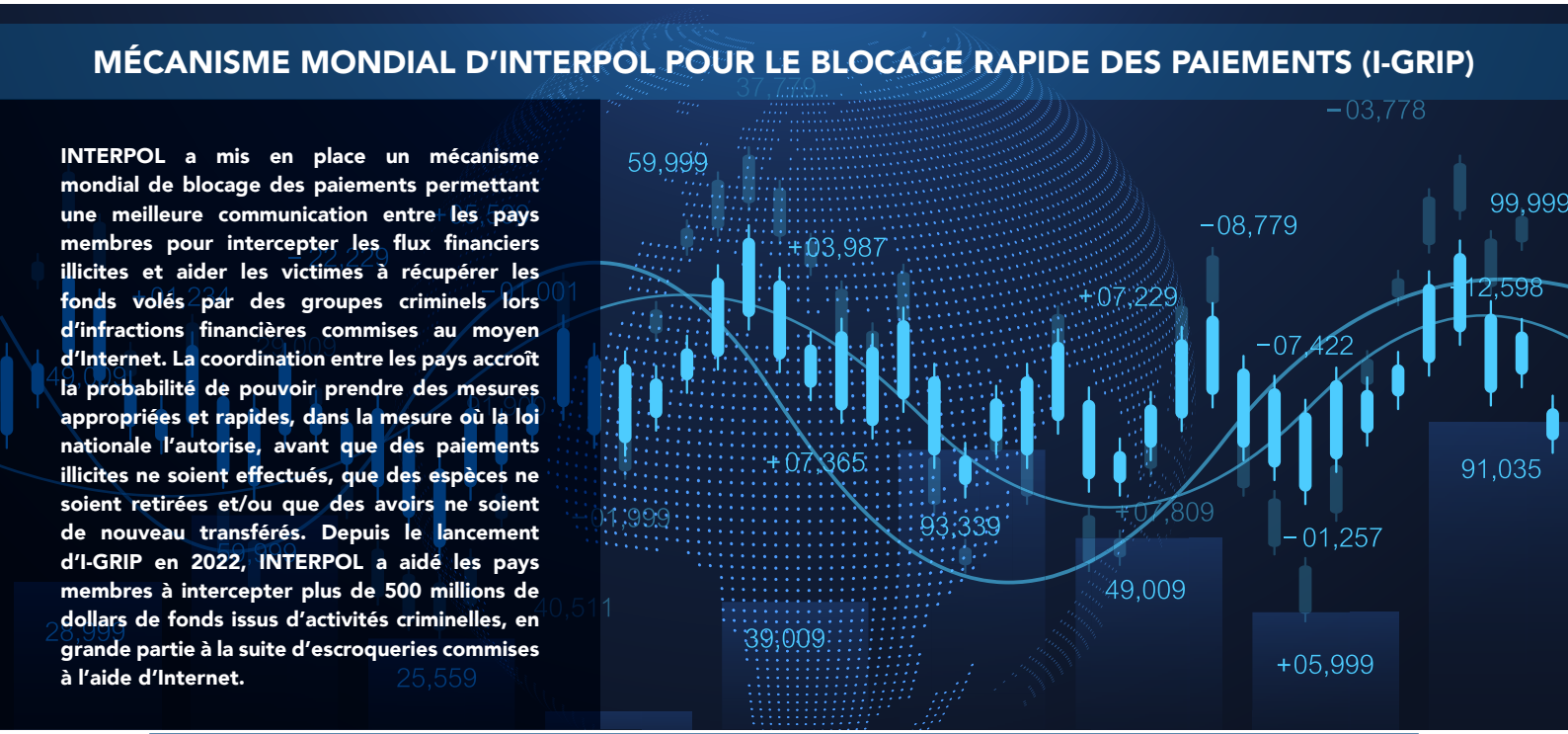
INTERPOL a pu observer que les groupes criminels organisés ou confréries d'Afrique de l'Ouest suivent en général un modèle hiérarchique dans lequel chaque membre remplit un rôle spécifique et se voit attribuer des missions bien définies. Des sources ont néanmoins indiqué à INTERPOL que ces organisations essayaient souvent de brouiller les pistes des enquêtes policières en utilisant des titres trompeurs pour décrire leur structure. Dans le cas des confréries ouest-africaines, la structure hiérarchique peut également varier d'un pays à l'autre.

D'autres groupes criminels organisés impliqués dans des escroqueries financières opèrent également de manière plus décentralisée en proposant des services dans le cadre du modèle CaaS. Les groupes opérant au sein de ce modèle sont moins rigides et leurs relations sont souvent plus éphémères[20]. Selon un rapport rédigé conjointement par INTERPOL et ses partenaires, un groupe criminel pratiquait la CaaS et proposait des services de blanchiment d'argent à des malfaiteurs spécialisés dans les escroqueries en ligne.

Dans le cadre de ce rapport, INTERPOL et ses partenaires ont pu identifier plusieurs organisations criminelles se livrant à des escroqueries financières depuis différentes régions. Les données disponibles révèlent que des groupes criminels d'Asie de l'Est, d'Amérique latine, d'Afrique de l'Ouest et d'Europe se livrent à différents types d'escroquerie financière et à du blanchiment d'argent. En utilisant les technologies de l'information et de la communication au niveau mondial pour commettre des cyberescroqueries, ces groupes criminels peuvent cibler des victimes dans n'importe quel pays du monde.

MÉCANISME MONDIAL D'INTERPOL POUR LE BLOCAGE RAPIDE DES PAIEMENTS (I-GRIP)

INTERPOL a mis en place un mécanisme mondial de blocage des paiements permettant une meilleure communication entre les pays membres pour intercepter les flux financiers illicites et aider les victimes à récupérer les fonds volés par des groupes criminels lors d'infractions financières commises au moyen d'Internet. La coordination entre les pays accroît la probabilité de pouvoir prendre des mesures appropriées et rapides, dans la mesure où la loi nationale l'autorise, avant que des paiements illicites ne soient effectués, que des espèces ne soient retirées et/ou que des avoirs ne soient de nouveau transférés. Depuis le lancement d'I-GRIP en 2022, INTERPOL a aidé les pays membres à intercepter plus de 500 millions de dollars de fonds issus d'activités criminelles, en grande partie à la suite d'escroqueries commises à l'aide d'Internet.



20 GAFI, INTERPOL, Groupe Egmont, Flux financiers illicites provenant des cyberfraudes, novembre 2023

Conclusions

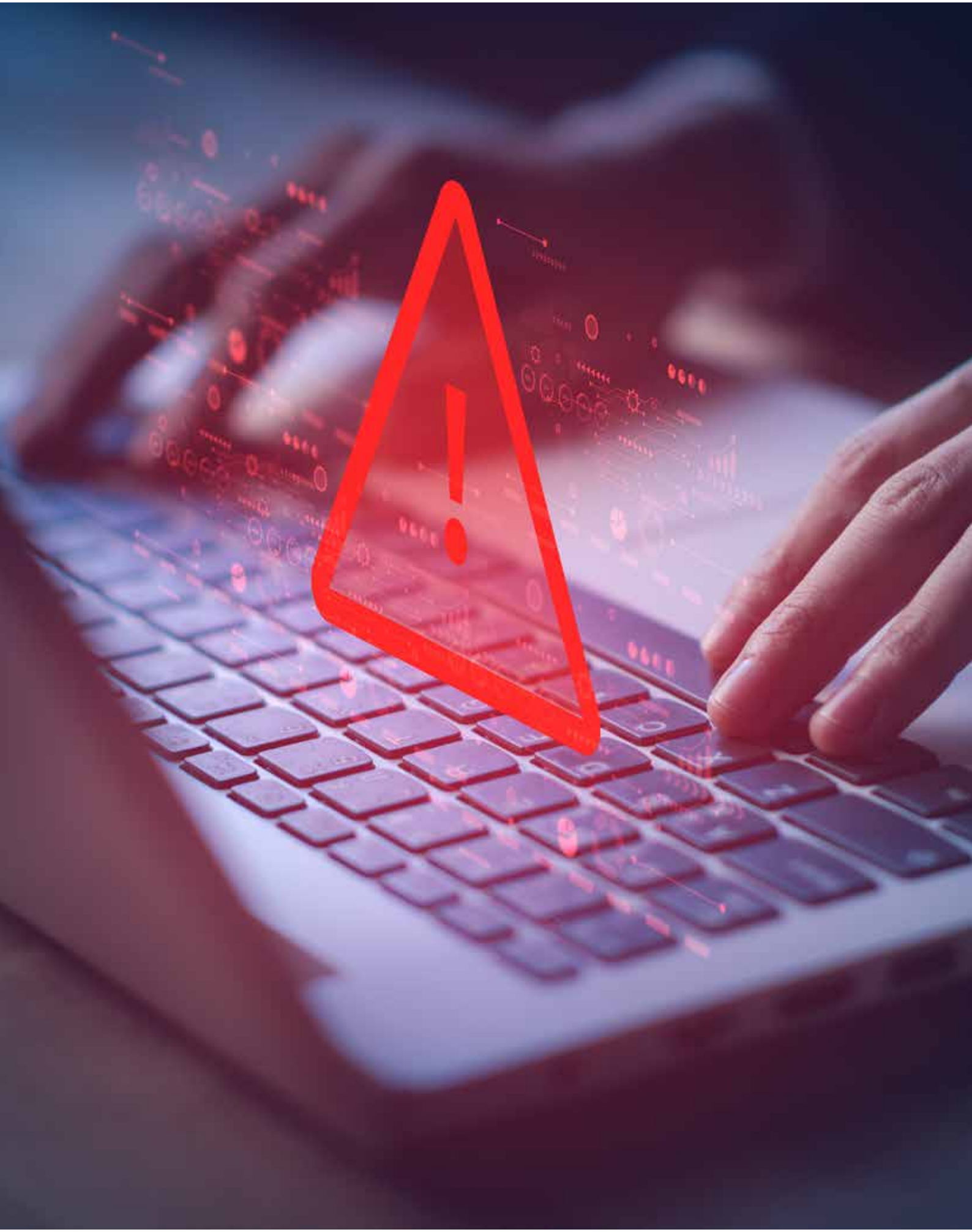
Le présent rapport visait à analyser les données d'INTERPOL pour comprendre l'évolution des tendances en matière d'escroquerie financière, mais aussi pour détecter les escroqueries qui menacent le plus les particuliers et les entreprises dans chaque région et dans le monde. Ce rapport a en outre examiné la convergence entre les escroqueries financières et d'autres infractions, notamment la traite d'êtres humains et le blanchiment d'argent, ainsi que les dynamiques des groupes criminels organisés qui commettent des escroqueries financières.

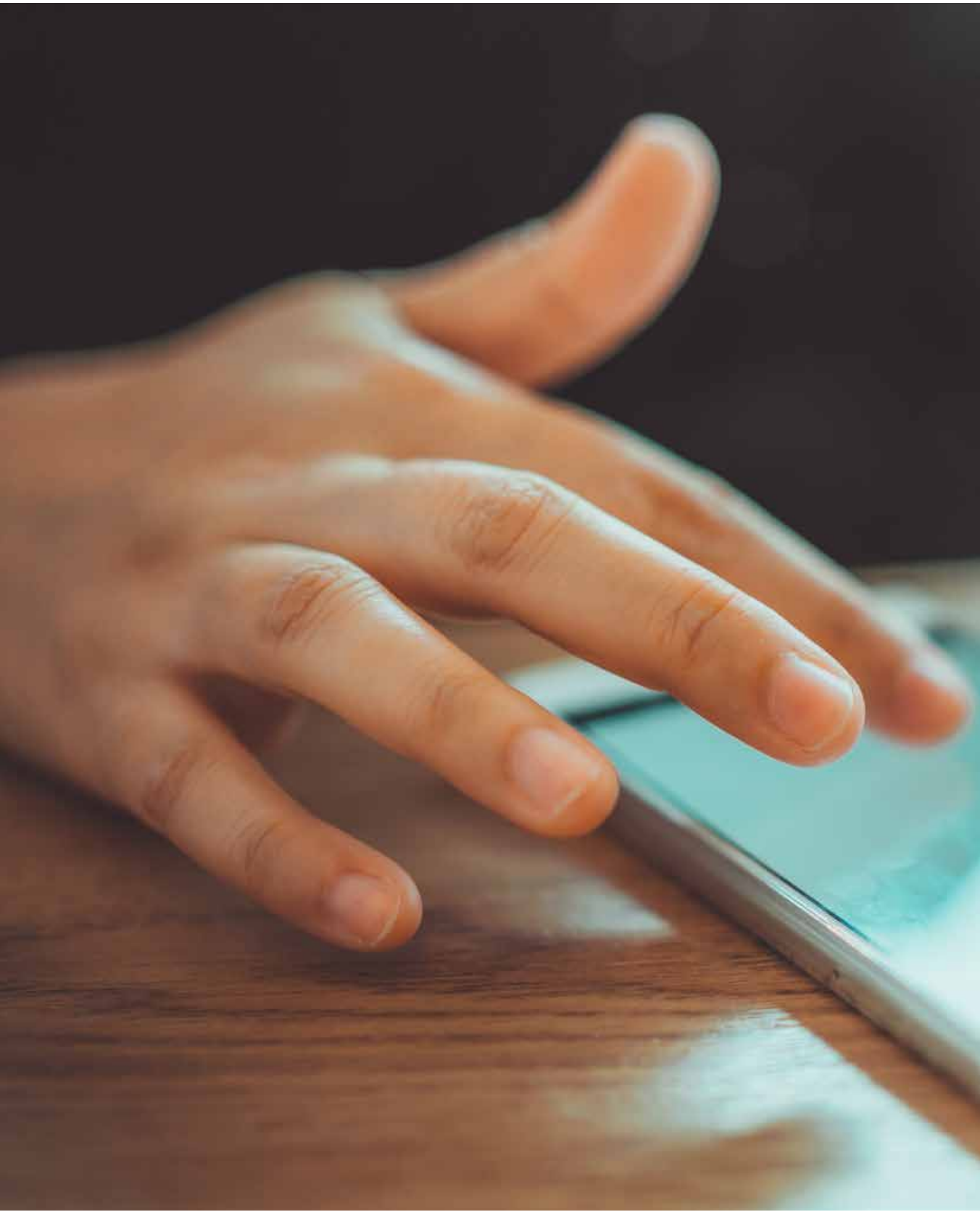
D'après les données d'INTERPOL, les escroqueries aux placements et aux FOVI continuent d'être les modes opératoires les plus répandus au niveau mondial. Si les escroqueries financières sont omniprésentes dans le monde entier, les types d'escroquerie varient d'une région à l'autre : les escroqueries aux sentiments et les usurpations d'identité sont les types d'escroquerie les plus répandus en Asie, alors qu'en Afrique ce sont les escroqueries à l'avance de frais, suivies des escroqueries aux FOVI et aux sentiments. Dans le cas de l'Europe, ce sont les FOVI, les fraudes aux télécommunications et les escroqueries aux sentiments. En ce qui concerne les Amériques, l'hameçonnage, les escroqueries à l'avance de frais et aux FOVI constituent les menaces les plus fréquentes.

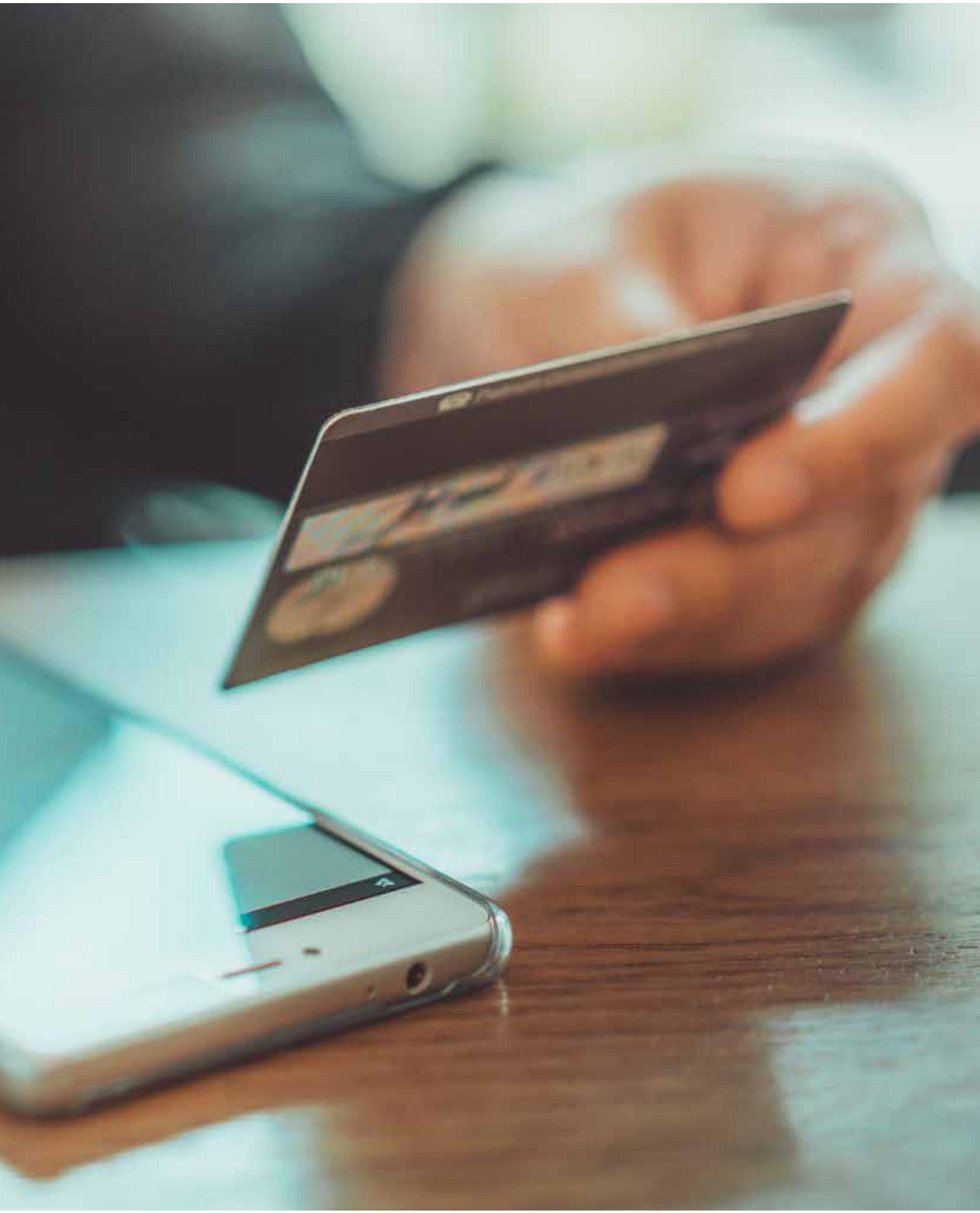
Les pays membres s'attendent à voir l'échelle et l'ampleur des escroqueries financières augmenter parallèlement aux progrès technologiques et à l'essor des services virtuels dans toutes les régions du monde. En effet, l'IA et les cryptomonnaies font déjà partie intégrante des nouvelles activités criminelles, et les escrocs utilisent aussi des techniques « hybrides » combinant escroqueries aux sentiments et escroqueries aux placements. Le degré d'élaboration des nouvelles techniques d'escroquerie n'est toutefois pas un frein pour les malfaiteurs qui maîtrisent peu les technologies. Les fournisseurs de services criminels, notamment de criminalité en tant que service et de blanchiment d'argent en tant que service, sont devenus des éléments essentiels pour pouvoir commettre des escroqueries financières à grande échelle.

Les escroqueries financières, en particulier les escroqueries commises à l'aide d'Internet, qui sont par nature mondiales et anonymes, sont souvent le fait de groupes criminels organisés transnationaux. Pour mieux comprendre comment et dans quelle mesure les groupes criminels organisés commettent des escroqueries financières, il sera nécessaire de recueillir plus d'informations. Toutefois, les groupes criminels recensés dans ce rapport montrent que les malfaiteurs s'organisent au niveau mondial, semblent partager leurs expériences et connaissances en matière de criminalité, et surtout collaborent afin d'optimiser les possibilités et d'augmenter les profits.

INTERPOL continue d'évaluer le degré de menace que constituent les escroqueries financières, commises tant par des malfaiteurs isolés que par des groupes, aussi bien au niveau régional qu'au niveau mondial. Pour effectuer une analyse précise, les données des 196 pays membres de l'Organisation sont essentielles. Les conclusions du présent rapport serviront de base à la stratégie de l'Organisation pour aider les pays membres à lutter contre les escroqueries financières. Elles seront par ailleurs développées pour être ensuite intégrées au rapport d'INTERPOL intitulé « Évaluation des menaces criminelles au niveau mondial », qui sera publié en novembre 2024.







INTERPOL

À PROPOS D'INTERPOL

Le rôle d'INTERPOL est de permettre aux polices de ses 196 pays membres de travailler ensemble pour lutter contre la criminalité transnationale et rendre le monde plus sûr. L'Organisation gère des bases de données mondiales contenant des informations de police relatives aux malfaiteurs et aux infractions ; elle apporte également un appui opérationnel et un soutien en matière de police scientifique, fournit des services d'analyse et organise des formations. Ces capacités policières sont mises à disposition dans le monde entier et viennent à l'appui de quatre programmes mondiaux sur la criminalité financière et la corruption, l'antiterrorisme, la cybercriminalité, et la criminalité organisée et les nouvelles formes de criminalité.

NOTRE VISION : « RELIER LES POLICES POUR UN MONDE PLUS SÛR »

Notre vision est celle d'un monde dans lequel chaque professionnel des services chargés de l'application de la loi pourra, par la voie d'INTERPOL, transmettre, échanger et consulter en toute sécurité des informations de police vitales, à tout moment et en tout lieu où il en aura besoin, afin d'assurer la sécurité des personnes sur toute la surface du globe. Nous apportons et travaillons à offrir continuellement des solutions innovantes et de pointe aux problèmes qui se posent à l'échelle mondiale en matière de police et de sécurité.

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