جامعة نايف العربية
للعلوم الأمنية
NAIF ARAB UNIVERSITY
FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

سلسلة دراسات أمنية

دور المؤسسات المالية في الحد من الجرائم المعلوماتية: الاحتيال المالي أنموذجًا

دار جامعة نايف للنشر - 2021

جامعة نايف العربية
للعلوم الأمنية
NAIF ARAB UNIVERSITY
FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

سلسلة دراسات أمنية

دور المؤسسات المالية في الحد من الجرائم المعلوماتية

الاحتيال المالي نموذجًا

عبدالرزاق المرجان
كينغون كيم
عامر عثمان
سندرسن رامشندان
ألكسندر ريش
جورج سبير
ندى نبيه

2021

Security Studies Series

The Role of Financial Institutions in Reducing Online Financial crimes

Financial Fraud as a Model

Abdulrazaq Al-Morjan
Kyounggon Kim
Amir Osman
Sundaresan Ramachandran
Alexander Resch
George Spir
Nada Nabih

2021

دور المؤسسات المالية في الحد من الجرائم المعلوماتية: الاحتيال المالي نموذجًا

د. عبدالرزاق المرجان، د. كينغون كيم، عامر عثمان، سندرسن رامشندان، ألكسندر ريش، جورج سبير، ندى نبيه

جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية
منظمة الشرطة الجنائية الدولية (الإنتربول)

The Role of Financial Institutions in Reducing Online Financial crimes: Financial Fraud as a Model

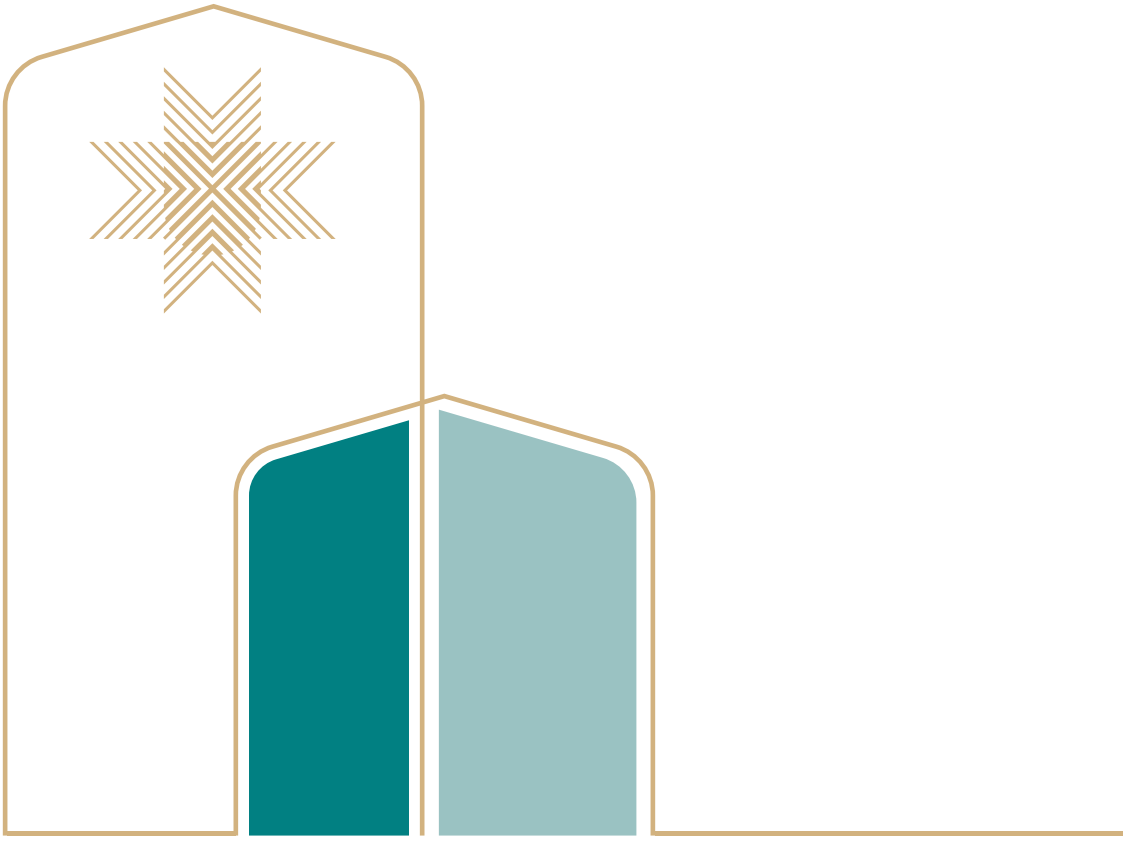
Dr. Abdulrazaq Al-Morjan, Dr. Kyounggon Kim, Amir Osman Nasar, Sundaresan Ramachandran, Alexander Resch, George Spir, Nada Nabih

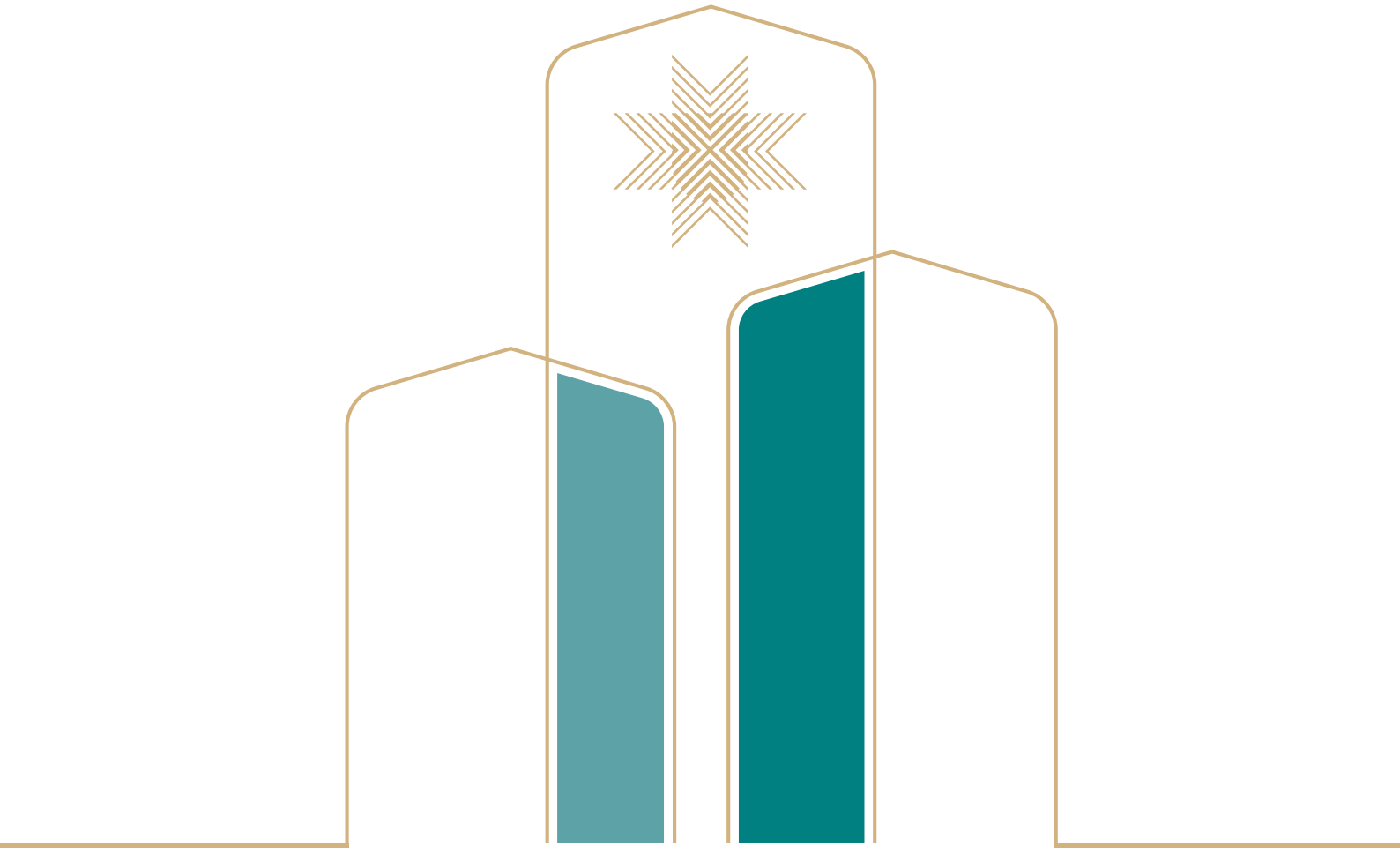
Naif Arab University for Security Sciences, Riyadh, Saudi Arabia
The International Criminal Police Organization (INTERPOL)

ردمك (ورقـــي) ISSNp 978-603-8235-99-7
ردمك (إلكتروني) ISSNe 978-603-8235-96-6
إيداع (ورقـــي) DEPOSITp 1443/3490
إيداع (إلكتروني) DEPOSITp 1443/3461
DOI:10.26735/978-603-8235-96-6

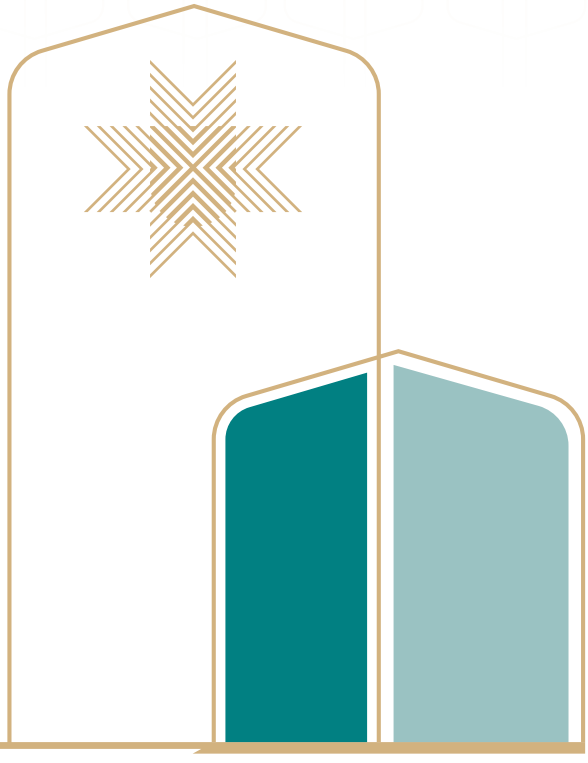
مركز البحوث الأمنية
سلسلة دراسات أمنية

ردمد (ورقـــي) ISSN(Print) 1658-8762
ردمد (إلكتروني) ISSN(Online) 1658-8770

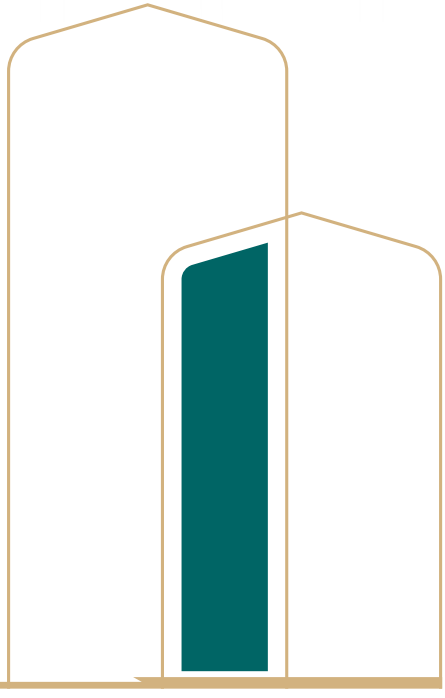





بسم الله الرحمن الرحيم

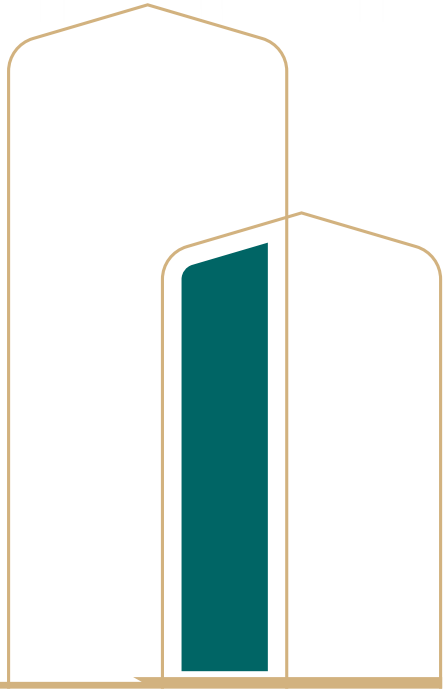


المحتويات



قائمة الرموز

الرمز	المعنى
ICANN	Internet Corporation for Assigned Names and Numbers
SIM	Subscriber Identity Module
إيفاد	(International Fund for Agricultural Development (IFAD
OTP	One - Time Password
IP	Internet Protocol
GPS	Global Position System
FATF	Financial Action Task Force
TLD	Top - Level Domain
IANA	Internet Assigned Numbers Authority
ISOC	Information Security Operations Center
DNS	Domain Name System
gTLDs	Generic Top - Level Domain
ccTLD	Country Code Top - Level Domain
GDPR	General Data Protection Regulation
RBL	Realtime Blackhole List
DAAR	Domain Abuse Activity Reporting
ARMA	Asset Recovery and Management Agency
RAT	Recovery Asset Team
AMON	Advanced Monitoring
GAFILAT	The Latin America Anti - Money Laundering Group
STAR	Stolen Asset Recovery Initiative
GFPN	.Gender Focal Point Network
NCPC	National Crime Prevention Council
AMLD	Anti - Money Laundering Directives



قائمة المصطلحات

قائمة المصطلحات

الهندسة الاجتماعيَّة:

هي مجموعة من الحيل والتقنيات المستخدَمة لخداع الناس وجعلهم يقومون بعملٍ ما أو يُفصحون عن معلومات سريَّة وشخصيَّة.. قد تُستخدم الهندسة الاجتماعيَّة دون الاعتماد على أي تقنية، بالاعتماد فقط على أساليب الاحتيال للحصول على معلومات خاصَّة من الضحيَّة. وتتم الهندسة الاجتماعيَّة في الغالب عن طريق الهاتف أو البريد الإلكتروني مع انتحال شخصية ذات سلطة أو فتاة جميلة على مواقع التواصُل الاجتماعي أو ذات عمل يسمح للمحتال أو المخترق بطرح أسئلة شخصيَّة دون إثارة الشبهات لدى الضحيَّة.

التصيُّد الإلكتروني:

هو أحد أنواع الجرائم الإلكترونيَّة الأكثر انتشارًا، ويُعد أحد أساليب الاحتيال عبر الإنترنت؛ وذلك لمحاولة الحصول على معلومات شخصيَّة أو ماليَّة عن طريق رسائل البريد الإلكتروني أو من خلال مواقع الإنترنت.

جيل الألفيَّة أو جيل «واي» أو بنو الألفيَّة:

هو مصطلح مُستخدَم لوصف الفئات السكانيَّة التي تتكوَّن من الأشخاص الذين وُلدوا بين عامي 1981 و1996م. ويُعرف الناس في هذه المُدَّة بجيل الألفيَّة. ويرتفع معدَّل المواليد في هذه المدة، ارتفاعًا يشبه نسبة ارتفاع المواليد بعد الحرب العالميَّة الثانية. ولأن أولويَّات جيل الألفيَّة الذي ترعرع في عصر ازدهار الإنترنت ووسائل التواصُل الاجتماعي تختلف عن أولويَّات أي جيل سابق؛ حيث تشير الدراسات إلى أن 90% من جيل الألفيَّة، بأعمار ما بين 18 و29، موجودون على مواقع التواصُل الاجتماعي، وأن هذه المواقع تؤدِّي دورًا رئيسًا في كيفيَّة تفاعُل 90% من جيل الألفيَّة مع الآخرين؛ حيث إنهم يقضون ما يقارب 15 دقيقة في تحرير منشور لنشره على وسائل التواصُل الاجتماعي، و42% منهم يتحققون من صحة المعلومات المنشورة على وسائل التواصُل الاجتماعي؛ لهذا تحتاج العلامات التجاريَّة للوصول إلى هذا الجيل إلى أن تكون موجودة على وسائل التواصُل الاجتماعي، وتحتاج أيضًا إلى إنشاء محتوى يجذب انتباههم بطريقة مميَّزة.

الجيل «Z»:

هو الجيل الذي يلي جيل الألفيَّة، ولا توجد تواريخ محددة لبدء هذا الجيل وانتهائه، الباحثون وعلماء الديموغرافيا يعتبرون مواليد ما بين منتصف عقد التسعينيات ومنتصف العقد الأول بعد عام 2000م نقطة بدء الجيل، ومواليد أواخر العقد الأول بعد عام 2000م إلى منتصف العقد الثاني بعد عام 2000م نقطة انتهاء له. وأبرز ما يميِّز هذا الجيل هو استخدامه الواسع للإنترنت منذ سن مبكرة. أبناء الجيل «Z» عادةً ما يكونون متكيِّفين مع التكنولوجيا، والتفاعل على مواقع التواصُل الاجتماعي يشكِّل جزءًا كبيرًا من حياتهم الاجتماعيَّة. ويشير بعض المعلقين إلى أن الترعرع خلال فترة الركود الاقتصادي أعطى هذا الجيل شعورًا بانعدام الأمن والاستقرار.

منصة «فُرجت»:

أدرجت منصة وزارة الداخليَّة الإلكترونيَّة (أبشر) خدمة «فُرجت» في تطبيق «أبشر أفراد الجديد»، التي تُمكِّن أهل الخير المتبرعين من مساعدة المحكومين في قضايا ماليَّة غير جنائيَّة، وسداد ديونهم سدادًا آمِنًا. وتتميز خدمة «فُرجت» بعد إضافتها إلى تطبيق «أبشر أفراد الجديد»، بالبحث عن الحالات المستحقة، واستعراض تفاصيل الحالات، مثل: مدة الحكم والعمر وعدد أفراد الأسرة والمبلغ المتبقي، والتحقُّق من رقم الفاتورة للتأكُّد من صحة إدراجها في الخدمة، وعرض الموقوفين الأكثر استحقاقًا آليًّا، وَفقَ الحالات المدرجة فيها. ويستطيع المتبرِّعون الآن الوصول إلى الخدمة من منصتي «أبشر» و«إحسان»، حرصًا على تسهيل سبل الخير الآمنة للتبرُّع للمستفيدين من الخدمة، دون الوقوع في عمليات احتيال أو دخول مواقع وهميَّة، كما يجب على المتبرعين التأكُّد من صحة الفواتير التي يرغبون في سدادها من خلال منصتي «أبشر» و«إحسان»، إضافة إلى موقع «ناجز» التابع لوزارة العدل، والتأكُّد من مقدار المبلغ المدخل المراد التبرُّع به لفواتير «فُرجت» قبل إتمام عملية الدفع.

«Dark Web»:

هو محتوى الشبكة العنكبوتيَّة العالميَّة الموجود في الشبكات المظلمة الذي يستخدم الإنترنت، لكنه يحتاج إلى برمجيات وضبط وتفويض خاص للولوج إليه. يشكِّل «Dark Web» جزءًا صغيرًا من الويب العميق، وهو جزء من الويب لا تُفهرسه محرِّكات البحث، تتكوَّن الشبكات المظلمة من شبكات صغيرة. ويشير مستخدمو «Dark Web» إلى الإنترنت العادية باسم «كلير نت»، التي تعني بالعربيَّة «الشبكة النظيفة» بسبب طبيعتها

غير المشفَّرة. في حين أن الإنترنت المظلمة تعمل على نظام التشفير. وتُعد الإنترنت المظلمة جزءًا مهمًّا من منظومة الإنترنت، حيث تسمح بإصدار المواقع الإلكترونيَّة ونشر المعلومات دون الكشف عن هُويَّة الناشر أو موقعه.

النقطة الذكيَّة:

يتولَّى قطاع المعلومات والحكومة الذكيَّة في هيئة تنظيم الاتصالات والحكومة الرقميَّة المسؤوليَّة عن دعم البنى التحتيَّة والإستراتيجيَّات التي تدفع عجلة التحوُّل الذكي للجهات الحكوميَّة في دولة الإمارات، وذلك من خلال تنفيذ خطط الحكومة الذكيَّة، تماشيًا مع إستراتيجيَّة الحكومة للتحوُّل الإلكتروني والذكي.

مجموعة العمل المالي (FATF):

هي هيئة حكوميَّة دوليَّة تتولَّى مهمَّة دراسة التقنيات واتجاهات غسل الأموال وتمويل الإرهاب وإعداد وتطوير السياسات المتعلِّقة بمكافحة غسل الأموال وتمويل الإرهاب محليًّا ودوليًّا. ركَّزت المجموعة، منذ تأسيسها في باريس سنة 1989م، جهودها على اعتماد وتنفيذ تدابير ترمي إلى مواجهة استغلال المجرمين للنظام المالي. وقد أصدرت مجموعة العمل المالي سنة 1990م سلسلةً من التوصيات، وراجعتها سنوات 1996 و2003 و2012م لتواكب التطوُّرات التي عرفتها التهديدات الناتجة عن غسل الأموال. وتتابع مجموعة العمل المالي التقدُّم الذي أحرزته الدول الأعضاء في تنفيذ التدابير اللازمة وتعمل عملًا وثيقًا جدًّا مع ثماني منظمات إقليميَّة على شاكلة مجموعة العمل المالي، وتدرس المجموعة أساليب غسل الأموال وتمويل الإرهاب والتدابير اللازمة لمكافحة هذه الظواهر، وتشجِّع اعتماد وتنفيذ التدابير المناسبة على الصعيد العالمي، وتتعاون مع الهيئات الدوليَّة الأخرى المعنيَّة في مجال مكافحة غسل الأموال وتمويل الإرهاب.

نطاق المستوى الأعلى أو النطاقات العلويَّة (TLD) :

هو أحد أعلى المستويات في نظام اسم النطاق الهرمي للإنترنت. ويعتبر الجزء الأخير من اسم أي نطاق، وهو التصنيف الأخير لاسم نطاق مؤهَّل بالكامل. مثلًا: في النطاق www.example.com، فإن نطاق المستوى الأعلى هو «.com». إن مسؤوليَّة إدارة معظم نطاقات المستوى الأعلى مُعطاة لمؤسسات محدَّدة من قبل «آيكان» (ICANN)، التي تدير «أيانا» (IANA)، وهي مسؤولة عن نظام أسماء النطاقات (DNS).

الملخص التنفيذي

في خضمِّ التحوُّل الرقمي، وازدهار التجارة الإلكترونيَّة، والثورة المتسارعة في طرق الدفع، والابتكار في الإعلانات عبر الإنترنت، برز تحدٍّ أمني جديد يهدِّد اقتصادات الدول، وهو الاحتيال المالي عبر الإنترنت؛ لكونها تستهدف جميع شرائح المجتمع وتُعتبر من الجرائم العابرة للحدود.

وقدَّر مكتب الأمم المتَّحدة للمخدِّرات والجريمة نسبة جرائم غسل الأموال في سنة واحدة بما بين 2% و5% من الناتج المحلي الإجمالي العالمي، بما يعادل 800 مليار إلى 3 تريليونات دولار أمريكي. وذكر تقرير أن إجمالي عدد الضحايا في 31 دولة 140 مليون ضحية، أي ما يعادل 3% من سكان العالم؛ حيث بلغت نسبة الذين يتعرَّضون لعمليات احتيال مالي عبر الإنترنت ووسائل التقنية 103 و102 لكل 1000 مواطن في الهند والإمارات على التوالي، بينما أفادت بعض التقارير المتخصصة أنَّ نصيب الفرد من المبالغ المفقودة من هذه الجرائم يصل إلى نصف مليون يورو في المملكة العربيَّة السعوديَّة.

وركَّزت هذه الدراسة على معرفة أسباب مشكلة تزايُد جرائم الاحتيال المالي عبر الإنترنت، الموجَّهة للدول العربيَّة، وأفضل الممارسات الدوليَّة الناجحة للتعامُل مع هذه الجرائم وتحسين إجراءات الاستجابة لها والإسهام في الحدِّ منها، وتقدِّم هذه الدراسة توصيات ومقترحات نوقِشت مع الممارسين والمختصين والخبراء الدوليين على المستويين الإقليمي والدولي.

وجُمِعت بيانات هذه الدراسة عن طريق مجموعتين، هما: مجموعة التركيز للحصول على بيانات من المصادر الخاصة عن طريق الممارسين والمختصين العرب لتحديد أنواع جرائم الاحتيال المالي والوقوف على التحديات التي تواجه الجهات المعنية في التعامُل مع جرائم الاحتيال المالي، وجرى اللجوء إلى هذه الطريقة بسبب عدم توافُر بيانات عن هذه الجرائم في المصادر العامَّة وسريَّتها. والمجموعة الثانية: فريق جامعة نايف العربيَّة للعلوم الأمنيَّة، للحصول على بيانات من المصادر المفتوحة للتعرُّف إلى الأساليب الإجراميَّة للمواقع الاحتياليَّة والتحديات التي تواجه الجهات الأمنيَّة في التعامُل معها. وجُمِع فيها نحو 500 رابط لإعلانات احتياليَّة، بالإضافة إلى مناقشة وتحليل حالات دراسيَّة لبعض ضحايا الاحتيال المالي والمحتالين الذين يديرون المواقع الاحتياليَّة عبر الإنترنت بالتعاون مع «الإنتربول».

وخلال اجتماع مجموعة التركيز حُدِّدت جرائم الاحتيال المالي الأكثر شيوعًا في الدول العربيَّة، وهي: الاحتيال في مجال الاستثمارات، والمجال الرومانسي، والابتزاز الجنسي، والتصيُّد، والاحتيال عبر الرسائل النصيَّة، والبريد الإلكتروني للأعمال. وحُدِّد استخدام 24 أسلوبًا إجراميًّا لارتكاب هذه

الجرائم في الدول العربيَّة، من ضمنها: استخدام المواقع الموثوقة لنشر الإعلانات الاحتياليَّة/ التصيُّد الإلكتروني، والبدء في استخدام العملات المشفَّرة لمحاولة إخفاء تتبُّع عائدات الجريمة واقتفاء أثرها خارج حدود الدولة، ورُصِدت مجموعة من التطبيقات الحكوميَّة السعوديَّة المزوَّرة في متجر «جوجل» كمنصة «فُرِجت» ومنصة «جود» ومنصة «أبشر»، وحُمِّلت في حدود 14 ألف مرة. وحُدِّد أيضًا 22 تحديًا يواجه جهات إنفاذ القانون والنيابة والبنوك للتعامُل مع جرائم الاحتيال المالي، من أهمها: البطء في تبادُل البيانات والحصول على الموافقات، وتعقُّب الأصول/ الأموال واستردادها، وعزوف الضحايا عن التبليغ.

وأجرى فريق الدراسة مسحًا عبر الإنترنت لمعرفة آليَّات البلاغات الإلكترونيَّة المتاحة لضحايا الاحتيال الإلكتروني بعد وقوعهم في الجريمة ومدى سرعة التجاوُب مع هذه الجرائم. وعند رصد آليات البلاغات الإلكترونيَّة للدول العربيَّة تبيَّن وجود فوارق مهمَّة بين أعضاء الدول العربيَّة فيما يتعلَّق باستعدادها لمواجهة الجرائم الماليَّة عبر الإنترنت. في حين طوَّرت دول مجلس التعاون الخليجي وسائل استقبال البلاغات الإلكترونيَّة، وعيَّنت بعض فرق العمل والوحدات لتولِّي مسؤولية هذه الجرائم. إلَّا أنَّ بعض الدول العربيَّة لا توجد لديها أيٌّ من هذه الاستعدادات حتى إعداد هذه الدراسة، فبعض المواقع الإلكترونيَّة لا تعمل، بينما يصعب العثور على مواقع أخرى أو تصفُّحها.

وتشير نتائج تحليل الروابط الاحتياليَّة إلى أن هناك أسلوبًا إجراميًّا مُركَّبًا صُمِّم لاستهداف الضحية مرتين وبطريقتين مختلفتين، شريطة أن يكون قد وقع ضحيَّة للأسلوب الإجرامي الأول، وهو الإيقاع بالضحيَّة المحتملة عن طريق الإعلانات الاحتياليَّة الاستثماريَّة. ومن ثَمَّ يُستهدَف عن طريق إعلانات شركات استشارات قانونيَّة لاسترداد الأموال.

وتشير الدراسة إلى استغلال المحتالين نماذج الإعلانات الإلكترونيَّة لوكلاء الإعلانات عبر الإنترنت والاستفادة من الذكاء الاصطناعي في شركات الإعلانات للوصول إلى الضحايا المحتمَلين. وتؤكِّد الأدلة أن المحتالين ينشرون إعلاناتهم في المواقع المشهورة والموثوقة عن طريق وكلاء الإعلانات، ومن أهم هذه المواقع التي تنشر الإعلانات الاحتياليَّة: محرك البحث «جوجل» وموقع «مايكروسوفت» الإخباري باللغة العربيَّة، و«روسيا اليوم» وصحيفة التحرير و«سي إن إن» العربيَّة. وتصدرت وكالة الإعلانات «Speakol» الوكالات الإعلانية في نشر الإعلانات الاحتياليَّة بـ171 إعلانًا، تلتها شركة «Google» بنشر 136 إعلانًا، وجاءت وكالة الإعلانات «Gecko» في المرتبة الثالثة بنشر 48 إعلانًا، وحلت وكالة الإعلانات «Postquare» رابعةً بنشر 24 إعلانًا. وتشير الدراسة إلى وصول عدد الزيارات اليوميَّة للمواقع الاحتياليَّة إلى أكثر من 130 ألف زيارة.

وتؤكِّد الدراسة أن من أهم التحديات التي تواجه الجهات المعنيَّة: إخفاء المسجِّل المعتمد لنطاقات الإنترنت بيانات النطاقات الاحتياليَّة عبر الإنترنت؛ حيث إن 86% من النطاقات الاحتياليَّة كانت تخفي بياناتها، ما يخلق لهم فرصة لخلق تحديات لجهات التحرِّي والاستدلال. وتشير الإحصاءات إلى أن عدد النطاقات الاحتياليَّة المسجلة بين عامي 2017 و2021م وصل إلى 112 نطاقًا احتياليًّا، 72% منها سُجلت في عامي 2020 و2021م خلال جائحة «كورونا». وأشارت الدراسة إلى أن أعلى خمسة نطاقات محتالة نشرت في حدود 40 ألف رابط إعلاني عبر الإنترنت، ثلاثة من هذه النطاقات محجوبة من هيئة الاتصالات وتقنية المعلومات بالمملكة العربيَّة السعوديَّة. ورُصِد انتحال مؤسسات ماليَّة سعوديَّة وصحف سعوديَّة والإعلان عنها في مواقع إلكترونيَّة معروفة ومشهورة عبر وكلاء الإعلانات لتصيُّد الضحايا، وهو ما يؤكِّد غياب الرقابة على المحتوى الإعلاني.

وكشفت الدراسة عن أن نتائج تحليل الروابط الاحتياليَّة تؤكِّد استغلال المحتالين آلية تسجيل نطاقات الإنترنت؛ حيث سُجِّل 93% من النطاقات الاحتياليَّة في نطاقات المستوى الأعلى العامَّة، و7% من النطاقات الاحتياليَّة في نطاقات المستوى الأعلى لرمز الدول، من أهمها 9 نطاقات احتياليَّة مسجلة في نطاق دولة كولومبيا، و8 مسجلة في نطاق الإمارات العربيَّة المتَّحدة، و5 مسجلة في نطاق المملكة المتَّحدة. وكشفت الدراسة أيضًا عن أن أعلى ثلاثة مسجلين معتمدين سجَّلوا نطاقات احتياليَّة في الإنترنت: شركة «Godaddy» بتسجيل 62 نطاقًا احتياليًّا، وشركة «Namecheap» بتسجيل 48 نطاقًا احتياليًّا، وشركة «Tucows Domains» بتسجيل 8 نطاقات احتياليَّة.. وخلال الاجتماع مع منظمة «ICANN»، اتضح أن هناك اختلافًا في طريقة إدارة نطاقات المستوى الأعلى للإنترنت. وأوضحت المنظمة أن السبب الرئيس في إخفاء المسجل بيانات النطاقات الاحتياليَّة هو تنفيذ لائحة حماية البيانات العامَّة للاتحاد الأوروبي في 25 مايو 2018م. وأكدت المنظمة أن سياسة حجب المواقع ليست مُجدية في الحلول المستدامة؛ لذا فمن المهم اتباع أفضل الممارسات لإغلاق مواقع الاحتيال عبر الإنترنت.

وأكَّدت الدراسة، عند مقابلة الضحايا، توافُق الأساليب الإجراميَّة التي وقعوا فيها ضحايا مع ما حُدِّد سابقًا مع المختصين والممارسين في اجتماع مجموعة التركيز، وتوجُّه المحتالين للاختراق عن طريق البرامج الخبيثة بحجة تقديم برامج تدريبيَّة. وكذلك تطابُق التحديات مع ما نُوقِش مع مجموعة التركيز، ومن أهمه: عزوف بعضهم عن الإبلاغ عن جريمة الاحتيال. وخلال مقابلة المحتالين، اتضح توجُّههم إلى استغلال أساليب تطوُّر الدفع الإلكتروني بتحصيل عوائد الاحتيال عن طريقة بطاقات الدفع (مثال بطاقة مدى) وليس التحويل البنكي بسبب تتبُّع البنوك هذه الحسابات المشبوهة. ويتضح أن المحتالين يعتمدون في رسم سيناريوهات الاحتيال لتصيُّد الضحايا على الأحداث

الاقتصاديَّة المهمَّة محليًّا ودوليًّا، والأخبار المفبركة، وكذلك منظومة الدفع المتقدِّمة للدول لتحصيل عوائد الاحتيال.

وبناءً على خطة التنمية المستدامة للأمم المتَّحدة لعام 2030 والغايات/ المؤشرات المتعلِّقة بها التي لها صلة بإحصاءات الجريمة والعدالة الجنائيَّة كالحد بقدر كبير من التدفقات غير المشروعة للأموال والأسلحة، وتعزيز استرداد الأصول المسروقة وإعادتها ومكافحة جميع أشكال الجريمة المنظمة بحلول عام 2030، رُوجِعت أفضل الممارسات الدوليَّة الناجحة للحدِّ من جريمة الاحتيال المالي عبر الإنترنت للقطاعين الحكومي والمالي، واتضح أن أغلب هذه الممارسات حديثة، بدأت منذ عام 2017م. واشتملت الممارسات في القطاع الحكومي على عدة مرتكزات رئيسة، هي: استقبال البلاغات، وإنشاء مكاتب مركزيَّة متخصِّصة للاحتيال المالي تجمع الجهات المعنيَّة في مكان واحد، وتعقُّب الأصول واعتراض الأموال، ونظم الإنذارات التي تستهدف المواقع المشبوهة. وفي القطاع المالي ارتكزت على مشاركة المعلومات، وتعقُّب أصول الجريمة، والشراكة بين القطاعين، والسماح للشركات الخاصَّة بالمشاركة.

وبناءً عليه، وُضِعت توصيات غير ملزمة للدول العربيَّة لتطوير قدراتها في الحدِّ من جريمة الاحتيال المالي، تتوافق مع أفضل الممارسات الدوليَّة الناجحة، من ضمنها: تطوير الإستراتيجيات والهياكل التنظيميَّة، وتطوير الجوانب التحقيقيَّة والتنفيذيَّة والتكتيكيَّة، ويتم ذلك عن طريق إنشاء مراكز متخصِّصة تجمع كل المرتكزات الرئيسة للحدِّ من الجريمة وجميع الأطراف ذات العلاقة. وإعادة بناء السياسات وتطويرها لمنع وكالات الإعلانات من استغلال النطاقات المعروفة لنشر الإعلانات الاحتياليَّة باللغة العربيَّة، وهو ما يُسهِم في الحدِّ من انتشار الإعلانات الاحتياليَّة في المواقع المعروفة والمشهورة، وتفعيل المنتدى العربي لاسترداد الأموال تحت مظلة أمانة وزراء الداخليَّة العرب.

وتوصي الدراسة بأن يكون هناك عمل مشترك بين الجامعة وجهات إنفاذ القانون في الدول العربيَّة للعمل على إغلاق المواقع التي رُصِدت بتكوين فريق عمل مشترك، وتأسيس الجامعة نظامًا مقترحًا للإنذار بمواقع الاحتيال المالي باللغة العربيَّة لرصد الأساليب الإجراميَّة الناشئة، وجمع روابط المواقع الاحتياليَّة التي تستهدف المنطقة العربيَّة لخداع مواطنيها والمقيمين فيها. وسيوفِّر النظام حلولًا تكتيكيَّة لتحديد المواقع الاحتياليَّة وآليَّات إغلاقها، ومساعدة وكالات إنفاذ القانون العربيَّة على التحقُّق من المواقع الاحتياليَّة، وسيُسهم في بناء برامج لتطوير القدرات البشريَّة في عدة مسارات كالبحث والتحري والتحقيق، بناءً على أفضل الممارسات. وسيُسهم هذا التعاون في إصدار مجموعة من الأدلَّة الاسترشاديَّة، وإجراء البحوث المتخصِّصة، وتنظيم اجتماع دولي بين الدول العربيَّة والدول المتقدِّمة لتبادُل الخبرات وأفضل الممارسات في الحدِّ من جريمة الاحتيال المالي.

fraudulent advertisements (Ads), and further discussed and analyzed study cases of some victims of financial fraud and fraudsters running fraudulent websites.

During a meeting of the focus group, most common financial fraud offences in the Arab States were identified as follows: investment fraud, romance scams, sextortion, phishing, smishing and business e-mail compromise (BEC). The use of 24 criminal methods to commit such crimes has been identified in the Arab States, including the use of reliable websites to publish fraudulent ads (phishing attacks), the introduction of cryptocurrencies to try to hide the tracking and tracing of proceeds of crime outside the borders of the State., A number of false Saudi government apps in the Google Store have been also spotted. These apps were portraying as "Farjat," "Jude" and "Absher" platforms, some of which were accessed up to 14,000 times. It also identified 22 challenges facing law enforcement, prosecutors, and banks in dealing with financial fraud, the most important of which were slow exchange of data and access to approvals, tracing and recovery of assets/funds, and failure of victims to report.

The STeam conducted an online survey of the mechanisms of electronic communications available to victims of electronic fraud after they had committed a crime and how quickly they responded to such crimes. While monitoring the electronic communications mechanisms, significant differences were observed among the members of the Arab States regarding their willingness to confront financial crimes via the Internet. Gulf Cooperation Council States have developed means of receiving electronic communications, and some task forces and units have been designated to take charge of these crimes. However, some Arab States do not have such measures in place until the elaboration of this study. For example, some websites do not work, while others are difficult to find or browse.

The results of the fraud link analysis indicate that there is a composite criminal method designed to target the victim twice and in two different ways. If an individual has been the victim of the first criminal method, which is to lure potential victims through fraudulent investment announcements.

Executive Summary

Digital transformation has enhanced e-commerce and related business functions such as online payments methods, online advertising, and online tracking of postage and deliveries. This has instigated new security challenges that threatens the economies of states, namely, online financial fraud because they target all segments of society and are considered cross-border crimes.

The United Nations Office on Drugs and Crime (UNODC) estimated the proportion of money-laundering offences in one year to be between 2 and 5 per cent of world GDP, equivalent to $800 billion to $3 trillion. The total number of victims in 31 states was reported to be 140 million, equivalent to 3 per cent of the world population. The proportion of people exposed to financial fraud via the Internet and the means of technology was 103 and 102 per 1000 in India and the United Arab Emirates, respectively, while some specialized reports indicated that half a million euros in Saudi Arabia were lost per capita.

This study focused on the causes of the increasing problem of online financial fraud in the Arab States and on the understanding of successful international best practices for dealing with such crimes, improving response procedures, and contributing to their reduction. The study makes recommendations and proposals that have been discussed with international practitioners, specialists, and experts at the regional and international levels.

The data for this study were collected through two groups: A Focus Group was formed to obtain data from private sources through Arab practitioners and specialists to identify types of financial fraud offences and to identify the challenges faced by stakeholders in dealing with those offences, especially the challenge of lack of data on such crimes in public sources. Another group that constituted a team from Naif Arab University for Security Sciences (NAUSS), was formed to obtain data from open sources to identify the criminal methods of fraudulent sites and the challenges facing security agencies in dealing with them. The team, in cooperation with the Interpol, collected about 500 links to

several key pillars that include receiving reports, setting up specialized central financial fraud offices to bring stakeholders together, tracing assets and intercepting funds, and alert systems to detect suspicious sites. In the financial sector, it was based on sharing information, tracing crime assets, public partnerships and allowing private companies to participate.

Accordingly, non-binding recommendations have been made for the Arab States to develop their capacity to reduce the financial fraud crime, consistent with successful international best practices including development of organizational strategies and structures, and development of investigative, operational, and tactical aspects, through the establishment of specialized centers bringing together the main pillars of crime reduction and all relevant parties. The study also proposes development of policies to prevent advertising agencies from exploiting known ranges for the dissemination of fraudulent advertisements in Arabic. This will contribute to the reduction of the spread of fraudulent advertising in well-known and reputed sites, and the instigation of the Arab Money Recovery Forum under the umbrella of the Secretariat of Arab Ministers of the Interior.

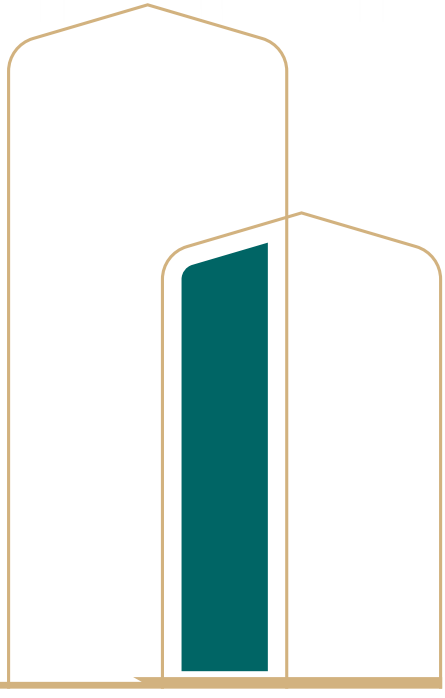
The study recommends that there should be joint action between the League and law enforcement agencies in the Arab States to ensure the closure of sites monitored by a joint working group. NAUSS proposes to establish a Deep Learning Model for Arabic-language financial fraud sites to monitor emerging criminal methods and collect links to fraudulent sites targeting the Arab region. This model will provide tactical solutions for the identification of fraudulent sites and their closure mechanisms, assist Arab law enforcement agencies in verifying fraudulent sites, and contribute to building human capacity development programmes in several tracks, such as search, detection, and investigation, based on best practices. This cooperation will contribute to the production of a series of guides, specialized research, and the organization of an international meeting between Arab and developed states to exchange experiences and best practices in reducing the financial fraud crime.

The perpetrators impersonated as legal recovery consulting firms.

The study indicates that fraudsters exploit online advertising models and use artificial intelligence in advertising companies to reach potential victims. Evidence confirms that fraudsters post their ads on popular and trusted sites through advertising agents, the most important of which publish fraudulent ads such as Google search engine, Microsoft news site in Arabic, Russia Today, Al Tahrir and CNN Arabic. “Speakol” led the advertising agencies in publishing fraudulent ads by 171, followed by Google with 136, “Gecko” with 48, and “Postquare” with 24. The study indicates that the number of daily visits to fraudulent sites has reached over 130,000.

The study stresses that one of the most important challenges facing stakeholders is hiding the fraudulent domain data over the Internet by the certified Internet domain recorder, where 86% of the fraudulent ranges had hidden their data, making the detection very challenging. Statistics indicate that the number of fraudulent ranges recorded between 2017 and 2021 reached 112 ranges, 72% of which were recorded in 2020 and 2021 during the COVID-19 pandemic. The study indicated that the top five scams were published in the range of 40,000 online advertising links, three of which are blocked by the Saudi Arabian Communications and Information Technology Commission (CITC). Saudi Arabian financial institutions and newspapers were impersonated and advertised on well-known and popular websites through advertising agents to lure victims, which confirms the absence of censorship of advertising content.

This study contributes to achieving the United Nations Sustainable Development Plan 2030 and related targets associated with combating crime. and to significantly reduce the illicit flow of funds and firearms., The study also promotes asset recovery and the fight against all forms of organized crime and adoption of successful international best practices to reduce online financial fraud in the government and financial sectors. Some of these best practices have been in place since 2017. Practices in the government sector included



1. المقدّمة

1. المقدِّمة

عرَّفت مؤسَّسة النقد العربي السعودي الاحتيال بأنه أي ممارسة تنطوي على استخدام الخداع للحصول المباشر، أو غير المباشر، على شكلٍ من أشكال الاستفادة الماليَّة لمرتكِب الجريمة، أو تسهيل ذلك لغيره، لتؤدِّي إلى شكل من أشكال الخسارة للطرف الذي تعرَّض للاحتيال (مؤسَّسة النقد العربي السعودي، 2008م).

وتشير التقارير الدوليَّة إلى أن الجرائم الماليَّة ما زالت تمثل مصدر قلق عالمي، وهي في تزايُد مستمر، لا سيَّما في ظل التقدُّم التقني الذي نعيشه، وأجمعت هذه التقارير على تضاعُف خسائر الاقتصاد العالمي بسبب الجرائم الماليَّة؛ حيث قدَّر بنك «إتش إس بي سي» الخسائر في عام 2018م بحوالي 2.1 تريليون دولار، في حين قدَّرها منتدى الاقتصاد العالمي «دافوس» بحوالي 2.4 تريليون دولار للعام ذاته (الشياظمي، 2020م).

وأشار تقرير The Global State of Scams, 2020، الذي ناقش نتائج دراسة شملت 31 دولة، من ضمنها المملكة العربيَّة السعوديَّة والإمارات العربيَّة المتَّحدة، إلى أن هذه الدول خسرت 36 مليار يورو في عام 2019م، وأن إجمالي عدد جرائم الاحتيال فيها بلغ 139.327.796 جريمة (Abraham et al., 2020). كما تضمَّنت نتائج الدراسة أن أغلب هذه الدول قد سجلت ارتفاعًا ملحوظًا في جرائم الاحتيال عبر الإنترنت؛ حيث أتت بولندا في المرتبة الأولى بأعلى ارتفاع بنسبة 70%، ثم الهند بنسبة 50%، تلتها نيوزيلندا بنسبة 41%، ثم أمريكا بنسبة 33%، ومن بعدها بلجيكا بنسبة 27%. بينما حلَّت جرائم الإنترنت في المراتب الأولى في ثلاث دول، هي: بريطانيا بنسبة 33% من إجمالي الجرائم، وروسيا بنسبة 14%، وسنغافورة بنسبة 27% (Abraham et al., 2020).

وذكر تقرير Scamwatch أن أعلى خسائر للأستراليين كانت بسبب الاحتيال في الاستثمار عبر الإنترنت، ووصلت إلى 328 مليون دولار أمريكي، ثم الخسائر في الاصطياد الرومانسي بمبلغ 131 مليون دولار، وأخيرًا البريد الإلكتروني للشركات بمبلغ 128 مليون دولار أمريكي (Australian Competition & Consumer Commission, 2020).

وذكر تقرير نشرته المفوضية الأوروبيَّة في يونيو 2020م بعنوان «استرداد الأصول ومصادرتها.. ضمان ألَّا تفيد الجريمة» أن أرباح جماعات الجريمة المنظَّمة من الاحتيال وصلت إلى 110 مليارات يورو سنويًّا في الاتحاد الأوروبي. ومع ذلك، وَفقًا لـ«يوروبول»، لم يُسترجَع إلا 1% فقط. وخلال اجتماع فريق البحث بمركز مكافحة الاحتيال المالي في سنغافورة عبر تقنية الاتصال المرئي عن بُعد،

أكَّد أن إجمالي الجرائم في سنغافورة ارتفع في عامي 2019 و2020م بسبب ازدياد جرائم الاحتيال المالي. ففي عام 2019م سجل إجمالي الجرائم 35 ألف جريمة، من ضمنها 9500 جريمة احتيال مالي، وفي عام 2020م سجل إجمالي الجرائم 37 ألف جريمة من ضمنها 15700 جريمة احتيال مالي. وهو ما يؤكِّد أن جريمة الاحتيال المالي قضية دوليَّة تمس جميع الدول.

1.1 مشكلة الدراسة

يُعد التطوُّر الكبير والمستمر في استخدام أدوات وأساليب مختلفة للجرائم الماليَّة عبر الإنترنت معضلة تقف أمامها المنظَّمات الدوليَّة بمحاولات لتقصِّي مَن خلف تلك الجرائم وتتبُّعه؛ وذلك للحدِّ منها. وحسب التقارير التي جُمِعت وعُمِل عليها في هذه الدراسة فهناك كثيرٌ من التكتيكات المستخدمة لشنِّ هذا النوع من الجرائم واستغلال الضحايا بطرق متقدِّمة يصعب الكشف عنها. على سبيل المثال وليس الحصر لتلك التكتيكات: الهندسة الاجتماعيَّة، والتصيُّد الإلكتروني، وانتحال الشخصيَّة، ما أدَّى إلى ارتفاع هذه الجرائم وتكبيد الاقتصادات خسائر عالية، خصوصًا في الدول العربيَّة، وذلك وَفقَ الأرقام والإحصاءات الرسميَّة. يدلُّ ذلك على الأهمية البالغة لتطوير آليَّة للتعامل مع هذه الجرائم لتواكب تلك التحديات كما هو معمول به في بعض الدول، كأمريكا وهونج كونج.

1.2 أهمية الدراسة

تكمن أهمية هذه الدراسة في دورها في التعرُّف إلى المعضلات التي خلف التزايُد المستمر في جرائم الاحتيال المالي عبر الإنترنت ووسائل التقنية، ومراجعة أفضل الممارسات الدوليَّة للتعامل مع هذه الجرائم لتحسين إجراءات الاستجابة لها والإسهام في الحدِّ منها بمراجعتها لجميع الحلول والتوصيات والمقترحات التي ستتضمَّنها هذه الدراسة مع الممارسين والمختصين والخبراء الدوليين على المستويين الإقليمي والدولي، مُمثِّلين في إدارة الجرائم الماليَّة بالشرطة الدوليَّة (الإنتربول) ومكتب الأمم المتَّحدة المعني بالمخدِّرات والجريمة وغيرهما من الجهات ذات العلاقة. أيضًا تتضمن هذه الدراسة مقترحات تعتمد على التقنيات الحديثة التي تُسهِم بدورها في معالجة هذا النوع من الجرائم لاعتمادها على أساليب تقنية متقدِّمة يمكن تحديثها باستمرار للتوافق مع أبرز الأساليب والأدوات للمحتالين الماليين.

1.3 أهداف الدراسة

تحاول هذه الدراسةُ تحقيقَ مجموعة من الأهداف، تتضمن:

- التعرُّف إلى الأدوات والأساليب والتكتيكات الإجراميَّة للمحتالين عبر الإنترنت وآليَّة وصولهم إلى الضحايا (شركات الاستثمار الوهميَّة عبر الإنترنت).
- رصد ومناقشة أفضل النماذج والممارسات والأساليب الدوليَّة للدول المتقدِّمة للتصدي لجرائم الاحتيال المالي.
- تقديم إطار عمل يُسهم في تحسين سرعة الاستجابة لجرائم الاحتيال، يعتمد على أفضل الممارسات الدوليَّة.

1.4 منهجيَّة الدراسة

نظرًا لطبيعة الدراسة ونوعيَّتها وصعوبة الحصول على البيانات والمعلومات من الجهات الرسميَّة وندرة هذه البيانات في المصادر المفتوحة، استُخدِمت منهجيَّة البحث النوعي (Qualitative Research) من خلال تحديد مجموعة التركيز المكوَّنة من الممارسين والمختصين والخبراء العرب لتشخيص المشكلة والحلول ومناقشتها معهم، سعيًا إلى الوصول إلى إطار عمل للحدِّ من هذا النوع من الجرائم ووَفقَ توصيات الخبراء والممارسين في المجالات ذات العلاقة ووَفقَ أفضل الممارسات العربيَّة والدوليَّة. وشُكِّل فريق دراسة من مركز الجرائم السيبرانيَّة والأدلَّة الرقميَّة بجامعة نايف والشرطة الدوليَّة (الإنتربول) للاستفادة من الخبرات الدوليَّة في الحدِّ من هذه الجريمة.

والبحث النوعي هو منهج عِلْمي للملاحظة من أجل الحصول على بيانات غير رقميَّة. ويشير هذا النوع من البحث إلى المعاني والمفاهيم والتعريفات والخصائص والاستعارات والرموز ووصف الأشياء، وليس إلى إحصائها أو قياسها. ويجيب هذا البحث عن الكيفيَّة والأسباب الممكنة لحدوث ظاهرة معيَّنة، بدلًا من الإجابة عن عدد مرات حدوثها. وتوظَّف مداخل البحث النوعي عبر كثيرٍ من التخصُّصات الأكاديميَّة؛ إذ تركِّز تحديدًا على العناصر البشريَّة للعلوم الطبيعيَّة والاجتماعيَّة. وتشمل مجالات التطبيق البعيدة عن السياقات الأكاديميَّة: أبحاث السوق النوعيَّة، والأعمال

التجاريَّة، والخدمات التوضيحيَّة التي تقدِّمها المنظَّمات غير الربحيَّة، والصحافة. وتُعتبر المناهج النوعيَّة هي الأفضل في بحث كثيرٍ من مسائل التجرِبة البشريَّة في جوانبها التفسيريَّة والوصفيَّة، في اتخاذ قرارٍ على سبيل المثال (ليس فقط ما أو أين أو متى أو مَن)، لديه أساس قوي في مجال علم الاجتماع بهدف فهم البرامج الاجتماعيَّة والحكوميَّة. ويُستخدم البحث النوعي على نطاق واسع لدى الباحثين في مجالات العلوم السياسيَّة والعمل الاجتماعي والتربية. تكوَّنت مجموعة التركيز من خبراء عرب يمثلون عدة جهات ذات علاقة بالاحتيال المالي، وهي من جهات إنفاذ القانون، والأدلَّة الجنائيَّة، والنيابة العامَّة، والبنوك المركزيَّة والتجاريَّة، وتم توجيه الدعوة لهذه الدول لتمثل عينة من الدول العربية وهي 3 دول من قارة آسيا و3 دول من قارة إفريقيا:

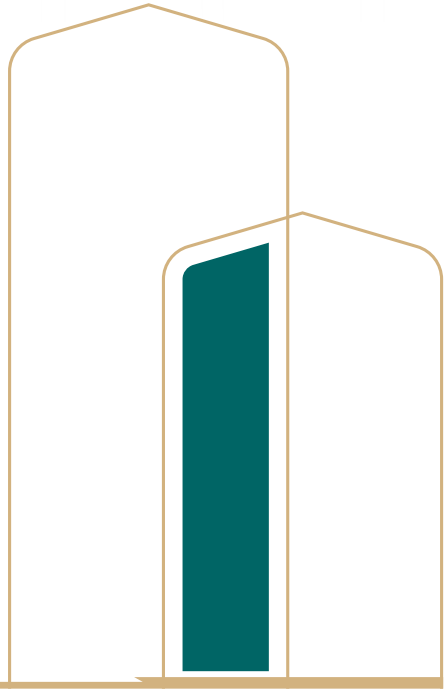
- الإمارات العربيَّة المتَّحدة.
- المملكة العربيَّة السعوديَّة.
- دولة الكويت.
- جمهوريَّة مصر العربيَّة.
- المملكة المغربيَّة.
- جمهوريَّة موريتانيا.

ووُضِعت ثلاثة أسئلة لتشخيص جريمة الاحتيال المالي والتعرُّف إلى اتجاهاتها، هي:

- ما أنواع الجرائم السيبرانيَّة الأكثر شيوعًا التي جرى الإبلاغ عنها والتصدِّي لها من جانب السلطات؟
- مَن المسؤولون عن التعامُل مع هذه الجرائم (على سبيل المثال: إجراء التحقيقات والتعاوُن بشأنها)؟
- ما التحديات التي تواجهها السلطات عند التعامُل مع هذه الجرائم؟

وجُمِعت أيضًا عينة من الروابط ذات الطابع الاحتيالي في حدود 500 رابط إلكتروني للتعرُّف إلى اتجاهات المحتالين عبر الإنترنت وأساليبهم. وعُقِد اجتماع مع هيئة الإنترنت للأسماء والأرقام المخصصة (ICANN) لمناقشة ما يلي:

- التحقُّق من روابط المواقع الاحتياليَّة التي جُمِعت خلال الدراسة للتأكُّد من النتائج التي جرى التوصُّل إليها.
- التحديات التي تواجه الجهات المعنيَّة في التحرِّي والبحث عن سجلات أسماء نطاقات المواقع الاحتياليَّة والمعلومات التقنية الخاصَّة بالمسجل وخوادم الأسماء المرتبطة بالشركات المضيفة.
- التعرُّف إلى أفضل الممارسات المتبعة في حالات البحث والتحري.



2. منظومة الدفع في الدول العربيَّة

2. منظومة الدفع في الدول العربيَّة

إن التطوُّر الكبير لخدمات الدفع وتحوُّلها إلى الدفع الإلكتروني منح أنظمة الصرف الآلي ونقاط البيع وخدمات الدفع الإلكتروني على الإنترنت أبعادًا غير مسبوقة من المرونة والسرعة والقبول. وأصبح المحتالون يضعون منظومة الدفع في حسبانهم لرسم سيناريو الاحتيال والحصول على الأموال بطريقة لا تثير شكوك الضحيَّة. وهنا تكمن أهمية تسليط الضوء على منظومة الدفع في الدول العربيَّة.

تمثِّل البلدان العربيَّة مجموعة غير متجانسة من البلدان مختلفة الوسائل والخصائص، وكذلك معدل الاختراقات الشبكيَّة والبنكيَّة؛ فبينما يرتفع معدل الاختراق إلى أكثر من 90% في البحرين والإمارات العربيَّة المتَّحدة وقطر، ينخفض إلى أقل من 40% في اليمن وسوريا والعراق (Ecommpay, 2021). وبالنظر إلى تفاوت البنى التحتيَّة، يختلف النمو الرقمي في القطاع المالي من بلد إلى آخر؛ ومن ثَمَّ تختلف الخدمات المُقدَّمة.

بالإضافة إلى ذلك، بينما تتشابه أساليب الدفع بين سكان البلدان المختلفة، بوصفها شعوبًا تتشارك ثقافة ما زالت تفضِّل الدفع نقدًا وتثق به، يقطن البلدان العربيَّة مجموعةٌ من الشباب الأكثر انفتاحًا، يدركون مزايا التحوُّل الرقمي في طرق الدفع، مقارنةً بالأساليب التقليديَّة التي يتبعها الجيل السابق.

2.1 طرق الدفع في الدول العربيَّة:

2.1.1 التصنيف النوعي لطرق الدفع وأساليبه في الدول العربيَّة

يمكننا ذكر طرق الدفع المتبعة في البلدان العربيَّة/ الأعضاء بمجلس وزراء الداخليَّة العرب، وهي: الدفع نقدًا، والطريقة الهجين، والبطاقة، والمحفظة الرقميَّة، والتحويلات المصرفيَّة أو التحويلات عبر شركات تحويل الأموال.

ملحوظة: بينما يزداد تداول الحديث عن العملات المشفَّرة بين الجيل الشاب في المنطقة كغيرها من المناطق الأخرى، لا تستخدم هذه العملات ضمن طرق الدفع في المنطقة حاليًّا، ولا يزال مجرد موضوع متخصِّص يتداوله خبراء التقنية الشباب.

الدفع نقدًا

ما زال الدفع نقدًا هو الطريقة الأساسيَّة لشعوب المنطقة، بينما يبلغ عدد مستخدمي الإنترنت في منطقة الشرق الأوسط وشمال إفريقيا 146 مليونًا، تفضل الأغلبية الدفع نقدًا عند التسليم. وما زالت المنطقة عامَّةً تعتمد على الأموال النقديَّة وتستخدمها.

استخدام البطاقات للدفع

بالنسبة للبطاقات الائتمانيَّة، فإن «فيزا» و«ماستر كارد» هما جهتا التشغيل الأساسيتان، لكن طرق الدفع المحليَّة تشهد تزايدًا من خلال استخدام بعض البطاقات المحليَّة القائمة على مشروعات محليَّة للبطاقات، وأحيانًا بالتعاون مع أكبر الأسماء في القطاع.

وتُعد زيادة استخدام بطاقات الائتمان والخصم الفوري ونمو الثقة والمعرفة بالأنظمة المصرفيَّة ثورة جديرة بالذكر. ويشكِّك معظم الأشخاص في الدفع ببطاقات الائتمان والخصم الفوري باستثناء البلدان الأعضاء بمجلس التعاون الخليجي؛ ففي عام 2010م كان لـ10% فقط من الشعب المصري حسابات مصرفيَّة، ولـ4% فقط بطاقات خصم فوري، ولـ2% بطاقات ائتمان (Ecommpay, 2021).

ملحوظة: مع ذلك، يمكننا التأكيد أن انعدام الثقة بالمصارف قد تفاقم في لبنان، الذي يعاني حاليًّا كبرى أزماته الاقتصاديَّة التي يتمثل السبب الرئيس فيها في المصارف. وقد انعدمت ثقة اللبنانيين بالمصارف بشأن مدخراتهم منذ عدة سنوات.

الطريقة الهجين

إحدى طرق الدفع التي لا يُستهان بها والمشهورة في البلدان الإفريقيَّة هي تحويل الأموال عبر الجوال؛ إذ يمكن للفرد تحويل الأموال وتسلُّمها مباشرةً من جواله عبر شبكة شركة اتصالات. ومن الأمثلة على ذلك: إطلاق شركتي «فودافون» و«أورانج» في مصر هذه الخدمات.

فمثلًا، عبر «أورانج كاش» يمكن للفرد تسلُّم/ تحويل الأموال من أي محفظة وإليها، إلى جانب إعادة شحن الرصيد ودفع فاتورة الهاتف، والإنترنت المنزلية، والكهرباء، والمياه، والغاز الطبيعي. يمكنك أيضًا دفع مصروفات المدارس والجامعات، واشتراكات النوادي والنقابات، وأقساط التأمين، وتذاكر السفر والسينما، والتبرُّع لأي منظَّمة غير حكوميَّة. يمكنك أيضًا سداد المدفوعات التجاريَّة باستخدام خاصيَّة رمز الاستجابة السريع عبر تطبيق «أورانج كاش». وتتوافر خدمتا الإيداع والسحب في فروع «أورانج»، وماكينات «فوري»، وماكينات الصراف الآلي.

ويتضمَّن ذلك التعاوُن بين طريقتين من طرق الدفع المحلي، هما: «أورانج كاش» و«فوري» في هذه الحالة.

2.1.2 تزايد طرق الدفع المحلي

عند اللجوء إلى الدفع باستخدام بطاقة أو بطريقة هجين، يتزايد الإقبال على طرق الدفع المحليَّة، التي تكون عن طريق الشبكة أو بطرق دفع جديدة كليًّا، أو بطاقات جديدة قائمة على مشروعات أو أنظمة صُمِّمت لها. ونذكر فيما يلي بعض الأمثلة:

الدفع النقدي/ الطريقة الهجين

«فوري» في مصر: يدفع المستهلك عند الشراء عبر الإنترنت، أو يسدد الفواتير نقدًا، في أكثر من 194500 موقع موزع على 300 مدينة في جميع أنحاء مصر.

البطاقة

«كي - نت» في الكويت: مشروع بطاقات محلي يُتيح للتجار قبول جميع بطاقات الخصم الفوري المحليَّة الصادرة عن المصارف الأعضاء البالغ عددها 11 مصرفًا في الكويت، وتمثل هذه الطريقة 80% من التحويلات عبر الإنترنت في البلاد.

«عمان نت» في عمان: مشروع بطاقات محلي، يعمل بالدفع ببطاقات الخصم الفوري في عمان وبلدان شبكة مجلس التعاون الخليجي، ويغطي جميع بطاقات الخصم الفوري الصادرة عن المصارف المحليَّة العمانية؛ أي 90% من مدفوعات البطاقات في البلاد.

«كيو باي» في قطر: بطاقة رقميَّة صادرة عن المصارف المحليَّة، تُستخدم للدفع عبر الإنترنت.

«مدى» في المملكة العربيَّة السعوديَّة: بطاقة خصم فوري صادرة عن المصارف المحليَّة في السعوديَّة، ويمكن استخدامها للدفع عبر الإنترنت في أكثر من 160 ألف نقطة بيع طرفية، ويوجد ملايين منها في دول العالم عبر شبكات «فيزا» و«ماستر كارد» و«مايسترو». ويبلغ عدد بطاقات «مدى» المتداولة 30 مليون بطاقة.

الصيرفة المتنقلة

«كريم باي» في الإمارات العربيَّة المتَّحدة: خدمة ماليَّة متنقِّلة داخل تطبيق «كريم» يمكن استخدامها لدفع أجرة الرحلات («كريم» أيضًا خدمة أجرة سيارات تشبه «أوبر»)، والمشتريات،

والتوصيل، ولتحويل الرصيد من هاتف إلى آخر.

تتيح الخدمة لكبريات شركات الاتصالات المحليَّة في الشرق الأوسط خدمات مماثلة.

المحفظة الرقميَّة

«بنفت باي» في البحرين: تطبيق يُتيح للمستهلك الدفع عبر الإنترنت عن طريق مسح رمز الاستجابة السريع.

2.1.3 تحوُّل رقمي متنامٍ في منظومة الدفع في بلدان منطقة مجلس وزراء الداخليَّة العرب

من المتوقَّع أن تنمو سوق المدفوعات الرقميَّة في منطقة الشرق الأوسط وشمال إفريقيا بمعدل سنوي مركَّب مقداره 13.3% بين عامي 2021 و2026م. وقد سجَّل قطاع الدفع الرقمي معدلَ نموٍّ عاليًا بوجود مقدِّمي خدمات جدد، ومنصَّات وأدوات دفع جديدة. بالإضافة إلى ذلك، ستؤدِّي إلى زيادة معدل اختراق الهواتف المحمولة والإنترنت لنمو سوق المدفوعات الرقميَّة في المنطقة. ووَفقَ الجمعيَّة الدوليَّة لشبكات الهاتف المحمول[1]، فمن المتوقَّع أن تشهد منطقة الشرق الأوسط وشمال إفريقيا ثاني أسرع معدل لنمو المشتركين بعد منطقة جنوب الصحراء الكبرى. فمن المتوقَّع أن يزداد المعدل من 318 مليون مشترك في خدمات المحمول في 2018م إلى 459 مليون مشترك. وحسب تقديرات البنك الدولي، يملك 75% من سكان قطر، و73% من سكان الإمارات العربيَّة المتَّحدة، و60% من سكان السعوديَّة هواتف محمولة.

علاوةً على ذلك، تنمو خدمات الهاتف المحمول، وتزداد جاذبيَّة المدفوعات غير النقديَّة والخدمات المصرفيَّة الرقميَّة في الشرق الأوسط وشمال إفريقيا.

أحدث اتجاهات السوق

في الشرق الأوسط وشمال إفريقيا، يعرف واحد من بين كل 3 مقدمين لخدمات التحويل عبر الجوال الذين يتيحون تطبيقًا للهواتف الذكيَّة أن 20% أو أكثر من قاعدة العملاء النشطين يحوِّلون

(1) تمثِّل الجمعيَّة الدوليَّة لشبكات الهاتف المحمول مصالح مشغِّلي شبكات الهاتف المحمول حول العالم، وتجمع أكثر من 750 مشغلًا لنحو 400 شركة في منظومة الهواتف المحمولة.

الأموال عبر التطبيق، وأن عددًا متزايدًا من عمليات الإيفاد (IFAD) في الشرق الأوسط يشهد تنفيذ أكثر من نصف المعاملات عبر تطبيقات الهواتف الذكيَّة.

وتشير دراسة استقصائيَّة حديثة، أجرتها «ماستركارد»، إلى احتماليَّة نمو المدفوعات الرقميَّة في الشرق الأوسط بسرعة؛ إذ أفاد أكثر من 70% من المشاركين بأنهم مستعدون لاستخدام الهواتف المحمولة للدفع. وقد يؤثِّر التحوُّل إلى الهواتف بشدة في الاقتصاد؛ فوَفقَ الدراسات، قد يُضاف 95 مليار دولار أمريكي إلى إجمالي الناتج المحلي في الشرق الأوسط بحلول عام 2020م (Mordor Intelligence, 2021).

فضلًا عن ذلك، من المقرر إطلاق شركة التقنيات الماليَّة والخدمات المصرفيَّة الرقميَّة في دبي «جينغل باي» خدمات المحفظة الرقميَّة في الإمارات العربيَّة المتَّحدة عام 2020م (وسيكون الإطلاق خطوة جديدة في المنطقة؛ إذ تتردد بلدان الشرق الأوسط وشمال إفريقيا في السماح لشركات التقنية الماليَّة بأداء دور المصارف). وتعمل الشركة الناشئة على طلب تراخيص في الإمارات العربيَّة المتَّحدة، وإندونيسيا، والفلبين؛ لكون لوائح تلك البلدان لا تسمح حاليًّا لشركات التكنولوجيا الماليَّة بالتحوُّل إلى مصارف. وتهدف الشركة إلى الاستفادة من علامات تجاريَّة ذات قواعد مستهلكين من جيل الألفيَّة وجيل «Z»، الأمر الذي يتطلَّب خدمات سريعة برسوم تحويل زهيدة، ودون قيود، مثل: مطلب الحد الأدنى للرصيد (Mordor Intelligence, 2021).

وعلى نحو مماثل في مارس 2020م، أعلنت «أورانج» المغرب إطلاق «أورانج موني» بعد الحصول على موافقة «بنك المغرب». ومن المتوقَّع أن تسمح هذه الخدمة للشعب المغربي بدفع الأموال وتحويلها عن طريق الهاتف المحمول. جدير بالذكر أن هذه الخدمة متاحة بالفعل في مصر، ويستخدمها كثيرٌ من عملاء الشبكة.

2.1.4 شركات التقنيات الماليَّة وغير المتعاملين مع المصارف

لدى عدد من شعوب البلدان العربيَّة/ الأعضاء في مجلس وزراء الداخليَّة العرب معرفة ضئيلة بأنظمة المصارف، والمصطلحات والعمليَّات الماليَّة. واعترفت شركات التقنيات الماليَّة بحاجتها إلى خدمات مُعدَّة خِصِّيصَى، ويمكن لها أن تعمل في مجال الاستشارات؛ لذا زادت شعبيَّة منصات الإقراض البديلة. يأتي ذلك جنبًا إلى جنب مع التقنيات الحديثة، كالخوارزميَّات، وتعلُّم الآلة وغيرهما، التي تعمل على إيجاد أفضل خطة ممكنة لغير المتعاملين مع المصارف الذين هم بحاجة إلى خطة معدة خِصِّيصَى بأكبر قدر ممكن (Central Bank of Egypt, 2021).

2.1.5 تأثير «كوفيد-19» في سلوكات العملاء والمؤسَّسات الماليَّة

لا شكَّ في تعجيل استخدام طرق الدفع الرقميَّة في خضمِّ جائحة فيروس «كورونا»؛ فمع فرض الإغلاق والقيود حول العالم، اتجه المستهلكون تلقائيًّا إلى الدفع عبر الإنترنت وخدمات التوصيل، بدءًا من البقالة إلى التسوُّق عبر الإنترنت؛ وذلك لاحتياج المستهلك إلى اتباع هذا السلوك في أثناء الجائحة.

وفي حين أن خدمات التوصيل مستقرَّة في الشرق الأوسط، يُطلَب التوصيل عادةً عبر الهاتف، ويُسدَّد الثمن نقدًا على عكس المواقع وطرق الدفع عبر الإنترنت التي تشهد رواجًا. الآن تمثل المنطقة المهيمن عليها الدفع نقدًا فرصة نمو لشركات التقنية؛ إذ يفضِّل المتسوقون عبر الإنترنت الآن استخدام طرق الدفع الرقميَّة (حسب دراسة أجراها موقع Checkout.com، مقدِّم أنظمة الدفع في لندن).

«يستخلص التقرير وجهات النظر المأخوذة من دراسة استقصائيَّة إقليميَّة جمعت أكثر من 5000 مستهلك من الإمارات العربيَّة المتَّحدة، والمملكة العربيَّة السعوديَّة، ومصر، والأردن، وقطر، والكويت، والبحرين، وباكستان. [أظهرت الدراسة أن] 47% من المستهلكين أعربوا عن توقعهم زيادة تسوُّقهم عبر الإنترنت خلال العام التالي، في حين توقَّع 15% فقط منهم تراجُع التسوُّق عبر الإنترنت، بينما توقَّع الـ38% الباقون حفاظهم على نمط التسوُّق ذاته عبر الإنترنت. جدير بالذكر أن هذه الطفرة المتوقَّعة في التجارة الإلكترونيَّة ملحوظة وثابتة في جميع البلدان» (Buller, A., 2020).

وحسب ما ذكره محمد علي يوسف، المدير الإقليمي لموقع Checkout.com، فلقد ساقت الجائحة ولا تزال تسوق «حصة كبيرة» من العملاء إلى التسوُّق عبر الإنترنت، ومن ثَمَّ الدفع بالمعاملات الرقميَّة، وذكر أن الجائحة وراء هذا التغير بنسبة 40%.

وأضاف محمد علي يوسف: «لقد شهدنا هذا التحوُّل المطرد إلى المدفوعات الرقميَّة على مدار السنوات الست الأخيرة، ولكن كانت الجائحة حقًّا بمنزلة عامل محفز حقَّق نموًّا يتطلَّب خمس سنوات في بضعة أشهر. وعلى الرغم من حدوث طفرة مفاجئة في التجارة الإلكترونيَّة والمدفوعات الرقميَّة هذا العام بسبب تأثير (كوفيد 19)، فإن ما نراه اليوم أكثر من مجرد تغيُّر مؤقت في سلوك المستهلك» (Buller, A., 2020).

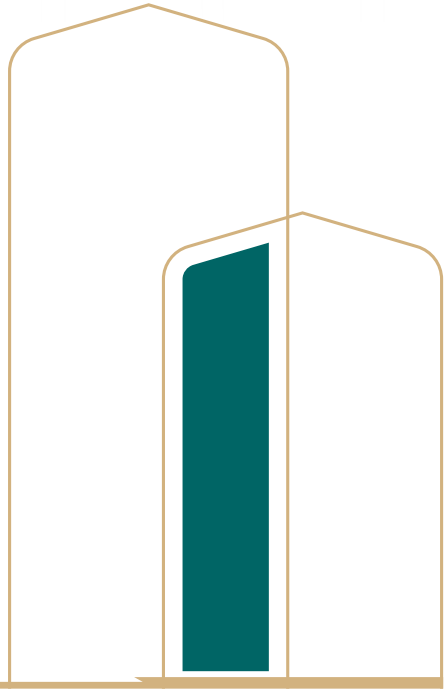
ومع ذلك، لا يزال نظام الدفع عند التسلُّم شائعًا بنسبة كبيرة، لكن السوق تُقدِّم فرصة نمو حقيقيَّة الآن. وحسب ما قاله محمد علي يوسف: «أصبحت خيارات الدفع الرقمي المتينة جزءًا لا يتجزَّأ ممَّا يتوقَّعه المستهلكون من التجار، وبخاصَّةٍ بعد أن أصبحت التجارة الإلكترونيَّة أكثر انتشارًا

في المنطقة»، لا سيَّما أن 62% من الذين يتسوَّقون مرة واحدة في الشهر - على الأقل - عبر الإنترنت، عادةً ما يدفعون بالبطاقة، أو بطرق دفع رقميَّة أخرى.

ومع هذا القول، يجب تقييم التحديات المتعدِّدة، كما يجب تنفيذ جميع التحسينات المطلوبة لإتاحة ازدهار التحوُّل الرقمي بكامل إمكاناته.

ووَفقَ ما ذكره محمد علي يوسف، فـ«لا تزال عمليَّة التجزئة عائقًا رئيسًا أمام نمو قطاع الدفع الرقمي. تُقَسَّم المنطقة على حسب طرق الدفع، والسياسات والأنظمة، والبنية التحتيَّة، وتفضيل المستهلك، وتُجَزَّأ الساحة أيضًا عامَّةً من حيث شركاء الدفع؛ فغالبًا ما يتعيَّن على التجار تطبيق إستراتيجيَّة المدفوعات على مستوى دقيق» (Buller, A., 2020).

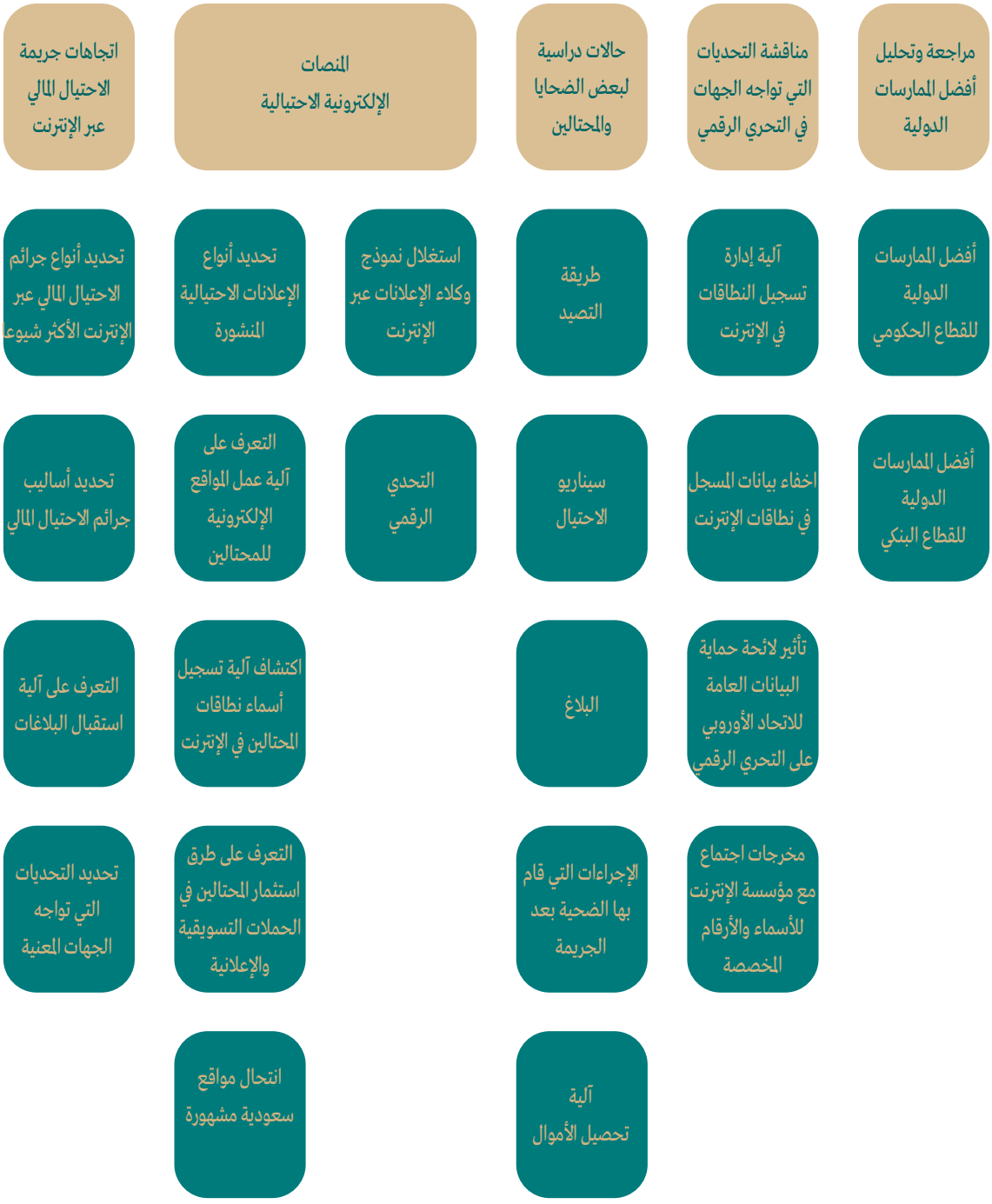
وقد أكَّد «غوراف دهار» - المستثمر العالمي في مجال التكنولوجيا الماليَّة والرئيس التنفيذي لشركة مارشال للمدفوعات بدبي - هذه التحديات، وأشار إلى أن شركات المدفوعات الرقميَّة يجب أن تهتم بالفروق الدقيقة والعميقة في جميع دول الشرق الأوسط، من حيث التركيبة السكانيَّة، والمستهلكين، والاستعداد الرقمي، قائلًا: «يلزم وجود فهم حقيقي لكل فئة بعينها؛ فالأشخاص يتسمون بالتغيير مقارنةً بالمنطقة؛ ففي حين أن حاجز التكنولوجيا وغيره من الحواجز سيختفي في نهاية المطاف، قد يشكِّل انعدام الخبرة الإقليميَّة العميقة عائقًا مستمرًّا أمام نمو المدفوعات الرقمي، ويجب أن يثمر التنسيق والجهود المشتركة بين البلدان عن توفير الوقت والمال» (Buller, A., 2020).



3. مناقشة تحليليَّة متعمِّقة

في هذا الفصل سيُحلَّل الاحتيال المالي ويُناقَش من عدَّة جوانب كما بالشكل التوضيحي رقم «1»، وهي كالآتي:

- مناقشة واقع الاحتيال المالي في مجموعة من الدول العربيَّة للوصول إلى الجرائم الأكثر شيوعًا والأساليب الإجراميَّة والتحديات التي تواجه الجهات المعنيَّة في التعامُل مع جرائم الاحتيال المالي ومعرفة استعداد هذه الدول العربيَّة لمواجهة هذه الجرائم بناءً على مسح عبر الإنترنت أجراه فريق الدراسة.
- مناقشة نتائج عيِّنة الروابط ذات الطابع الاحتيالي التي جُمِعت وحُلِّلت عن طريق مركز الجرائم السيبرانيَّة والأدلَّة الرقميَّة بجامعة نايف العربيَّة للعلوم الأمنيَّة للتعرُّف إلى الطرق التي ينتهجها المحتالون للانتشار عبر الإنترنت وطرق وصولهم إلى الضحايا المحتملين، ومناقشة الطرق التي استغلها المحتالون لإخفاء أثرهم في الإنترنت.
- مناقشة الطرق التي تساعد الجهات المعنيَّة في البحث والتحرِّي للوصول إلى المحتالين وإغلاق مواقعهم على الإنترنت.
- مناقشة حالات دراسيَّة لبعض ضحايا الاحتيال المالي للتحقُّق من أساليب الاصطياد التي تعرَّضوا لها، وكذلك لبعض المحتالين لمعرفة أساليب جمع عائدات الجريمة.
- مناقشة أفضل الممارسات الدوليَّة للحدِّ من جريمة الاحتيال المالي، التي تشمل عدَّة مرتكزات، من أهمها الإستراتيجيَّة الوطنيَّة، وتأسيس نظام استقبال مركزي للبلاغات، وتأسيس مراكز متخصِّصة ومؤهَّلة، وتعقُّب الأصول واعتراض الأموال ونظام إنذار المواقع الاحتياليَّة.



الشكل التوضيحي رقم «1»: مكونات المناقشة التحليليَّة

3.1 اتجاهات جرائم الاحتيال المالي السائدة في الدول العربيَّة

للتعرُّف إلى اتجاهات جرائم الاحتيال المالي في الدول العربيَّة، عُقِد اجتماع مع مجموعة التركيز العرب، التي تضم مجموعة من الممارسين والمختصين العرب وفريق الدراسة المكوَّن من مركز الجرائم السيبرانيَّة والأدلَّة الرقميَّة ومنظَّمة الإنتربول ونُوقِش الآتي:

- ما أنواع الجرائم السيبرانيَّة الأكثر شيوعًا التي جرى الإبلاغ عنها والتصدِّي لها من جانب السلطات؟
- مَن المسؤولون عن التعامُل مع هذه الجرائم (على سبيل المثال: إجراء التحقيقات والتعاون بشأنها)؟
- ما التحديات التي تواجهها السلطات عند التعامُل مع هذه الجرائم؟

وللتعرُّف إلى استعدادات هذه الدول العربيَّة لمواجهة جرائم الاحتيال المالي، أجرى فريق «الإنتربول» مسحًا عبر الإنترنت وراجع آليَّة البلاغات المتوافرة للضحايا عبر الإنترنت.

3.1.1 أنواع جرائم الاحتيال المالي عبر الإنترنت

من أهم الجرائم الماليَّة عبر الإنترنت التي جرى الإبلاغ عنها في الدول العربيَّة:

- الاحتيال في مجال الاستثمارات.
- الاحتيال الرومانسي والابتزاز الجنسي.
- التصيُّد.
- الاحتيال عبر الرسائل النصيَّة.
- البريد الإلكتروني للأعمال.

وبرز الاحتيال المالي في مجال الاستثمارات بسبب كثرة القضايا في عدة دول عربيَّة والاستفادة من طرق الدفع الحديثة للدول العربيَّة. وتمكَّنت وزارة الداخليَّة السعوديَّة من استرجاع مبالغ ماليَّة للضحايا بنسبة تقريبيَّة وصلت إلى 85% على المستوى المحلي. أما على المستوى الخارجي فكانت هناك صعوبات لاسترجاع الأموال المسروقة، وكانت نسبة الاسترجاع منخفضة جدًّا ولا تزيد على 7%. وسجَّلت المملكة المغربيَّة 1480 قضية احتيال في عام 2019م.

3.1.2 الأساليب الإجراميَّة

خلال اجتماع مجموعة التركيز العرب، رُصِد 23 أسلوبًا إجراميًّا للاحتيال المالي موجَّهة للأفراد والشركات. ويتضح أن أغلب الأساليب الإجراميَّة استهدفت الأفراد بعدَّة طرق مختلفة.

الأساليب الإجراميَّة التي تستهدف الشركات

تركَّزت طرق استهداف الشركات باستخدام البرمجيَّات الخبيثة للحصول على فدية، وقد انتشرت هذه الجرائم منذ عام 2017م، والبريد الإلكتروني للأعمال، وكذلك معرفة المحتال بتفاصيل الشحنة وبيانات المستفيد مسبقًا وإرسال روابط نصيَّة محتالة لتصيُّد الضحايا المحتملين. ومن الأساليب الإجراميَّة يُخترَق البريد الإلكتروني للموردين، ومن ثَمَّ ينتحل المخترقون شخصيَّة إحدى المؤسسات التي يكون للضحيَّة المستهدف تعاقدات فعليَّة معها للحصول على الأموال.

الأساليب الإجراميَّة التي تستهدف الأفراد

رُصِدت عدة طرق للاحتيال التي تستهدف الأفراد، من أهمها:

1- اتفق الغالبية على أن أكثر الأساليب الاحتياليَّة شيوعًا هي استخدام المواقع الموثوقة لنشر الإعلانات الاحتياليَّة/ التصيُّد الإلكتروني. ويهدف هذا الأسلوب إلى استدراج الضحايا المحتملين للمواقع الاحتياليَّة، ومن ثَمَّ جمع المعلومات الشخصيَّة والتواصُل المباشر مع الضحيَّة عبر الهاتف الجوال أو البريد الإلكتروني، أو عبرهما معًا. وتركَّزت هذه الإعلانات تركُّزًا كبيرًا في الاستثمارات الوهميَّة في الأسهم والعملات والمعادن. ومن ضمن الإعلانات: الإعلان عن وظائف؛ حيث كشفت وزارة الداخليَّة السعوديَّة عن شبكتين إجراميتين إحداهما مكونة من 6 مقيمين من الجنسيتين الباكستانيَّة والهنديَّة على ارتباط بشخصين آخرين خارج المملكة، والأخرى مكونة من 4 مقيمين من بنجلاديش وفَّرت وسائل الاتصال وشرائحه، نفَّذوا عمليَّات احتيال تمثَّلت في الإعلان عن وظائف وإجراء مقابلات شخصيَّة عبر الاتصال المرئي، واستدراج الضحايا بالحصول على معلوماتهم الشخصيَّة والبنكيَّة، مكَّنتهم من الحصول على قروض تمويليّة بأسمائهم. وتخطَّت المبالغ التي استولوا عليها 1.5 مليون ريال سعودي، وضُبط بحوزتهم 40 ألف ريال ومصوغات ذهبية و4800 شريحة اتصال محليَّة (وكالة الأنباء السعوديَّة، 2021م).

2- برز في المملكة العربيَّة السعوديَّة أحد أساليب التصيُّد الإلكتروني، وهو تزوير المواقع والتطبيقات الحكوميَّة، ورُصدت مجموعة من التطبيقات الحكوميَّة المزوَّرة في متجر «جوجل»، هي: منصات «فُرجت» و«جود» و«أبشر»، وحُمِّلت هذه التطبيقات المزوَّرة في حدود 14 ألف مرة.

3- ذكر أحد المختصين في البنوك أن هناك طرقًا حديثة بدأت في الظهور، هي: استخدام العملات المشفَّرة لمحاولة إخفاء تتبُّع عائدات الجريمة واقتفاء أثرها خارج حدود الدولة. ويتم ذلك بتحويل عائدات الجريمة/ الأموال إلى المحتال عبر العملات الرقميَّة المشفَّرة، ويطلب المحتال من صاحب الحساب الوسيط شراء عملات رقميَّة من شخص عبر «تليجرام» وتحويلها إلى محفظته الرقميَّة. ورُصِدت مجموعة من الحسابات في «تليجرام» تسوِّق لبيع العملات النقديَّة المشفَّرة.

4- طلب تحديث البيانات البنكيَّة كان من القضايا الأبرز. وذكرت إحدى الصحف السعوديَّة أن وزارة الداخليَّة في السعوديَّة قبضت على 24 مقيمًا من الجنسيَّة الباكستانيَّة امتهنوا ارتكاب 16 ألف عملية احتيال استولوا من خلالها على مبالغ ماليَّة تجاوزت 35 مليون ريال، من خلال استهداف المواطنين والمقيمين بإرسال رسائل نصيَّة تتضمَّن ادعاءات وهميَّة، كالفوز بجوائز ماليَّة أو طلب تحديث البيانات البنكيَّة، وبعد الإفصاح وتزويد المحتالين تُنفَّذ عمليَّات ماليَّة (صحيفة سبق، 2021م).

5- استخدام المحتالين برامج Inbox Mass Mailer التي تتيح لهم إرسال آلاف الرسائل إلى الضحايا. ويُوجَّه الضحيَّة إلى تطبيق يطلب منه معلومات سريَّة. ويبيع المحتالون هذه المعلومات في الشبكة المظلمة (Dark Web). واستُخدِم هذا الأسلوب في مصر عندما استخدم المحتالون اسم بنك في مصر (البنك التجاري الدولي - CIB) وأرسلوا رسائل بريد إلكتروني ونماذج للعملاء.

6- يتصل المحتال بالضحيَّة، ويوضح له أنه ينتمي إلى إحدى الشركات المعروفة، ويُخبر الضحيَّة أنه سيتلقَّى كلمة مرور لمرة واحدة (OTP) في صورة رسالة قصيرة، وعندما يتلقَّى الضحيَّة كلمة المرور تلك يظن أن المكالمة الهاتفيَّة قانونيَّة. ويزوِّدهم بالرقم السري الذي وصل إلى جواله المسجل في البنك. وبعد ذلك يتم الدخول إلى حسابه.

ويوضح الجدول رقم «1» أهم أساليب الاحتيال المالي التي نُوقِشت خلال اجتماع مجموعة التركيز.

الجدول رقم «1»: أهم أساليب الاحتيال المالي التي نُوقِشت خلال اجتماع مجموعة التركيز

الأساليب الإجراميَّة	الأفراد	الشركات
استخدام المواقع الموثوقة لنشر الإعلانات الاحتياليَّة	✓	
تزوير المواقع الحكوميَّة	✓	✓
الدخول غير المشروع على تطبيق «واتساب»	✓	
الاحتيال عن طريق البريد إلكتروني للأعمال		✓
تعاوُن أشخاص داخل الدولة مع أشخاص خارج الدولة لإتمام عمليَّات الاحتيال	✓	
استغلال الأفراد الذين ليس لديهم محافظ إلكترونيَّة في منصات بيع العملات الرقميَّة المشفَّرة وشرائها، وبيع العملات لهم بسعر أعلى	✓	
معرفة المحتال بتفاصيل الشحنة وبيانات المستفيد سابقًا وإرسال رابط مزيَّف لتسلُّم الأموال	✓	✓
انتحال الشخصيَّة الاعتباريَّة للجهات الخاصَّة بإرسال روابط نصيَّة محتالة لتصيُّد الضحايا	✓	
انتحال الشخصيَّة الاعتباريَّة للجهات الخاصَّة بالتواصُل الهاتفي ثم إرسال روابط محتالة لتصيُّد الضحايا	✓	
تقديم عروض احتياليَّة عبر المواقع الإلكترونيَّة للتسويق لبيع برامج وألعاب إلكترونيَّة	✓	
تقديم عروض وإغراءات احتياليَّة محدودة خلال ساعات للدفع عبر روابط احتياليَّة	✓	
عرض مساعدة فنيَّة لحل المشكلات التقنية عن طريق روابط محتالة للدخول غير المشروع	✓	✓
إرسال رسائل نصيَّة محتالة لطلب تحديث البيانات البنكيَّة	✓	
تقديم جوائز وهميَّة عن طريق البريد الإلكتروني للضحايا	✓	
نقل الأموال إلى المحتال عبر العملات الرقميَّة المشفَّرة، ويطلب المحتال من صاحب الحساب الوسيط شراء عملات رقميَّة من شخص عبر «تليجرام» وتحويلها إلى محفظته الرقميَّة	✓	
إنشاء حسابات وهميَّة للأعمال الخيريَّة	✓	
إنشاء مواقع وهميَّة لتقديم وجبات سريعة	✓	
قرصنة حساب البريد الإلكتروني وتوجيه رسائل للأصدقاء لطلب مساعدة ماديَّة عاجلة	✓	
تقديم خدمات وهميَّة عن طريق مواقع التواصُل الاجتماعي ومواقع الإنترنت	✓	
تقديم خصومات كبيرة وهميَّة عبر مواقع إلكترونيَّة	✓	
استخدام البرمجيَّات الخبيثة للحصول على فدية		✓
استخدام وسطاء ماليين لإخفاء عائدات الجريمة/ أموال ضحايا الاحتيال المالي، عبر تحويل أموالهم بين حسابات الوسطاء في البنوك	✓	✓
استخدام هواتف لأشخاص آخرين لإجراء اتصال أو إرسال رسالة نصيَّة لضحايا تحتوي على روابط احتياليَّة دون علمهم	✓	
استخدام شرائح تحمل أسماء وهميَّة	✓	

3.1.3 آليَّة استقبال البلاغات وإجراءاتها

بعد أن يقع المواطن أو المقيم ضحيةً لجريمة الاحتيال المالي، تبدأ إجراءات تقديم بلاغ للجهات المعنيَّة. وجرى خلال اجتماع مجموعة التركيز التعرُّف إلى جهات استقبال البلاغات في الدول الست. ويتضح أن هناك تفاوتًا في الجهات المخوَّلة باستقبال بلاغات الاحتيال المالي في الدول العربيَّة. في السعوديَّة ومصر ينتهجون الأسلوب ذاته في عمليَّة استقبال بلاغات الاحتيال من الضحايا عن طريق جهات إنفاذ القانون والبنوك. أما في الإمارات العربيَّة المتَّحدة والكويت فهناك طريقة واحدة لتقديم البلاغات، وهي عن طريق جهات إنفاذ القانون.

في المغرب، تُستقبَل بلاغات الاحتيال المالي عن طريق جهتي إنفاذ القانون والنيابة العامَّة. وتفرَّدت موريتانيا باستقبال بلاغات الاحتيال عن طريق النيابة العامَّة فقط. ويوضِّح الجدول رقم «2» جهات استقبال البلاغات في بعض الدول العربيَّة.

الجدول رقم «2»: جهات استقبال البلاغات في بعض الدول العربيَّة

الدول	جهات استقبال البلاغات في الدول العربيَّة		
	إنفاذ القانون	النيابة العامَّة	البنوك
الإمارات	X		
السعوديَّة	X		X
مصر	X		X
موريتانيا		X	
المغرب	X	X	
الكويت	X		

الإمارات العربيَّة المتَّحدة

بعد تسلُّم البلاغات من جهات إنفاذ القانون، تجمع وحدة الأدلَّة الرقميَّة الأدلَّة وترفع تقريرًا كاملًا عنها. ويستغرق إعداد التقرير التقني 15 يومًا تقريبًا، لا سيَّما عندما يكون التحقيق متعلقًا بعمليَّات احتيال عبر الهاتف، بينما يُعدُّ في وقت أسرع من ذلك في حالات الاحتيال الأخرى.

المملكة العربيَّة السعوديَّة

هناك خطوات يتبعها الضحيَّة لإبلاغ الشرطة عن قضية الاحتيال، هي:

- يبلِّغ الضحايا الشرطة التي تبدأ في إجراء تحقيقاتها بعد الحصول على موافقة النيابة (وهذا يستغرق من 4 إلى 5 أيام). أو يُقدَّم البلاغ عن طريق تطبيق «كلنا أمن».
- تتصل الشرطة بالمصارف المركزيَّة طالبةً الحصول على مزيدٍ من المعلومات، وهذا الإجراء يستغرق عدة أيام.
- بعد تحديد هُوية المجرم والتوصُّل إلى أنه موجود داخل المملكة العربيَّة السعوديَّة يجري الآتي:

- تحويل القضية إلى السلطة المسؤولة عن المنطقة من أجل إلقاء القبض عليه، وَفقًا للمادة 107 من النظام.

- في حالة وجود المجرم في منطقة أخرى في المملكة، تستغرق عملية تحديد هُويته وقتًا أطول.

- بالنسبة للمجرمين الموجودين خارج المملكة العربيَّة السعوديَّة، تتم الإجراءات عبر المنظَّمة الدوليَّة للشرطة الجنائيَّة (INTERPOL).
- سوف يبلِّغ العميلُ/ الضحيَّةُ المصرفَ والشرطةَ بما حدث، بعدها يزوِّد المصرفَ برقم بلاغ الشرطة، ويرسل المصرفُ المعلومات مباشرةً إلى الشرطة باستخدام الرقم دون الانتظار حتى تتصل الشرطة به.

البنوك السعوديَّة

بالنسبة للبنوك السعوديَّة فقد صدر نظام لمكافحة الرسائل الخادعة في عام 2020م، يمنح المؤسَّسات الماليَّة صلاحيتين للحصول على عائدات الجريمة، هما:

- إمكانية تجميد حسابَي المجرم والضحيَّة بوصفه إجراءً وقائيًّا.
- إمكانية أن تطلب البنوك من بنوك أخرى تجميد حسابٍ ما بعد تزويدها بأدلَّة قويَّة.

في المملكة العربيَّة السعوديَّة، كانت المؤسَّسات الماليَّة ذات سلطة محدودة.. ومنذ عام 2020م، وفي ظل زيادة وتيرة عمليَّات الاحتيال، أصبح للمؤسَّسات الماليَّة دور أكبر؛ فالبنوك في المملكة العربيَّة السعوديَّة أصبحت لديها فرق عمل قادرة على الإيقاع بالمجرمين، من خلال التعاون مع خدمات البنوك التجاريَّة في المملكة العربيَّة السعوديَّة عبر حملات توعية لبيان طرق العمل التي يلجأ إليها المجرمون.

التجميد الوقائي

بعد إجراء تحقيق داخلي، يجري التجميد الوقائي مباشرةً للحساب من جانب البنك ونشر المعلومات للبنوك الأخرى. أو بناءً على نصيحة ما، يُجمَّد الحساب لمدة 3 أيام من أجل إجراء تحقيق. وترد توصيات النيابة العامَّة بشأن هذا الموضوع في خلال 3 أسابيع لاتباع وسائل التواصُل التقليديَّة. أما فيما بين المصارف، فإن الإجراءات تكون أسرع بكثير؛ لأن جميعها يجري عبر الإنترنت.

الكويت

يجري الإبلاغ عن طريق جهات إنفاذ القانون. في حالة وجود المتهم/ المشتبه به في الكويت، فمن السهل الوصول إليه، حيث تمتلك الوحدات المتخصِّصة القدرة على تحديد هُوية المجرمين من خلال بطاقة تحديد هوية المشترك (SIM) أو من خلال تتبُّع التحويلات المصرفيَّة الخاصَّة بهم.

وتُخزَّن القضايا والمعلومات - مثل بروتوكول الإنترنت (IP) والمنفذ (Port) والرقم التسلسلي (Serial number) - في قواعد بيانات التحليل الجنائي الخاصَّة لمدة تصل إلى 6 شهور، ما يساعد في تحديد قضايا جنائيَّة أخرى من خلال الربط بين الأدلَّة التي جُمِعت. ويمكن أن تتعاون المصارف مع وحدات الشرطة الوطنيَّة في حالة وجود تعاون دولي، وتقدم الدعم والمعلومات الخاصَّة بعنوان بروتوكول الإنترنت (IP) وتحظر التطبيق المصرفي. ويجري أيضًا التعاون مع المنظَّمة الدوليَّة للشرطة الجنائيَّة (INTERPOL) لتتبُّع أصحاب الرسائل الخادعة على المستوى الدولي.

علاوةً على ذلك، بمقدور موظفي التحقيقات طلب معلومات استخباراتيَّة من الشركات المالكة لوسائل التواصُل الاجتماعي متعلِّقة بالصفحات الشخصيَّة للمجرمين على الإنترنت، ويجري الطلب بموجب طلبات رسميَّة قضائيَّة.

مصر

يجري الإبلاغ في جمهورية مصر العربيَّة عن طريق الآتي:

- مكاتب النيابة العامَّة، الشؤون الماليَّة والتجاريَّة.
- البنوك.

وبعد ذلك، تنتقل القضايا إلى وحدة مكافحة الاحتيال، لتتولَّى التحقيق في القضيَّة الجنائيَّة.

ولا تزال الإدارة الموجودة في البنك المركزي المصري جديدة ومحدودة النطاق. من ناحية أخرى، في عام 2020م سُنَّ قانون جديد يفعِّل التشريع المتعلِّق بالتقنيات الجديدة.

المغرب

بمقدور الضحيَّة التوجُّه إلى مكتب النيابة العامَّة أو قسم الشرطة أو المصرف لتجميد بطاقة الصراف الآلي الخاصَّة به وغيرها.

وفي خلال عملية التحقيق، تكون المعامل المتخصِّصة في جرائم الاحتيال الإلكتروني مسؤولة عن التحرِّي عن الهواتف والأرقام المستخدَمة، وتحديد الموقع وَفقًا للنظام العالمي لتحديد المواقع (GPS) من خلال الهاتف والشركة المشغِّلة.

موريتانيا

أُنشئت الهيئة التي تتعامل هذه الأنواع من الجرائم في عام 2004م. ويُحقَّق في القضية وتُحوَّل إلى مكتب النيابة العامَّة ومنها إلى مكتب خاص بها، هذا المكتب الخاص مسؤول عن تحويل الأموال إلى الضحايا في النهاية.

يُعد البنك المركزي الموريتاني مسؤولًا عن المعلومات والتعاوُن مع السلطة القضائيَّة.

لجنة ثلاثيَّة موريتانيَّة

تجتمع هذه اللجنة، التي تضم أعضاء ممثلين للنيابة العامَّة والبنك المركزي ووكالات إنفاذ القانون، لبحث قضايا الاحتيال، ويحدث التعاوُن والتواصل عبر البريد الإلكتروني في حالة وجود أمر عاجل يتطلَّب ذلك.

وهناك تعاون جيد بين السلطات المختلفة في الدولة، يتم خلال مدة تتراوح بين يومين وثلاثة أيام.

ويوضِّح الجدول رقم «3» آليَّة تقديم البلاغات في بعض الدول العربيَّة.

الجدول رقم «3»: آليَّة تقديم البلاغات في بعض الدول العربيَّة

الدول	آليَّة تقديم البلاغات			
	الاتصال برقم موحد	موقع إلكتروني	الحضور إلى الجهات المعنيَّة	النقطة الذكيَّة
الإمارات	X	X	X	X
السعوديَّة	X	X	X	
مصر	X	X		
موريتانيا			X	
المغرب			X	
الكويت			X	

3.1.4 المصادر والآليَّات الإلكترونيَّة لإبلاغ الشرطة ووكالة إنفاذ القانون

أجرى فريق الدراسة مسحًا عبر الإنترنت لمعرفة آليَّات البلاغات الإلكترونيَّة المتاحة لضحايا الاحتيال الإلكتروني بعد وقوعهم في الجريمة ومدى سرعة التجاوُب مع هذه الجرائم. وعند رصد آليَّات البلاغات الإلكترونيَّة للدول العربيَّة، اتضح وجود فوارق مهمَّة بين أعضاء الدول العربيَّة فيما يتعلق باستعدادها لمواجهة الجرائم الماليَّة عبر الإنترنت.

في حين طوَّرت بعض الدول العربيَّة، وبخاصَّةٍ دول مجلس التعاون الخليجي، وسائل استقبال البلاغات الإلكترونيَّة لتسهيل وصول الضحايا إلى جهات إنفاذ القانون، وخصَّصت وسائل للإبلاغ عن هذا النوع من الجرائم، وعيَّنت بعض فرق العمل والوحدات لتولِّي مسؤوليَّة هذه الجرائم. إلا أنَّ بعض الدول العربيَّة لا توجد لديها أيٌّ من هذه الاستعدادات حتى إعداد هذه الدراسة. وفي الواقع، يُعد الإبلاغ عن الجرائم من خلال آليَّات الإبلاغ عبر الإنترنت أمرًا صعبًا أو يكاد يكون مستحيلًا في بعض البلدان؛ فبعض المواقع الإلكترونيَّة لا تعمل، بينما يصعب العثور على مواقع أخرى أو تصفُّحها.

ويؤدي عدم وجود طرق فعَّالة وسهلة للإبلاغ عن الجريمة إلى حدوث تأخير في التعامُل مع الجرائم، وقد يحول ذلك دون استرداد الأصول/ الأموال المسروقة. وتُعد حالات التأخير أهم التحديات التي تتعلَّق بالجرائم الماليَّة عبر الإنترنت، التي يرتكبها المجرمون للحصول على أموال الضحايا، وينقلونها بسرعة من خلال المنصات الرقميَّة وعبر الإنترنت. وهنا يكمن استغلال المحتالين لطرق الدفع الحديثة للدول العربيَّة التي انتهجتها مؤخرًا.

3.1.5 التحديات التي تواجه الجهات في التعامُل مع الاحتيال المالي

تُعتبر الجرائم الماليَّة من الجرائم المنظَّمة العابرة للحدود؛ لذا يشكل التعاوُن على المستويين الإقليمي والدولي تحديًا يواجه الدول العربيَّة يخصُّ تبادل المعلومات، وهناك دول لا تتعاون في تبادُل المعلومات، وإن كان هناك تعاون ثنائي بين الدول تتسم عملية تبادُل المعلومات بالبطء. وهناك دول عربيَّة تعاني ضعف تبادُل المعلومات بسبب اللغة.

وعلى المستوى المحلي، تتسم الإجراءات بين الجهات داخل الدولة بالبطء أيضًا؛ حيث تحتاج جهات إنفاذ القانون إلى الحصول على موافقة النيابة العامَّة للبدء في إجراءات التحقيق والحصول على معلومات من البنوك، وهذا يستغرق وقتًا طويلًا يصل في بعض الأحيان إلى أسابيع أو أشهر لاستخدامها وسائل تواصل تقليديَّة وعدم استغلال وسائل التواصُل الحديثة، وكذلك صعوبة تبادُل المعلومات.

إن المحتالين مبتكرون دائمًا؛ فهناك أساليب إجراميَّة مستجدة ومتغيِّرة باستمرار، وهناك عدة طرق للتواصل مع الضحايا عبر الهاتف، على سبيل المثال: عندما يؤدِّي استخدامُ أرقام دوليَّة إلى شعور الضحايا بشكوك تجاهها، يستخدم المحتالون أرقامًا محليَّة لرفع مستوى الثقة لدى الضحيَّة. وهناك تحدٍّ آخر هو استخدام شرائح اتصال تحمل أسماء وهميَّة محليَّة يستخدمها المحتالون للتواصُل مع الضحايا. وأعلنت شرطة منطقة الرياض، بالمملكة العربيَّة السعوديَّة، عن القبض على 3 مواطنين و3 مقيمين من الجنسيَّة المصرية، ومقيم من الجنسيَّة الهندية، وآخر من الجنسيَّة الباكستانية، لتنفيذهم 100 عملية نصب واحتيال عبر منصات إلكترونيَّة تنتحل صفة هيئات ماليَّة وحكوميَّة تُدار من خارج المملكة، وعملوا على بثِّ رسائل وإعلانات وهميَّة للاستثمار والتداوُل وتعاونوا مع المتهمين في الخارج بتأمين 1300 شريحة اتصال بأسماء وهميَّة (وكالة الأنباء السعوديَّة، 2021م).

وعند استخدام المحتالين أرقامًا دوليَّة يمكن إيقافها من جانب شركات الاتصال المحليَّة، لكن التحدي يظل مستمرًّا عندما يستخدم المحتالون تطبيق «واتساب» للتواصُل مع الضحايا ومن ثَمَّ يبتعد المحتالون عن رقابة الجهات المختصَّة ولا يمكن تتبعها وتعقبها من الجهات المختصة.

وهناك تحدٍّ برز مؤخرًا، هو ثقة بعض أفراد المجتمع في المحتالين وجهلهم بالأساليب والسيناريوهات المختلفة للاحتيال، من صورها: استخدام المحتالين هواتف وأرقامًا تخص شخصًا لا يرتكب أي مخالفات قانونيَّة لإرسال الرسائل الاحتياليَّة، ربما تتوصَّل التحقيقات للقبض على ذلك الشخص الذي لا توجد بينه وبين التنظيم الإجرامي أي صلة.

ويُعتبر عزوف بعض الضحايا عن الإبلاغ عن قضايا الاحتيال من أهم التحديات، لا سيَّما في حالات الابتزاز والرسائل الرومانسيَّة الخادعة خوفًا من تشويه السمعة.

ويعتبر تعقُّب الأصول/ الأموال واستردادها أمرًا معقدًا؛ نظرًا لأن المحتالين يستغلون طرق الدفع السريعة التي توفرها البنوك في تحويل الأموال إلى عدَّة حسابات مصرفيَّة ثم يسحبونها نقدًا من خلال أجهزة الصراف الآلي للحيلولة دون إمكانية تتبُّعها، أو إعادة إيداعها في حسابات أخرى، وتُستخدم أيضًا مَحافِظ إلكترونيَّة. وفي الوقت ذاته يستغل المحتالون بطء الإجراءات القانونيَّة في الحصول على المعلومات وتبادلها محليًّا وخارجيًّا. وهو ما يجعلنا نسلِّط الضوء على أفضل الممارسات الدوليَّة لتعقب الأصول واعتراض الأموال ومعايير مجموعة العمل المالي (فاتف) التي تدعم عمل جهات إنفاذ القانون لتسهيل عمليَّات تبادل المعلومات، ما يُسهم في سرعة تعقُّب الأصول واعتراض الأموال.

ومن ضمن التحديات: عدم تطوير وكالات إنفاذ القانون وسائل التحري لديها لتواكب تطوُّر الأساليب الإجراميَّة المتسارعة.

في بعض الدول العربيَّة، لا تتخذ وكالات إنفاذ القانون الإجراءات الضرورية بالكامل للحفاظ على الأدلَّة الرقميَّة التي حُصِل عليها من الإنترنت، ما يجعل من الصعب اعتراف هيئة المحكمة بها.

ويمكن تقسيم التحديات التي جُمِعت خلال مجموعة التركيز إلى خمسة تحديات: تقنية، وإجرائيَّة، وتوعويَّة، وقانونيَّة، وتعاون دولي بين الدول، كما هو موضَّح في الجدول رقم «4».

الجدول رقم «4»: أنواع التحديات التي تواجه الدول العربيَّة

التحديات	تقنية	إجرائيَّة	توعويَّة	قانونيَّة	تعاون دولي
استخدام رقم هاتف دولي في عمليَّات الاحتيال	✓				
استخدام أرقام هواتف تعود ملكيتها إلى أشخاص غادروا الدولة أو وهميَّة		✓			
استخدام هواتف أشخاص آخرين بوصفها أداة لاصطياد ضحايا آخرين ومحاولة إخفاء مسرح الجريمة الافتراضي والأدلَّة الرقميَّة لتعقُّب المحتالين			✓		
عدم تعاون بعض الدول في توفير البيانات أو مشاركتها، كمعلومات بعض النطاقات وعناوين الإنترنت... إلخ					✓
صعوبة الحصول على معلومات عن المحتالين أو ضبطهم في حالة عدم وجود اتفاقيَّات بين الدول				✓	
بطء التواصُل بين الجهات المعنيَّة لتبادل المعلومات		✓			
استغراق وقت طويل في الإجراءات الإداريَّة في التحريات والتحقيق		✓			
عدم وجود الإمكانات والقدرات والمهارات لتتبُّع العملات الرقميَّة المشفَّرة وغياب الرقابة على شراء العملات والمنصات	✓				
قصور الجهات المعنيَّة في توعية المواطنين، خصوصًا كبار السن، بطرق الاحتيال المتعددة			✓		
عدم وجود ربط بين البلاغات المتلقاة بالاحتيال المالي للتعرُّف إلى الأساليب الإجراميَّة المرتكبة	✓				
عدم إمكانية استرجاع الأموال التي تُحوَّل خارج الدولة				✓	✓
عدم إمكانية تتبُّع عمليَّات الاحتيال التي تتم في الإنترنت المظلمة (Deep Web)	✓				
عدم تعاوُن بعض الضحايا ورفضهم التبليغ			✓		
عدم تعاوُن شركات التواصُل ومزوِّدي خدمات الإنترنت في الدول الأخرى				✓	
صعوبة تعقُّب الهجمات الخارجيَّة لاستخدام عناوين إلكترونيَّة تخص أشخاصًا آخرين	✓				
قصور في الإطار القانوني الخاص بالجرائم الإلكترونيَّة				✓	
قصور البنوك في متابعة أنماط الاحتيال المتعدِّدة (الهندسة الاجتماعيَّة) التي تُستخدم من قِبَل المحتالين لمحاولة استباقها وتوعية عملائها	✓				
عدم وجود تشريع يُلزم جهات الاتصال بالاحتفاظ بالبيانات لمدة أطول		✓			
نقص في تأهيل جهات التحرِّي والتحقيق للتعرُّف إلى أنماط جرائم الاحتيال المالي وأساليبها	✓				
عدم توافر التقنيات الحديثة والبرامج التي تساعد في مكافحة الاحتيال المالي	✓				
الرسائل أو الروابط الاحتياليَّة من خارج الدولة	✓			✓	✓
الضحايا لا يوثقون عملية الاحتيال لإثبات الشكوى (screen shot)			✓		

3.1.6 خلاصة نتائج اجتماع مجموعة التركيز

استطاع فريقُ الدراسة الحصولَ على نتائج مهمَّة من اجتماع مجموعة التركيز، تمثَّلت في تحديد أنواع جرائم الاحتيال المالي الأكثر شيوعًا في الدول الست، وهي: الاحتيال في مجال الاستثمار، والاحتيال الرومانسي والابتزاز الجنسي، والاحتيال عبر الرسائل النصيَّة، والبريد الإلكتروني للأعمال. وتمثل هذه الجرائم هاجسًا كبيرًا للجهات الأمنيَّة في الدول العربيَّة، وبخاصَّةٍ الاحتيال في مجال الاستثمار لاستهداف شرائح متعددة في المجتمع. ويظل المحتالون يبتكرون أساليب متعددة لتصيُّد الضحايا واستهداف الأفراد والشركات، وصلت إلى 24 أسلوبًا إجراميًّا، واستدراج الضحايا لمواقعهم المحتالة والحصول على عوائد من جرائم الاحتيال وإخفاء أثر تعقُّب عوائد جرائم الاحتيال. ولوحظ استغلال المحتالين العملات المشفَّرة كالبيتكوين لإخفاء تعقُّب أثر عائدات جرائم الاحتيال المالي عن طريق استخدام أساليب دفع إلكترونيَّة متعدِّدة وسريعة يصعب تعقُّبها كشراء بطاقات تسوُّق، مثل: بطاقات «ريزر جولد» (Razer Gold) التي تُدفع قيمتها عن طريق بطاقة «مدى» أو بطاقة ائتمانيَّة أو «Apple Pay» أو «باي بال». واستغل المحتالون التطوُّر الكبير للدول العربيَّة عامَّةً والخليجيَّة خاصَّةً في الدفع الإلكتروني وانتعاش التجارة الإلكترونيَّة وتوافُر فرص الاستثمار وكذلك فتح الحسابات البنكيَّة عبر الإنترنت خلال جائحة «كورونا».

ورُصِد 22 تحديًا، متمثلًا في الجوانب التقنية والإجرائيَّة والتوعويَّة والقانونيَّة والتعاون الدولي، يواجه جهات إنفاذ القانون، والنيابة العامَّة، والمؤسَّسات الماليَّة. ولكن من أهم التحديات الكبيرة التي تواجه المنظومة الأمنيَّة والعدليَّة في التعامُل مع هذا النوع من الجرائم: البطء الشديد في الإجراءات الجزائيَّة بين الجهات المعنيَّة، كالحصول على موافقة النيابة العامَّة والتواصُل مع البنوك لتتبُّع عائدات الجريمة وتبادُل المعلومات. وهذا البطء لا يتواكب مُطلقًا مع القفزات الكبيرة في مجالات الاقتصاد والتنمية التي تشهدها الدول العربيَّة عامَّةً والخليجيَّة خاصَّةً، وقد يخلق عدم ثقة بالتجارة الإلكترونيَّة؛ لذا فهناك ضعف كبير في تحصيل عوائد جرائم الاحتيال التي تتجه خارج حدود الدول على الرغم من أن توصيات مجموعة العمل المالي (فاتف) تحثُّ على تسريع تبادُل البيانات مع الجهات الأمنيَّة.

وكما جرى التنويه سابقًا، فهناك تفاوُت بين الدول في الاستعداد للتعامُل مع جرائم الاحتيال المالي من حيث آليَّات استقبال البلاغات، وسرعة التجاوُب، واسترجاع الأموال. ولاحظ فريق الدراسة عدم وجود مراكز متخصِّصة للتعامُل مع الاحتيال المالي عبر الإنترنت تُسهِم في عمليَّة تسهيل التواصُل بين الجهات المعنيَّة داخل الدولة (إنفاذ القانون، والنيابة العامَّة، والبنوك) وخارج الدولة؛ حيث إنَّ أغلب عائدات الاحتيال المالي تتجه إلى خارج الحدود.

3.2 المنصَّات الإلكترونيَّة الاحتياليَّة (نتائج عيِّنة الروابط ذات الطابع الاحتيالي)

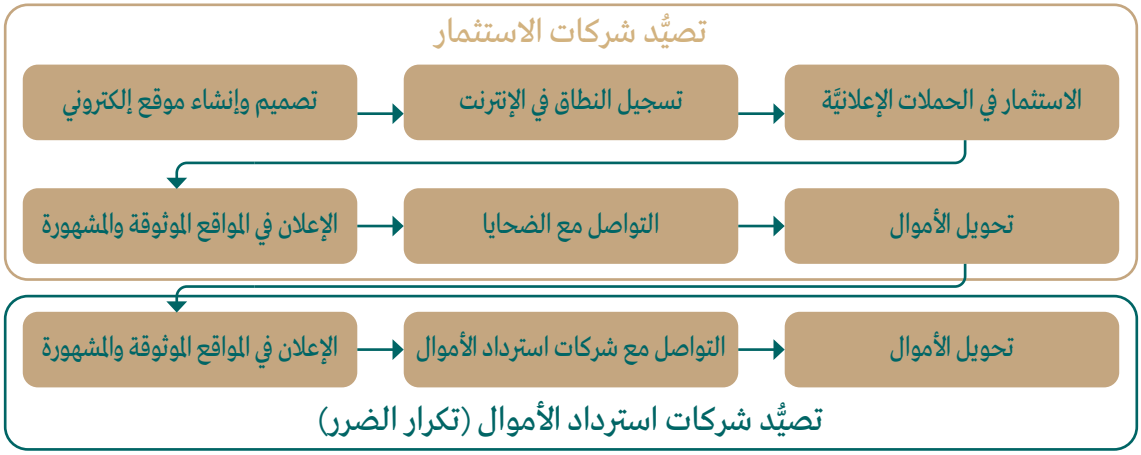
نظرًا للانتشار الكبير والملحوظ في استخدام المواقع الموثوقة لنشر الإعلانات الاحتياليَّة في مجالات الاستثمارات الوهميَّة، رصد مركز الجرائم السيبرانيَّة والأدلَّة الرقميَّة 503 إعلانات احتياليَّة، ووصل عدد زيارات هذه النطاقات الاحتياليَّة إلى 137 ألف زيارة يوميَّة. وجرى التركيز في هذه الدراسة على التعرُّف إلى الأسباب التي أدَّت إلى انتشار المنصَّات الإلكترونيَّة للمحتالين واكتشاف الطرق التي ينتهجونها للانتشار على الإنترنت وطرق وصولهم إلى الضحايا المحتملين. واتضح من التحليل ما يلي:

3.2.1 أنوع الإعلانات الاحتياليَّة المنشورة

عند تحليل الإعلانات الاحتياليَّة، يتضح أن هناك نوعين رئيسين من الإعلانات، هما:

- إعلانات احتياليَّة استثماريَّة، وهي تحاول التدليس على الضحايا للاستثمار في هذه الشركات الوهميَّة.
- إعلانات لشركات استشارات قانونيَّة لاسترداد الأموال، وهذه الشركات تتصيَّد الضحايا الذين كانوا ضحايا للإعلانات الاحتياليَّة الاستثماريَّة.

وتكمن الخطورة في تكرار الضرر على الضحايا؛ فقد يلجأ الضحايا إلى شركات الاستشارات القانونيَّة المحتالة لمحاولة استرجاع أموالهم المنهوبة من شركات الاحتيال الاستثماريَّة، لكنهم قد يقعون ضحايا لجريمة احتيال ثانية وتزداد خسائرهم الماليَّة ومعاناتهم النفسية. ويبيِّن الشكل التوضيحي رقم «2» الفرق بين تصيُّد شركات الاستثمار الوهميَّة عبر الإنترنت وإمكانيَّة تكرار الضرر على الضحيَّة عند وقوعه ضحيةَ تصيُّد لشركات استرجاع الأموال.



الشكل التوضيحي رقم «2»: الفرق بين تصيُّد شركات الاستثمار الوهميَّة عبر الإنترنت وإمكانيَّة تكرار الضرر على الضحيَّة عند وقوعه ضحيةَ تصيُّد لشركات استرداد الأموال

3.2.2 نطاق عمل المواقع الإلكترونيَّة للمحتالين

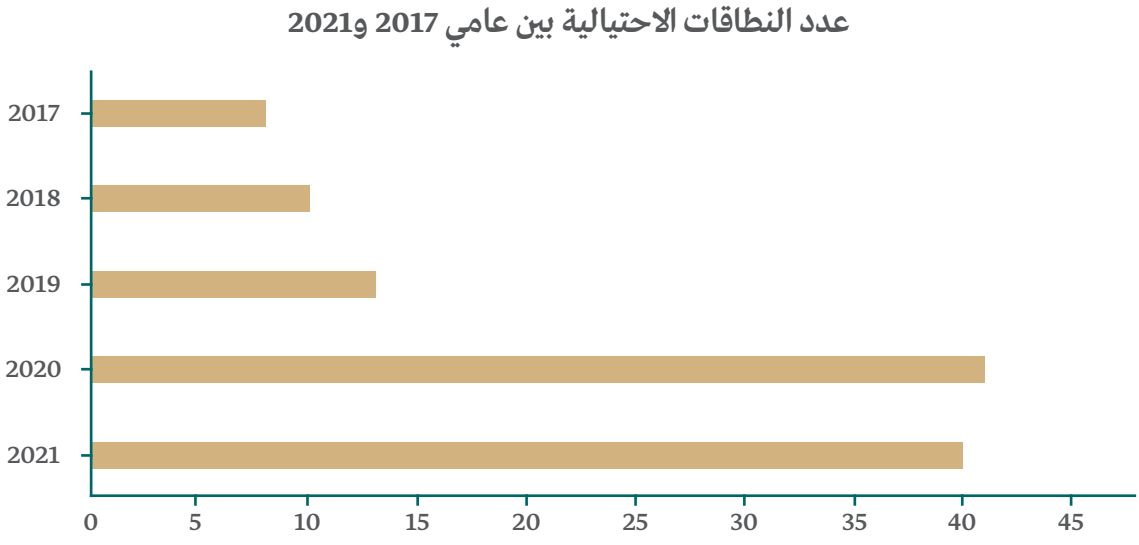
يُنشئ المحتالون موقعًا إلكترونيًّا لنشاطهم الوهمي ويسوِّقون له، مثل ما يلي:

شركة وساطة ماليَّة تسمح للعميل بالمضاربة في الأسواق الماليَّة العالميَّة كشراء أو بيع العملات الرقميَّة وأسهم الشركات الأمريكيَّة والمضاربة في السلع والعملات النقديَّة، تُوهِم الضحايا بأنَّ دورها فتح محافظ استثماريَّة وتقديم نصائح استثماريَّة والمحافظة على رأسمال الضحيَّة.

شركة قانونيَّة تقدِّم خدمة استرداد الأموال من الشركات المحتالة.

3.2.3 تسجيل النطاقات الاحتياليَّة عبر الإنترنت

عند تحليل النطاقات الاحتياليَّة، نجد أنه في خلال خمس سنوات سُجِّل 112 نطاقًا احتياليًّا. ويتضح ازدياد عدد النطاقات الاحتياليَّة في عامي 2020 و2021 بتسجيل 36% في كلٍّ منهما. وسجل أقل عدد نطاقات في عام 2017م بنسبة 7%. ويتزامن ازدياد نسبة تسجيل النطاقات الاحتياليَّة مع جائحة «كوفيد 19». ويبيِّن الشكل التوضيحي رقم «3» أعداد تسجيل النطاقات الاحتيالية عبر الإنترنت بين عامي 2017 و2021م.



الشكل التوضيحي رقم «3»: عدد تسجيل النطاقات الاحتياليَّة بين عامي 2017 و2021م

3.2.4 آليَّة تسجيل أسماء نطاقات المحتالين في الإنترنت

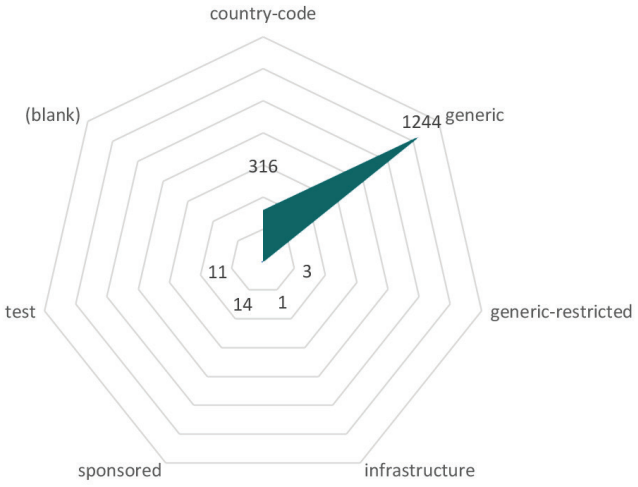
بعد تصميم المواقع الاحتياليَّة وإنشائها، يحتاج المحتال إلى التسجيل في نطاق الإنترنت حتى يستطيع اصطياد الضحيَّة والإيقاع به؛ لذا سنركِّز هنا على كيفيَّة تسجيل المحتال لنطاق في الإنترنت، عن طريق:

- وكلاء تسجيل أسماء النطاقات للمواقع المحتالة.
- أسماء النطاقات العلويَّة التي يستغلها المحتالون.

وكلاء التسجيل

يستخدم وكلاء التسجيل نموذجًا يُعرف باسم «Registrar Model»، وهو من الممارسات الدوليَّة المهمَّة في مجال أسماء النطاقات، ويتيح تقديم خدمات تسجيل أسماء النطاقات من قِبَل وكلاء معتمدين. ويسمح هذا النموذج لوكيل التسجيل أيضًا بدمج خدمات التسجيل مع خدمات أخرى وتقديمها للمسجلين والعملاء، مثل الاستضافة والبريد الإلكتروني من خلال منصَّة موحَّدة.

وحسب «IANA» توجد خمسة أنواع لنطاقات المستوى الأعلى: country-code وgeneric وgeneric-restricted وinfrastructure وsponsored وtest. وإجمالي النطاقات 1589 نطاقًا، كما في الشكل التوضيحي رقم «4».



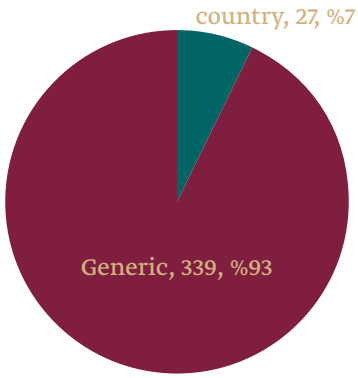
الشكل التوضيحي رقم «4»: أنواع وإجمالي نطاقات المستوى الأعلى في الإنترنت

3.2.5 نطاقات المستوى الأعلى الذي يستغلُّه المحتالون

عند تحليل النطاقات التي يستغل فيها المحتالون الخدمات المقدَّمة من وكلاء تسجيل أسماء النطاقات، اتضح أن المحتالين يركِّزون على النطاقين التاليين:

- نطاقات المستوى الأعلى العامَّة (Generic TLDs) بنسبة 93%.
- نطاقات المستوى الأعلى لرمز الدولة (Country code) بنسبة 7%.

ويبيِّن الشكل التوضيحي رقم «5» هذه النسب.



الشكل التوضيحي رقم «5»: نسبة نطاقات المستوى الأعلى في الإنترنت

نطاقات المستوى الأعلى العامَّة التي استغلها المحتالون

تقع مسؤوليَّة إدارة نطاقات المستوى الأعلى العامَّة على القطاعات غير الحكوميَّة المكوَّنة من ثلاثة أحرف لاتينيّة. ومن التحليل يتضح أن المحتالين استغلوا 366 اسمًا من عدة نطاقات (.COM, .NET, .ORG, .Online) وشكلت ثلاثة نطاقات نسبة 94% من استخدام إجمالي النطاقات، هي:

.COM

تدير «VeriSign Global Registry Services» جميع النطاقات المسجلة في النطاق الأعلى العام لـ«.com» وهو يرمز للمواقع التجاريَّة، وهو اختصار لكلمة «تجاري» (commercial)، ويعتبر من أشهر نطاقات الإنترنت. ووصل إجمالي عدد المسجلين في هذا النطاق إلى 154.6 مليون على مستوى العالم (VERSIGIN, 2021).

ويشير التحليل، من الروابط المحتالة التي جُمِعت، إلى أن عدد النطاقات المسجلة من قِبَل المحتالين في «com.» هو الأعلى بـ292 نطاقًا بنسبة 86% من إجمالي النطاقات المستخدمة من قِبَل المحتالين. ومن أهم الشركات المحتالة التي تستخدم هذا النطاق: lp.axiainvestments.com، ويزور موقعها أكثر من 8000 زائر يوميًّا، وسجلت في النطاق بتاريخ 27/3/2019م. ومن شركات الاستشارات القانونيَّة لاسترداد الأموال التي سجلت في نطاق «com.» شركة alqasim - lawyer. com، وسجلت في نطاق الإنترنت بتاريخ 8/6/2020م، ووصل عدد الزيارات إلى 2600 زيارة يوميًّا.

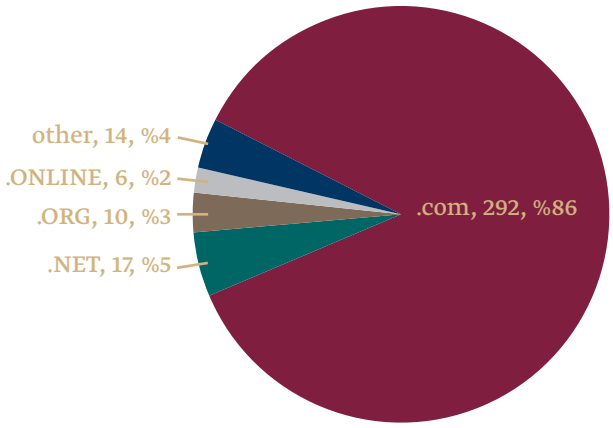
.NET

تدير شركة VeriSign Global Registry Services»» أشهر نطاقات الإنترنت، من ضمنها جميع النطاقات المسجلة في النطاق الأعلى العام لـ«net.»، ويرمز للمنظَّمات ذات العلاقة بالشبكات (Network). ووصل عدد المسجلين في هذا النطاق إلى 13 مليونًا على مستوى العالم (VERSIGIN, 2021). ويشير تحليل الروابط الاحتياليَّة إلى أن عدد النطاقات المسجَّلة من قِبَل المحتالين في «net.» 17 نطاقًا بنسبة 5% من إجمالي النطاقات المستخدمة من المحتالين. ومن أهم الشركات المحتالة التي رُصِدت والتي تستخدم هذا النطاق: news500.net، ويزور موقعها أكثر من 4500 زائر يوميًّا، وسجلت في النطاق بتاريخ 27/6/2019م. وكذلك mashreiq.net التي تستخدم صور شخصيات اعتبارية لإغواء الضحايا بالاستثمار، ويزوره في اليوم نحو 200 زائر، وسُجِّل في تاريخ 16/6/2021م.

.ORG

يُدار «org.» بواسطة مؤسَّسة Public Interest Registry (PIR) غير الهادفة للربح، وهي منظَّمة تتمثَّل مهمتها في دعم جمعيَّة الإنترنت (ISOC) غير الهادفة للربح. ويُستخدم «org.» للمنظَّمات غير الربحيَّة والشركات والجمعيَّات المهنيَّة والمجموعات المدنيَّة. وقد وصل عدد المسجلين في هذا النطاق إلى 10.4 مليون على مستوى العالم (VERSIGIN, 2021).

ويُشير التحليل إلى أن عدد النطاقات المسجلة من قِبَل المحتالين في «org.» وصل إلى 6 نطاقات بنسبة 2%. ومن أهم الشركات المحتالة التي رُصِدت والتي تستخدم هذا النطاق forex.ae.org، ويزور موقعها أكثر من 1800 زائر يوميًّا، وسجلت في النطاق بتاريخ 8/10/2019م. ويبيِّن الشكل التوضيحي رقم «6» نسبة نطاقات المستوى الأعلى العامَّة المستخدمة من المحتالين.



الشكل التوضيحي رقم «6»: نسبة نطاقات المستوى الأعلى العامَّة المستخدمة من المحتالين

يتضح من تحليل الروابط أن المحتالين يتركزون في النطاق العلوي «.com» بنسبة 86% و«.net» بنسبة 5% من إجمالي النطاقات (339) ويدير هذين النطاقين شركة «VeriSign Global Registry Services»، المزوِّد العالمي لخدمات تسجيل النطاقات والبنية التحتيَّة للإنترنت.

نطاق المستوى الأعلى لرمز الدول (Country Code TLD) التي استغلها المحتالون

النطاق الأعلى في ترميز الدول هو نطاق يتبع دولةً ما أو منطقةً ما.

تتولَّى الدول إدارة خدمات تسجيل أسماء النطاقات وتنظيمها ضمن النطاقات العلويَّة للدول، ومنها النطاق العلوي بالأحرف اللاتينيَّة، على سبيل المثال: «.UK» هو امتداد خاص بالعناوين الإلكترونيَّة للمواقع التي تنتمي إلى المملكة المتَّحدة، و«.ME» هو امتداد خاص بالعناوين الإلكترونيَّة للمواقع التي تنتمي إلى مونتينيغرو/ الجبل الأسود.

وتهدف خدمات التسجيل إلى تمكين المستخدم من اختيار اسم النطاق الخاص به بناءً على اللوائح والتنظيمات الخاصَّة بأسماء النطاقات للدول ومن ثَمَّ تسجيله وإدارته.

وخلال تحليل الروابط، لوحظ أن المحتالين يستغلون نطاقات المستوى الأعلى الذي يتبع الدول. ووصل عدد نطاقات الدول المستخدمة من قِبَل المحتالين إلى 7% من إجمالي النطاقات الاحتياليَّة التي رُصِدت. ويتضح أن المحتالين يستغلون أسماء النطاقات التابعة لدول كولومبيا والمملكة المتَّحدة حسب ما هو موضَّح في الجدول رقم «5».

الجدول رقم «5»: نطاقات المستوى الأعلى للدول، المستغلة من المحتالين

م	الدولة	Country	عدد النطاقات
1	جزيرة الكريسماس - أستراليا	Christmas Island	1
2	كولومبيا	Colombia	9
3	مونتينيغرو/ الجبل الأسود	Montenegro	3
4	توكلو	Tokelau	1
6	المملكة المتَّحدة	United Kingdom	5

من النطاقات المحتالة التي رُصِدت واستغلت تسجيل أسماء نطاقات الدول: نطاق .offer sabtradings.co.uk، وسجل في النطاق الخاص بالمملكة المتَّحدة، ورقم الإنترنت الخاص بالموقع 172.67.152.156، ووصل عدد الزيارات اليوميَّة لهذا الموقع إلى 21400 زيارة، وتاريخ تسجيل النطاق للموقع 2021/4/19م عن طريق وكيل التسجيل (Namecheap Inc).

وكذلك نطاق شركة الجديد (aljadded.me)، وسجل في النطاق الخاص بدولة مونتينيغرو/ الجبل الأسود، ورقم الإنترنت الخاص بالموقع 142.93.174.168، ووصل عدد الزيارات اليوميَّة لهذا الموقع المحتال إلى 2700 زيارة، وتاريخ تسجيل النطاق للموقع المحتال 2021/4/13م، وتحت استضافة Namecheap Inc.

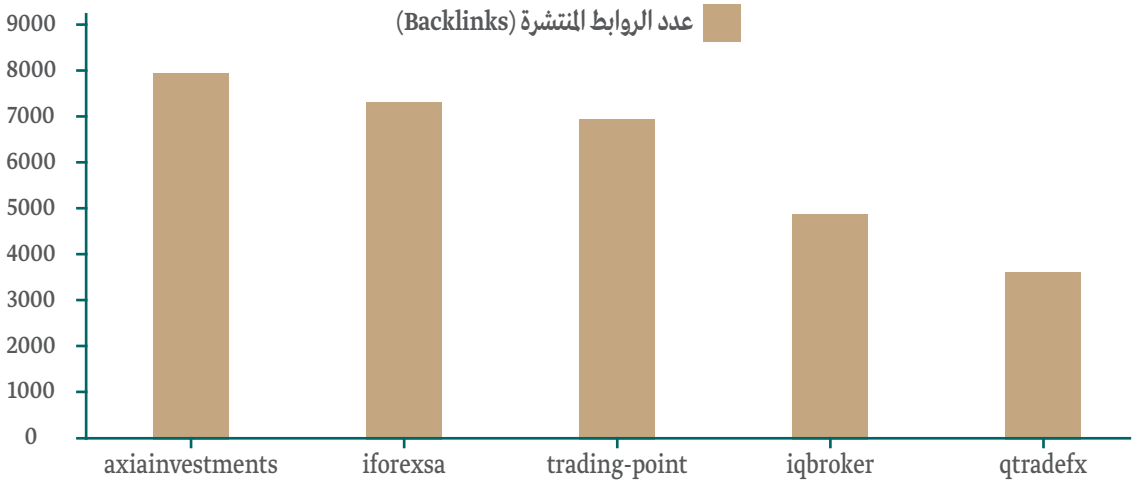
ولوحظ أن شركات الاستشارات القانونيَّة لاسترداد الأموال تسجل في النطاقات الخاصَّة بالمملكة المتَّحدة، حيث سجلت ثلاث شركات لاسترداد الأموال في النطاق من إجمالي خمس شركات مسجلة فيه. ومن ضمنها شركة capital - lawyer.co.uk برقم إنترنت 88.218.117.137، وسجلت في نطاق الإنترنت بتاريخ 2020/8/16م، ووصل عدد الزيارات إلى 200 زيارة يوميَّة.

3.2.6 التعرُّف إلى استثمار المحتالين في الحملات التسويقيَّة والإعلانيَّة

بعد بناء الموقع الإلكتروني واختيار اسم نطاق للموقع المحتال، ينتقل المحتال إلى مرحلة اختيار آليَّة للوصول إلى الضحايا للمحتملين، فما الآليَّة التي يتبعها المحتالون لتصيُّد الضحايا؟

يستثمر المحتالون في التوسُّع في نشر مواقعهم الاحتياليَّة عبر الإنترنت بطريقة تُوهم الضحايا بأن مواقعهم موثوقة وآمنة. واتضح خلال رصد أسماء النطاقات المحتالة وتحليلها أن أعلى خمس شركات محتالة نشرت في حدود 40 ألف رابط، كما في الشكل التوضيحي رقم «7»، وهي:

- نشرت أكسيا للاستثمار (axiainvestments.com) أكثر من 8000 رابط عبر الإنترنت.
- نشرت آي فوركس (iforexsa.com) في حدود 7400 رابط عبر الإنترنت.
- نشرت تريدنغ بوينت (trading - point.com) في حدود 7000 رابط على الإنترنت، وحجبت هيئةُ الاتصالات وتقنية المعلومات بالمملكة العربيَّة السعوديَّة هذا الموقع.
- نشرت آي كيو بروكور (iqbroker.com) في حدود 4900 رابط على الإنترنت، وحجبت هيئةُ الاتصالات وتقنية المعلومات بالمملكة العربيَّة السعوديَّة هذا الموقع.
- نشرت كيو ترايد إف إكس (qtradefx.com/public/application/index/index) في حدود 3600 رابط عبر الإنترنت، وحجبت هيئةُ الاتصالات وتقنية المعلومات بالمملكة العربيَّة السعوديَّة هذا الموقع.



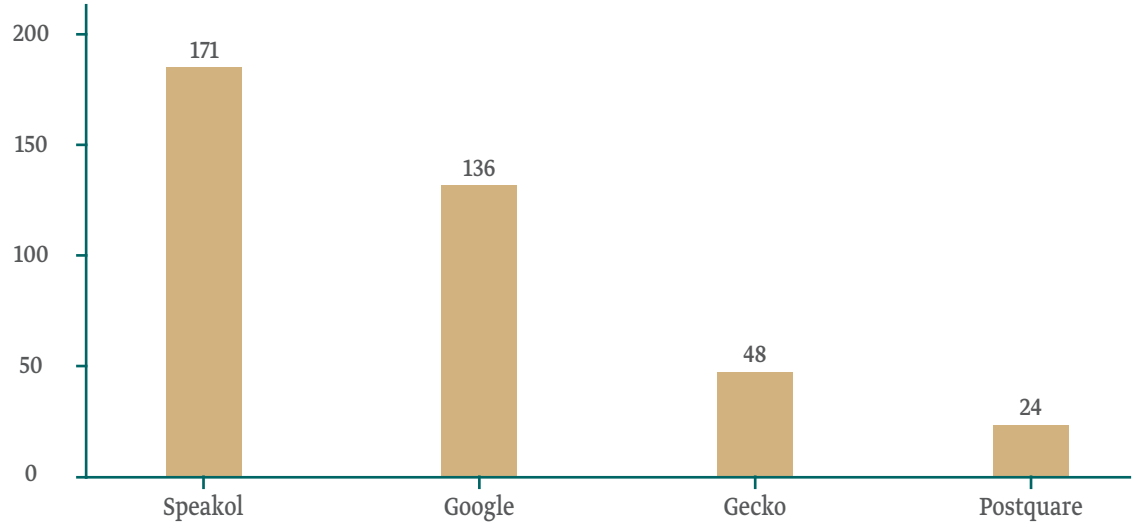
الشكل التوضيحي رقم «7»: قائمة أعلى خمس شركات محتالة نشرت روابط عبر الإنترنت

ومن أشهر الأساليب التي ينتهجها المحتالون للتسويق والإعلان للوصول إلى فئات الضحايا المحتملين وتحقيق أعلى نسب انتشار وأرباح ما يلي:

الإعلان عن طريق وكيل إعلاني عبر الإنترنت

يقدِّم الوكيل الإعلاني الإعلانات الذكيَّة في منطقةٍ جغرافيَّةٍ ما تعتمد على التقنيات الحديثة، حيث تمكِّن الناشرين (المواقع المشهورة) أو المعلنين (المحتالين) من زيادة معدَّل تفاعل الزائرين والربح من محتوى المواقع الإلكترونيَّة في إطار مساعدة المعلنين على استهداف عملاء جدد والترويج لمنتجاتهم. ويتم ذلك عن طريق الحصول على مساحة إعلانيَّة مخصَّصة في المواقع المشهورة والمعروفة لعرض إعلانات الشركات ومن ضمنها شركات الوساطة الماليَّة المحتالة.

ومن التحليل، اتضح استغلال المحتالين الخدمات والمزايا التي يقدِّمها وكلاء الإعلانات للوصول إلى مواقع مشهورة وموثوقة على المستوى العربي. وسيُعرض أعلى عدد إعلانات احتياليَّة نُشِرت عن طريق وكلاء الإعلانات كما هو مبيَّن في الشكل التوضيحي رقم «8»، وهي كالآتي:



الشكل التوضيحي رقم «8»: أعلى عدد إعلانات احتياليَّة نُشِرت من وكلاء الإعلانات «سبيكول» (Speakol)

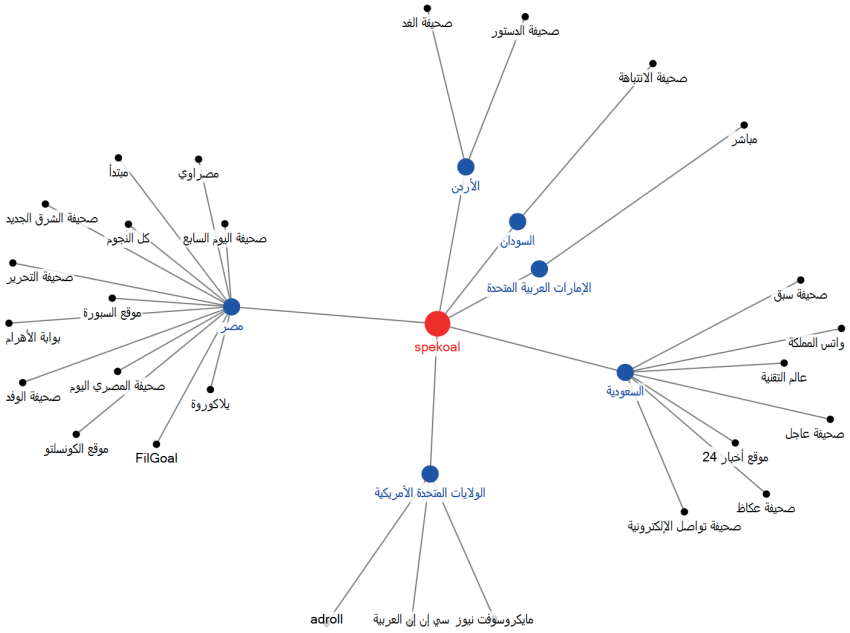
تركز «سبيكول» في صناعة الإعلانات الذكيَّة في الخليج والشرق الأوسط. وحسب موقع إحصاءات الشركة، تنشر شركة «سبيكول» الإعلانات في 296 موقعًا إلكترونيًّا.

وتصدرت شركة «سبيكول» قائمة وكلاء الإعلانات؛ حيث رُصِد 171 إعلانًا احتياليًّا من إجمالي 503 إعلانات.

ويبيِّن الشكل التوضيحي رقم «9» أن شركة «سبيكول» تنتشر في الدول العربيَّة: في مصر في حدود 13 موقعًا إلكترونيًّا، من ضمنها مواقع معروفة ومشهورة، كصحيفتي التحرير واليوم السابع وبوابة الأهرام ومصراوي ويلاكورة. وفي المملكة العربيَّة السعوديَّة حضرت وكالة الإعلان «سبيكول» في عدة مواقع معروفة ومشهورة كصحيفة سبق، وصحيفة عكاظ، وصحيفة عاجل، وصحيفة تواصُل الإلكترونيَّة، وعالم التقنية. ولم تخلُ المواقع الإلكترونيَّة الأمريكية المشهورة من وجود شركة «سبيكول» في موقع مايكروسوفت نيوز (MSN) وسي إن إن العربيَّة. وحسب موقع «سبيكول» فقد وصل إجمالي مشاهدات جميع الإعلانات المنشورة في المواقع إلى مليار مشاهدة. ومن أهم الشركات المحتالة التي تعلن في شركة «سبيكول»: كابيتال جينيوس (alarabiyaalnas.com) ويزور الموقع أكثر من 9000 زائر يوميًّا، وسجلت في النطاق عن طريق شركة Namecheap Inc بتاريخ 11/14/2019م. ونشرت في موقع مباشر وصحيفة اليوم السابع.

ومن شركات الاستشارات القانونيَّة لاسترداد الأموال التي تعلن في شركة «سبيكول»: شركة capital - lawyer.co.uk، ووصل عدد الزيارات، كما ذُكِر سابقًا، إلى 200 زيارة يوميًّا، ونشرت في موقع مصراوي وصحيفة تواصُل الإلكترونيَّة وموقع مباشر.

ويبيِّن الشكل التوضيحي رقم «9» خريطة انتشار الإعلانات الاحتياليَّة عبر مساحات إعلانيَّة لشركة «سبيكول» على أهم المواقع الإلكترونيَّة العربيَّة والدوليَّة، ما يُسهِم في إضفاء المصداقيَّة والموثوقيَّة على هذه الإعلانات الاحتياليَّة التي تهدف إلى التصيُّد الإلكتروني.



الشكل التوضيحي رقم «9»: خريطة انتشار الإعلانات الاحتياليَّة عبر الإنترنت عن طريق شركة «سبيكول» الإعلانيَّة

«جوجل» (Google)

تمتلك «جوجل» شبكة ضخمة للإعلانات تتمثَّل في شبكة البحث، والمواقع الإلكترونيَّة والمدونات، ومنصة «يوتيوب» وتطبيقات الجوال. وتنقسم شبكة «جوجل» إلى مجموعتين رئيستين تمنحان مزيدًا من التحكُّم في تحديد المكان الذي ترغب في ظهور الإعلان فيه، كما في الجدول رقم «6».

الجدول رقم «6»: المجموعتان الرئيستان لشبكة «جوجل» الإعلانيَّة

شبكة البحث	الشبكة الإعلانيَّة
- بحث «جوجل» والمشتريات والخرائط	– يُعرض الإعلان في مواقع «جوجل» و«YouTube» والمدونات والبريد الإلكتروني، إلى جانب الآلاف من مواقع الإنترنت الشريكة
- المواقع الإلكترونيَّة المعنيَّة بالبحث التي دخلت في شراكة مع «جوجل»	

عندما يبحث المستخدم على Google.com عن شيءٍ ما يظهر له نوعان من النتائج: نتائج البحث، والإعلانات. وتظهر نتائج البحث في صورة روابط في صفحات نتائج البحث، وهي تشكل جزءًا من «جوجل» الإعلانيَّة، أما الإعلانات فتظهر تحت تصنيف الإعلانات، وقد تُعرَض في عدة مواضع حول نتائج البحث المجانيَّة.

أنواع الإعلانات على شبكة البحث في «جوجل»:

- الإعلانات النصيَّة والإعلانات الديناميكيَّة على شبكة البحث وإعلانات الاتصال فقط

تعتبر أكثر أنواع الإعلانات مع تصنيف «إعلان» أو «إعلانات» على صفحة نتائج البحث، وقد تحمل تصنيف «إعلانات Google» على مواقع الشركاء.

- الإعلانات المصورة وإعلانات الفيديو

يمكن لشركاء البحث استضافة الإعلانات المصوَّرة وإعلانات الفيديو.

وتُرتَّب الإعلانات استنادًا إلى تركيبة من عرض السعر الأقصى للنقرة للمجموعة الإعلانيَّة بالكامل ومدى الصلة بموضوع البحث.

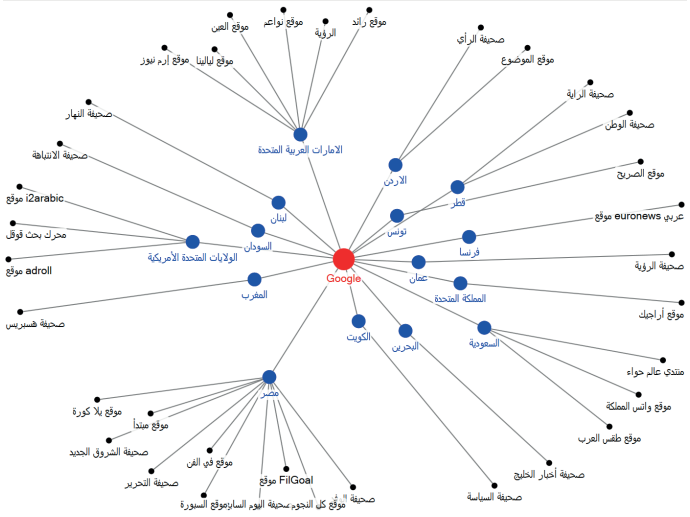
استغلال المحتالين لشبكة «جوجل» الإعلانيَّة

يتضح من الرصد أن المحتالين استغلوا شبكة «جوجل» للوصول إلى الضحايا المحتملين عن طريق Google Ads. فقد رُصِد 136 إعلانًا من 503 إعلانات احتياليَّة باستخدام الأساليب التالية:

- الإعلان في صفحة Google.com عن طريق محركات البحث في «جوجل». ورُصِد 74 إعلانًا من إجمالي 136 إعلانًا. ورُصِدت مجموعة من المواقع ترتكب جرائم معلوماتيَّة بانتحال مواقع صحف سعوديَّة، على سبيل المثال: انتحال شعار صحيفة الرياض السعوديَّة من موقع lp.eraplanetz.com، ويحمل رقم إنترنت 35.213.190.144، وسجلت في نطاق الإنترنت عن طريق GoDaddy.com LLC بتاريخ 2019/4/16م ويزور الموقع في حدود 200 زائر، الشكل التوضيحي رقم «10» يبيِّن انتحال صحيفة الرياض السعوديَّة وفبركة موضوعات لاستدراج الضحايا وتصيُّدهم وجمع معلوماتهم الشخصيَّة.

- رُصِدت إعلانات احتياليَّة موجَّهة للفئات العمرية أكثر وأقل من 18 عامًا لتصيُّد الضحايا من قِبَل الموقع الاحتيالي akhbarona.club الذي يحمل عنوان إنترنت 107.180.56.147 ومسجل في نطاق الإنترنت عن طريق GoDaddy.com LCC بتاريخ 9/9/2019م ويزور الموقع في حدود 200 زائر يوميًّا.
- وكذلك رُصِد استخدام صور لشخصيات اقتصاديَّة مؤثرة على مستوى الشرق الأوسط.
- الإعلان في المواقع الإلكترونيَّة، وتحصل «جوجل» على مساحة إعلانيَّة في المواقع المشهورة والمعروفة (الناشر) لعرض المحتوى الإعلاني، وتُستغل من الشركات المشبوهة. ورُصِد 62 إعلانًا من 136 إعلانًا بـGoogle Ads. ورُصِد انتشار المساحات الإعلانيَّة لشركة «جوجل» في المواقع الإلكترونيَّة لعدة دول عربيَّة وأجنبيَّة كموقع «يورونيوز» العربيَّة وصحيفة الرّأي وصحيفة الرؤية وصحيفة «هسبريس» ولبنان 24 وصحيفة بوابة الأهرام وصحيفة اليوم السابع وموقع يلاكورة.

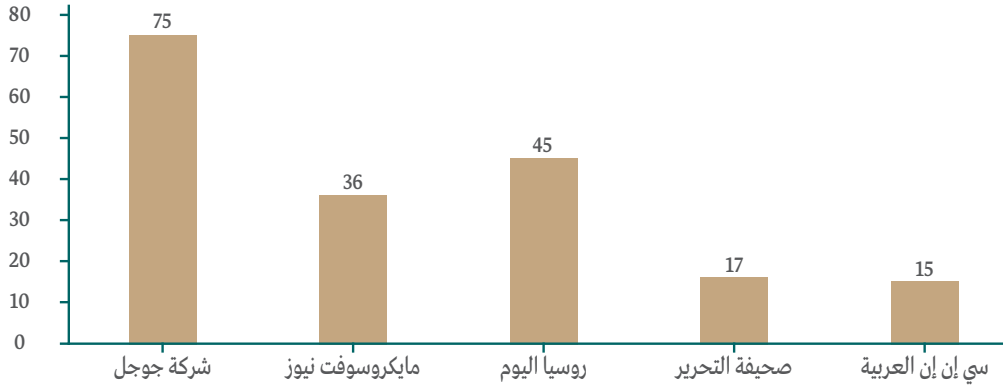
ويبيّن الشكل التوضيحي رقم «12» خريطةً لانتشار الإعلانات الاحتياليَّة عبر مساحات إعلانيَّة لشبكة «جوجل» الإعلانيَّة على أهم المواقع الإلكترونيَّة العربيَّة والدوليَّة، ما أسهم في إضفاء المصداقيَّة والموثوقيَّة على هذه الإعلانات الاحتياليَّة التي تهدف إلى التصيُّد الإلكتروني.



الشكل التوضيحي رقم «12»: خريطة انتشار الإعلانات الاحتياليَّة عبر الإنترنت عن طريق شبكة «جوجل» الإعلانيَّة

- الإعلان في منصة «يوتيوب» عن طريق الإعلان في مقاطع الفيديو الأكثر مشاهدة، ورُصِد إعلان لشركة arba7- news التي تحمل عنوان إنترنت 31.220.54.249 والمسجلة في الإنترنت بتاريخ 29/11/2020م، في حساب أحد المطربين في «يوتيوب» لإحدى أشهر أغانيه التي وصل عدد مشاهداتها إلى أكثر من 11 مليون مشاهدة.

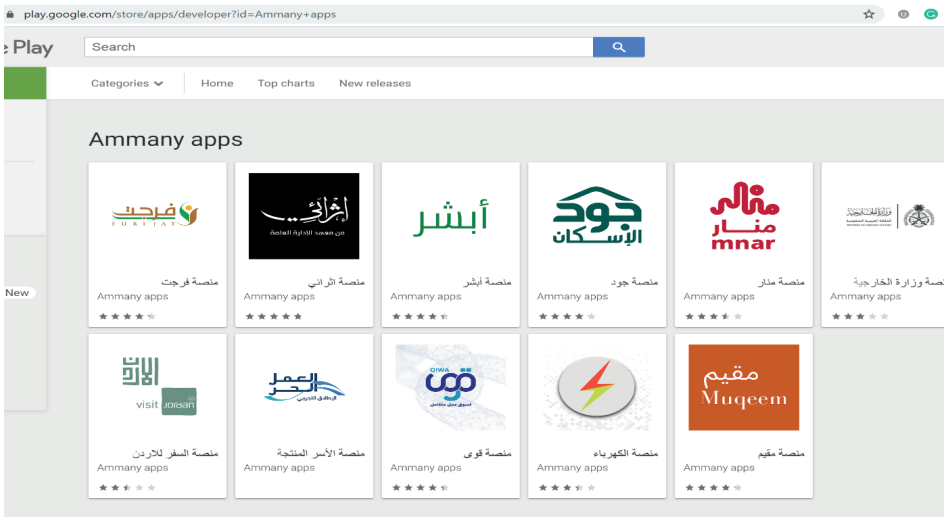
ويتضح أن المحتالين يستهدفون وكلاء الإعلان الذين توجد لديهم مساحات إعلانيَّة في المواقع المعروفة والأكثر انتشارًا وذات معدلات الزيارات العالية في الدول العربيَّة للوصول إلى الضحايا المحتملين. وخلال الرصد اتضح أن وكلاء الإعلان ينشرون الإعلانات الاحتياليَّة كثيرًا في المواقع الإخباريَّة المشهورة والمعروفة، كموقع مايكروسوفت نيوز، وموقع روسيا الإخباري باللغة العربيَّة (RT AR-ABIC)، وصحيفة التحرير. ويستخدم المحتالون صفحة محركات البحث للوصول إلى الضحايا المحتملين. وعادة يصل الضحايا المحتملون إلى المواقع الاحتياليَّة عن طريق الكلمات المفتاحيَّة؛ حيث تمنح شركة «جوجل» الأفضليَّة عند البحث للشركات الاحتياليَّة. والشكل التوضيحي رقم «15» يبيِّن أعلى خمسة مواقع إلكترونيَّة ناشرة للإعلانات الاحتياليَّة.



الشكل التوضيحي رقم «15»: أعلى خمسة مواقع إلكترونيَّة ناشرة للإعلانات الاحتياليَّة

تطبيقات «جوجل»

رُصِدت مجموعة من التطبيقات الحكوميَّة السعوديَّة المزيَّفة في «جوجل بلاي»، هي: «أبشر» و«فُرجت» و«جود الإسكان»، وتهدف إلى تصيُّد الضحايا. وحُمِّلت هذه التطبيقات في حدود 14 ألف مرة. وما زالت هذه التطبيقات موجودة في «جوجل بلاي» حتى هذه اللحظة. الشكل التوضيحي رقم «16» يبيِّن التطبيقات الحكوميَّة السعوديَّة المزيَّفة في متجر «جوجل».



الشكل التوضيحي رقم «16»: التطبيقات الحكوميَّة السعوديَّة المزيَّفة في متجر «جوجل» «Gecko»

هي شركة تقنية إعلانيَّة تركِّز على المستفيد وتعتمد على البيانات في تحديد الاتجاهات الحديثة ومعرفة تغيُّرات سلوك المستخدم. تهدف إلى الحفاظ على جودة الإعلانات لاستفادة كلٍّ من المعلنين والناشرين عبر تقنيات ذات مستوى عالمي تتطور باستمرار لدعم أعلى معايير الإعلان. ووصل عدد الزيارات الشهرية للمواقع التي نشرت عبر «Gecko» إلى 4.5 مليون من خلال 7 آلاف ناشر (https://gecko.me).

وأسهمت هذه الشركة في نشر إعلانات لإحدى شركات الاحتيال https://gmmcoin.com/fayezalmal_2btns_ar/ ، وعنوان الإنترنت لهذه الشركة هو 85.79.115.142، وهي مستضافة من شركة Godday.com، وسُجِّل هذا النطاق في الإنترنت بتاريخ 2020/11/16م، ويُزار الموقع في حدود 200 زيارة يوميًّا.

وتستخدم هذه الشركة خبرًا مفبركًا لأحد الممثلين السعوديين المشهورين للإيقاع بالضحايا المحتملين، ونُشِر هذا الإعلان في أحد أشهر المواقع المعروفة، وهو MSN.com، وكذلك نُشِر الإعلان في موقع روسيا اليوم (RT). وهذه الإعلانات الاحتياليَّة المنشورة في مواقع مشهورة ومعروفة تُسهم في تصيُّد الضحايا المحتملين. الشكل التوضيحي رقم «17» يبيِّن استخدام الأخبار المفبركة للممثلين السعوديين المشهورين لتصيُّد الضحايا المحتملين ونشرها في المواقع العالميَّة الموثوقة.

«بوست كوير»

بدأت هذه الشركة في عام 2014م، وتعتمد على أساس خوارزمي ذكي يدرس تصرفات القارئ وتقنية متطورة على أعلى المستويات تضم وحدات إعلانيَّة مميَّزة تسمح للمعلنين وأصحاب المواقع بالنجاح والتميُّز في السوق الرقميَّة.

وهي عبارة عن منصة توصيات محتوى رقمي وتسويق إعلانات رائدة في مجال المضامين الرقميَّة في منطقة الشرق الأوسط وشمال إفريقيا صُمِّمت خِصِّيصَى لمتحدِّثي اللغة العربيَّة؛ حيث تسمح للمعلنين بالوصول إلى ملايين المستخدمين يوميًّا من خلال شبكة تحتوي على أكبر المواقع العربيَّة وأهمها، كما أن الآليَّة تقدم خصائص متميزة تعطي المعلنين إمكانيَّة نشر علاماتهم التجاريَّة وحملاتهم تلقائيًّا وإمكانيَّة الاستجابة المباشرة لنتائج حملاتهم، ومقر الشركة في لندن.

وعند التحليل، اتضح أن هناك شركات احتياليَّة نشرت إعلانات عن طريق شركة «بوست كوير»، من ضمنها الموقع الاحتيالي news.arabfinance.info، الذي يحمل عنوان إنترنت 185.111.89.170، وسُجِّل اسم النطاق في شركة Namecheap INC f بتاريخ 2021/4/13م، ومستضاف من شركة Webonic kft. Td في المجر. ونُشِر الإعلان في موقع CNN العربيَّة.

3.2.7 انتحال مواقع سعوديَّة مشهورة للتصيُّد الإلكتروني

رُصِد انتحال مواقع عدّة صحف سعوديَّة والإعلان عنها ونشرها على مواقع مشهورة وموثوقة، وهي كالآتي:

- انتحال صحيفة الرياض السعوديَّة، ونُشِر في موقع صحيفة أخبار الخليج عن طريق وكيل الإعلان Jubna. واسم نطاق المحتال هو Radeef.net.
- انتحال صحيفة عكاظ السعوديَّة، ونُشِر في صحيفة الرأي الأردنية عن طريق وكيل الإعلان «جوجل»، واسم نطاق المحتال هو ilakhbarsaudisa.com.
- انتحال صحيفة عكاظ السعوديَّة، ونُشِر في «تويتر» للإعلانات، واسم نطاق المحتال هو saudi - alyoumar.com، وقد سَجَّل هذا النطاق المحتال معدل عدد زيارات يوميَّة 4200 زيارة.
- انتحال صحيفة عكاظ السعوديَّة، ونُشِر في موقع رائد الإماراتي عن طريق وكيل الإعلان

«جوجل»، واسم نطاق المحتال هو ilakhbarsaudisa.com. ولم يتعدَّ معدل الزيارات اليوميَّة 200 زيارة.

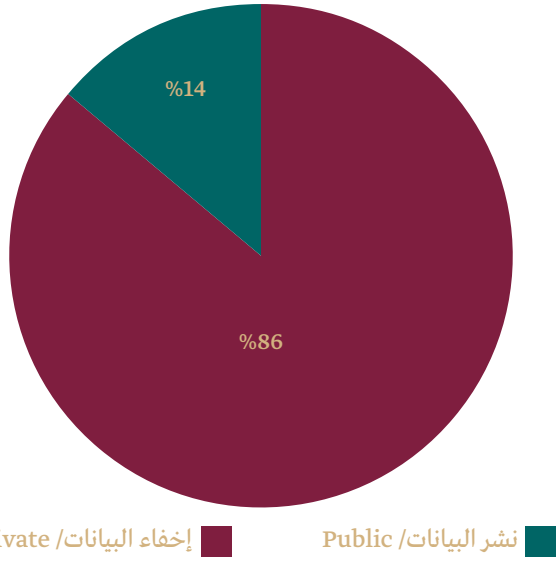
كذلك رُصِد انتحال مؤسسات ماليَّة سعوديَّة نُشِر في عدة مواقع معروفة وموثوقة، هي:

- شعار «الراجحي» الماليَّة، نُشِر في موقع إرم نيوز الإماراتي عن طريق وكيل الإعلان Jubna. واسم نطاق المحتال هو ratatui.online. ولم يُحصَل على عدد الزيارات اليوميَّة.
- شعار «الراجحي» الماليَّة، نُشِر في موقع لبنان 24 اللبناني عن طريق وكيل الإعلان Jubna. واسم نطاق المحتال هو ratatui.online.
- شعار شركة الأهلي كابيتال، نُشِر في موقع لبنان 24 اللبناني عن طريق وكيل الإعلان Jubna. واسم نطاق المحتال هو salmaninvest.com، وقد سُجِّل اسم النطاق بتاريخ 31/5/2021م، ولم يتعدَّ عدد الزيارات اليوميَّة 200 زيارة.

ويتضح غياب الرقابة على المحتوى الإعلاني الذي تنشره المواقع الاحتياليَّة وارتكابها جرائم معلوماتيَّة بانتحال الصحف والمؤسَّسات الماليَّة السعوديَّة، وهو ما يسهِّل عملية تصيُّد الضحايا.

3.2.8 التحدي الرقمي

أحد أهم التحديات في التحقيق الجنائي الرقمي: معرفة أصحاب هذه المواقع الاحتياليَّة؛ فقد كانت جميع هذه المواقع تُخفي بيانات أصحابها وأرقام التواصُل معهم، وهو ما يصعب من التحري والتحقيق على مستوى الإنترنت. واتضح أن نسبة عدم الإفصاح بمعلومات عن أصحاب المواقع وصلت إلى 65%. أيضًا أحد أهم التحديات التي تواجه جهات التحري والاستدلال: معرفة بيانات المحتال المسجل في نطاق الإنترنت؛ فقد كانت غالبية هذه المواقع تُخفي بيانات أصحابها وأرقام التواصُل معهم، وهو ما يصعب من التحري والتحقيق على مستوى الإنترنت. وأشارت نتائج التحليل إلى أن نسبة 86% من النطاقات المسجلة للمحتالين مخفية (Privacy) ولا يمكن للجهات الأمنيَّة الاطلاع عليها عن طريق خدمة whois التي تقدمها شركات خدمات تسجيل النطاقات في الإنترنت. الشكل التوضيحي رقم «18» يبيِّن نسبة إخفاء بيانات المسجلين المحتالين في نطاقات الإنترنت.



الشكل التوضيحي رقم «18»: نسبة إخفاء بيانات المسجلين المحتالين في نطاقات الإنترنت

3.2.9 الخلاصة

يتضح لنا من التحليل أن الأسباب الرئيسة التي أسهمت في ظهور المواقع الاحتياليَّة وبروزها هي:

1- استغلال نموذج وكلاء الإعلانات عبر الإنترنت

يتضح أن المحتالين استغلوا نموذج وكلاء الإعلان الذي يؤدِّي دور الوسيط بين المعلنين (المواقع الاحتياليَّة) والناشرين (المواقع المشهورة والمعروفة) الذين ينشرون إعلانات المواقع الاحتياليَّة. وتتم هذه العملية عن طريق حصول وكلاء الإعلانات على مساحة إعلانيَّة في المواقع الإلكترونيَّة للناشرين (المواقع الموثوقة) ومن ثَمَّ تأجيرها للمعلنين (المواقع الاحتياليَّة)؛ فالمحتال لا يتواصل مباشرة مع الناشر، بل عن طريق الوكيل الإعلاني.

وخلق هذا النموذج الإعلاني ثغرة جرى استغلالها من المحتالين، هي عدم وقوع المواقع الإلكترونيَّة المشهورة والمعروفة في مسألة قانونيَّة؛ حيث إن هذه المساحة مؤجَّرة لوكيل إعلاني. والإعلان المنشور غير ثابت ويتغيَّر بطريقة ديناميكيَّة، وجرى استغلال المحتالين ضعف الرقابة في الدول العربيَّة على المحتوى الإعلاني في المواقع الإلكترونيَّة؛ حيث إن إعلانات المواقع الاحتياليَّة منتشرة في أغلب المواقع الموثوقة والمشهورة عربيًّا.

2- استغلال المحتالين للتقنيات الحديثة التي يُقدِّمها وكلاء الإعلانات عبر الإنترنت

استغل المحتالون الخدمات التي تقدمها وكالات الإعلانات، والتي تعتمد على البيانات والتقنيات الحديثة، كالذكاء الاصطناعي، في معرفة الاتجاهات الحديثة ومعرفة تغيُّرات سلوك المستخدمين/الضحايا.

3- حصول المواقع الموثوقة (الناشرين) على مصادر دخل

تمثِّل الإعلانات للمواقع الإلكترونيَّة الموثوقة مصدر دخل؛ نظرًا لكثافة زُوَّار المواقع ومرتاديها. وتحدِّد هذه المواقع مساحات إعلانيَّة على صفحاتها وتؤجِّرها لوكلاء الإعلانات عبر الإنترنت الذين يؤجِّرونها للمعلنين أصحاب النطاقات الاحتياليَّة. وهناك انتشار كبير للمعلنين للنطاقات الاحتياليَّة في المواقع الإلكترونيَّة المعروفة والمشهورة والتي تُعرف بالناشر مقابل الحصول على مصدر دخل.

4- ضعف الرقابة على عملية تسجيل نطاقات في الإنترنت

استغل المحتالون سهولة إجراءات تسجيل أسماء النطاقات في الإنترنت بنوعيه: المستوى الأعلى العام والمستوى الأعلى للدول.

5- إخفاء بيانات مسجل النطاق في الإنترنت

مَنحت الخصوصيَّةُ للمحتال استغلالَ خاصيَّة إخفاء بيانات المسجل في نطاق الإنترنت من أجل إحباط جهود إنفاذ القانون الرامية إلى كشف بيانات النطاق المسجل للمحتال، ما يخلق له بيئة خصبة لارتكاب الاحتيال المالي وتعظيم عائدات الجريمة.

6- ضعف الرقابة على الإعلانات المدفوعة من قِبَل الدول العربيَّة

يتضح أن النطاقات الاحتياليَّة تستثمر في الإعلانات المدفوعة عن طريق وكلاء الإعلانات (طرف ثالث) للنشر في مواقع موثوقة ومعروفة ومشهورة عربيَّة وعالميَّة، ما يُسهِم في تسهيل عمليَّة التصيُّد الإلكتروني للضحايا. ويعتمد المحتالون (المعلنون) على استدراج الضحايا بسبب ثقتهم بالمواقع

المعروفة والمشهورة (الناشر). ويتم ذلك عن طريق ما يلي:

- الإعلان عن طريق شركة إعلانيَّة (وكيل إعلاني) متخصِّص

يستأجر الوكيل الإعلاني مساحة إعلانيَّة من المواقع المشهورة والمعروفة في الدول العربيَّة لعرض إعلانات الشركات، ومن ضمنها شركات الوساطة الماليَّة المشبوهة؛ لذلك يُعتبر الوكيل الإعلاني هو الوسيط بين الناشرين (المواقع الموثوقة) والمعلنين (المواقع المحتالة).

- الإعلان عن طريق شركة «جوجل»

تحصل شركة «جوجل» أيضًا على مساحة إعلانيَّة في المواقع المشهورة والمعروفة لعرض المحتوى الإعلاني، تُستغل من الشركات المشبوهة، وكذلك الإعلان عن المواقع الاحتياليَّة في محركات البحث والمدونات و«يوتيوب».

وقد استغلَّ المحتالون الماكينة الإعلاميَّة الضخمة في الإنترنت للانتشار عبر محركات البحث والمواقع الإلكترونيَّة والمدونات وبرامج التواصُل الاجتماعي و«يوتيوب» لتصيُّد الضحايا المحتملين. وفي الوقت ذاته نجد غيابًا تامًّا للرقابة على محتوى الإعلانات المدفوعة، سواء في وسائل التواصُل الاجتماعي أو «جوجل» أو المواقع الإلكترونيَّة.

7- استغلال الأحداث السياسيَّة والمتغيِّرات الاقتصاديَّة والصحيَّة لتصميم سيناريوهات الاحتيال

يستخدم المحتالون عدة فرص لبناء سيناريوهات الاحتيال لتتواكب مع متغيِّرات الأسواق الماليَّة من فرص استثماريَّة، مثل: فرص استثماريَّة لصناديق استثماريَّة أو اكتتاب أسهم، أو انخفاض العملات الرقميَّة أو ارتفاعها، أو انخفاض أسعار النفط أو ارتفاعها، أو اللقاحات المضادة لـ«كورونا». وبدا واضحًا رسم السيناريوهات على الفرص الاستثماريَّة لصندوق الاستثمارات السعوديَّة. ويتضح استخدام المحتالين قصصًا أمنيَّة مفبركة وقصصًا مفبركة لفنانين سعوديين وإعلاميين عن الثراء الفاحش، وكذلك صُمِّمت سيناريوهات متعددة عن تصريحات سمو ولي العهد السعودي عن المشاريع المستقبلية للمملكة العربيَّة السعوديَّة.

8- تعدُّد طرق الاستدراج عبر الإعلانات

يحدث الاستدراج إلى المواقع المشبوهة بعدة طرق، من أهمها:

- عبر الصور (Image)

يُستخدَم هذا الأسلوب في الإعلانات المنشورة في المواقع المعروفة والمشهورة، وتعتمد بعض المواقع الاحتياليَّة على عرض الصور كصورٍ لولي العهد السعودي أو فنانين سعوديين أو خبر أمني بصيغة صور، ولا توجد أي كلمات مفتاحيَّة للوصول إلى الموقع كموقع aljadded.me الذي نشر أكثر من 1100 صورة في أكثر من 2700 موقع حسب برنامج Semrush.

- عبر الكلمات المفتاحيَّة

ويستخدم المحتالون كلمات مفتاحيَّة لتصيُّد الضحايا عن طريق البحث في محركات البحث على سبيل المثال، عندما يبحث الضحيَّة بكلمة الاستثمار في الأسهم، أو الاستثمار في العملات الرقميَّة، وكلمة «فوركس» في محركات بحث «جوجل» ستظهر إعلانات مدفوعة الثمن خاصَّة بالشركات المحتالة في قائمة البحث.

- عبر مزيج من الصور والكلمات المفتاحيَّة

تعتمد بعض المواقع على الدمج بين الكلمات المفتاحيَّة والصور، على سبيل المثال: موقع axiainvestments.com نشر أكثر من 4000 صورة بوصفها مادة إعلانيَّة، بالإضافة إلى استخدام 377 كلمة مفتاحيَّة.

9- استخدام الهندسة الاجتماعيَّة عبر المواقع الإلكترونيَّة

يعتمد المحتال في تصميم الموقع الإلكتروني على طريقة لجمع المعلومات الشخصيَّة للضحايا المحتملين، وهي: الاسم والبريد الإلكتروني والدولة ورقم الجوال.

10- التطوُّر التقني للدفع الإلكتروني

أغلب السيناريوهات الاحتياليَّة بُنيت على التطوُّر السريع لطرق الدفع الإلكترونيَّة عن طريق الدفع بالبطاقة أو التحويلات البنكيَّة.

ونجد أن المحتالين استغلوا التقنيات الحديثة في التجارة الإلكترونيَّة وطرق الدفع، والتقنيات الحديثة في الإعلانات عبر الإنترنت وشهرة المواقع وضعف الرقابة وبحث الضحايا عن فرص استثماريَّة مجزية لاصطياد ضحاياهم والحصول على عوائد جرائم الاحتيال المالي. وفي المقابل شكَّلت هذه المزايا تحديات جديدة على جهات إنفاذ القانون.

3.3 حالات دراسيَّة لبعض ضحايا الاحتيال المالي والمحتالين:

3.3.1 حالات دراسيَّة لبعض ضحايا الاحتيال المالي

بعد جمع البيانات من جانب وكالات إنفاذ القانون بالدول العربيَّة والروابط الاحتياليَّة التي جُمِعت وحُلِّلت، عُقِد اجتماع مع ثلاثة ضحايا تفضلوا مشكورين بشرح سيناريو الاحتيال الذي تعرضوا له لمقارنة سيناريو الاحتيالات التي تعرَّضوا لها بما جُمِع من معلومات. وسنركِّز على الضحيَّة رقم «1»؛ نظرًا لاستخدام المحتالين عدة أساليب احتياليَّة. الجدول رقم «7» يوضِّح آليَّة التصيُّد وسيناريو الاحتيال، وعائدات الجريمة وطرق تحصيلها وجنس الضحيَّة.

الجدول رقم «7»: تفاصيل عمليَّات الاحتيال التي تعرَّض لها ثلاثة ضحايا

	الضحيَّة رقم «1»	الضحيَّة رقم «2»	الضحيَّة رقم «3»
آليَّة التصيُّد	اتصال هاتفي	إعلان إلكتروني	إعلان إلكتروني
السيناريو	تواصل معه عدة أشخاص وانتحلوا عدة جهات اعتباريَّة وشخصيَّة	تواصلت معها سيدة وانتحلت شخصيَّة موظفة بنك الاعتماد السعودي للاستثمار وطلبت منها تحويل المبلغ المراد الاستثمار به	الاشتراك بأحد مواقع السوق المالية للتداول، وأدلى ببياناته الشخصيَّة ورقم الحساب، ومن ثَمَّ تواصل معه شخص وطلب منه الرقم السري وسحب المبلغ
عائدات الجريمة	2000 ريال سعودي	30000 ريال سعودي	100 ألف ريال سعودي
طريقة تحصيل عائدات الجريمة	تحويل إلى حساب داخلي	تحويل إلى حساب داخلي	تحويل إلى حساب داخلي
البلاغ	لم يبلغ الجهات المعنيَّة	بلَّغت في مركز الشرطة	بلَّغ في مركز الشرطة
الجنس	ذكر	أنثى	ذكر

3.3.1.1 مرحلة التصيُّد:

الوسيلة

التواصُل مع الضحية عبر الهاتف الجوال، عبر رقم صادر من برامج الإنترنت. وقد استقبل الضحيَّة عدة اتصالات من أرقام هواتف جوال مختلفة، من ضمنها: 0598353288. وكان التواصُل من طرف واحد من المحتالين بالضحيَّة.

3.3.1.2 سيناريو الاحتيال:

انتحال شخصيَّة:

1- امرأة؛ لإيهامه بأنها شريك مع الهيئة العامَّة للاستثمار

انتحلت المتصلة صفة موظفة تعمل بالهيئة العامَّة للاستثمار في المملكة العربيَّة السعوديَّة، . وأكدت له أن هناك فرصًا استثماريَّة للمواطنين السعوديين، وإذا كان لديه رغبة في الاستثمار في هذه المشاريع سوف يتواصل معه أحد الأشخاص من الشركة الاستثماريَّة، وهي إحدى الأذرع الاستثماريَّة للهيئة لشرح فكرة الاستثمار المعروضة للمواطنين السعوديين المدعومة بنسبة 100% من الهيئة العامَّة للاستثمار.

2- رجل؛ لإقناعه بالبدء في الاستثمار والحصول على مبلغ

تواصل مع الضحيَّة شخصٌ انتحل شخصيَّة موظَّف في الشركة الاستثماريَّة، وادعى أنه شريك مع الهيئة العامَّة للاستثمار لإيجاد مصادر دخل للمواطن السعودي. وأرسلوا له رابطًا للمنصة الإلكترونيَّة للبدء في الاستثمار في البترول والأسهم. وطلب منه المحتال تحويل ألفي ريال سعودي لفتح حساب استثماري في المنصة، يكون من ضمنها تقديم دورة تدريبيَّة للاستثمار في المنصة. وأرسل المحتال للضحية عبر «واتساب» مستندات وهميَّة لشركة لمحاولة إيهامه بأن هذه الشركة مرخَّصة للاستثمار. وبعد ذلك أرسل المحتال للضحية رقم حساب مواطن سعودي لتحويل المبلغ إليه.

3- عضو هيئة تدريس؛ للوصول إلى جهاز الضحيَّة

بعد الحصول على مبلغ ألفي ريال، حُدِّد موعد لبداية الدورة التدريبيَّة، وأفادوا بأن من سيقدم الدورة عضو هيئة تدريس بإحدى الجامعات السعودية، وهذا انتحال لشخصيَّة عضو هيئة تدريس. تواصل معه منتحل شخصيَّة الدكتور وطلب منه تحميل برنامج Teamviewer للبدء في التدريب. هذا البرنامج يمنح الصلاحية للمحتال للوصول إلى جهاز الضحيَّة بموافقته بعد أن يمرِّر له رقم المستخدم والرقم السري لهذا البرنامج.

طلب المحتال من الضحيَّة تزويده برقم المستخدم والرقم السري لبرنامج Teamviewer ليتمكَّن من مشاركة الشاشة، واستطاع المحتال البدء في التحكُّم في جهاز الضحيَّة. وبدأت الدورة التدريبيَّة بعد أن استطاع المحتال التحكُّم في جهاز الضحيَّة، وبدأ في شرح الاستثمار وأسعار البترول والذهب، وبدأ بالتطبيق العملي في الاستثمار في البترول بالشراء بألفي ريال، ومن ثَمَّ أوهمه بأنَّ الهيئة العامَّة للاستثمار أسهمت معه بالاستثمار بدفع ألفي ريال، وجرى إدخال أرباح هذه الصفقة التي وصلت إلى 100% في المحفظة الوهميَّة.

احتماليَّة استخدام البرامج الخبيثة

فتح المحتال ملفًّا بعنون «ملف التدريب» بصيغة PDF، كان قد أرسله مسبقًا للضحية، وشعر الضحيَّة بعد ذلك بأن جهازه أصبح ثقيلًا وبدأ في البطء، وهذه مؤشرات تفعيل البرامج الخبيثة والتجسُّس.

تقديم عروض احتياليَّة للضحيَّة

بعد هذه الدورة، قُدِّمت عدة عروض للضحيَّة للحصول على مبالغ ضخمة، وقد شعر الضحيَّة بأن لديهم معلومة عن المبلغ الموجود لديه في حسابه البنكي؛ حيث كانوا يشددون على أنَّ لديه القدرة على الاستثمار بمبلغ 300 ألف ريال. وقدموا له عرضًا للاستثمار في الذهب بمبلغ 300 ألف ريال مناصفةً مع الهيئة العامَّة للاستثمار؛ حيث يدفع 150 ألف ريال وستقدِّم له الهيئة العامَّة للاستثمار 150 ألف ريال، ورفض العرض، ثم أُعيد العرض بالاستثمار بمبلغ 150 ألف ريال مناصفة مع الهيئة بمبلغ 75 ألفًا لكل منهما، وأن الأرباح ستكون 200% في خلال يومين فقط.

ممارسة الضغط على الضحيَّة

بدأت ممارسة الضغط على الضحيَّة يوم الخميس للحصول على أرباح يوم الجمعة، واستُخدِم الصوت العالي، وتحوَّل المحتال إلى شخصٍ يُصدر أوامر بلهجة حادة، ثم بدأ بسرد الآيات والأحاديث عن الخوف من الله والشبهات. والدخول في مجال الفتاوى والقصص عن الصحابة، وفرصة تأمين مستقبل لأبنائه.

استرجاع الأموال ومحاولة سرقة أموال أكبر

حاول الضحيَّة الوصول إلى المحفظة الوهميَّة لتحويل المبلغ الموجود فيها، لكنه لم يستطِع الوصول إلى المحفظة. بعد ذلك، طلب الضحيَّة من المحتال استرجاع المبلغ، وبعد مشادات أرسلوا له رابطًا لتعبئة النموذج الإلكتروني. وعند البدء في إجراءات تعبئة النموذج كان الرابط لا يعمل.

عرض المحتال على الضحيَّة مساعدته بأن يحوِّل المبلغ والأرباح إلى حسابه البنكي، وطلب المحتال منه إرسال اسم المستخدم والرقم السري لحسابه البنكي لتحويل المبلغ. وبعد رفض الضحيَّة طلبه، أغلق المحتال هاتفه وتغيَّر الرقم وانقطع الاتصال بين الضحيَّة والمحتال.

3.3.1.3 البلاغ

لم يقدِّم بلاغًا للشرطة بسبب أن المبلغ لم يتجاوز ألفي ريال وأن الإجراءات ستأخذ وقتًا طويلًا، وكذلك خوفًا على توريط صاحب الحساب الذي حُوِّل المبلغ إليه في هذه القضية وعدم رجوع المبلغ له.

3.3.1.4 الإجراءات التي قام بها الضحيَّة بعد تعرضه للاحتيال

قام الضحيَّة بعدة إجراءات للحدِّ من الخسائر التي تعرَّض لها، هي:

- فتح حساب جديد في بنك آخر.
- تغيير رقم الهاتف المعتمد في أبشر والبنك.
- تغيير الرقم السري الخاص بمنصة أبشر.
- تغيير رقم الجوال.
- عدم الثقة بالتعامُلات التي تتم عبر الهاتف الجوال.

3.3.1.5 مناقشة الحالات الدراسيَّة

يتضح من سيناريو الجريمة أنها تتوافق مع الأساليب الإجراميَّة التي نُوقِشت مع مجموعة التركيز، وهي:

المحتال رقم «1» واستهداف الضحيَّة رقم «1»:

- انتحال الشخصيَّة الاعتباريَّة للجهات الحكوميَّة، وهي الهيئة العامَّة للاستثمار في المملكة العربيَّة السعوديَّة.
- التواصُل الهاتفي ثم إرسال روابط محتالة لتصيُّد الضحايا.

بالإضافة إلى وصولهم إلى جهاز الضحيَّة ومحاولة تفعيل برامج خبيثة. وقد استخدم المحتالون أيضًا الهندسة الاجتماعيَّة بعد أن زوَّدهم باسمه؛ حيث جمعوا معلومات كثيرة من المصادر المفتوحة عن الضحيَّة كوظيفته الحاليَّة، واهتماماته الشخصيَّة.

ويتوافق أيضًا مع بعض التحديات التي نُوقِشت في مجموعة التركيز، وهي: عدم تعاون بعض الضحايا ورفضهم التبليغ، واستخدام أرقام وهميَّة و«واتساب» للتواصُل مع الضحيَّة.

المحتال رقم «2» واستهداف الضحيَّة رقم «2»

انتحال شخصيَّة وهميَّة باسم بنك الاعتماد السعودي للاستثمار وإنشاء موقع وهمي وانتحال شخصيَّة موظف بنك الاعتماد السعودي للاستثمار.

المحتال رقم «3» واستهداف الضحيَّة رقم «3»

الوصول إلى الموقع عن طريق أحد المواقع المعروفة للاشتراك بأحد مواقع السوق المالية للتداوُل، وأدلى ببياناته الشخصيَّة ورقم الحساب، ومن ثَمَّ تواصل معه شخصٌ وطلب منه الرقم السري وسُحِب المبلغ.

3.3.1.6 أدوات الاحتيال الإلكترونيَّة

استخدم المحتالون عدة أدوات إلكترونيَّة في هذه الجريمة، هي:

- جميع المحتالين الثلاثة استخدموا مواقع إلكترونيَّة وهميَّة.
- المحتالان الأول والثالث استخدما محافظ وهميَّة في مواقعهما.
- جميع المحتالين الثلاثة استخدموا أرقام تواصُل وهميَّة لتسهيل عمليَّة تصيُّد الضحيَّة وانتحال شخصيَّة وإقناع الضحايا بالاستثمار.
- المحتال رقم «1» استخدم برنامج teamviewer للوصول إلى جهاز الضحيَّة رقم «1» والتحكم في جهازه، وبناءً على تصرفات الجهاز بعد تفعيل ملف PDF هناك مؤشرات على احتماليَّة تفعيل المحتال برامج خبيثة في جهاز الضحيَّة لسرقة البيانات البنكيَّة والشخصيَّة.
- استخدم المحتال الأول روابط إلكترونيَّة للحصول على البيانات البنكية للضحية رقم «1».

3.3.1.7 الفرص

كانت هناك فرصة لإنجاح سيناريو الاحتيال المالي وتصيُّد الضحيَّة، وتكمن في ثلاث نقاط، هي:

- استغل المحتالون الخطط الاقتصادية في المملكة لإقناع الضحايا بأنهم يتماشون مع الخطط السعوديَّة.
- استغل المحتال رقم «1» طبيعة عمل الهيئة العامَّة للاستثمار في المملكة في استقطاب شركات دوليَّة للاستثمار في المملكة وأوهم الضحيَّة بأنه شريك للهيئة؛ حيث إن الهيئة لا تستثمر مباشرةً مع المواطنين ولكن من خلال هذه الشركات الوهميَّة.
- استغل المحتالون الفرص الاستثماريَّة الكبيرة في المملكة ومواكبتهم بأحدث الأخبار الاقتصاديَّة والفرص الاستثماريَّة لإقناع الضحايا والتفاؤل الكبير من السعوديين بالمرحلة الذهبيَّة التي يعيشها الاقتصاد السعودي.

3.3.1.8 الأسلوب الإجرامي للوصول إلى جهاز الضحيَّة

استخدم المحتال رقم «1» خدمة تقديم دورة تدريبيَّة عن بُعد للوصول إلى جهاز الضحيَّة رقم «1» والتحكُّم فيه عن طريق Teamviwer، وهو ما يمنحه التحكُّم الكامل في الجهاز، واحتماليَّة تفعيل برنامج خبيث قد يكون موجودًا في ملف من نوع PDF للتدريب، أرسله المحتال وفتحه، ولكن بانتحال شخصيَّة أستاذ جامعي لطمأنة الضحيَّة.

3.3.1.9 إخفاء الأدلَّة الرقميَّة

هيَّأ الضحيَّة رقم «1» أجهزة الجوال وجهاز الحاسب المحمول ومسح جميع الروابط بعد أن وقع ضحيةً لهذه الجريمة. ولم يوثِّق أي دليل رقمي باستثناء رقم جوال وهمي ورقم الحساب الذي حوَّل إليه المبلغ.

3.3.1.10 عدم تعاون بعض الضحايا ورفضهم التبليغ

يُعتبر الضحيَّة رقم «1» من الضحايا الذين تعرضوا لجريمة الاحتيال ولم يبلغ الجهات الرسميَّة، وهو ما يبعد هذه القضايا عن الدخول في إحصائيَّة الجرائم المرتكبة. وهنا يظهر تساؤل مهم، حول عدم معرفة الجهات الرسميَّة بعدد ضحايا الاحتيال المالي وحجم الخسائر الحقيقيَّة لهذه الجرائم، وهذا يؤكِّد أيضًا أن هناك بعض المبالغ الصغيرة لدى الضحايا لا يودون استرجاعها أو يجدون تكلفة استرجاعها أكبر بكثير من المبلغ المفقود.

3.3.1.11 الأضرار - انعدام الثقة

غيَّر الضحيَّة رقم «1» البنك الذي يتعامل معه؛ حيث كانت لديه افتراضيَّة أن هناك تسريبًا للمعلومات البنكيَّة من قِبَل أحد موظفي البنك لهؤلاء المحتالين. وقد بنى هذه الافتراضيَّة على تزامُن توقيت اتصال المحتال مع ترقية حسابه إلى الفئة الذهبية في البنك الذي يتعامل معه، وتأكيد المحتالين له قدرته الماليَّة على الاستثمار إلى 300 ألف ريال سعودي، وهو متطابق مع المبلغ الموجود بالحساب البنكي للضحية خلال ترقية الحساب إلى الفئة الذهبية. أما الضحيَّتان «2» و«3» فلم يغيِّرا حساباتهما.

3.3.1.12 استفسارات الضحايا المحتملين

رُصِدت مجموعة استفسارات من بعض الضحايا المحتملين عن بنك الاعتماد السعودي للاستثمار في «تويتر». وكانت استفسارات بعضهم موجَّهة للبنك السعودي المركزي، مثل: «هل بنك الاعتماد السعودي للاستثمار معتمَد لدى مؤسَّسة النقد السعودي؟». الشكل التوضيحي رقم «19» يبيِّن مجموعة الاستفسارات.

الشكل التوضيحي رقم «19»: رصد مجموعة من استفسارات الضحايا المحتملين عن بنك الاعتماد السعودي للاستفسار الوهمي

ويتضح من المصادر المفتوحة أيضًا اصطياد بنك الاعتماد السعودي للاستثمار مجموعة من الضحايا. ورُصِد أحد أساليب الاصطياد التي يستخدمها هذا البنك المحتال؛ حيث رُصِد استفسار أحد أصحاب الحسابات في «تويتر» عن آليَّة سحب المبلغ من بنك الاعتماد السعودي للاستثمار بعد طلب الضحيَّة من البنك سحب المبلغ الذي استثمرت فيه وأُرسِل رابط وهمي لشركة الراجحي الماليَّة لتملأ طلب سحب المبلغ. وقد تجاوب حساب «الراجحي» الماليَّة مع استفساره على الخاص. الشكل التوضيحي رقم «20» يبيِّن إرسال روابط احتياليَّة من بنك الاعتماد السعودي للاستثمار الوهمي.

الشكل التوضيحي رقم «20»: إرسال روابط احتياليَّة من بنك الاعتماد السعودي للاستثمار الوهمي

3.3.1.13 الخلاصة

يتضح أن الأساليب الإجراميَّة التي حُدِّدت ونُوقِشت مع مجموعة التركيز العرب تتطابق مع مجموعة الأساليب التي استخدمها المحتالون للاحتيال على الضحايا، وهي: انتحال الشخصيَّة الاعتباريَّة للجهات الحكوميَّة، والتواصُل الهاتفي، وإرسال روابط محتالة لتصيُّد الضحايا، واستخدام البرامج الخبيثة، والإعلان عبر الإنترنت.

وهم يختارون التوقيت المناسب لاستغلال الفرص وإقناع الضحيَّة. أما عدم تعاون الضحيَّة ورفضه التبليغ فيعتبران من أهم التحديات التي حدَّدها الخبراء العرب. وتوقَّع الضحيَّة أن يكون هناك تعاون من أحد موظفي البنك مع المحتالين بتزويدهم ببياناته. وقد بنى هذه الافتراضية على تزامُن تواصُل المحتالين مع ترقية حسابه إلى فئة الحسابات الذهبيَّة في البنك.

ويتضح من جرائم الاحتيال استخدام المحتالين حسابات بنكية عائدة لمواطنين لتحصيل عوائدهم الإجراميَّة لإخفاء أثر هذه العوائد، وقد تنتقل هذه العوائد في عدة حسابات بنكيَّة محليَّة قبل توجهها لحسابات بنوك خارج الدولة، وهذا أحد الأساليب الإجراميَّة التي حُدِّدت في اجتماع مجموعة التركيز العرب (استخدام وسطاء ماليين لإخفاء عائدات الجريمة/ أموال ضحايا الاحتيال المالي عبر تحويل أموالهم بين حسابات الوسطاء في البنوك).

أيضًا، يتضح لجوء ضحيتين للتبليغ في مراكز الشرطة وعدم استخدام وسائل التبليغ الإلكتروني، وعدم وجود رصد لمواقع الاحتيال المالي، حيث رُصدت مجموعة من الضحايا المحتملين يستفسرون عن اعتماديَّة بنك الاعتماد السعودي للاستثمار في المملكة العربيَّة السعوديَّة دون ردٍّ. وهنا يتضح عدم وجود مرجعيَّة للضحايا المحتملين للتأكُّد من مصداقيَّة هذه المواقع المحتالة التي تنتحل أسماء البنوك.

3.3.2 حالات دراسيَّة لبعض شركات الاحتيال المالي

بعد مناقشة بعض الحالات جرى التواصُل مع محتالين ينتسبون إلى هذه النطاقات المحتالة:

- SABTRADINGS.
- ar.a3t.live.
- axiainvestments.

وجرى أيضًا التواصُل عبر «تليجرام» مع أحد الحسابات التي تعرض بيع العملات المشفَّرة.

3.3.2.1 أسلوب التواصُل

جرى التواصُل مع الشركة المحتالة عن طريق الإعلانات عبر الإنترنت، وبعد ذلك تواصل المحتالون مباشرةً عن طريق هواتف و«واتساب» بأرقام وهميَّة. ويوضِّح الجدول رقم «8» أهم النقاشات مع المحتالين، التي تشمل آليَّة التواصُل وسيناريو الاحتيال وآليَّة تحصيل عوائد الجريمة.

الجدول رقم «8»: الشركات الاحتياليَّة التي جرى التواصُل معها

	A3TRADING	SABTRADINGS	AXIAINVESTMENTS
التواصُل جوال وتطبيق «واتساب»	جوال: 0573915599 0523995272 0529194727 «واتساب»: 00966115207782	جوال: 0542142073	جوال وتطبيق «واتساب»: 97145734604 97145866494 97145866430 0526010025 0526010028 0526010024 0526010027
سيناريو الاحتيال (العروض)	– خبير اقتصادي لتقديم الاستشارات الاقتصاديَّة – دورات تدريبيَّة على استخدام التطبيقات – صفقات محميَّة لتعويض خسائر رأس المال – تقديم بونص 100% بدفع 100% من المبلغ المراد الاستثمار فيه	– صفقات محميَّة لتعويض خسائر رأس المال – تقديم بونص 100% بدفع 100% من المبلغ المراد الاستثمار فيه	– خبير اقتصادي لتقديم الاستشارات الاقتصاديَّة – دورات تدريبيَّة على استخدام التطبيقات – تقديم بونص 100% بدفع 100% من المبلغ المراد الاستثمار فيه
الحد الأدنى للاستثمار	$200	$200	$200
آليَّة تحصيل عوائد الجريمة	الدفع المباشر باستخدام بطاقات الدفع	التحويل السريع لحساب بنكي لأحد المصارف المحليَّة	الدفع المباشر باستخدام بطاقات الدفع

3.3.2.2 الهندسة الاجتماعيَّة

زُوِّد المحتالون بالبيانات المطلوبة في موقعهم عبر الإنترنت، وهي: الاسم، والبريد الإلكتروني، وكذلك رقم الجوال للتواصُل.

3.3.2.3 استخدام أرقام هواتف محليَّة أو دوليَّة للتواصُل مع الضحايا المحتملين

بعد الحصول على رقم الضحيَّة وبياناته، يلجأ المحتالون إلى انتحال شخصيَّة مدير حسابات الشركة الاستثماريَّة الوهميَّة ويتواصل مباشرةً مع الضحايا المحتملين بإحدى الطريقتين التاليتين أو بكلٍّ منهما:

- عن طريق البريد الإلكتروني لجمع مزيدٍ من المعلومات.
- استخدام أرقام هواتف وهميَّة للتواصُل مع الضحايا للإيقاع بهم في الاستثمار الوهمي، على سبيل المثال: تستخدم شركة أكسيا axiainvestments.com عدة أرقام وهميَّة، هي: 97145866430 و97145866494، للتواصُل مع الضحايا المحتملين ويجري إيهامهم وإغراؤهم بالصفقات الوهميَّة والمكاسب وآليَّة فتح المَحافظ.

3.3.2.4 الضغط النفسي على الضحايا لتحصيل عوائد الاحتيال

لوحظ أن هذه الشركات الوهميَّة تمارس الضغط النفسي على الضحايا بطلب إحضار البطاقات البنكيَّة للدفع وتمرير المعلومات البنكيَّة كاسم البنك ورقم البطاقة للمحتالين بشكل عاجل ومحاولة منع الضحيَّة من إغلاق الهاتف؛ حيث استخدمت axiainvestments.com وa3trading الأسلوب ذاته في الضغط للحصول على أرقام بطاقة الدفع. وعند إغلاق الهاتف يجري التواصُل على الضحايا بشكل متواصل من عدة أرقام مختلفة، وهو نوع من أنواع ممارسة الضغط.

3.3.2.5 طرق تحصيل عوائد الاحتيال المالي

خلال التواصُل المباشر، جرى التخيير بأسلوب الدفع المتوافر لديهم، وهو أسلوب الشراء المباشر (debit Card) ببطاقة «مدى» لتحويل المبالغ عن طريق الموقع الإلكتروني أو عن طريق التحويل البنكي باستخدام نظام التحويلات الماليَّة السريعة والمعروف اختصارًا بـ«سريع»، وهو من أحدث نظم المدفوعات والتسويات البنكيَّة.

أسلوب الشراء المباشر ببطاقة «مدى»:

لوحظ اتجاه المحتالين إلى هذا الأسلوب بعد تضييق الخناق عليهم من البنوك المحليَّة لبعض الدول كالمملكة العربيَّة السعوديَّة. وقد طلب المحتال من مجموعة a3trading دفع المبلغ عن طريق بطاقة «مدى».

أسلوب التحويل البنكي:

طلب المحتال من شركة SABTRADINGS تحويل المبلغ لأحد الحسابات البنكيَّة المحليَّة ورفضوا الدفع عن طريق البطاقة.

وخلال اجتماع مجموعة التركيز، ذكر أحد الخبراء في مكافحة الاحتيال المالي اعتماد المحتالين على تحويل الأموال من حساب بنكي إلى عدة حسابات بنكيَّة محليَّة قبل تحويلها إلى وجهة خارج البلاد لمحاولة إخفاء تتبُّع الأموال. وخلق هذا الأسلوب ازدياد رقعة الضحايا؛ حيث إن أصحاب الحسابات المحوَّلة إليهم المبالغ هم أيضًا ضحايا للمحتال؛ حيث جرى إيهام أصحاب الحسابات البنكيَّة بأنهم محصلون ماليون للشركة الوهميَّة وعليهم تحويل المبالغ التي تصل إلى حساباتهم إلى حسابات أخرى.

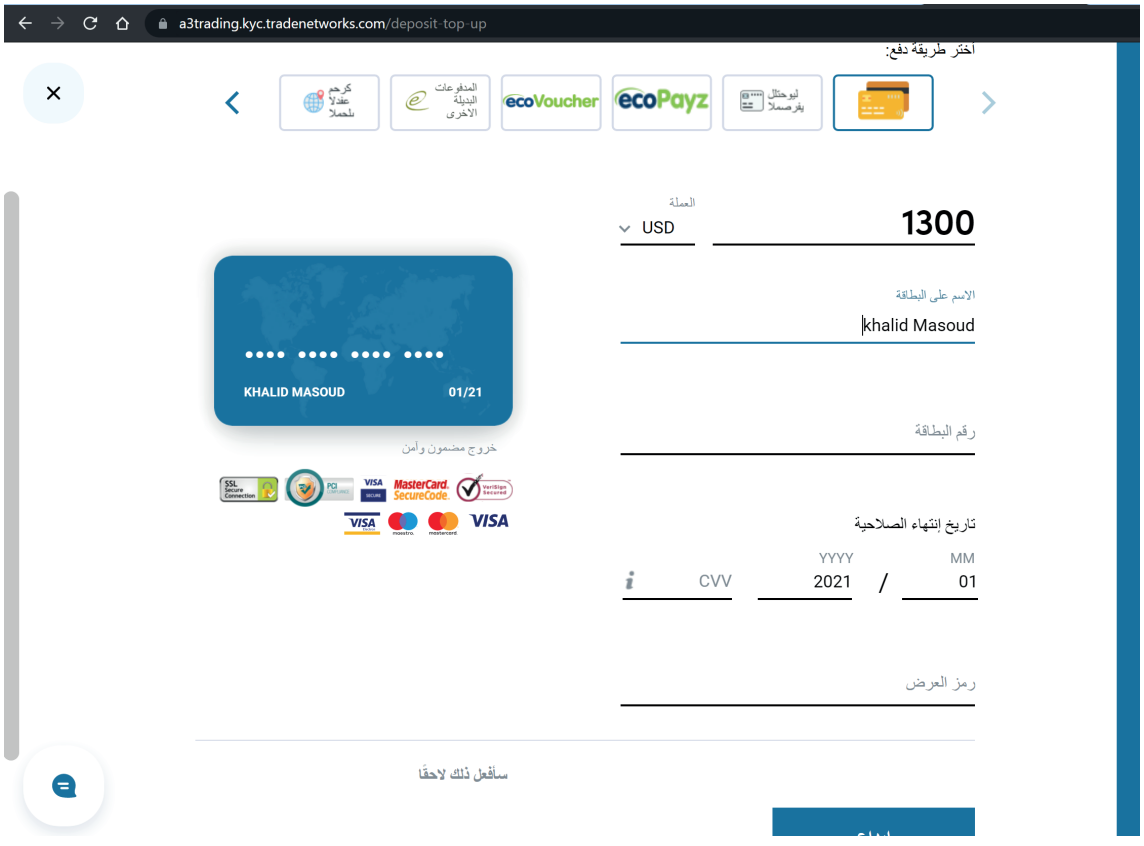
3.3.2.6 طرق حديثة للاحتيال

ومن طرق الاحتيال، ينتحل المحتال من شركة axiainvestments شخصيَّة الضحايا لإتمام عمليَّة تحصيل الأموال نيابةً عنهم، ويحدث ذلك بالتواصُل مع الضحايا المحتملين عن طريق الهاتف، ويطلب منهم تزويده ببيانات البطاقة البنكيَّة الخاصَّة بهم (رقم البطاقة وتاريخ انتهائها ورقم الأمان) لسحب المبالغ المطلوبة من حساباتهم البنكيَّة. وبعد ذلك يطلب المحتال من الضحايا المحتملين تزويده برقم التحقُّق الثنائي الذي وصل إليهم من البنوك عن طريق هواتفهم المسجلة لدى البنوك. وبهذا يتجاوز المحتال أفضل الممارسات العالميَّة التي تطبقها معظم البنوك كالبنوك السعوديَّة لتقديم حماية إضافية للعملاء الذين يستخدمون الإنترنت أو غيرها من قنوات الخدمة الذاتيَّة.

3.3.2.7 رسالة أمن وأمان الاحتياليَّة

من طرق الاحتيال الحديثة التي استخدمها المحتالون في مجموعة a3t.live لسرقة المبلغ بالكامل من الحساب دون علم الضحيَّة: استدراج الضحيَّة إلى الموقع والطلب منه كتابة اسمه كما هو في البطاقة البنكيَّة وكتابة رقم البطاقة وتاريخ انتهائها والرقم الموجود في ظهرها. وبذلك يكون المحتالون قد حصلوا على جميع البيانات البنكيَّة التي تساعد على تحصيل عوائد الاحتيال المالي. وتبيِّن الصورة في الشكل التوضيحي رقم «21» طريقة الاحتيال المبتكرة لسرقة البيانات البنكيَّة للضحية دون علمه، بتحديد المبلغ المراد الاستثمار فيه، وكتابة بيانات الضحيَّة البنكيَّة.

وتبقى للمحتالين خطوة أخيرة للحصول على المبلغ، هي رقم التحقُّق الذي يرسله البنك على هاتف الضحيَّة المسجَّل لديهم للتحقُّق من العمليَّة. وطريقة الاحتيال التي تُستخدم هنا هي أن يهيِّئ المحتالون الضحيَّة لأنه سوف تصل إليه رسالة أمن وأمان ويجب على الضحيَّة إرسالها للمحتال لتفعيل المحفظة، وبذلك يجري الحصول على عوائد الاحتيال.



الشكل التوضيحي رقم «21»: سرقة البيانات البنكيَّة للضحايا بطريقة مبتكرة

3.3.2.8 الخلاصة

يستخدم المحتالون أرقامًا وهميَّة متعددة. وجميع أسئلة المحتالين في الشركات الثلاث موحدة، وإجراءاتهم أيضًا موحدة، وتميل إلى أنهم مجموعة واحدة متجانسة، ولديهم إلمام بتقسيم أرقام البطاقات البنكيَّة التي تتكوَّن من أربعة أقسام و16 رقمًا. ومعرفتهم القسم الأول من أرقام البطاقة البنكيَّة، الذي يرمز إلى هُوية البنك؛ فعندما يحدِّد لهم الضحيَّة اسم البنك فإنهم يعطونه أول أربعة أرقام من بطاقته البنكيَّة لرفع مستوى الطمأنينة لدى الضحيَّة.

وبدا الآن واضحًا توجُّه المحتالين إلى استخدام آليَّة تحصيل عوائد جريمة الاحتيال ببطاقة «مدى» وليس التحويل البنكي، وعند سؤالهم عن السبب، كانت إجاباتهم جميعًا: حتى تجري حماية العميل من الملاحقة القانونيَّة من جرائم غسل الأموال.

أيضًا لوحظت احترافية بعض المحتالين بتمكُّنهم من استخدام الهندسة الاجتماعيَّة للحصول على أموال الضحايا عن طريق الآتي:

1- الحصول على معلومات البطاقة البنكيَّة «مدى»

صَمَّم أحد المواقع الاحتياليَّة بطاقة وهميَّة، ويطلب من الضحايا ملء بيانات بطاقتهم البنكيَّة الخاصَّة بهم في هذا النموذج المزور حتى تُفتَح حسابات ومحافظ استثماريَّة للضحايا. وعند إكمال ملء النموذج يكون المحتال قد حصل على رقم البطاقة البنكيَّة واسم الضحيَّة وتاريخ انتهاء البطاقة البنكيَّة والرقم الخلفي للبطاقة.

2- الحصول على رقم مرور كلمة واحدة لإتمام العمليَّة

يستغل المحتال معرفته بنظام كلمة مرور مرة واحدة/ صالحة لعمليَّة واحدة (OTP) التي تستخدمها المؤسَّسات الماليَّة للتأكُّد من شخصيَّة العميل لإتمام العمليَّة البنكيَّة. وتُرسَل رسالة نصيَّة إلى جوَّال الضحيَّة المسجَّل في البنك للتأكُّد من شخصيته. ويُشعر المحتال الضحيَّة أنه سيستقبل كلمة مرور لمرة واحدة (OTP) عن طريق جواله المسجل في البنك، للتأكُّد من هويته. وعندما يتلقَّى الضحيَّة كلمة المرور من البنك يظن أنها كلمة المرور الخاصَّة بهذه الشركة الوهميَّة. فيمرِّرها للمحتال الذي يستكمل العمليَّة ويستحوذ على الأموال. وهنا يستغل المحتال نقطة ضعف في نظام كلمة مرور مرة واحدة، هي عدم توضيح العمليَّة الماليَّة المرتبطة بكلمة المرور التي تسلَّمها.

ولوحظ أيضًا ممارسة المحتالين الضغط النفسي على الضحايا للتعجيل بالدفع، وتكرار التواصُل المستمر مع الضحايا للحصول على مبالغ.

3.4 مناقشة التحديات التي تواجهها الجهات المعنيَّة في البحث والتحرِّي عن بيانات المسجل مع مؤسَّسة «ICANN»

بعد تحليل المواقع المحتالة عبر الإنترنت والتعرُّف إلى مجموعة من التحديات في عمليَّات البحث والتحرِّي، واكتشاف أن 86% من النطاقات الاحتياليَّة تُخفي بياناتها المسجَّلة وصعوبة حصول جهات البحث والتحرِّي على معلومات عن هذه النطاقات الاحتياليَّة، عُقِد اجتماع مع مؤسَّسة الإنترنت للأسماء والأرقام المخصصة (ICANN) فيما يتعلق بسجلات نظام تسمية النطاقات (DNS) وآثارها التقنية في تحديد المعلومات المتعلقة بالمجال، مثل المسجل وخوادم الأسماء المرتبطة بالشركات المضيفة.

3.4.1 تعريف عن مؤسَّسة الإنترنت للأسماء والأرقام المخصصة (ICANN)

تخصِّص مؤسَّسة «ICANN» عنوانًا فريدًا، بحيث يتمكَّن كل جهاز من العثور على الطرف الآخر، وتنسيق المعرفات الفريدة حول العالم لتتمكَّن الإنترنت من التناسُق والتواصُل؛ لذا تُسهم هذه المؤسَّسة في الحفاظ على إنترنت آمنة ومستقرة وتطور سياسة معرفات الإنترنت الفريدة. ولا تتحكم مؤسَّسة «ICANN» في المحتوى على الإنترنت.

يوفِّر نظام تسمية النطاق (DNS) خدمة الإنترنت للأفراد، وتتعرف الأجهزة بعضها إلى بعض في الإنترنت عن طريق مجموعة من الأرقام المخصصة/ المميزة تسمى عنوان «IP» المربوط بالأجهزة المختلفة. ويستخدم «DNS» الحروف نيابةً عن الأرقام، ومن ثَمَّ يربط أسماء المواقع والنطاقات بعنوان «IP».

ويشمل اسم النطاق عنصرين أساسيين، هما: ما قبل النقطة، وما بعدها. الجزء عن يمين النقطة، مثل «com», «org»، يُعرف باسم «النطاق عالي المستوى» (TLD)، شركة واحدة في كل حالة (تسمى المسجل) تكون مسؤولة عن كل النطاقات التي تنتهي بهذا النطاق المحدد عالي المستوى ولها حق الوصول المباشر إلى القائمة الكاملة للنطاقات تحت هذا الاسم، كما هو الحال في عنوان «IP» الذي ترتبط به هذه الأسماء. الجزء الذي يسبق النقطة هو اسم النطاق الذي اختاره العميل وسجَّله، والذي يُستخدم فيما بعد ليمتد إلى النظم الأخرى للجهة، مثل الشبكات الإلكترونيَّة، والبريد الإلكتروني. هذه النطاقات تُباع بأعداد كبيرة من قِبَل المسجلين، وأحيانًا دون مقابل حسب رغباتهم، على النقيض في كل حالة يدفعون رسومًا لكل نطاق لمكان التسجيل الذي يُسجَّل اسم النطاق نسبةً له.

تؤدِّي مؤسَّسة «ICANN» الدور الإداري ذاته مع عناوين «IP» المستخدمة من قِبَل الحاسوب كما يُفعل مع أسماء النطاقات التي يستخدمها الأفراد. وفي السياق ذاته لا يمكنك أن تجد جهازين يحملان عنوان «IP» نفسه في الإنترنت.

ولا تشغِّل المؤسَّسة النظام، ولكن تساعد في تنسيق عناوين «IP» وتوفيرها لتجنُّب التكرار والتصادُم. وتعد المؤسَّسة أيضًا المخزن الرئيس لعناوين «IP»، التي منها تُوفَّر المسجلات الإقليميَّة التي بدورها توزِّعها على مزوِّدي الإنترنت.

وعليه، ينحصر دور المؤسَّسة في الإشراف على الإنترنت العالميَّة والمعرفات الفريدة التي تسمح للحواسيب على الإنترنت بعثور بعضها على بعض.

وتتكوَّن مؤسَّسة «ICANN» من ثلاث منظَّمات، هي:

- المنظَّمات التي تتعامل مع عناوين «IP».
- المنظَّمات التي تتعامل مع أسماء النطاقات (gTLDs).
- مديرو بلاد النطاقات عالية المستوى (ccTLDs). وهنا استثناء لـ«رموز نطاقات البلاد عالية المستوى» (ccTLDs) مثال ذلك: .de لألمانيا وuk. للمملكة المتَّحدة. وهناك ما يزيد على 250 نطاقًا عالي المستوى (ccTLDs)، بعضهم لديهم عقود مع «ICANN»، وبعضهم لديهم اتفاقيات موقعة عاملة مع «ICANN»، وبعضهم يتوجَّب عليه إدخال اتفاقيات رسميَّة مع «ICANN»، ومع ذلك فإن «ICANN» تقوم بوظيفة تعريف بـ«IANA» التي تضع قوائم بالعناوين الرئيسة لكل النطاقات عالية المستوى (ccTLDs).

وخلال الاجتماع مع مؤسَّسة الإنترنت للأسماء والأرقام المخصصة (ICANN)، نُوقِشت آليَّة إدارة النطاقات المسجلة في الإنترنت والأسباب التي تمنع ظهور بيانات النطاقات المسجلة في خدمة الاستفسارات (WHOIS) ومدى قدرة المؤسَّسة على تسهيل عمل الجهات الأمنيَّة.

3.4.2 اختلاف إدارة تسجيل النطاقات في الإنترنت

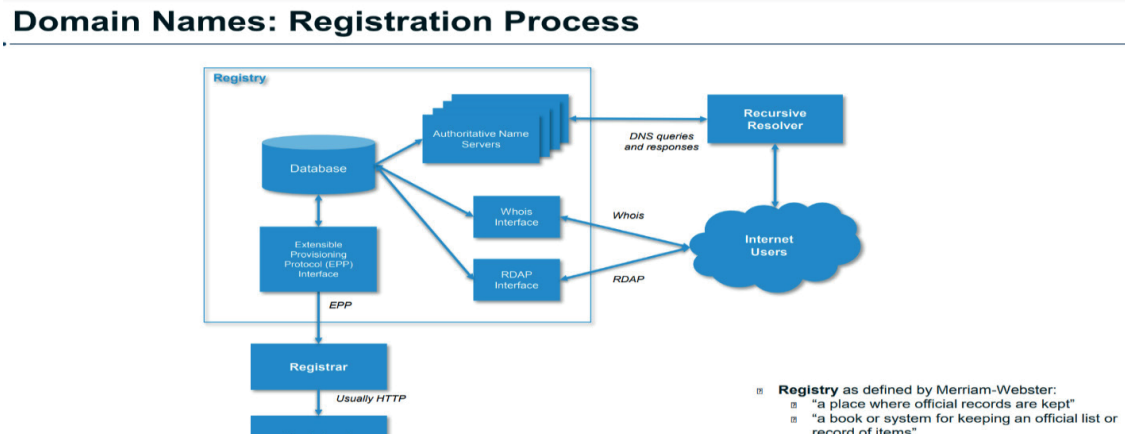
خلال النقاش، اتضح أن هناك اختلافًا في عمليَّة إدارة النطاقات وتسجيلها، يتمثل فيما يلي:

النطاقات الأعلى العامَّة (gTLDs): على جميع مسجلي النطاقات الحصول على اعتماد المسجل من منظمة «ICANN» واتفاقية اعتماد المسجل.

النطاقات الأعلى للدول (ccTLDs): لكل دولة الحرية في اتباع نظامها الخاص في تسجيل المسجلين في النطاقات. وبعض هذه الدول يستخدم اعتماد «ICANN» للمسجلين وبعضها يحصل على اعتماد من جهات أخرى.

3.4.3 إخفاء بيانات المسجل في نطاق الإنترنت

من أهم الخدمات التي يوفرها المسجل: صفحة تفاعليَّة على الإنترنت لتقديم خدمة الاستفسارات (WHOIS) عن البيانات المتعلِّقة بجميع الأسماء المسجَّلة النشطة التي يرعاها المسجل في أي نطاق (gTLD)، وهي بيانات النطاق المسجل وعنوانه وأرقام التواصُل. وهذه البيانات تفيد جهات التحري والاستدلال للتعرُّف إلى أصحاب المواقع الإلكترونيَّة المحتالة. ولكن عند تحليل أسماء النطاقات المحتالة، كما ذُكِر سابقًا، كانت هناك نسبة 86% من المسجلين في النطاقات يخفون بياناتهم. والشكل التوضيحي رقم «22» يبيِّن طريقة الاستفسار عن بيانات النطاقات عبر الإنترنت.



الشكل التوضيحي رقم «22»: طريقة الاستفسار عن بيانات النطاقات عبر الإنترنت

المصدر : عرض مرئي مقدم من ICANN

الصورة توضح أن مستخدمي الإنترنت (Internet User)، ومن ضمنهم جهات التحرِّي والاستدلال، يستطيعون الاستفسار من قاعدة البيانات (Database) للحصول على الاستفسارات الخاصَّة ببيانات صاحب الموقع الإلكترونيَّة؛ لكونها معلومات عامَّة. ولكن أصبح المسجل (Registrant) يسمح لنطاقات بإخفاء بياناتها، وهو ما يصعب عمليَّة اقتفاء أثر المحتالين باستخدام خدمة الاستفسارات.

3.4.4 تأثير لائحة حماية البيانات العامَّة للاتحاد الأوروبي (GDPR) على عمليَّات التحرِّي والاستدلال

في 25 مايو 2018م، دخلت لائحة حماية البيانات العامَّة للاتحاد الأوروبي حيز التنفيذ، واعتُمِدت اللائحة العامَّة لحماية البيانات عبر دول الاتحاد الأوروبي، وتهدف إلى حماية جميع مواطني الاتحاد الأوروبي والمقيمين فيه من انتهاكات الخصوصيَّة والبيانات، وينطبق ذلك على جميع الشركات التي تعالج البيانات الشخصيَّة للأشخاص المقيمين في الاتحاد الأوروبي وتحتفِظ بها بغض النظر عن موقع الشركة.

وأثَّر هذا القرار في خدمات دليل التسجيل والاستفسار (WHOIS) بتحويل المعلومات العامَّة المتاحة عبر الإنترنت (خدمة الاستفسار) إلى معلومات سريَّة، وأصبح التأثير كالآتي:

- الوصول إلى البيانات يتم عبر عدة طبقات مختلفة؛ فهناك معلومات عامَّة ومعلومات سريَّة.
- تحويل البيانات الشخصيَّة لصاحب الموقع إلى سريَّة، وهو عبارة عن تنقيح معلومات المسجل وحمايتها من سجلات «Whois» العامَّة، لتصبح معلومات المسجل محميَّة.
- تواصُل الطرف الثالث (كالجهات الأمنيَّة) مع المسجل المعتمد للحصول على بيانات صاحب الموقع.

وبذلك أصبح من الصعب على جهات البحث والتحرِّي الحصول على المعلومات للتعرُّف إلى أصحاب مواقع الاحتيال المالي.

3.4.5 مخرجات الاجتماع

في نهاية الاجتماع، جرى الخروج بمجموعة من التوصيات، هي:

- على جهات البحث والتحرِّي اتباع الممارسة المعياريَّة للإبلاغ عن الإساءة وتقديم الأدلَّة والمبررات التفصيليَّة لسوء الاستخدام أو إساءته والتواصُل مع المسجل المعتمد.
- يمكن لـ«ICANN» تقديم مزيدٍ من الدعم للدول العربيَّة بناءً على تقارير الإساءة المقدَّمة إلى المسجل. ونحتاج إلى العمل مع الدول العربيَّة لتطوير آليَّة عمل للدول العربيَّة.

- عدم فعالية حجب الموقع لمنع الاحتيال المالي، وأفضل ممارسة هي إلغاء المحتوى وحظر الموقع.
- بناء مركز الجرائم السيبرانيَّة والأدلَّة الرقميَّة بجامعة نايف العربيَّة للعلوم الأمنيَّة قاعدة بيانات لرصد مواقع الاحتيال المالي لعدم وجود قاعدة بيانات خاصَّة بمواقع الاحتيال المالي المخصَّصة باللغة العربيَّة، تكون ذا مصداقيَّة وحياديَّة للدول. وبإمكان قاعدة البيانات الإسهام في قوائم حظر المواقع المشبوهة (RBL).

وتُنشَأ عادة قوائم «RBL» وتُصان بواسطة موفِّري الخدمات التجاريَّة والباحثين ومجتمعات المصلحة العامَّة التي تشغل الوسائل لاكتشاف أو تلقي الإخطار بالتهديدات الأمنيَّة. وتختلف القوائم من حيث التركيز وطرق الكشف، وتتخصَّص كثيرٌ من القوائم في نوع واحد من التهديدات، لكن قوائم «RBL» التي تُدار جيدًا عادةً ما تحتوي على معايير محددة جيدًا لإدراج المعرّف كتهديد بالإضافة إلى عمليَّة إزالته من القائمة. مع «RBLs»، الدقة هي الأولويَّة، ولدى «RBLs» اهتمام واضح بالمصداقيَّة وجودة عملهم، وإذا كانت القائمة غير دقيقة وجديرة بالثقة بشكل مقبول، فلن يستخدمها أحد.

وأنشأت المؤسَّسة نظام التبليغ عن نشاط انتهاك النطاق (DAAR) لمجتمع «ICANN». وفي عام 2019م دُعيت نطاقات المستوى الأعلى للدول للمشاركة في نظام «DAAR» لتوسيع المشاركة في النظام. ويقدِّم المدير الفني المسؤول في «ICANN» تقارير شهريَّة مخصَّصة إلى نطاقات الدول المشاركة في النظام. وانضم 16 نطاقًا من نطاقات الدول فقط.

عند مقارنة الدول الـ16 التي انضمت إلى نظام التبليغ عن نشاط انتهاك النطاق، نجد أنها خالية من الدول التي سجل المحتالون نطاقاتهم فيها ((ICANN, 2021.

3.4.6 الخلاصة

خلال الاجتماع مع مؤسَّسة «ICANN»، اتضح أن أسباب عدم تعاون بعض الدول في توفير أو مشاركة البيانات، كمعلومات بعض النطاقات وعناوين الإنترنت... إلخ للجهات الأمنيَّة في الدول العربيَّة تتمثل في الآتي:

- السبب الأول: اختلاف إدارة تسجيل النطاقات في الإنترنت؛ فالنطاقات الأعلى للدول (ccTLDs) تعطي لكل دولة الحرية في اتباع نظامها الخاص في تسجيل المسجلين في النطاقات، ما قد يصعب عمليَّة الحصول على معلومات النطاقات الاحتياليَّة حالَ عدم تعاون هذه الدول.

- السبب الثاني: منذ 25 مايو 2018م، ودخول لائحة حماية البيانات العامَّة للاتحاد الأوروبي حيز التنفيذ واعتماد اللائحة العامَّة لحماية البيانات عبر دول الاتحاد الأوروبي خلقا بيئة خصبة لنمو عمليَّات الاحتيال بسبب تحويل بيانات المسجل (بيانات النطاقات الاحتياليَّة) في خدمة الاستفسارات (Whois) إلى بيانات سريَّة وسمحت للمسجلين المعتمدين بإخفاء بيانات النطاقات المحتالة عن الظهور للجهات الأمنيَّة.
- السبب الثالث يتعلق بالتحدي في وجود نقص في تأهيل جهات التحرِّي والتحقيق في الدول العربيَّة، حيث يتضح أنهم لم يتلقوا التدريب المناسب المتعلق بالإجراءات الجديدة في التبليغ عن إساءة استخدام النطاقات من المحتالين بعد تحويل بيانات المسجل في خدمة الاستفسارات إلى بيانات سريَّة، وبخاصَّةٍ أن 93% من نطاقات المحتالين توجد في النطاقات الأعلى العامَّة (TLDs). وتؤكِّد اتفاقية اعتماد المسجل الصادرة من مؤسَّسة «ICANN» توفير البيانات للجهات المعنيَّة بعد اتباع الإجراءات الجديدة في التبليغ.

إنَّ اتباع السياسة التقليديَّة في التعامُل مع المواقع الإلكترونيَّة، كحجب المواقع، ليس ذا فعالية على المدى البعيد، وقد تكون حلولًا مؤقتة لمدة محددة. والطريقة المثلى للتعامل مع هذه الجرائم هي التواصُل مع المسجلين المعتمدين وتقديم الإثبات للسير في إغلاق هذه المواقع. ولوحظ عدم وجود جهات من الدول العربيَّة تُعنى برصد مواقع الاحتيال المالي عبر الإنترنت، وبخاصَّةٍ الجهات المدنية، كالجامعات، للإسهام في رصد مواقع الاحتيال المالي والكشف عنها.

لذا، فمن المناسب أن تقوم جامعة نايف العربيَّة للعلوم الأمنيَّة بالريادة في الإسهام والتنسيق في بناء قاعدة بيانات مركزيَّة لرصد مواقع الاحتيال المالي عبر الإنترنت والكشف عنها، ورصد الأساليب الإجراميَّة والطرق التي ينتهجها المحتالون لخروج الأموال عبر الحدود. وسوف تستفيد الجامعة من إجراء البحوث والإسهام في الوقاية من جريمة الاحتيال المالي، وستستفيد من خبرة منظمة الإنتربول في نقل العلم والمعرفة في إعداد التقارير الدوريَّة والنشرات والأساليب الإجراميَّة، ما يُسهِم في الحدِّ من جرائم الاحتيال المالي عبر الإنترنت والوقاية منها. وسوف تستفيد الجامعة أيضًا من خبرة مؤسَّسة الإنترنت للأسماء والأرقام المخصصة (ICANN) لتدريب الجهات على اتباع أفضل الممارسات الدوليَّة لرفع البلاغات للمسجلين المعتمدين وإغلاق النطاقات الاحتياليَّة باللغة العربيَّة. وفي المقابل، سوف تستفيد المؤسَّسة من هذه المبادرة لرصد النطاقات الاحتياليَّة باللغة العربيَّة ومنع هذه النطاقات من استغلال ثغرة إخفاء بياناتها من خدمة الاستفسارات (Whois).

3.5 أفضل الممارسات الدوليَّة للحدِّ من جريمة الاحتيال المالي عبر الإنترنت

بعد تحديد التحديات التي تواجه الجهات المعنيَّة، نركِّز في هذا الفصل على أفضل الممارسات في الحدِّ من جريمة الاحتيال المالي في القطاع الحكومي (الأمني) والقطاع البنكي، بمشاركة القطاعين الحكومي والخاص وإسهامهما. وتشمل أفضل الممارسات في القطاع الأمني عدة مرتكزات رئيسة كما في الشكل التوضيحي رقم «23». ونجد أن هناك تكاملًا بين القطاعين في الحدِّ من جرائم الاحتيال المالي عبر الإنترنت.

الشكل التوضيحي رقم «23»: أفضل الممارسات للحدِّ من جريمة الاحتيال المالي عبر الإنترنت

3.5.1 أفضل الممارسات الدوليَّة للحدِّ من جريمة الاحتيال المالي عبر الإنترنت - القطاع الحكومي:

3.5.1.1 الإستراتيجيَّات الوطنيَّة

نُفِّذت إستراتيجيَّات وطنيَّة ونُشرت في كثيرٍ من البلدان للتصدِّي للجرائم السيبرانيَّة عامَّةً وجرائم الاحتيال المالي عبر الإنترنت خاصَّةً، والجرائم الماليَّة والاقتصاديَّة أو إحداها.

ويمكننا هنا أخذ المملكة المتَّحدة مثالًا: خطة الجريمة الاقتصاديَّة من 2019 إلى 2022م مع أولويَّاتها الإستراتيجيَّة:

وَفقَ خطة الجريمة الاقتصاديَّة، فإن تعريف «الجريمة الاقتصاديَّة» أوسع من مصطلحات أخرى مثل: «الجريمة الماليَّة»، ومن ثَمَّ يوفر استجابة شاملة لكثيرٍ من أنواع الإجرام. ويشمل هذا رقعة واسعة من عمليَّات الاحتيال بجميع أشكالها، مثل عمليَّات الاحتيال ضد الفرد والقطاعين الخاص والعام (UK Government Digital Service, 2021).

وتأتي الأولويَّات الإستراتيجيَّة على النحو الآتي (UK Government Digital Service, 2021):

- فهم التهديد الذي تشكِّله الجريمة الاقتصاديَّة وأدائنا في مكافحتها فهمًا جيدًا.
- السعي إلى تحسين تبادُل المعلومات واستخدامها لمكافحة الجريمة الاقتصاديَّة - داخل القطاعين العام والخاص وبينهما - بين جميع المشاركين.
- التأكُّد من أن الصلاحيَّات والإجراءات وأدوات إنفاذ القانون، ونظام العدالة والقطاع الخاص، فعَّالة قدر الإمكان.
- تعزيز قدرات إنفاذ القانون، ونظام العدالة، والقطاع الخاص، للكشف عن الجريمة الاقتصاديَّة وردعها.
- تعزيز القدرة على مواجهة الجريمة الاقتصاديَّة من خلال دعم إدارة أخطار الجريمة الاقتصاديَّة في القطاع الخاص ودعم النهج الإشرافي القائم على تحديد الأخطار.
- تحسين أنظمتنا من أجل شفافية ملكيَّة الكيانات القانونيَّة والإجراءات القانونيَّة.
- تقديم إستراتيجيَّة دوليَّة طَموحٍ لتعزيز الأمن والازدهار والتأثير العالمي للمملكة المتَّحدة.

3.5.1.2 نموذج استقبال البلاغات

تصنِّف كثيرٌ من الدولِ الاحتيالَ المالي عبر الإنترنت ضمن نطاق الجرائم السيبرانيَّة؛ لذا نجد أن بعض الدول تستقبل البلاغات ضمن مركز الأمن السيبراني، كأستراليا والولايات المتَّحدة الأمريكيَّة والمملكة المتَّحدة، أو تُنشئ مراكز متخصِّصة في استقبال بلاغات جرائم الاحتيال كما هو معمول به في كندا، أو مراكز استقبال بلاغات شاملة لجميع الجرائم كنموذج هونج كونج، ونستعرض فيما يلي أهم النماذج:

أستراليا.. مركز الأمن السيبراني الأسترالي - الإبلاغ السيبراني (ReportCyber)

الإبلاغ السيبراني هو المنصة المركزيَّة للإبلاغ عن الجرائم السيبرانيَّة[2].

وتشمل الأنواع الشائعة من الجرائم السيبرانيَّة: سرقة الهُويَّة، وعمليَّات الاحتيال، وعمليَّات الاحتيال عبر الإنترنت، وعمليَّات إساءة الاستخدام عبر الإنترنت، والابتزاز بالصور عبر الإنترنت، واختراق الأجهزة الإلكترونيَّة (Australian Cyber Security Center, 2021).

كندا.. المركز الكندي لمكافحة الاحتيال

المركز الكندي لمكافحة الاحتيال هو المستودع المركزي في كندا للحصول على معلومات حول عمليَّات الاحتيال، يشترك في إدارته: شرطة الخيَّالة الكنديَّة الملكيَّة، والمكتب المعني بالمنافسة في كندا، وشرطة مقاطعة أونتاريو. ويساعد المركزُ المواطنين والشركات على الإبلاغ عن حالات الاحتيال أو النصب أو الجرائم السيبرانيَّة. وتكون الشرطة المحليَّة هي المسؤولة عن التحقيق. ويساعد المركز على إنفاذ القانون من خلال الاحتفاظ بمستودع معلومات مركزي للمساعدة في التحقيقات (Canadian Anti - Fraud Center, 2021).

شرطة الخيَّالة الكنديَّة الملكيَّة.. نظام جديد للإبلاغ عن الجرائم السيبرانيَّة وحالات الاحتيال

يهدف نظام الإبلاغ الجديد إلى تسهيل الإبلاغ عن الجرائم السيبرانيَّة وحالات الاحتيال، وبمجرد تطبيقه وتشغيله بالكامل (يُتوقع ذلك بحلول عام 2023م) سيتمكن كلُّ مَن يقع ضحية لجريمة سيبرانيَّة أو يشهد عليها من استخدام هذا النظام للإبلاغ عن الجريمة عبر الإنترنت.

وقد بدأ التشغيل التجريبي للخدمة الجديدة عبر الإنترنت في مارس 2020م. ويعاد توجيه عدد قليل من المستخدمين كل يوم من نظام الإبلاغ عن الاحتيال عبر الإنترنت التابع للمركز الكندي لمكافحة الاحتيال الحالي إلى النظام الجديد. وإلى أن يكتمل نظام الإبلاغ الجديد، يجب على الكنديين والشركات الكنديَّة الاستمرار في الإبلاغ عن الجرائم السيبرانيَّة والاحتيال من خلال نظام الإبلاغ عن الاحتيال المتاح على موقع المركز الكندي (Royal Canadian Mounted Police, 2021).

[2] الجريمة السيبرانيَّة هي استخدام الحاسوب أو الإنترنت لارتكاب جرائم، مثل: الاحتيال، والابتزاز بالصور عبر الإنترنت، وسرقة الهُويَّة أو التهديد والترهيب. وبما أن الجريمة السيبرانية في حالة تطوُّر مستمر، بدأ المجرمون في استهداف الأفراد، والشركات، والمؤسَّسات التعليميَّة، والحكومات.

هونج كونج (الصين).. مركز الإبلاغ الإلكتروني لقوات شرطة هونج كونج

صُمِّم مركز الإبلاغ الإلكتروني للإبلاغ أو الاستفسار في الحالات غير الطارئة، حيث يمكن الإبلاغ عن مجموعة كبيرة من الحوادث والحالات الإجراميَّة، بما في ذلك الجرائم السيبرانيَّة والاحتيال المالي عبر الإنترنت وكذلك حوادث الطرق (Anti - Deception Coordination Center, 2021).

المملكة المتَّحدة.. المركز الوطني للإبلاغ عن الاحتيال والجرائم السيبرانيَّة (ACtionFraud)

«ACtionFraud» هو المركز الوطني في المملكة المتَّحدة للإبلاغ عن الاحتيال والجرائم السيبرانيَّة؛ حيث يمكن للأشخاص الإبلاغ إذا تعرَّضوا للنصب، أو الاحتيال، أو جريمة سيبرانيَّة أخرى في إنجلترا، أو ويلز، أو أيرلندا الشماليَّة. ويمثل أيضًا نقطة اتصال مركزيَّة للحصول على معلومات عن الاحتيال والجرائم الإلكترونيَّة ذات الدوافع الماليَّة. ويمكن أيضًا تلقي الشكاوى من الأفراد القاطنين خارج المملكة المتَّحدة حالَ تحويلهم أموالًا إلى حسابات مصرفيَّة داخل المملكة المتَّحدة أو خداعهم من قِبَل جهات داخل أراضي المملكة.

تدير الخدمةَ شرطةُ مدينة لندن، بالتعاون مع مكتب الاستخبارات الوطني المعني بالاحتيال، ويتوليان مسؤوليَّة تقييم التقارير، كما أن شرطة مدينة لندن هي الجهاز الذي يتولَّى أعمال الشرطة فيما يخص الجرائم الاقتصاديَّة.

يتيح المركز وموقعه مجموعة كبيرة من المعلومات عن الاحتيال وجرائم الإنترنت، بهدف منعها ورفع الوعي بشأنها (National Fraud & Cyber Crime Reporting Center, 2021).

الولايات المتَّحدة.. مركز شكاوى جرائم الإنترنت التابع لمكتب التحقيقات الفيدرالي

يتيح مركز شكاوى جرائم الإنترنت للعامَّة آليَّة إبلاغ موثوقًا بها ومريحة لإرسال معلوماتهم إلى مكتب التحقيقات الفيدرالي فيما يخص أنشطة الجريمة المشتبه بها والميسرة بالإنترنت. ويشكِّل المركز تحالفات فعَّالة مع جهة إنفاذ القانون، وشركاء المجال. وتخضع المعلومات للتحليل، وتوزَّع لأغراض التحقيق والاستخبارات لإنفاذ القانون وتوعية العامَّة. ويقدم قسم الأسئلة المتكررة تعريفًا لجريمة الإنترنت[3].

[3] تشمل جرائم الإنترنت أي نشاط غير قانوني ينطوي على مكون واحد من مكونات الإنترنت أو أكثر، مثل: المواقع الإلكترونية، وغرف المحادثة، والبريد الإلكتروني. وتنطوي جرائم الإنترنت على استخدام الإنترنت لإرسال عروض مزيَّفة أو احتياليَّة للمستهلكين. على سبيل الذكر لا الحصر: قد تحتوي هذه الجرائم على مخطط رسوم مسبقة، أو العزوف عن إرسال البضائع أو إجراء الخدمات، أو اختراق الحاسوب، أو مخطط فرصة عمل أو فرصة نشاط تجاري.

إذا كان أيٌّ من الضحيَّة أو الجاني المزعوم في جريمة الإنترنت داخل الولايات المتَّحدة، فيمكن تقديم شكوى إلى جانب الشهادة الدوليَّة للحاسب والإنترنت.

يتيح المركز والموقع أيضًا مجموعة كبيرة من المعلومات، بما فيها إنذارات للمستهلكين والقطاعات (Internet Crime Complaint Center, 2021).

3.3.1.3 نموذج المكاتب المركزيَّة المتخصِّصة

عند مراجعة أفضل الممارسات الدوليَّة الحديثة في التعامُل مع جرائم الاحتيال، برز إنشاء مراكز متخصِّصة للتعامُل مع الجرائم السيبرانيَّة، ومن ضمنها: جرائم الاحتيال المالي، أو مركز متخصِّص في جرائم الاحتيال. ويتضح من الممارسات الدوليَّة أن نموذج المكاتب المركزيَّة المتخصِّصة حديث، وأغلب الدول بدأت بهذه التجرِبة منذ عام 2017م. واتضح أن هناك نموذجين لإدارة هذه المراكز، النموذج الأول يُدار من جهات إنفاذ القانون، ويندرج تحت مركز الأمن السيبراني أو مركز متخصِّص للاحتيال، أما النموذج الثاني فيُدار من جهاز النيابة العامَّة والقضاء.

النموذج الأول: جهات إنفاذ القانون

أستراليا.. مركز الأمن السيبراني الأسترالي

يتبع مركز الأمن السيبراني الأسترالي مديرية الإشارات الأستراليَّة. ويقود المركز جهود الحكومة الأستراليَّة لتحسين الأمن السيبراني؛ إذ يتابع التهديدات السيبرانيَّة حول العالم، ويقدِّم المشورة والمعلومات فيما يخصُّ الحماية على الإنترنت. وبتتبع حوادث الأمن السيبراني، يقدم المركز المشورة في الوقت المناسب للأفراد، والشركات، ومشغلي الهياكل الأساسيَّة في البنية التحتيَّة (Australian Cyber Security Center, 2021).

كندا.. وحدة التنسيق الوطنيَّة للجرائم السيبرانيَّة

أسست كندا عام 2020م هذه الوحدة التي تتكوَّن من شرطة الخيَّالة الكنديَّة الملكيَّة ومدنيين من جميع الخلفيَّات. وتعمل هذه الوحدة مع جهة إنفاذ القانون وشركاء آخرين للمساعدة على تقليص

تهديد الجريمة السيبرانيَّة، وأثرها، والوقوع ضحية لها في كندا. فيكمن دور الوحدة ومهمتها في تنسيق التحقيقات في الجرائم السيبرانيَّة في كندا، والعمل مع شركاء من جميع الدول لمكافحة مجموعة كبيرة من حوادث الجريمة السيبرانيَّة، وتقديم نصائح ومشورة إلى الشرطة الكنديَّة في مجال التحقيق.

تتضمَّن الأنشطة المستقبليَّة إنتاج معلومات استخباراتيَّة يمكن اتخاذ إجراءات بشأنها للشرطة الكنديَّة، وتطبيق نظام جديد للإبلاغ عن الجرائم السيبرانيَّة والاحتيال للمواطنين الكنديين والشركات بالتعاون مع المركز الكندي لمكافحة الاحتيال. ومن المخطط أن تصل الوحدة إلى كامل قدرتها التشغيلية في عام 2023 (Royal Canadian Mounted Police, 2021).

فرنسا.. فريق العمل الوطني لمكافحة النصب

في ضوء ارتفاع معدل عمليَّات النصب والاحتيال الممكَّنة والميسرة في أثناء جائحة «كوفيد 19»، جاء تكوين فريق العمل الوطني لمكافحة النصب والاحتيال المتعلقين بأزمة «كوفيد 19» في أبريل 2020م بأمر الحكومة الفرنسيَّة. تقود فريق العمل المديرية العامَّة للتنافسيَّة والاستهلاك وردع الاحتيال.

تكمن مسؤوليَّة فريق العمل في تبادُل التحذيرات والمعلومات للتعامل سريعًا مع أي حالة احتيال، واستغلال عدم اليقين والضعف، والنمو الاقتصادي نتيجة الأزمة. كما يتيح توجيهات لمنع حوادث النصب والاحتيال (DGCCRF, 2021).

هونج كونج (الصين).. مركز التنسيق لمكافحة الغش

تكثيفًا لأنشطة مكافحة الغش وزيادة وعي العامَّة بشأن مختلف أنواع النصب، أسست شرطة هونج كونج مركز التنسيق لمكافحة الغش الخاضع لمكتب الجريمة التجاريَّة بغرض توحيد كل الجهود المعنيَّة للشرطة في مكافحة الجريمة ومنعها. منذ بدء تشغيل المركز في 20 يوليو 2017م وهو يتيح خطًّا ساخنًا للاستفسار باسم «شرطة مكافحة النصب 18222»، يعمل على مدار 24 ساعة لتقديم المشورة الفوريَّة للعامَّة، وتحسين دعم وحدات الخط الأمامي للشرطة بهدف التعامُل مع حالات الغش المشتبه بها بطريقة أكثر فعالية.

ويقوم المركز بالمهام الرئيسة الآتية:

- وضع التوجهات الإستراتيجيَّة وتطبيقها لمكافحة الغش.
- تقديم خدمة المشورة الفوريَّة للعامَّة عبر التليفون فيما يخص مكافحة الغش من أجل تقديم المساعدة في الوقت المناسب إلى مَن يحتاج إليها.
- تحسين التعاوُن بين الشرطة والإدارات الحكوميَّة الأخرى وأصحاب المصلحة بالداخل والخارج لمكافحة الغش ومنعه.
- تنظيم مواد الإعلان عن مكافحة الغش وحملات التثقيف المقدَّمة من وحدات الشرطة المختلفة، وتقديم الدعم الفوري لوحدات الخط الأمامي للشرطة.
- متابعة اتجاهات الغش وتحليلها، وتوفير تقييم للأخطار، واتخاذ إجراءات في التوقيت المناسب (Hong Kong Police Force, 2021).

سنغافورة.. مركز مكافحة النصب

هو وحدة تابعة لإدارة الشؤون التجاريَّة لقوات الشرطة السنغافوريَّة، مهمته هي منع النصب وردعه والكشف عنه. وفيما يلي موجز لأنشطته:

- معالجة المعلومات.
- التدخُّل (بنهج التعطيل: التجميد المركزي للحسابات المصرفيَّة، ووقف خطوط الهاتف، وإزالة إعلانات الإنترنت المشتبه بها).
- التحقيق والاستخبارات.
- المبادرات والابتكار.
- التعاون الدولي.

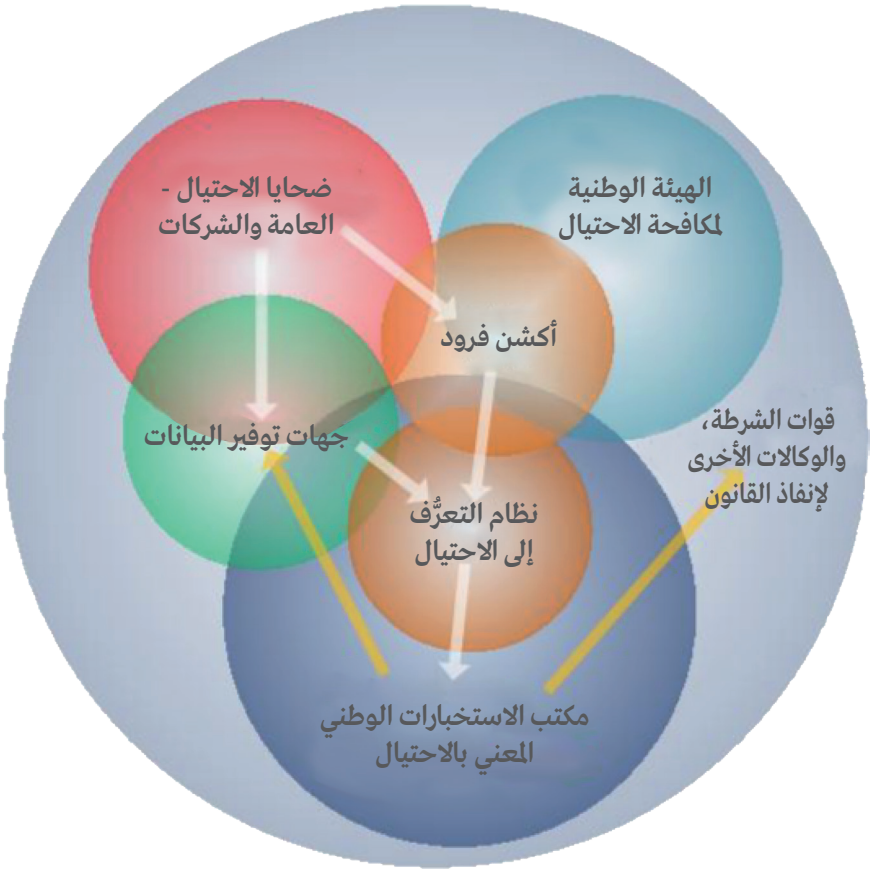
يعمل مركز مكافحة النصب في شبكة مكونة من أكثر من ثلاثين مصرفًا وشخصًا اعتباريًّا لمحاربة النصب. في خلال السنة الأولى من تأسيس المركز (2019م)، ساعد في استعادة 21 مليون دولار أمريكي، وجمَّد - على الأقل - 6100 حساب مصرفي مشتبه به، وأقام شراكات حيويَّة مع كثيرٍ من شركاء المجال ((Singapore Police Force, 2021.

المملكة المتَّحدة.. مكتب الاستخبارات الوطني المعني بالاحتيال

يعمل مكتب الاستخبارات الوطني المعني بالاحتيال جنبًا إلى جنب مع «ACtionFraud» التابع لشرطة مدينة لندن التي تمثل الجهاز الذي يتولَّى أعمال الشرطة فيما يخص الجرائم الاقتصاديَّة. ويتلقَّى المكتب جميع تقارير «ACtionFraud»، ويستخدم ملايين من تقارير الاحتيال والجريمة السيبرانيَّة للتعرُّف إلى المجرمين، ومجموعات الجريمة المنظَّمة، والبحث عن الأنواع الناشئة من الجرائم. ويستمد البيانات من ثلاث قنوات رئيسة:

- تقارير الأفراد والشركات الصغيرة (إما مباشرةً وإما عبر قوات الشرطة) المقدمة إلى «ACtionFraud» عبر التليفون أو الإنترنت.
- بيانات الاحتيال من الصناعة ذاتها أو من القطاع العام الذي يشمل المصارف، والتأمينات، والاتصالات، والإدارات الحكوميَّة.
- مجموعة متنوعة من المصادر الاستخباراتيَّة التي تشمل، على سبيل الذكر لا الحصر: أنظمة الشرطة الجنائيَّة/ الاستخباراتيَّة الوطنيَّة والدوليَّة.

يعمل بالمكتب ضباط شرطة وموظفو استخبارات من المنظَّمات العامَّة، والخاصَّة، والخارجيَّة، بما فيها: نظام تجنُّب الاحتيال في قطاع الائتمان (خدمة مكافحة الاحتيال في المملكة المتَّحدة)، وشرطة مدينة لندن، والهيئة الوطنيَّة لمكافحة الاحتيال، ومكتب مكافحة جرائم الاحتيال الخطيرة، وهيئة مكافحة الجريمة المنظَّمة الخطيرة، وهيئة تنظيم المحامين (National Fraud & Cyber Crime Reporting Center, 2021) & (City of London, 2021). والشكل التوضيحي رقم «24» يبيِّن الجهات البريطانيَّة المشاركة في مكافحة الاحتيال.



الشكل التوضيحي رقم «24»: الجهات البريطانيَّة المشاركة في مكافحة الاحتيال

المملكة المتَّحدة.. المركز الوطني للجرائم الاقتصاديَّة

أُطلِق المركز الوطني للجرائم الاقتصاديَّة في أكتوبر 2018م بهدف إحداث فارق في تعامُل المملكة المتَّحدة مع الجريمة الاقتصاديَّة. وحقَّق المركز، لأول مرة، الجمع بين وكالات إنفاذ القانون وهيئات العدالة، والإدارات الحكوميَّة، والهيئات التنظيميَّة، والقطاع الخاص، بهدف مشترك هو العمل على خفض معدل الجريمة الاقتصاديَّة المنظَّمة والخطيرة، وحماية العامَّة وضمان ازدهار المملكة المتَّحدة وسمعتها، كونها مركزًا ماليًّا. ينظم المركز ويوزع المهام في إطار تعامُل المملكة المتَّحدة مع الجريمة الاقتصاديَّة، ويسخِّر الاستخبارات والإمكانات من القطاعين العام والخاص لمعالجة الجريمة الاقتصاديَّة بطريقة أكثر فاعلية.

يضمن المركز اقتفاء أثر المتهمين بالاحتيال على المواطنين البريطانيين، ومهاجمة الصناعة في المملكة المتَّحدة، وإساءة استخدام الخدمات الماليَّة بالمملكة المتَّحدة، بالإضافة إلى ضمانِهِ تثقيف الصناعات المختلفة والأجهزة الحكوميَّة في المملكة المتَّحدة بكيفيَّة الحماية من الجرائم الاقتصاديَّة، وتكثيف حماية مواطني المملكة المتَّحدة (National Crime Agency, 2021).

الشكل التوضيحي رقم «25» يسرد الأجهزة الممثلة في المركز الوطني للجرائم الاقتصاديَّة.

الشكل التوضيحي رقم «25»: المركز الوطني للجرائم الاقتصاديَّة يجمع الجهات المعنيَّة في بريطانيا في مكان واحد

النموذج الثاني: النيابة العامَّة والقضاء

البوَّابة الأوروبيَّة للقضاء الإلكتروني

صُمِّمت البوَّابة الأوروبيَّة للقضاء الإلكتروني لتكون «مجمعًا (إلكترونيًّا)» للمعلومات عن القضاء الأوروبي، وللوصول إلى الإجراءات القضائيَّة الأوروبيَّة. تستهدف البوَّابة المواطنين، والشركات، والممارسين القانونيين، والجهاز القضائي. ويتمتَّع المواطنون بالحق في الوصول إلى أنظمة القضاء في الدول الأعضاء الأخرى كحقهم في دولهم. وتُسهم البوَّابة الأوروبيَّة للقضاء الإلكتروني بطريقة عمليَّة في إزالة العوائق بإتاحة المعلومات بثلاث وعشرين لغة ومجموعة هائلة من الروابط للمواقع الإلكترونيَّة والوثائق ذات الصلة.

وعلى الرغم من أن مسؤوليَّة محتوى البوَّابة وإدارتها مقسمة بين المفوضيَّة الأوروبيَّة والدول الأعضاء بالاتحاد الأوروبي، فإن المتحكِّم في بيانات البوَّابة الأوروبيَّة للقضاء الإلكتروني هو المفوضية الأوروبيَّة.

وتحتوي على موضوعات رئيسة في مجالات فرعية، هي:

- الأنظمة القضائيَّة (معلومات عن تنظيم القضاء في الاتحاد الأوروبي وعلى المستوى الوطني).
- الذهاب إلى المحكمة (إرشادات ومعلومات عن الإجراءات القانونيَّة العابرة للحدود).
- المساعدة القانونيَّة (للمواطنين، والشركات، والممارسين القانونيين، والجهاز القضائي).
- ضحايا الجريمة (معلومات عامَّة عن حقوق الضحيَّة).
- أدوات المحاكم والممارسين (خاصَّة للإجراءات العابرة للحدود في الأمور المدنيَّة والجنائيَّة).
- السجلات (شاملة الشركات، والأراضي، وسجلات الإعسار) (European Justice, 2021).

ألمانيا.. المكتب المركزي للجرائم السيبرانيَّة بافاريا

منذ إطلاق المكتب المركزي للجرائم السيبرانيَّة بافاريا في يناير 2015م، وكان مقره في مكتب النائب العام في بامبرغ/ بافاريا (ألمانيا)، وتتمثل مسؤوليَّته في التعامُل مع إجراءات التحقيق المتقدِّمة في مجال الجرائم السيبرانيَّة داخل بافاريا. ويجري التحقيقات بالتعاون مع المختصين ذوي الصلة من الشرطة أو المكتب الجنائي الفيدرالي وشركاء دوليين، على سبيل المثال: في حالات الهجوم على القطاعات الاقتصاديَّة الكبرى أو في حالات الجرائم السيبرانيَّة المنظَّمة والاقتصاديَّة أو إحداهما. حتى في حالة الإجراءات الجنائيَّة العامَّة عند الحاجة إلى مستوى رفيع من التحقيق في مجال الحاسبات وتكنولوجيا المعلومات، يتدخَّل وكلاء النيابة بالمكتب المركزي. وتختلف الحالات المتطلبة لتعامُل المكتب؛ حيث تتراوح بين هجمات القرصنة ومجموعة كبيرة من حالات النصب والاحتيال عبر الإنترنت، على سبيل المثال عن طريق المتاجر المزيفة، بالإضافة إلى حالات إرسال الفيروسات، والاتجار في الأسلحة والمخدِّرات والنقود المزيَّفة عبر الإنترنت المظلمة (Bavarian State Ministry of Justice, 2021).

المملكة المتَّحدة.. إنشاء محكمة جرائم اقتصاديَّة (وَفقًا لإستراتيجيَّة مكافحة الجريمة الاقتصاديَّة، 2025م)

تقدِّم إستراتيجيَّة مكافحة الجريمة الاقتصاديَّة رؤية رفيعة المستوى، تتضمَّن الالتزام بضمان محاكمة الشخص المعني على المخالفة التي ارتكبها في الوقت المناسب، وإشراك الضحايا والشهود في ثنايا القضية وتغطية جميع إجراءات القضية. وتمثل منطوق الدور الذي تؤدِّيه دائرة الادعاء الملكيَّة، مُسهِمةً في تحسين نتائج القضاء الجنائي في محاربة الجرائم الاقتصاديَّة.

تتضمن الإستراتيجيَّة مجموعة من الالتزامات، منها:

- مراجعة الهياكل والإمكانات لضمان امتلاك الموارد المناسبة في المكان المناسب.
- دعم عقد جلسات افتراضيَّة أكثر من ذي قبل لقضايا الجرائم الاقتصاديَّة؛ للمساعدة على تقليل عدد القضايا المتأخرة وتحقيق العدالة للضحايا والشهود بشكل أكثر فاعلية.
- استرداد عائدات الجريمة، وحرمان المجرمين من مكاسبهم غير المشروعة، والسعي إلى تعويض الضحايا قدر الإمكان.
- استغلال الفرص التي تتيحها التقنية لدعم المحاكمات الفعَّالة للقضايا الاقتصاديَّة، مع الحفاظ على الحق في محاكمة عادلة وفي الحفاظ على الخصوصية.
- دعم إنشاء أول محكمة اقتصاديَّة على الإطلاق واستغلال المحاكم المؤقَّتة (محاكم نايتنجيل) لقضايا الاحتيال.

وتدير دائرة الادعاء الملكيَّة بالفعل وحدة مخصصة لتعقُّب الأصول واستردادها، تُقدَّر عائداتها بأكثر من 100 مليون جنيه إسترليني من مكاسب المجرمين غير المشروعة في عامي 2019 و2020م (The Crown Prosecution Service, 2021).

3.5.1.4 تعقُّب الأصول واعتراض الأموال

تعقُّب الأصول واستردادها من المشكلات الدوليَّة المتأصِّلة على الساحة الحالية للاحتيال المالي عبر الإنترنت/ السيبراني؛ فعلى الرغم من الجهود المبذولة على مدار السنوات القليلة الماضية، فمعدَّل تعقُّب الأصول المكتسبة بأساليب غير مشروعة واعتراضها ومصادرتها وإعادتها إلى الوطن لا يزال منخفضًا، وقد يكون ذلك بسبب التحديات المؤسَّسيَّة، والقانونيَّة، وصعوبة التواصُل. ما فاقم تعقيد ساحة الاحتيال الممكَّن عبر الإنترنت وغسل الأموال المقترن به هو ظهور تقنيات سلسلة الإمداد، وزيادة استخدام الأصول الافتراضيَّة، إلى جانب التقنيات الماليَّة الصاعدة الأخرى. وتتطلَّب هذه الظاهرة مراقبة وكالات إنفاذ القانون ويقظتها.

وتتضمَّن عمليَّة تعقُّب الأصول واستردادها مراحل عدَّة، مثل:

- التعرُّف إلى الأصول المكتسبة بطرق غير مشروعة وتعقبها.
- تجميد الأصول وحجزها تحسُّبًا لمصادرتها فيما بعد.

- إدارة الأصول المجمَّدة والمحتجزة للحفاظ على قيمتها.

- التصرُّف في الأصول المصادَرة، بطرقٍ منها: إعادة استخدامها لأغراض عامَّة أو اجتماعيَّة.

ولقد أصدرت، مؤخرًا، مجموعة العمل المالي (فاتف)، المراقب العالمي لغسل الأموال وتمويل الإرهاب، تصريحًا مفاده: «ينبغي للحكومات إعطاء أجهزة التحقيق السلطة لتعقُّب الأصول المكتسبة عن طريق الجرائم، وحجزها، ومصادرتها نهائيًّا، إلى جانب تحديد إطار العمل اللازم للسماح للأجهزة المعنيَّة بتبادُل المعلومات بين بعضها البعض، ومع أقرانها في البلدان الأخرى[4] ويُعد هذا التصريح دعوةً مباشرة لمنظمة الإنتربول لتستخدم مكانتها الفريدة لعمل منصة لتبادل معلومات إنفاذ القانون لاسترداد الأصول.

وتتدفَّق العائدات الإجراميَّة من جرائم الاحتيال عبر الإنترنت بسرعة عبر الحدود والسلطات التشريعيَّة الوطنيَّة. ويسعى المحتالون إلى إيجاد طرقٍ لنقل عائدات الجريمة قبل اكتشاف عمليَّات النصب. ولتعزيز إمكانيَّة استعادة الأموال، يُعد الاهتمام بالوقت هو الأساس. وينبغي أولًا تحديد موقع الأصول وحجزها عقب بلاغ الضحيَّة.

في هذا الفصل الفرعي، تُعطَى الأهمية لمكون تعقُّب الأصول وحجز الأموال، ودائمًا ما يكون للوقت الأهمية القصوى عندما يتعلَّق الأمر بالمدفوعات العابرة للحدود المكتسبة من الاحتيال، التي يجب أن تخضع لجهود التعقُّب الفوري للأصول، وحجز الأموال.

ويُعد أيضًا تجميد الأصول الإجراميَّة ومصادرتها أداتين فعالتين لمكافحة الجرائم المنظَّمة والخطيرة على المستوى الدولي. وتتضمَّن اتفاقية الأمم المتَّحدة لمكافحة الجريمة المنظَّمة (الصادرة عام 2000م) واتفاقية الأمم المتَّحدة لمكافحة الفساد (الصادرة عام 2003م) أحكامًا تتطلَّب من الدول الأطراف ما يلي:

السماح بتعقُّب الأصول غير المشروعة، وتجميدها، ومصادرتها على أراضيها.

- تبادُل المعلومات والتعاون في عمليَّة استرداد الأصول.

- وتُطَبَّق هاتان الاتفاقيتان دوليًّا بتصديق أكثر من 185 بلدًا.

وفي سياق مكافحة غسل الأموال وتمويل الإرهاب، تنطوي معايير مجموعة «فاتف» على إجراءات مشابهة، وتتطلَّب من البلدان تطبيق إجراءات متينة للتجميد والمصادرة إلى جانب القدرة على

[4] مجموعة «فاتف»، ما المقصود بغسل الأموال؟ sptth://www.fatf-fiag.org/qaf/money-laundering/، (تاريخ آخر وصول: 32 أغسطس 0202م).

التعاون لاسترداد الأصول. وتعترف مجموعة «فاتف» بأن «تقليص مكاسب الجريمة يؤثِّر في الموازنة بين المخاطرة والمكسب، وقد تردع احتماليَّة خسارة الأرباح بعض الناس عن ارتكاب الجرائم، وقد يسمح ذلك أيضًا بتعويض ضحية الجريمة جزئيًّا أو كليًّا حتى عند نقل عوائد الجريمة حول العالم. ويحدث ذلك خاصَّةً في حالة استرداد الأصول» (المفوضية الأوروبيَّة، 2020).

تقرير مجموعة «فاتف»: التحديات التنفيذيَّة لاسترداد الأصول.. إجراءات تحسين الفاعليَّة العالميَّة

يعرض تقرير مجموعة «فاتف» المتوقَّع نشره لأعضاء المجموعة لاحقًا في 2021م نظرةً عامَّةً شاملةً على التحديات التنفيذيَّة، ويقدم توصيَّات جوهريَّة لتحسين فاعليَّة إجراءات تعقُّب الأصول واستردادها، وتطبيق هذه الإجراءات.

يُنسَّق التقرير على هيئة فقرات متعددة تغطي المجالات والموضوعات الرئيسة التالية:

- تحديد الأولويَّات والتنظيم الإستراتيجي والتنفيذي: بناء ثقافة استرداد الأصول.
- التعقُّب الفعَّال للأصول.
- إطار العمل الدولي لتيسير استرداد الأصول العابرة للحدود.
- تمكين السلطات القانونيَّة للتأمين والتجميد والحجز الفعَّال.

ويحتوي هذا التقرير على مجموعة من التوصيات الجوهريَّة لكل مجال وموضوع، وتستحق التوصيات اهتمام صُنَّاع السياسات والقرارات بوضعها في الحسبان، وقد تساعد في تحسين جهود آليَّات وأنشطة تعقُّب الأصول ونتائجها.

الشبكات والقنوات المختصَّة

تشمل اتفاقيَّة الأمم المتَّحدة لمكافحة الجريمة المنظَّمة 41 مادة، من أهمها: مُصادرة عائدات الجريمة وتعزيز التعاون الدولي، وتنص على تدابير للتدريب وإجراء البحوث وتبادل المعلومات، وتشجِّع على اعتماد سياسات عامَّة وتدابير وقائيَّة. وعند مراجعة أفضل الممارسات في تعقُّب الأصول واستردادها، اتضح أنها تقوم على قسمين رئيسين، الأول: الممارسات على المستوى المحلي، والثاني: الممارسات على المستوى الإقليمي لتعقُّب الأصول واستردادها.

المستوى المحلي:

ألمانيا (النيابة العامَّة).. مكتب التنسيق المركزي لتعقُّب الأصول واستردادها

يعمل مكتب التنسيق المركزي لتعقُّب الأصول واستردادها في بافاريا (ZKV BY) - وقد أُسس في عام 2018م - في مكتب النائب العام في ميونيخ (بافاريا/ ألمانيا). ويدعم مكتب «ZKV BY» المحاكم البافارية والمدعين العموم بها ويساعدهم في تحقيق الهدف من تنفيذ التعقُّب المستمر للأصول مجهولة المصدر ومصادرتها في مختلف أنحاء البلاد، كما يعد المكتب، باستمرار، أداة فعَّالة لمكافحة الجريمة المنظَّمة والجريمة الاقتصاديَّة وجرائم المخدِّرات، فضلًا عن دوره في الحدِّ من تمويل مرتكبي الأعمال الإرهابيَّة والجمعيَّات المعاونة لهم.. وتحقيقًا لهذه الغاية، يقوم المكتب بما يلي على وجه التحديد:

- تنسيق مهام نقاط الاتصال لحل المسائل الإجرائيَّة المتداخلة.
- توفير برامج تدريبيَّة في مجال تعقُّب الأصول واستردادها بالتنسيق مع وزارة العدل البافارية.
- إسداء المشورة للمحاكم والمدعين العموم بشأن المسائل الإجرائيَّة الفرديَّة المعقدة (Bavarian State Ministry of Justice, 2021).

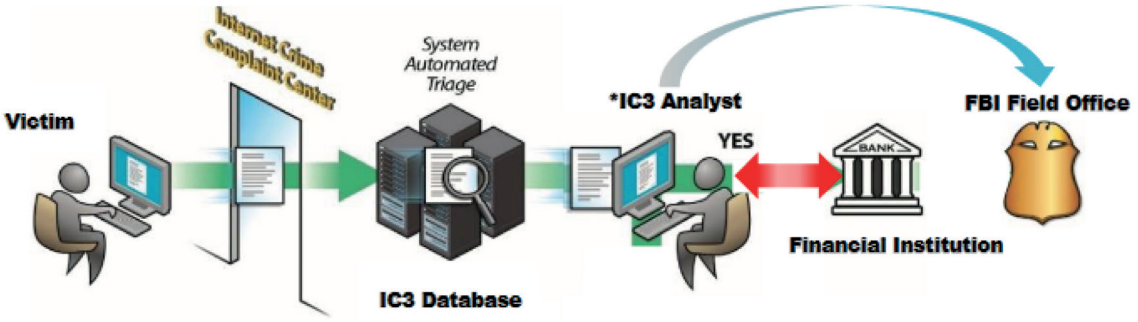
أوكرانيا.. وكالة استرداد الأصول وإدارتها (ARMA)

تُعد وكالة «ARMA» هيئة حكوميَّة خاصَّة مأذونًا لها بصياغة سياسة الدولة وتنفيذها فيما يتعلَّق بتعقُّب الأصول المعرَّضة للحجز أو المُراد حجزها والعثور عليها، وكذلك إدارة الأصول المحجوزة بسبب دعاوى جنائيَّة. كما تعمل بوصفها وكالة وطنيَّة لدى أوكرانيا، وتختص بالعثور على الأصول المكتسَبة من الفساد وغيره من الجرائم الأخرى وتعقُّبها وإدارتها.

ويحقُّ لها، بوصفها وكالة وطنيَّة، أن تدعم قضايا التحقيق الجنائي باتخاذ إجراءات من أجل تعقُّب الأصول والعثور عليها بناءً على طلب المحققين، والمفتشين، وسلطات التحقيق قبل المحاكمة، ومكتب النائب العام، والمحاكم، كما يحق لها أن تتعاون مع هذه السلطات من أجل حجز هذه الأصول ومصادرتها (EUACI, 2021).

الولايات المتَّحدة.. فريق استرداد الأصول (RAT) التابع لمركز شكاوى جرائم الإنترنت

أُسِّس فريق استرداد الأصول التابع لمركز شكاوى جرائم الإنترنت (RAT) في فبراير 2018م لتيسير التواصُل مع المؤسَّسات الماليَّة، ومساعدة المكاتب الميدانيَّة لمكتب التحقيقات الفيدرالي في تجميد أموال الضحايا الذين حوَّلوا إلى حسابات محليَّة بعد تعرُّضهم لعمليَّات احتيال. ويُعد الفريق حلقة وصل بين مؤسَّسات إنفاذ القانون والمؤسَّسات الماليَّة؛ إذ يدعمهما بالتحاليل الإحصائيَّة والاستقصائيَّة. والشكل التوضيحي رقم «26» يبيِّن المراحل المختلفة لعمليَّة تقديم الشكاوى. تُقدَّم الشكاوى عن طريق موقع إلكتروني ومن ثم تتجه لفريق الاسترداد المكون من الجهات ذات العلاقة الذي يجمِّد التحويلات المالية حتى انتهاء التحقيق.



الشكل التوضيحي رقم «26»: المراحل المختلفة لعمليَّة تقديم الشكاوى

المصدر: مركز شكاوى جرائم الإنترنت - تقرير جرائم الإنترنت 2020م: تُظِهر الصورة المراحل المختلفة لعمليَّة تقديم الشكاوى إلى فريق استرداد الأصول

أهداف فريق استرداد الأصول وشراكاته مع المؤسَّسات الماليَّة:

- المساعدة على تحديد الحسابات الاحتياليَّة المحتملة في جميع أنحاء القطاع.
- البقاء في طليعة الاتجاهات الناشئة فيما يخصُّ مخططات عمليَّات الاحتيال المالي الجديدة.
- تعزيز علاقة تكافليَّة تتشارك فيها المعلومات بشكل مناسب (Internet Crime Complaint Center, 2020).

على المستوى الإقليمي:

الشبكة التنفيذيَّة لمكافحة غسل الأموال (AMON)

أُطلقت الشبكة في عام 2012م، وهي شبكة دوليَّة تجمع ممارسي إنفاذ القانون العاملين في مجال تحقيقات مكافحة غسل الأموال. وتهدف إلى تعزيز التعاون عن طريق شبكة دوليَّة من ممارسي مكافحة غسل الأموال الممثلين حاليًّا لنحو 40 بلدًا/ سلطة تشريعيَّة وثلاث منظَّمات دوليَّة. يركِّز محققو الشبكة على جميع جوانب أنشطة غسل الأموال، مع التشديد على التعامُل السريع مع الأمور التنفيذيَّة. وتستضيف «يوروبول» الأمانة العامَّة للشبكة، وتساعد على تنظيم الاجتماع السنوي.

وبناءً على خبرة منظمة الإنتربول، تركِّز بعض نقاط الاتصال الوطنيَّة لشبكات «AMON» بشكل تنفيذي، ويمكن أن تساعد في الحالات العاجلة/ الخطرة على تعقب الأصول، واعتراض الأموال في الوقت المناسب.

المنتدى العربي لاسترداد الأصول

منذ إطلاق المنتدى العربي لاسترداد الأصول في عام 2012م وهو يعمل كونه منصة تجمع بين مجموعة السبعة، وشراكة دوفيل مع البلدان العربيَّة في المراحل الانتقاليَّة، والمراكز الماليَّة العالميَّة والإقليميَّة الجوهريَّة، بالإضافة إلى بلدان العالم العربي لتعزيز التعاون الدولي من أجل عودة الأصول المسروقة. وتشارك مبادرة استرداد الأصول المسروقة عن كَثَب في تنظيم المنتدى العربي وتسييره مدعومةً بعددٍ من الهيئات الدوليَّة.

منذ إطلاق المبادرة عام 2012م وهي تتناول الاحتياجات الملحَّة الرئيسة للدول العربيَّة بشأن استرداد الأصول، وقد كانت منصَّة للإجراءات والتعاون من المنظور العملي، وقد ولدت زخمًا سياسيًّا في الماضي بحشدها كلًّا من صُنَّاع السياسات وممارسيها، ورفعت درجة الوعي بالإجراءات الفعَّالة لاسترداد الأصول محليًّا ودوليًّا، وعزَّزت التعاون الداخلي، ويسَّرت التعاون الدولي في القضايا، كما قدَّمت التدريب والإرشاد لرفع كفاءة مسؤولي إنفاذ القانون وغيرهم من المسؤولين (Stolen Asset Recovery Initiative, 2021). ولا نعلم ما إذا كانت المبادرة لا تزال قائمة أم لا.

مكاتب استرداد الأصول في الدول الأعضاء بالاتحاد الأوروبي

حدَّد قرار المجلس الأوروبي رقم JHA/845/2007 (التعاون بين مكاتب استرداد الأصول في الدول الأعضاء بالاتحاد الأوروبي في مجال تعقُّب عائدات الجرائم أو الأملاك الأخرى المتعلِّقة بها وتحديدها) متطلبات تأسيس مكاتب استرداد الأصول في الدول الأعضاء بالاتحاد الأوروبي. وتهدف مكاتب استرداد الأصول إلى تيسير تعقُّب عائدات الجرائم وتحديدها، وقد تخضع هذه العائدات فيما بعدُ للتجميد، أو الحجز، أو المصادرة، في إطار التحقيق الجنائي أو المدني.

ويتعيَّن على بلدان الاتحاد الأوروبي أن تؤسِّس أو تعين مكتبًا واحدًا، على الأقل، لاسترداد الأصول (مكتبين بأقصى تقدير) على أراضيها، وتلتزم مكاتب استرداد الأصول بتبادُل المعلومات بعضها مع بَعْضٍ بِغَضِّ النظر عن وضعيِّتها (لإنفاذ القانون، أو تبادُل معلومات قضائيَّة، أو إداريَّة). وتعمل بوصفها نقاط اتصال مختصَّة للتبادُل الفعَّال للمعلومات والتنسيق على مستوى الاتحاد الأوروبي فيما يخص التطوُّرات الجديدة والمبادرات المطلقة بشأن إعادة استخدام الأصول المصادرة وتيسير تجميد الأصول المكتسبة دون شرعيَّة، بالإضافة إلى التعاون لتحسين إتاحة المعلومات بطرقٍ، من بينها: إنشاء قائمة بأوامر التجميد والمصادرة المعلَّقة في الاتحاد الأوروبي.

ولقد عيَّنت جميع الدول الأعضاء منذ عام 2015م مكاتبها لاسترداد الأصول، وقد أصبح تطبيق شبكة التبادُل الآمن للمعلومات التابع لـ«يوروبول» النظام المفضَّل للتبادُل الآمن للمعلومات لديهم. وقد ارتفعت نسبة تبادُل المعلومات بين مكاتب استرداد الأصول ارتفاعًا هائلًا على مدار ثماني سنوات، من 539 عمليَّة تبادُل في عام 2012م إلى 7659 عمليَّة تبادل في عام 2019م. ومنذ عام 2009م، نظَّمت المفوضية اجتماعات منصَّة مكاتب استرداد الأصول من أجل تبادُل أفضل الممارسات بينها، ومناقشة المشكلات الإستراتيجيَّة والتنفيذيَّة، وتيسير مشاركة المعلومات (المفوضية الأوروبيَّة، 2020م).

شبكة «كامدن» المشتركة بين الوكالات لاسترداد الأصول

شبكة «كامدن» لاسترداد الأصول هي شبكة غير رسميَّة أُسست عام 2004م لتضمَّ ممارسي إنفاذ القانون والممارسين القضائيين في مجال تعقُّب الأصول وتجميدها وحجزها ومصادرتها، وهي شبكة مشتركة بين الوكالات. ويمثل كل دولة عضو موظف لإنفاذ القانون، وخبير قضائي (نائب عام، أو قاضي تحقيقات، وغير ذلك حسب النظام القانوني).

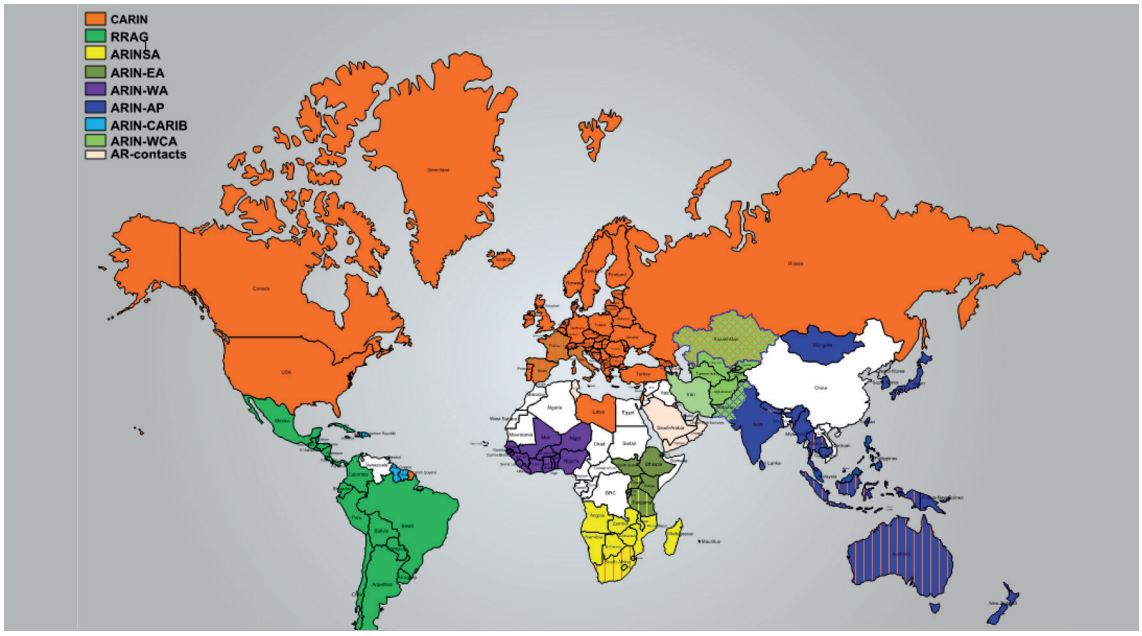
وتهدف شبكة «كامدن» إلى تعزيز فاعليَّة جهود أعضائها على أساس متعدد الوكالات لحرمان المجرمين من أرباحهم غير المشروعة، وتدعم كل نقاط الاتصال بشبكة «كامدن» عمليَّة الاسترداد الكامل للأصول، بدءًا من نقطة التحقيق المتضمنة لتعقُّب الأصول، مرورًا بتجميدها، وحجزها، وإدارتها، وحتى التجريد منها/ مصادرتها، بما في ذلك أي مشاركة ضروريَّة لتبادُل الأصول بين السلطات القضائيَّة.

وبناءً على خبرة منظمة الإنتربول، تركز بعض نقاط الاتصال الوطنيَّة لشبكات «كامدن» بشكل تنفيذي، ويمكن أن تساعد في الحالات العاجلة/ الخطرة في تعقُّب الأصول واعتراض الأموال في الوقت المناسب.

وتشترك مع شبكة «كامدن» بضع شبكات إقليميَّة مشتركة بين الوكالات لاسترداد الأصول تغطِّي المناطق التالية:

- آسيا والمحيط الهادي.
- جزر الكاريبي.
- شرق إفريقيا.
- جنوب إفريقيا.
- غرب إفريقيا.
- غرب آسيا ووسطها.

ولا توجد شبكة إقليميَّة تخدم أو تغطي منطقة الخليج وشمال إفريقيا (Camden Asset Recovery Inter - agency Network, 2021). والشكل التوضيحي رقم «27» يبيِّن الشبكة الدوليَّة لـ«كامدن».



الشكل التوضيحي رقم «27»: الشبكة الدوليَّة لـ«كامدن»

المصدر: الأمانة العامَّة لشبكة «كامدن» المشتركة بين الوكالات لاسترداد الأصول (يناير 2020م).

مجموعة «إيجمونت» وشبكة وحدات الاستخبارات الماليَّة

مجموعة «إيجمونت» هي هيئة متحدة مكوَّنة من 166 وحدة استخبارات ماليَّة. وعلى الرغم من أن مجموعة «إيجمونت» ليست شبكة لتعقُّب الأصول واستردادها في حد ذاتها، فإنها تتيح منصَّة لوحدات الاستخبارات الماليَّة الأعضاء لتبادُل الخبرات والاستخبارات الماليَّة بأمان لمكافحة غسل الأموال وتمويل الإرهاب. يحدث ذلك خاصة لأن المكانة الفريدة لوحدات الاستخبارات الماليَّة تؤهِّلها للتعاون ودعم الجهود الوطنيَّة والدوليَّة لمكافحة غسل الأموال، كما أنها هي البوَّابات المضمونة لمشاركة المعلومات الماليَّة محليًّا ودوليًّا.

لقد أطلقت مجموعة العمل المعنيَّة بتبادل المعلومات في مجموعة «إيجمونت» مبادرة لمعالجة التهديد الصاعد للجريمة الماليَّة عبر الإنترنت، وبخاصَّةٍ مخططات الاحتيال عبر بريد العمل الإلكتروني. في هذا السياق وبالإضافة إلى نشر بيان، أطلقت المجموعة «آليَّة الاستجابة السريعة»، وبدأت تفعيلها (Egmont Group, 2021).

تدعم كثيرٌ من وحدات الاستخبارات الماليَّة حاليًّا تقديمَ طلبات وقف المدفوعات الفوريَّة أو أوامر تجميد الأموال إلى أقرانها من وحدات الاستخبارات الماليَّة في بلدان أخرى. بالإضافة إلى ذلك، تطالب أيضًا وحدات الاستخبارات الماليَّة بمعلومات ماليَّة أو استخبارات فيما يتعلَّق بالحسابات المصرفيَّة الأجنبيَّة.

وتُشجَّع هيئات إنفاذ القانون على الوصول إلى وحدات الاستخبارات الماليَّة الخاصَّة بها لبدء عمليَّة تعقب الأصول واعتراض الأموال واستردادها، وينبغي لمحقق الشرطة إعلام وحدة الاستخبارات الماليَّة لبدء عمليَّة الاستجابة السريعة فور تلقيه الشكوى المبدئيَّة من الضحيَّة.

وتُعد وحدات الاستخبارات الماليَّة لدى كثيرٍ من الدول العربيَّة الأعضاء الرسميين في مجموعة «إيجمونت»، وهي: الأردن، والجزائر، والبحرين، ومصر، والسعوديَّة، والكويت، ولبنان، والمغرب، وفلسطين، وقطر، والسودان، وسوريا، وتونس، والإمارات العربيَّة المتَّحدة (Egmont Group, 2021).

ويرد دور وحدات الاستخبارات الماليَّة للدول الأعضاء بالاتحاد الأوروبي، ووظيفتها، وسلطتها في المبدأ التوجيهي رقم 2015/849 بشأن منع استخدام النظام المالي بهدف غسل الأموال أو تمويل الإرهاب، وبخاصَّةٍ في المادة 32 (Offcial Journal of the European Union, 2015).

وتنص المادة 32.7 على ما يلي:

«تضمن الدول الأعضاء تمكين وحدات الاستخبارات الماليَّة من اتخاذ الإجراءات العاجلة، بصورة مباشرة أو غير مباشرة، حالَ وجود شك في صلة معاملة بغسل الأموال أو تمويل الإرهاب، ولتعليق الموافقة على معاملة قائمة أو حجبها من أجل تحليلها، وتأكيد الشك ونشر نتائج التحليل بين السلطات المختصَّة. وتُمَكَّن وحدات الاستخبارات الماليَّة من اتخاذ هذه الإجراءات، بصورة مباشرة أو غير مباشرة، بطلب من وحدة الاستخبارات الماليَّة التابعة لدولة عضو أخرى بالفترات المعنيَّة، ووَفقَ الشروط المحددة في القانون الوطني الخاضعة له وحدة الاستخبارات الماليَّة المتلقية للطلب» (Egmont Group, 2021).

شبكة «GAFILAT» لاسترداد الأصول

يُعد فريق «GAFILAT» هو مجموعة «فايف» في أمريكا اللاتينيَّة. وقد أُنشئت شبكة «GA-FILAT» استنادًا إلى نموذج شبكة «كامدن» لاسترداد الأصول. وهي منصة وشبكة تضم نقاط الاتصال في المنطقة، وتهدف إلى تسهيل تحديد نوعيَّة الأصول، أو المنتجات، أو الأدوات الخاصَّة بالأنشطة غير المشروعة وموقعها، كما تسهل عمليَّة استردادها.

وقد عيَّن كل بلد من البلدان الأعضاء في شبكة «GAFILAT» نقطتي اتصال، هما: مكتب النائب العام، والشرطة.. غير أنه في بعض الحالات، تشارك مكاتب أخرى ذات صلة بمهام الشبكة في هذه العمليَّات، مثل: مكاتب إدارة الأصول واستردادها أو وحدات الاستخبارات الماليَّة.

ومن بين أهداف الفريق والتزاماته أن يعمل بوصفه مركزًا لنقل الخبرة في جميع الجوانب لمتابعة عائدات الجريمة، وتعزيز تبادُل المعلومات، وأن يعمل بوصفه فريقًا استشاريًّا للسلطات الوطنيَّة المختصَّة، وأن يُسدي المشورة وييسِّر المساعدة القانونيَّة المتبادَلة، وأن يتبادل - بمبادرةٍ منه - أفضل الممارسات والمعارف والخبرات. ومنذ أكتوبر 2010م، بدأ الفريق يتبادل المعلومات من خلال منصَّة إلكترونيَّة تضمن أمن الطلبات والردود وحمايتها. وتقع إدارة هذه المنصَّة في وحدة الاستخبارات الماليَّة في كوستاريكا.

وتعد شبكة استرداد الأصول هذه شبكةً إقليميَّةً مشتركةً بين الوكالات لاسترداد الأصول (GAFILAT, 2021).

الأمانة العامَّة لمنظمة الإنتربول

تقدم منظمة الإنتربول خدماتها للبلدان الأعضاء فيها - البالغ عددها 194 بلدًا - وتربطها عن طريق شبكة اتصالات تسمى I-24/7. وفي كل بلد، يوفر المكتب المركزي الوطني لمنظمة الإنتربول نقطة اتصال مركزيَّة للأمانة العامَّة وهيئات التنسيق الوطنيَّة الأخرى. وتستخدم البلدان هذه الشبكة الآمنة للاتصال ببعضها وبالأمانة العامَّة.

وقد أثبتت هذه الشبكة العالميَّة القائمة على اتصالات المكاتب المركزيَّة الوطنيَّة كفاءتها في نقل تنبيهات وقف الدفع العاجلة وطلبات اعتراض الأموال للمكتب المركزي الوطني النظير ليتعامل

مع الحساب المصرفي للمستفيد عند تلقِّيه الودائع النقديَّة في حالات الاحتيال. وقد عززت بعض المكاتب المركزيَّة الجهود الرامية إلى تلقي هذه المعلومات، التي يشكل الوقت عاملًا بالغ الأهمية فيها بشأن المعاملات العابرة للحدود في أسرع وقت ممكن، من سلطاتها المختصة على جبهة تلقِّي الشكاوى من الضحايا. وبمجرد تسلُّم هذه المعلومات، يُرسَل تنبيه بوقف الدفع وطلب اعتراض الأموال على الفور إلى المكتب المركزي الوطني لمنظمة الإنتربول في البلد المعني الذي يوجد فيه حساب المستفيد. وبالإضافة إلى ذلك، تقدم وحدة الجرائم الماليَّة التابعة لمنظمة الإنتربول الدعم التشغيلي والمساعدة في التحقيق في مثل هذه السيناريوهات والحالات العاجلة والخطيرة للمدفوعات العابرة للحدود (Interpol, 2021).

المبادرة الخاصَّة باسترداد الأصول المسروقة (STAR) وشبكة جهات الاتصال العالميَّة (GFPN)

منذ انطلاق مبادرة «STAR» التابعة لمنظمة الإنتربول مع شبكة جهات الاتصال العالميَّة (GFPN) في عام 2009م وهدفها مساعدة الممارسين على التغلُّب على الحواجز التشغيليَّة المرتبطة باسترداد الأصول على الصعيد الدولي من خلال توفير منصَّة آمنة لتبادُل المعلومات من أجل استرداد الأصول غير المشروعة. ويُعيَّن موظفو إنفاذ القانون المأذون لهم من كل بلد عضو (أي البلدان الأعضاء في منظمة الإنتربول) بوصفهم «نقاط اتصال»؛ إذ إنهم يكونون متاحين للاستجابة للطلبات الفوريَّة من أجل الحصول على مساعدة في استرداد الأصول من أي بلد عضو آخر. ويُعد الهدف الإستراتيجي المباشر لهذه المبادرة هو الاستجابة للشواغل المتعلِّقة بتجميد الأصول المسروقة وحجزها ومصادرتها واستردادها. ويتمثل أحد الأهداف المستمرة لهذه المبادرة في تيسير التبادُل الآمِن للمعلومات الحساسة فيما بين جهات الاتصال التابعة لوكالات مكافحة الفساد واسترداد الأصول (Stolen Asset Recovery Initiative, 2021).

وبدءًا من ديسمبر 2020م، أصبحت الشبكة تضم 246 جهة اتصال مخصصة ترشحها وكالات إنفاذ القانون الوطنيَّة والسلطات القضائيَّة والإداريَّة، كما أصبحت تمثل 137 دولة (بما في ذلك كثير من دول منطقة مجلس وزراء الداخليَّة العرب ومنطقة الشرق الأوسط وشمال إفريقيا) (Interpol, 2021).

3.5.2 الوضع في الاتحاد الأوروبي

يقدِّم هذا التقرير نظرة عامَّة جيدة على إطار العمل القانوني لتعقُّب الأصول واستردادها ومسؤوليَّات هذه العمليَّات ونتائجها ومعدَّل أدائها، ويحمل التقرير عنوان «استرداد الأصول ومصادرتها.. ضمان ألَّا تفيد الجريمة»، نشرته المفوضيَّة الأوروبيَّة في يونيو 2020م (European Commission, 2020).

وتُقدَّر أرباح جماعات الجريمة المنظَّمة بـ110 مليارات يورو سنويًّا في الاتحاد الأوروبي. ومع ذلك، وَفقًا لـ«يوروبول»، لا يُصادَر منها إلا نحو 1%.

ويحلِّل التقرير تنفيذ التوجيه المتعلِّق بتجميد عائدات الجريمة ومصادرتها، ويقيم جدوى إدخال مزيدٍ من القواعد المشتركة على مستوى الاتحاد الأوروبي وفوائده، ويبحث حقيقة الحاجة إلى أحكام أقوى لتعزيز تحديد نوعيَّة الأصول غير المشروعة وتعقُّبها وتجميدها وإدارتها ومصادرتها. كما يعرض نظرة عامَّة على عمل مكاتب استرداد الأصول والتحديات التي تواجهها عند القيام بمهامها اليوميَّة، وتتوقَّف إمكانية تجميد الأصول ومصادرتها على إمكانية تعقُّبها وتحديد نوعيتها بفعالية.

وقد أثيرت مجموعة من القضايا الأخرى، مثل:

- توفير الوصول السريع إلى مجموعة صغيرة من البيانات الموجودة في السجلات وقواعد البيانات الوطنيَّة لمكاتب استرداد الأصول.
- الحاجة إلى تعزيز صلاحيات مكاتب استرداد الأصول (على سبيل المثال: سلطات التجميد العاجلة للحسابات والعمليَّات الماليَّة، والقدرة على تعقُّب الأصول بعد الإدانة الجنائيَّة النهائيَّة).
- الحاجة إلى وضع حدود زمنيَّة ثابتة وصارمة يجب على مكاتب استرداد الأصول الاستجابة خلالها لطلب من مكتب نظير.

معلومات أساسيَّة

في عام 2014م، اعتمد البرلمان الأوروبي والمجلس الأوروبي المبدأ التوجيهي رقم EU /42 /2014، الذي يحدد القواعد الدنيا لتجميد الأصول غير المشروعة وإدارتها ومصادرتها. وهذا ألزم الدول الأعضاء بتحويل أحكامها إلى القانون الوطني بحلول الرابع من أكتوبر 2016م.

بالإضافة إلى هذا المبدأ التوجيهي، يُعد اعتماد اللائحة رقم 1805 /2018 (EU) بشأن الاعتراف المتبادَل بأوامر التجميد والمصادرة علامة أخرى بارزة فيما يتعلَّق باسترداد الأصول. وتهدف اللائحة

إلى تسهيل استرداد الأصول عبر الحدود وجعل تجميد الأصول غير المشروعة ومصادرتها في جميع أنحاء الاتحاد الأوروبي أسرع وأبسط. وتنطبق اللائحة على جميع أوامر التجميد والمصادرة المقدَّمة في إطار الدعاوى الجنائيَّة، بما في ذلك المصادرة القائمة على الإدانة أو عدمها.

وتتوقَّف إمكانيَّة تجميد الأصول ومصادرتها مباشرةً على إمكانية تعقُّبها وتحديد نوعيتها بفعالية. ويلزم قرار المجلس رقم JHA7 /845 /2007 الدول الأعضاء بإنشاء أو تعيين مكاتب استرداد أصول وطنيَّة، من أجل ضمان تعقُّب الأصول غير المشروعة على نطاق الاتحاد الأوروبي في أسرع وقت ممكن. كما اتُّخذت إجراءات على مستوى الاتحاد الأوروبي لضمان الحصول على المعلومات بصورة أسرع. وعلى مدى العقود الثلاثة الماضية، وضع الاتحاد الأوروبي إطارًا متينًا لمكافحة غسل الأموال، الذي نجم عنه أيضًا سجلات للملكيَّة الفعليَّة للكيانات القانونيَّة والإجراءات، وسجلات للحسابات المصرفيَّة المركزيَّة. كما يمنح المبدأ التوجيهي رقم 2019/ 1153، بشأن استخدام المعلومات الماليَّة، هيئات إنفاذ القانون ومكاتب استرداد الأصول - إمكانية الوصول المباشر إلى معلومات الحسابات المصرفيَّة بغرض مكافحة الجرائم الخطيرة (European Commission, 2020).

3.5.3 سجلات ومنصَّات عبر الإنترنت توفر الإرشادات والتعليمات وجهات الاتصال:

3.5.3.1 مشروع «سايروس» التابع لـ«يوروبول»

يُعد مشروع «سايروس»، الذي اشترك في تنفيذه كلٌّ من: «يوروبول» و«يوروجاست» (الوكالة الأوروبيَّة للتعاون القضائي) والشبكة القضائيَّة الأوروبيَّة، نقطةً مرجعيَّةً مركزيَّةً في الاتحاد الأوروبي لتبادُل المعرفة حول الوصول العابر للحدود إلى الأدلَّة الإلكترونيَّة؛ فأكثر من نصف التحقيقات الجنائيَّة اليوم تتضمَّن إرسال طلبٍ عبر الحدود للوصول إلى الأدلَّة الإلكترونيَّة (مثل البيانات من خدمات الرسائل الإلكترونيَّة، أو خدمات البريد الإلكتروني، أو وسائل التواصُل الاجتماعي). ويهدف مشروع «سايروس» إلى مساعدة المحققين على التعامُل مع حجم المعلومات المعقَّدة في بيئة سريعة التغيُّر مثل الإنترنت، من خلال توفير توجيهات بشأن مزوِّدي خدمات الإنترنت المُراد الوصول إليهم، والأدوات التي تساعد على التحقيق، بالإضافة إلى بيانات الاتصال الخاصَّة بمزوِّدي خدمات الإنترنت، كما يهدف المشروع إلى إتاحة الفرص أمام المحققين لتبادُل الخبرات مع أقرانهم. وجميع هذه الموارد متاحة على منصة محظورة على العامَّة ومتاحة لسلطات إنفاذ القانون والسلطات القضائيَّة للدول الأعضاء في الاتحاد الأوروبي والبلدان التي لديها اتفاقات تشغيليَّة مع «يوروبول» أو «يوروجاست» (EUROPOL, 2021).

3.5.3.2 سجلَّات الشرطة الوطنيَّة وجهات الاتصال الخاصَّة بالقطاع الخاص وتعليمات حول الإنذارات والطلبات

أنشأ عددٌ من قوات الشرطة في البلدان الأعضاء في «الإنتربول» سجلات داخليَّة على الإنترنت من أجل ضباطها ومحققيها. وتعمل هذه السجلات في مختلف المسائل المتعلقة بتعامُل وكالات إنفاذ القانون مع القطاع الخاص؛ إذ تجمع بيانات الاتصال المخصَّصة لمجموعة من أعمال القطاع الخاص وشركاته، وتجري صيانتها وإتاحتها. ويشمل ذلك جهات اتصال تعمل في قطاع الخدمات الماليَّة (مثل المصارف، وشركات التقنية الماليَّة، ومقدمي خدمات الأصول الافتراضيَّة، ومقدمي خدمات الدفع، ومكاتب خدمات الأموال)، ومنهم مقدمو خدمات الإنترنت، وشركات الاتصالات والكيانات الأخرى ذات الصلة التي قد تُستدعى في تحقيقات وكالات إنفاذ القانون للكشف عن المعلومات أو تقديم الإنذارات.

وقد تتضمَّن هذه السجلَّات توجيهات وكتيبات تنشرها «الإنتربول» أيضًا (مثل: الحصول على بيانات من القطاع الخاص: توجيهات لمحققي الاتجار بالبشر).

3.5.4 نُظُم الإنذار التي تستهدف المواقع والمحتويات المشبوهة عبر الإنترنت

لوحظ انتشار كبير للمواقع والنطاقات المحتالة باللغة العربيَّة الموجودة عبر الإنترنت. وما زالت بعض الدول تنتهج أسلوب حظر هذه المواقع لحفظ المجتمع، لكن هذا الأسلوب أصبح غير فعَّال، وهناك ممارسات وتجارِب دوليَّة للتعامُل مع مثل هذه الأحداث التي تستهدف المواقع والمحتويات المشبوهة عبر الإنترنت. وتنقسم هذه التجارِب إلى جزأين من حيث الإدارة، الجزء الأول: تُدار هذه المبادرة عن طريق الجهات المعنيَّة في الدول، والجزء الثاني: تُدار هذه المبادرة عن طريق المنظَّمات غير الحكوميَّة. وسنستعرض تجارِب بعض الدول الأوروبيَّة في هذا المجال، وهي كالآتي:

3.5.4.1 المملكة المتَّحدة.. نظام الإنذار بشأن الإعلانات الاحتياليَّة

في يونيو 2020م، أُطلق نظام الإنذار بشأن الإعلانات الاحتياليَّة بالشراكة مع منصَّات الإعلانات عبر الإنترنت ووسائل التواصُل الاجتماعي الكبرى، بما في ذلك «جوجل» و«فيسبوك»، للمساعدة على معالجة قضيَّة الإعلانات الاحتياليَّة عبر الإنترنت. ويهدف هذا النظام إلى استكمال العمل

الذي تقوم به بالفعل منصَّات الإعلان الرقمي ومنصَّات وسائل التواصُل الاجتماعي وغيرها من الهيئات التنظيميَّة، وتعزيزها لمعالجة الإعلانات الاحتياليَّة، وعلى نطاق أوسع الأنشطة الاحتياليَّة الأخرى عبر الإنترنت.

ومنذ بداية هذا العام، بدأ المستهلكون في الإبلاغ عن الإعلانات الاحتياليَّة التي تظهر في المواقع المدفوعة عبر الإنترنت على النظام الجديد عن طريق ملء استمارة عبر الإنترنت. وتوجد موارد مخصَّصة لتقييم هذه التقارير في غضون 24 ساعة، تُمكِّنهم من تنبيه المنصَّات بسرعة وفعالية بشأن الإعلانات الاحتياليَّة حتى يتمكَّنوا من إزالتها على الفور، وتعليق حسابات المعلنين، ووقف ظهور إعلانات مماثلة في المستقبل.

وتلقَّى الموقع منذ إطلاقه 1274 بلاغًا من عامَّة الجمهور؛ ما أدَّى إلى إرسال 121 إنذارًا إلى المنصَّات عبر الإنترنت، وهذا يعني أن واحدًا من كل عشرة بلاغات تلقاها الموقع أدَّى إلى إرسال تنبيه بشأن الإعلان.

واستجابت المنصَّات للتنبيهات في غضون 48 ساعة (88% من الوقت) لتؤكِّد أنهم قد أزالوا بالفعل الإعلان الاحتيالي المبلَّغ عنه (The Advertising Standards Authority, 2021).

3.5.4.2 فرنسا: مشروع فاروس (PHAROS) وموقع الإشارة عبر الإنترنت

لدى المديرية المركزيَّة للشرطة القضائيَّة - ارتباط خارجي - قسم وطني له ولاية تنفيذيَّة مشتركة بين الوزارات، ويهدف هذا القسم إلى مكافحة الجريمة المرتبطة بتقنية المعلومات والاتصالات، وهو المكتب المركزي لمكافحة الجريمة المرتبطة بتقنية المعلومات والاتصالات. وقد أطلق هذا المكتب منصة «فاروس» (وهي منصة لتعزيز المواءمة والتحليل والاسترداد والتوجيه المتعلق بالإبلاغ)، التي تتيح لمستخدمي الإنترنت وضحاياه الإبلاغ عن أي محتوى أو سلوك غير مشروع على الإنترنت (Interieur Gouv, 2016).

3.5.4.3 سنغافورة.. Scam Alert

يوفِّر نظام تنبيه الاحتيال أحدث تنبيهات ومعلومات الخداع، ويُعد تنبيه الاحتيال جزءًا من المجلس الوطني لمنع الجريمة (NCPC) الذي بدأ في عام 1981م، ويتألَّف المجلس من ممثلين من القطاعين التجاري والصناعي وكذلك من القطاع العام، وتلتزم قوة الشرطة السنغافورية

(SPF) بتعزيز الوعي العام والاهتمام بالجريمة ونشر مفهوم المساعدة الذاتيَّة في منع الجريمة. ويعد المركز الوطني لمكافحة الفساد حافزًا ومستشارًا وشريكًا لحشد دعم المجموعات والمنظَّمات والأفراد من المجتمع للعمل عن كثب مع قوة الشرطة السنغافورية (SPF) لمنع الجريمة.

وحدَّدَ تنبيه الاحتيال أهم 5 عمليَّات احتيال عبر الإنترنت في سنغافورة، وهي:

- عمليَّة احتيال الشراء عبر الإنترنت.
- احتيال الإنترنت في الحب.
- انتحال شخصيَّة الخداع.
- عمليَّة احتيال الاستثمار.
- الائتمان مقابل الاحتيال الجنسي.

ويحتوي موقع تنبيه الاحتيال الإلكتروني على ميزة للبحث عن عمليَّة الاحتيال في حقل البحث مع تحديد القائمة لنوع الاحتيال الذي يتضمَّن الحساب المصرفي والبريد الإلكتروني والمعرف/ اسم المستخدم ورقم الاتصال والكلمات الرئيسة (على سبيل المثال: تحويل الأموال وعناوين البريد الإلكتروني وأرقام الهواتف وأرقام الحسابات المصرفيَّة وما إلى ذلك).

ويوفر موقع تنبيه الاحتيال رقم خط المساعدة الخاص بمكافحة الاحتيال. كما يتضمن خاصيَّة مشاركة قصص الضحايا والتدابير الوقائيَّة وأشرطة الفيديو والملصقات التوعويَّة.

3.5.4.4 هولندا.. Scamadvisor

في عام 2012م، أُسس موقع على الإنترنت يُسمَّى «سكام أكسبو»، وفي وقت لاحق في عام 2018م استحوذت عليه مؤسَّسة التجارة الإلكترونيَّة، وهي منظمة مستقلَّة معروفة بالعمل مع كثيرٍ من المنظَّمات غير الحكوميَّة. وترتبط التجارة الإلكترونيَّة في مؤسَّسات التجارة الإلكترونيَّة الأخرى في جميع أنحاء العالم بمهمَّة تعزيز التجارة الرقميَّة العالميَّة.

وتتحقق شركة «Scaradviser» من موثوقيَّة المواقع الماليَّة، بما في ذلك مواقع تداول العملات الأجنبيَّة ومديري الاستثمار والصناديق ومحافظ «Bitcoin» الموثوقة ومواقع تداول «Bitcoin» الموثوقة، بالإضافة إلى مواقع التسوُّق عبر الإنترنت ومواقع التوظيف ومواقع الترفيه.

وتستخدم خوارزمية «Scadviser» 40 مصدرًا مستقلًّا للبيانات من عنوان IP لخادم الويب، لمعرفة مدى توافر تفاصيل الاتصال على موقع الويب، وعمر عنوان URL، والتقييمات على مواقع المراجعة لتحديد ما إذا كان موقع الويب شرعيًّا أم لا.

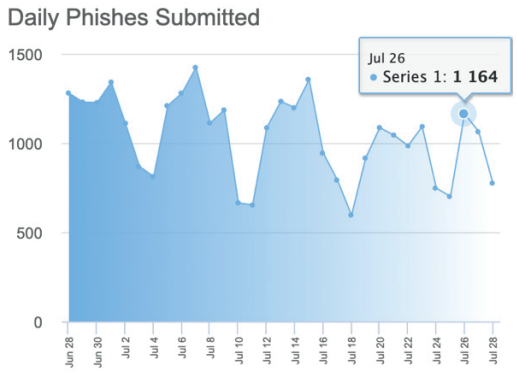
كما يقدم برنامج «Scadviser» كثيرًا من خدمات البيانات لجهات إنفاذ القانون وشركات الأمن وسلطات المستهلك ووكالات حماية العلامة التجاريَّة لمساعدتهم على فصل المواقع الموثوقة عبر الإنترنت عن مواقع الويب الاحتياليَّة عن طريق إنشاء «Trustscore API» للتحقُّق من المجال في الوقت الفعلي، ودمج موجز البيانات لحماية العملاء، وتحديد شبكات الاحتيال باستخدام «Domain Analyzer» وحظر النطاقات الخبيثة أو المزيفة بشكل نشط.

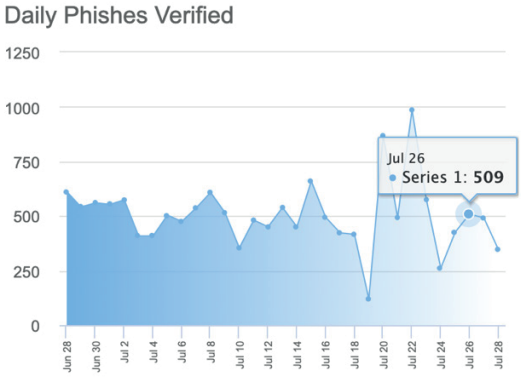
ويساعد برنامج «Scadviser» في حظر أسماء النطاقات من خلال شركاء مكافحة الفيروسات وفلتر «DNS» والقضاء على المحتالين من خلال العمل عن كَثَب مع شركائه مزودي حلول Group - IB الرائد الذي يهدف إلى اكتشاف الهجمات الإلكترونيَّة والاحتيال عبر الإنترنت ومنعها وحماية «IP» من التهديدات والإسناد ليس فقط لإزالة مواقع الويب الفرديَّة ولكن شبكات كاملة من عمليَّات الاحتيال ومجرمي الإنترنت.

3.5.4.5 أمريكا.. PhishTank

في عام 2006م، أسَّست «PhishTank» «OpenDNS» بهدف إيقاف جرائم التصيُّد الإلكتروني. «PhishTank» هو نظام مجاني قائم على أفراد المجتمع للتحقُّق من التصيُّد الاحتيالي، حيث يمكن للمستخدمين المسجلين إرسال رسائل بريد إلكتروني أو مواقع إلكترونية للتصيُّد الاحتيالي، ويصوِّت المستخدمون الآخرون، سواء أكان تصيُّدًا أم لا. ويمتلك «PhishTank» واجهة برمجة تطبيقات مجانيَّة (API)، ما يسمح للمطورين بدمج عناصر مكافحة التصيُّد في تطبيقاتهم باستخدام بيانات مجتمع «PhishTank». وحاليًّا، يُشغَّل «PhishTank» بواسطة «Cisco Talos Intelligence Group» بعد استحواذ «Cisco» على «OpenDNS». ويعمل «PhishTank» بفعَّالية ضد هجمات التصيُّد الاحتيالي من خلال اكتشاف آلاف روابط التصيُّد كل يوم. وهذه بعض الإحصاءات كما في الشكل التوضيحي رقم «28» (Phishtank, 2021):

- عدد الطلبات اليوميَّة لمواقع التصيُّد: 1164.
- عدد مواقع التصيُّد بعد التحقُّق منها: 509.





Phishes Verified as valid التحقُّق من مواقع التصيُّد		Suspected Phishes Submitted عدد المواقع المشتبه بها
Total إجمالي	2,911,717	6,983,773
Online	10,763	15,867
Offline	2,900,954	6,967,906

الشكل التوضيحي رقم «28»: إحصاءات «PhishTank» بعدد المواقع الاحتياليَّة المحتملة والتحقُّق منها

3.5.4.6 الخلاصة:

استقبال البلاغات

عند رصد آليَّات البلاغات الإلكترونيَّة للدول العربيَّة، اتضح وجود فوارق مهمَّة بين أعضاء الدول العربيَّة فيما يتعلَّق باستعدادها لمواجهة الجرائم الماليَّة عبر الإنترنت. وهناك تطوُّر ملحوظ لدول مجلس التعاون الخليجي في وسائل استقبال البلاغات الإلكترونيَّة كتسهيل وصول الضحايا لجهات إنفاذ القانون، وتخصيص وسائل للإبلاغ عن هذا النوع من الجرائم، وتعيين بعض فرق العمل والوحدات لتولِّي مسؤوليَّة هذه الجرائم. وفي بعض الدول العربيَّة يُعد الإبلاغ عن الجرائم عبر الإنترنت أمرًا صعبًا أو يكاد يكون مستحيلًا في بعضها؛ فبعض المواقع الإلكترونيَّة لا تعمل، بينما يصعب العثور على مواقع أخرى أو تصفُّحها.

ويؤدِّي عدم وجود طرق فعَّالة وسهلة للإبلاغ عن الجريمة إلى حدوث تأخير في التعامُل مع الجرائم، وقد يحول ذلك دون استرداد الأصول/ الأموال المسروقة. وتُعد حالات التأخير أهم التحديات التي تتعلَّق بالجرائم الماليَّة عبر الإنترنت التي يرتكبها المجرمون للحصول على أموال الضحايا، وينقلونها بسرعة من خلال المنصَّات الرقميَّة وعبر الإنترنت. وهنا يكمن استغلال المحتالين لطرق الدفع الحديثة للدول العربيَّة التي انتهجتها مؤخرًا.

المكاتب المركزيَّة المتخصِّصة

تعتبر تجرِبة المكاتب المركزيَّة المتخصِّصة من الممارسات الحديثة في العالم.. بدأت هذه التجرِبة منذ عام 2017م. ولم يُرصد في الدول العربيَّة، على المستوى الوطني، وجود مركز متخصِّص في التعامُل مع جرائم الاحتيال المالي، كمركز التنسيق لمكافحة الغش في هونج كونج، ومركز مكافحة النصب في سنغافورة، والمركز الوطني للجرائم الاقتصاديَّة في المملكة المتَّحدة. ومن النقاط المهمَّة في هذه المراكز أنها تجمع بين الجهات المعنيَّة في مكان واحد، كما هو معمول به في المركز الوطني للجرائم الاقتصاديَّة في المملكة المتَّحدة ومركز استقبال شكاوى الإنترنت في الولايات المتَّحدة الأمريكيَّة. ويوضِّح الجدول رقم «9» بعض الممارسات الدوليَّة للحدِّ من جرائم الاحتيال المالي ومقارنة بين الدول العربيَّة والدول الأخرى.

الجدول رقم «9»: بعض الممارسات الدوليَّة للحدِّ من

بعض الممارسات الدوليَّة للحدِّ من جرائم الاحتيال المالي	الوصف
استقبال البلاغات	هي منصّة مركزيَّة للإبلاغ عن الجرائم.
المكاتب المركزيَّة المتخصِّصة	مكاتب مخصَّصة للتعامُل مع جرائم الاحتيال والتحرِّي والتحقيق واسترداد الأموال.

جرائم الاحتيال المالي ومقارنتها بالوضع الحالي للدول العربيَّة

الدول العربيَّة	الدول الأخرى
لا يوجد لدى كثيرٍ من الدول استقبال بلاغات عن طريق الإنترنت باستثناء الدول الخليجيَّة كتطبيق «كلنا أمن» في المملكة، لكن هذه التطبيقات ليست مخصَّصة لجرائم الاحتيال المالي، بل للإبلاغ عن جميع الجرائم؛ فبعض المواقع الإلكترونيَّة لا تعمل، بينما يصعب العثور على مواقع أخرى أو تصفُّحها.	في عدَّة دول، لاحظنا وجود استقبال بلاغات مركزيَّة للجرائم السيبرانيَّة؛ حيث تُصنَّف جريمة الاحتيال المالي عبر الإنترنت من ضمنها كمركز الأمن السيبراني الأسترالي، أو مخصَّصة للاحتيال المالي كالمركز الكندي لمكافحة الاحتيال.
لا توجد مكاتب متخصِّصة للتعامل مع هذه الجرائم، تجمع بين الجهات المعنيَّة في مكان واحد لتسريع عمليَّة أخذ الموافقات من النيابة العامَّة وسرعة التواصُل مع البنوك لاسترجاع الأموال، بل توجد في بعض الدول العربيَّة إدارات للتحريات الماليَّة كما هو معمول به في المملكة العربيَّة السعوديَّة، يكون تركيزها على مكافحة تمويل الإرهاب وليس موجهًا للاحتيال المالي. وفي قطر، يوجد فريق مخصَّص للتعامُل مع هذه الجرائم وليس مركزًا.	هي ممارسات حديثة، وبدأت هذه التجرِبة منذ عام 7102م، كمركز التنسيق لمكافحة الغش في هونج كونج، ومركز مكافحة النصب في سنغافورة، والمركز الوطني للجرائم الاقتصاديَّة في المملكة المتَّحدة. ومن المحاور المهمَّة في هذه المراكز أنها تجمع بين الجهات المعنيَّة في مكان واحد، كما هو معمول به في المركز الوطني للجرائم الاقتصاديَّة في المملكة المتَّحدة، وهو ما يسهِّل عمليَّة تجميد الحسابات واعتراض الأموال واسترجاعها.

بعض الممارسات الدوليَّة للحدِّ من جرائم الاحتيال المالي	الوصف
تعقُّب الأصول واعتراض الأموال	جهة تكون مختصة بالسرعة في التواصُل مع المؤسَّسات الماليَّة لإيقاف الأموال وتجميدها واسترجاعها؛ فمعدّل تعقُّب الأصول المكتسبة بأساليب غير مشروعة واعتراضها، ومصادرتها، وإعادتها إلى الوطن لا يزال منخفضًا، وقد يكون ذلك بسبب التحديات المؤسَّسية، والقانونيَّة، وصعوبة التواصُل.
نظم الإنذارات التي تستهدف المواقع والمحتويات المشبوهة عبر الإنترنت	تحقُّق جهة حكوميَّة أو غير حكوميَّة من المواقع الإلكترونيَّة وإشعار الجهات المعنيَّة لإغلاق هذه المواقع أو تنبيه أفراد المجتمع من هذه المواقع الاحتياليَّة للوقاية من الجريمة.

الدول العربيَّة	الدول الأخرى
على المستوى الوطني خلال اجتماع مجموعة التركيز، لوحظ أن هناك تحديًا يواجه الجهات المعنيَّة في استرداد الأموال بسبب بطء الإجراءات وخروج أغلبها خارج الحدود.. على المستوى الإقليمي، رُصدت مبادرة باسم المنتدى العربي لاسترداد الأصول، الذي انطلق عام 2102م وكان يعمل بوصفه منصَّة تجمع بين مجموعة السبعة وشراكة «دوفيل» مع البلدان العربيَّة والمراكز الماليَّة الإقليميَّة والدوليَّة، بالإضافة إلى البلدان العربيَّة لتعزيز التعاون الدولي من أجل عودة الأصول المسروقة. ولكن لا نعلم إذا كانت هذه المبادرة ما زالت قائمة أم لا.	على المستوى المحلي، توجد فرق تعمل تحت إدارة المراكز المتخصِّصة كفريق استرداد الأصول (TAR) التابع لمركز شكاوى جرائم الإنترنت في الولايات المتَّحدة الأمريكية. وكذلك النموذج السنغافوري الذي يديره مركز متخصِّص في التعامُل مع جرائم الاحتيال المالي ويسترد الأموال. على المستوى الإقليمي، هناك نماذج مختلفة كالشبكة التنفيذيَّة لمكافحة غسل الأموال، وتضم 04 دولة. ومكاتب استرداد الأصول في الدول الأعضاء بالاتحاد الأوروبي، التي وضعت نموذجًا بأنَّه يتعيَّن على بلدان الاتحاد الأوروبي أن تؤسِّس مكتبًا واحدًا على الأقل لاسترداد الأصول (مكتبين بحد أقصى) على أراضيها. وتلتزم هذه المكاتب بتبادُل المعلومات فيما بينها، بغضِّ النظر عن وضعيتها لإنفاذ القانون أو تبادُل معلومات قضائيَّة. وطبقت شبكة التبادُل الآمِن للمعلومات التابعة لـ«يوروبول» النظام المفضَّل للتبادُل الآمِن للمعلومات لديهم. وكانت النتيجة ارتفاع نسبة تبادُل المعلومات على مدار ثماني سنوات، من 935 عمليَّة تبادل في 2102م إلى 9567 عمليَّة تبادل في 9102م. وكذلك مجموعة «إيجمونت» هي هيئة متحدة مكوِّنة من 661 وحدة استخبارات ماليَّة، وهي ليست شبكة تعقُّب الأصول بل تبادل الخبرات والاستخبارات الماليَّة ويوجد بعض الأعضاء من الدول العربيَّة، ومبادرة استرداد الأموال المسروقة (RATS) التابعة لمنظمة الإنتربول مع شبكة جهات الاتصال العالميَّة (NPFG)، وتهدف إلى توفير منصة آمِنة لتبادُل المعلومات من أجل استرداد الأصول غير المشروعة.
لا توجد مبادرات.	تنقسم هذه التجارِب إلى جزأين، الجزء الأول: تُدار هذه المبادرة عن طريق الجهات المعنيَّة في الدول، والجزء الثاني: تُدار من جهات غير حكوميَّة، على سبيل المثال: - نظام الإنذار بشأن الإعلانات الاحتياليَّة بالمملكة المتَّحدة الذي أُطلق عام 0202م بشأن الإعلانات الاحتياليَّة بالشراكة مع منصَّات الإعلانات عبر الإنترنت ووسائل التواصُل الاجتماعي، بما فيها «جوجل» و«فيسبوك» للمساعدة في معالجة قضية الإعلانات الاحتياليَّة عبر الإنترنت. - مشروع «فاروس» بفرنسا، ويهدف إلى مكافحة الجريمة المرتبطة بتقنية المعلومات والاتصالات. - مبادرة ROSIVDAMACS الهولنديَّة التابعة لمؤسَّسة التجارة الإلكترونيَّة، وهي منظَّمة مستقلَّة. وتتحقَّق من موثوقيَّة المواقع الماليَّة، بما في ذلك مواقع تداول العملات الأجنبيَّة. - مبادرة knaThsihP الأمريكية، وهي نظام قائم على مشاركة أفراد المجتمع للتحقُّق من التصيُّد الاحتيالي.

تقارير «فاتف» للتقييم المتبادَل للدول العربيَّة والشرق الأوسط وإفريقيا

حلَّل فريق الدراسة (الإنتربول) الفوارق بين البنية التحتيَّة وإمكانات البلدان في الشرق الأوسط وشمال إفريقيا عند النظر في تقارير التقييم المتبادَل. ومع ذلك، تجدر الإشارة إلى أنه ينبغي النظر في هذه المؤشرات بعناية بالغة؛ نظرًا لمرور أكثر من 10 سنوات على بعض التقارير. ولدى بعض البلدان العربيَّة أنظمة قانونيَّة راسخة تتيح لها العمل بفاعليَّة. وقد جرى التركيز على مؤشرين للتقييم، هما: التعاون الدولي I0.2، والمصادرة I0.8. والتوصية رقم 38: التقييم رقم 38 المساعدة القانونيَّة المتبادَلة في عمليَّات التجميد والمصادرة. لتحليل أكثر تفصيلًا لتقييمات «فاتف» في كل بلد، راجع المرفق الثالث.

3.5.5 أفضل الممارسات الدوليَّة والمبادرات لقطاع الخدمات الماليَّة:

3.5.5.1 المبادئ التوجيهيَّة الأوروبيَّة لمكافحة غسل الأموال

لقد قامت الجهات الإداريَّة بالاتحاد الأوروبي في السنوات القليلة الأخيرة بجهود شاملة لتقوية إطار العمل التشريعي للأنظمة والقواعد المتعلِّقة بمكافحة غسل الأموال وتمويل الإرهاب في الدول الأعضاء بالاتحاد الأوروبي. وجاء ذلك في ثلاثة مبادئ توجيهيَّة لمكافحة غسل الأموال، يُطلق عليها «AMLD»، وهي:

- المبدأ التوجيهي رقم EU /849/ 2015، المشهور بـ«AMLD 4»، الذي كان من المقرر أن يغيِّر الدول الأعضاء أحكامه في يونيو 2017م.
- المبدأ التوجيهي رقم EU /843/ 2018 المشهور بـ«AMLD 5»، الذي كان من المقرر أن يغيِّر الدول الأعضاء أحكامه في يناير 2020م.
- المبدأ التوجيهي رقم 2018/ 1673، المشهور بـ«AMLD 6»، الذي كان من المقرر أن يغيِّر الدول الأعضاء أحكامه في ديسمبر 2020م، وعلى الكيانات الخاضعة تطبيقه بحلول الثالث من يونيو 2021م.

يُصدر البرلمان الأوروبي المبادئ التوجيهيَّة للاتحاد الأوروبي بشأن مكافحة غسل الأموال بصورة دوريَّة لتطبقها الدول الأعضاء في إطار التشريعات المحليَّة. وتهدف المبادئ التوجيهيَّة إلى منع غسل الأموال وتمويل الإرهاب، وإيجاد بيئة تنظيميَّة متسقة في جميع أنحاء الاتحاد الأوروبي. ويُحقَّق ذلك من خلال معالجة الأنماط الصاعدة من جرائم غسل الأموال وتمويل الإرهاب، والمساعدة على سد فجوات الامتثال التي تتخلَّل عمليَّات مكافحة غسل الأموال.

وتوجد ملخَّصات للأحكام الأكثر صلة بـ AMLD 4 و5 و6 في مصادر مفتوحة. ويمكن إلقاء نظرة عامَّة فاحصة على هذا الرابط: https://complyadvantage.com/knowledgebase/eu-anti-money-laundering-directive/.

3.5.5.2 نشرة «ديلويت» الفنيَّة ومعهد الماليَّة الدوليَّة.. إطار العمل العالمي لمكافحة الجريمة الماليَّة

يُصنَّف قطاع الخدمات الماليَّة، بجميع أطرافه المعنيَّة، وبخاصَّةٍ المصارف، من بين أكثر الأعمال التجاريَّة تنظيمًا؛ إذ يستثمر كميات هائلة من الموارد للامتثال لمجموعةٍ من الجهود التشريعيَّة، لأسبابٍ من بينها مواجهة الجريمة الماليَّة. وعلى الرغم من ذلك، يزداد حجم المشكلة وأثرها مع تطوير المجرمين قدراتهم على استغلال إطار عمل مكافحة غسل الأموال المطبق حاليًّا. ويرجع ذلك إلى عدم وصول فاعليَّة إطار العمل التنظيمي الحالي إلى القدر الكافي لتمكين المؤسَّسات الماليَّة من محاربة الشبكات والأدوات المتطورة باستمرار والمتاحة للمجرمين.

نشرت «ديلويت»، بالاشتراك مع معهد الماليَّة الدوليَّة، أحد أبرز التقارير مؤخرًا، وقد حظي باهتمام كبير على المستوى الداخلي، وكان بعنوان «إطار العمل العالمي لمكافحة الجريمة الماليَّة»، ويبحث في سبعة مجالات رئيسة في تنظيم الجريمة الماليَّة، هي:

1- تحسينات عالميَّة منهجيَّة لإدارة أخطار الجريمة الماليَّة.

2- النهوض بالشراكات بين القطاعين العام والخاص.

3- تعزيز تبادُل المعلومات محليًّا وعبر الحدود.

4- تعزيز استخدام البيانات وجودتها.

5- تعديل عمليَّة الإبلاغ عن الأنشطة المشبوهة.

6- تخفيف التطبيق المتضارِب وغير المتسق لمعايير الامتثال والتوجيه الخاصَّة بالجريمة الماليَّة، والدفع بوضوح اللوائح التنظيميَّة.

7- زيادة استخدام التكنولوجيا وتحسينها لمكافحة التمويل غير المشروع.

ويحدد التقرير عددًا من أوجه القصور في إطار عمل مكافحة الجريمة الماليَّة، ويقدِّم توصيات لمعالجة الثغرات بشكل أفضل (ديلويت، 2021م).

3.5.5.3 مشاركة المعلومات عن التهديدات الماليَّة

مشاركة المعلومات عن التهديدات تعني تبادُل المعلومات المتعلِّقة بالتهديدات - سواء أكانت سيبرانيَّة، أم ماليَّة، أم غير ذلك - بين أعضاء مجتمع بغرض تحسين وضعها الأمني عن طريق حشد المعرفة الجماعيَّة والخبرات والقدرات الموجودة في المجتمع ضد التهديد، وعادةً ما يكون تبادل المعلومات عن التهديدات تحت شعار «كشف منظمة يصد الخطر عن الأخرى».

كسب كثيرٌ من أصحاب المصلحة والكيانات المشاركة في مجال الأمن السيبراني والمالي وعيًا بأهمية «تبادل المعلومات عن التهديد والاستخبارات» التعاوني وأثره، وهو يتيح الكشف عن الأنشطة الإجراميَّة القائمة على إساءة استخدام الحسابات المصرفيَّة ووقفها؛ إذ تُستغَل الحسابات لتسلُّم التدفقات الماليَّة غير المشروعة (من حملات الاحتيال مثلًا) وغسلها وتوجيه العائدات غير المشروعة المتأتية من مجموعة كبيرة من الجرائم الأصلية.

وبمجرد تحديد مصرف لمثل هذه «الحسابات المصرفيَّة سيِّئة السمعة/ المشبوهة»، يمكن مشاركة بياناتها مع اتحادٍ وعددٍ من المصارف الأخرى؛ ومن ثمَّ، تُمنَع أي معاملات مستقبليَّة من عملاء المصارف الأخرى/ الضحايا المحتمَلين إلى تلك «الحسابات المصرفيَّة سيِّئة السمعة» المحددة سابقًا. ولوسم تلك «الحسابات المصرفيَّة سيِّئة السمعة» وحظرها (فور التعرُّف إليها بوصفها حسابات غسل أو تهريب أموال) أثر عميق في منع التدفُّقات الماليَّة المستقبليَّة غير المشروعة إليها. ويتطلب ذلك التبادل التعاوني ومشاركة مثل هذه البيانات التكتيكيَّة (وبيانات الحسابات المصرفيَّة سيِّئة السمعة) للأفراد مع عناصر الاتحاد في قطاع الخدمات الماليَّة (مثل: المصارف، والمؤسَّسات الماليَّة، ومقدمي خدمات الدفع)، نشر الوعي بينهم بتلك «الحسابات المصرفيَّة سيِّئة السمعة» وتطبيق إجراءات الامتثال الداخلي، وإجراءات منع الاحتيال عليها.

وتحرص منظمة «الإنتربول» على تأسيس كثيرٍ من منصَّات ومجتمعات تبادُل المعلومات عن التهديدات السيبرانيَّة والماليَّة أو أيٍّ منهما في عددٍ من البلدان الأعضاء فيها، بالإضافة إلى تشغيلها. ولأنه لا تَذكر كل المجتمعات والاتحادات منصَّاتها رسميًّا أو تُروِّج لها، لا يمكننا ذكرها جميعًا.

ويوجد في هذه الاتحادات عامَّةً كيانٌ رائد مسؤول عن إدارة النظام والإبقاء عليه، والحفاظ على تدفُّق المعلومات وتعميمها بين الأعضاء. وتُبلَغ المصارف والكيانات المتعلقة بقطاع الخدمات الماليَّة دوريًّا (يوميًّا مثلًا) وتُزوَّد بمعلومات جديدة عن جهات التهديد (والحسابات المصرفيَّة سيِّئة السمعة)؛ بحيث يمكنها احتواء هذه البيانات ووسمها في أنظمتها الداخليَّة. وقد يمنع ذلك المصرف من إجراء تحويلات برقيَّة بالنيابة عن عملائه لهذه الحسابات المشتبه بها ومنعهم من التحوُّل إلى ضحايا للاحتيال مستقبلًا.

مركز مشاركة المعلومات عن الخدمات الماليَّة وتحليلها

مركز مشاركة المعلومات عن الخدمات الماليَّة وتحليلها هو مجتمع عالمي لمشاركة الاستخبارات السيبرانيَّة، تركيزه الوحيد على الخدمات الماليَّة، وتتيح المنصة استخباراتٍ ومعلوماتٍ فنيةً عن الإنذارات ومؤشرات التهديد/ الحوادث دوريًّا، ويمكِّن ذلك الأعضاء من الكشف عن التهديدات، والحد من الأخطار، وإعداد أدلَّة دفاع، إلى جانب التنبيه بشأن الحوادث التي يتعرَّض لها الأعضاء، وتحليل المنتسبين، ونصائح الشركاء (FS - ISAC, 2021).

«سيبرا»

«سيبرا» هي شركة تكنولوجيا ماليَّة مقرها في سويسرا، أسست سجلًّا وتديره، يحتوي على «الحسابات المصرفيَّة سيِّئة السمعة/ المشبوهة» المتورِّطة والمستخدَمة في القضايا والحملات السيبرانيَّة والممكَّنة عبر الإنترنت (مثل الاحتيال). وتزخر قاعدة البيانات بإسهامات قطاع الخدمات الماليَّة (المصارف وغيرها)، وأيضًا بإسهامات وكالات إنفاذ القانون التي أقامت شراكات بين القطاعين العام والخاص. وتُشارَك المعلومات عن التهديدات، وتُعمَّم بين الأعضاء والمشتركين بالمنصة؛ بهدف منع الحوادث الإجراميَّة المستقبليَّة وخسارة الضحايا المحتملين أموالهم. وأطلقت الشركة أيضًا نظامًا لتقديم الشكاوى عبر الإنترنت؛ إذ يمكن لضحايا الاحتيال إخطار «سيبرا»، التي بدورها تحاول التشاور مع مصرف المستفيد من أجل اعتراض الأموال في الوقت المناسب (Cybera Global, 2021).

3.5.5.4 العملات المشفَّرة

في مجال الأصول الافتراضيَّة والعملات المشفَّرة، تلاحظ «الإنتربول» تجميع عددٍ من «عناوين المحافظ سيِّئة السمعة/ المشبوهة» للشركات، والكيانات، والسجلات ومعلومات التهديدات المشابهة، وتخزينها، وإتاحتها، منها:

إساءة استخدام البيتكوين

موقع BitcoinAbuse.com هو قاعدة بيانات عامَّة تجمع عناوين البيتكوين التي يستخدمها المخترقون والمجرمون. يتيح الموقع والهيئة الإبلاغ عن عناوين البيتكوين، ويتضح من البلاغات أن هناك ارتفاعًا كبيرًا في عدد البلاغات عام 2020م مقارنةً بالعامين 2018 و2019م؛ حيث سجل عام 2020م 102721 بلاغًا، بينما سجل 77221 قضية عام 2019م و20642 قضية عام 2018م. انظر سجل البلاغات ومتابعة عناوين البيتكوين المسروقة (BitcoinAbuse, 2021).

«سيفرتريس»

«سيفرتريس» هي شركة مقرها في الولايات المتَّحدة، تعمل في مجال الأدلَّة الجنائيَّة لسلاسل الإمداد، ولديها كثير من الأدوات العاملة على مكافحة جرائم العملات المشفَّرة، على سبيل المثال: مكافحة غسل الأموال باستخدام العملات المشفَّرة، بالإضافة إلى خدمات لتحديد درجة خطورة المعاملات والعناوين (CipherTrace, 2021).

3.5.5.5 تصدِّي شراكات القطاعين العام والخاص للجريمة الماليَّة

أبرز وأشهر نموذج للشراكة بين القطاعين العام والخاص فيما يخص التصدِّي للجريمة الماليَّة هو «فريق العمل المشترك المعني باستخبارات غسل الأموال» في المملكة المتَّحدة، ويُعد مثالًا دوليًّا للممارسة الفُضلى، وقد يُنظر إليه بوصفه رائدًا لمنصَّات الشراكة بين القطاعين العام والخاص من هذا النوع. ومنذ تأسيسه، اتبعت فكرته البلدان والسلطات القضائيَّة الأخرى، وأطلقت منصَّات شراكة مشابهة بين القطاعين العام والخاص.

أُسس فريق العمل المشترك المعني باستخبارات غسل الأموال في عام 2015م لتبادُل المعلومات الماليَّة المتعلقة بغسل الأموال والتهديدات الإجراميَّة الاقتصاديَّة الأخرى وتحليلها. وتستضيف هذا الفريقَ الوكالةُ الوطنيَّة لمكافحة الجريمة في المملكة المتَّحدة، ويتكون من 40 مؤسَّسة ماليَّة وهيئات رئيسة في القطاع العام. وقد دعم منذ بدايته وأجرى أكثر من 600 تحقيق في مجال إنفاذ القانون، وأسهمت هذه التحقيقات في أكثر من 150 عمليَّة قبض، وفي حجز أو ضبط أكثر من 34 مليون جنيه إسترليني (حكومة المملكة المتَّحدة، 2021م).

ومن الضروري التصدِّي لمخططات غسل الأموال عالية المستوى، التي عادةً ما تتسم بالتعقيد وتعدُّد المؤسسات والجهات القضائيَّة، ويجب كذلك إنشاء منتدى لمشاركة المعلومات عن الأنماط الجديدة، ومَواطن الضعف القائمة، والاستخبارات التكتيكيَّة المباشرة.

ومنذ تأسيس فريق العمل المشترك في عام 2015م، اتبعت فكرته البلدان والسلطات القضائيَّة الأخرى وأطلقت منصَّات شراكة مشابهة بين القطاعين العام والخاص. وتقدم إحصائية «خمس سنوات من نمو الشراكات بين القطاعين العام والخاص لمكافحة الجريمة الماليَّة» ملخصات وصفيَّة عن 23 شراكة وطنيَّة وعبر الحدود الوطنيَّة لمشاركة المعلومات عن الجريمة الماليَّة، بالإضافة إلى رؤى جديدة حول تأثير تلك الشراكات في التصدِّي للجريمة الماليَّة (Royal United Services Institue, 2020).

وذُكرت الشراكات الوطنيَّة التالية في الإحصائية:

1- فريق العمل المشترك المعني باستخبارات غسل الأموال في المملكة المتَّحدة.

2- شراكة شبكة إنفاذ القوانين المعنيَّة بالجرائم الماليَّة في الولايات المتَّحدة.

3- جهاز الاستخبارات المشترك في أيرلندا.

4- تحالف Fintel Alliance الأسترالي.

5- شراكة في مجال مكافحة غسل الأموال وتمويل الإرهاب في سنغافورة.

6- فريق العمل المعني بالاحتيال واستخبارات غسل الأموال في هونج كونج.

7- فريق عمل مكافحة تمويل الإرهاب في هولندا.

8- فريق عمل مكافحة الجرائم الخطيرة في هولندا.

9- تحالف FinTell في هولندا.

10- الفريق المعني بتنسيق التعاون في لاتفيا.

11- شبكة الاستخبارات الماليَّة في ماليزيا.

12- فريق العمل المتكامل المعني بمكافحة غسل الأموال في جنوب إفريقيا.

13- فريق العمل المتكامل المعني بمكافحة غسل الأموال في السويد.

14- شبكة منع الجرائم الماليَّة في نيوزيلندا.

15- فريق الخبراء العامل في مجال مكافحة غسل الأموال وتمويل الإرهاب بالشراكة بين القطاعين العام والخاص في فنلندا.

16- مركز التميُّز في مكافحة غسل الأموال في ليتوانيا.

17- مبادرة Fintel AR في الأرجنتين.

18- تحالف مكافحة الجريمة الماليَّة في ألمانيا.

19- مبادرة الشراكة بين القطاعين العام والخاص في النمسا.

20- مبادرات «المشروع» الكندي لمكافحة الجرائم الماليَّة من خلال الشراكات.

3.5.5.6 حملات نشر التوعية والوقاية

ذُكر كثيرٌ من الأمثلة للجهود والحملات التي أجراها القطاع الخاص، مثل: قطاع الخدمات الماليَّة (إلى حدٍّ ما بالاشتراك مع القطاع العام)، لرفع مستوى الوعي بتهديدات الاحتيال المتزايدة. وأحد أمثلة هذه الحملات في المملكة المتَّحدة: حملة «تيك فايف»، وهي حملة وطنيَّة تقدِّم نصائح صريحة ونزيهة لمساعدة الجميع على حماية أنفسهم من الاحتيال المالي الممكن تفاديه. ويشمل ذلك: الخداع عبر البريد الإلكتروني والنصب عبر التليفون، وبخاصَّةٍ عندما ينتحل المجرمون شخصيَّة منظَّمات موثوق بها. تقود الحملة الجمعيَّة الماليَّة بالمملكة المتَّحدة؛ لذا، يقدمها مجموعة من الشركاء في قطاع المدفوعات، وشركات الخدمات الماليَّة، ووكالات إنفاذ القانون، ومقدمي شبكات الاتصالات، ومنظَّمات القطاع التجاري والعام والخارجي (UK Finance, 2021).

3.5.5.7 تعقُّب أصول الجريمة الماليَّة:

تعقُّب «فوكالينك» للجريمة الماليَّة

حصلت «ماستر كارد» على عددٍ من البيانات والآليَّات الجديدة، وجمعتها تحت اسم مبادرة «تعقُّب الجريمة الماليَّة»، التي تتضمَّن أيضًا إستراتيجيَّات لمنع الاحتيال في الشراء والعمل. وتمكِّن المبادرةُ المؤسَّسةَ الماليَّة من تحديد حسابات النشاط الإجرامي وغسل الأموال، عن طريق مراجعة المعاملة الماليَّة بالنظر إلى تفاصيلها وبياناتها المتداخلة المتاحة، مع مصارف مختلفة، بطريقة تحليليَّة شبكيَّة، وذلك باستخدام بيانات هائلة الحجم، وأساليب تحليل قائمة على تعلُّم الآلة التطبيقي، ورؤى ثاقبة على مستوى شبكي، والنظر إلى عمليَّة الدفع من بدايتها إلى نهايتها. بالإضافة إلى التطلُّع إلى زيادة قدراتها في سوق العملات المشفَّرة (Vocalink, 2019).

مبادرة هولندا لمراقبة المعاملات

هي مبادرة تقودها خمسة مصارف هولنديَّة: إيه بي إن أمرو، وآي إن جي، ورابو بنك، وبنك ترويدوس، ودي فولكس بنك. وبفضل هذه المبادرة، ستتمكَّن هذه المصارف من مراقبة عمليَّات الدفع لديها للبحث عن أي علامات قد تشير إلى غسل الأموال أو تمويل الإرهاب. وستحسن المراقبة الجماعيَّة للمعاملات الكشف عن التدفُّقات الماليَّة والشبكات الإجراميَّة. وبالإضافة إلى المراقبة الجماعية، ستستكمل المصارف مراقبتها لمعاملاتها وَفقًا لواجباتها المنصوص عليها في التشريع الهولندي لمكافحة غسل الأموال (قانون مكافحة غسل الأموال وتمويل الإرهاب).

ستبدأ المراقبة الجماعيَّة للمعاملات في عام 2021م بالتركيز على عمليَّات الدفع التجاريَّة. ويهدف ذلك إلى مراقبة جميع المعاملات في المصارف الخمسة. ويمكن للمصارف الأخرى الانضمام إلى هذه المبادرة في الوقت المناسب (TNML, 2021).

3.5.5.8 الخلاصة

من أهم الممارسات التي تسهم في التحوُّل إلى السياسة الاستباقيَّة ما يلي:

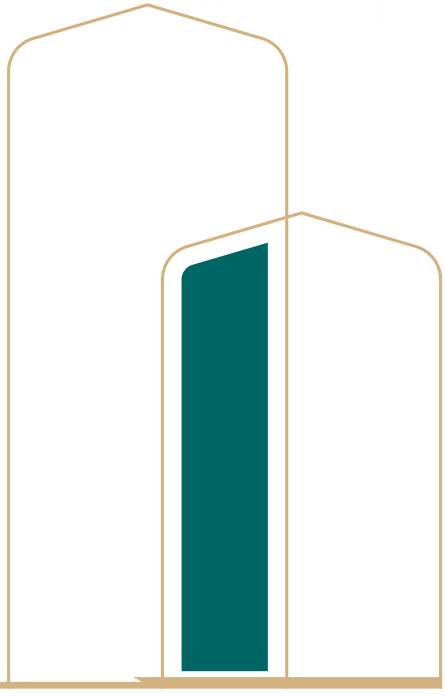
- مشاركة المعلومات عن التهديدات الماليَّة لتحسين الوضع الأمني بين القطاعات الماليَّة، وقد حقق ذلك نجاحًا كبيرًا في تبادُل المعلومات عن التهديدات ككشف الأنشطة الإجراميَّة المرتبطة بإساءة استخدام الحسابات المصرفيَّة المخصَّصة لتسلُّم التدفُّقات الماليَّة غير المشروعة (الاحتيال المالي). وتجري مشاركة الحسابات المصرفيَّة المشبوهة مع المصارف الأخرى والمؤسَّسات الماليَّة ومقدمي خدمات الدفع لمنع أي معاملات مستقبليَّة ماليَّة مع هؤلاء.
- مشاركة القطاع الخاص في الحدِّ من جريمة الاحتيال المالي، وهو ما تفتقده معظم الدول العربيَّة؛ فتدير شركة «سيبرا» الحسابات المصرفيَّة سيِّئة السمعة/ المشبوهة والمتورِّطة في الاحتيال المالي. وتتمثَّل إسهامات القطاعين العام والخاص في التزويد بقاعدة البيانات عن التهديدات بهدف منع الاحتيال المالي وخسارة الضحايا. وأطلقت شركة «سيبرا» نظامًا لاستقبال شكاوى الضحايا، ومن ثَمَّ تمريرها إلى البنوك من أجل اعتراض الأموال في الوقت المناسب.
- الشراكة بين القطاعين العام والخاص للحدِّ من الجريمة:

- التصدِّي للجريمة الماليَّة، ومن أهم النماذج المميزة والرائدة في هذه الشراكة: فريق العمل المشترك المعني باستخبارات غسل الأموال في المملكة المتَّحدة. وقد أُسِّس هذا الفريق عام 2015م لتبادُل المعلومات الماليَّة لتحليلها، ويتكوَّن من 40 مؤسَّسة ماليَّة وهيئات رئيسة في القطاع العام، ونجح في حجز وضبط أكثر من 34 مليون جنيه إسترليني، وما زالت كثيرٌ من الدول العربيَّة بعيدةً عن هذه الشراكة.

- حملات وطنيَّة لرفع مستوى الوعي وتقديم نصائح للمواطنين لحماية أنفسهم من الاحتيال المالي.

- تعقب أصول الجريمة الماليَّة باستخدام أحدث التقنيات، ومن أهم هذه التقنيات: مشاركة القطاع الخاص وتجربة Vocalink في تتبُّع الأموال؛ فهي تضم 15 بنكًا رئيسًا، بالإضافة إلى البنوك الكبرى في المملكة المتَّحدة، وتعمل على تتبُّع الأموال على مستويات

متعدِّدة. وعند تحويل المحتالين الأموال من حساب بنكي في بنكٍ ما إلى حساب آخر ضمن هذه البنوك تجري متابعته وإيقافه. وهذه من الأدوات التي تسهم في التعرُّف إلى عوائد الجريمة من الاحتيال المالي ومتابعتها بسرعة واعتراضها واسترجاعها. أما الوضع الحالي فإن أغلب البنوك في الدول العربيَّة تعمل على الرقابة الفردية دون وجود نظام يجمع هذه الحسابات تحت نظام واحد.



4. التوصيات

4. التوصيات

نقدِّم بعض التوصيات غير الملزمة، التي قد تساعد، فرديًّا أو جماعيًّا، على تحسين جهود التقصِّي والتصدِّي للجرائم الماليَّة السيبرانيَّة والحد من تأثيرها في المنطقة:

4.1 الإستراتيجيَّات والهياكل التنظيميَّة ومسؤوليَّات السلطات المختصَّة في المنطقة والبلدان العربيَّة

قد تنظر البلدان الأعضاء والسلطات المختصة في:

- وضع إستراتيجيَّة وطنيَّة بشأن التصدِّي للجريمة الاقتصاديَّة (بما في ذلك الجرائم الماليَّة الممكَّنة عبر الإنترنت) وتنفيذها، وكذلك بشأن تعقُّب الأصول واستردادها[5].
- إطلاق أو تنظيم موارد الإبلاغ عن الجريمة عبر الإنترنت، لتسهيل الإبلاغ الإلكتروني المركزي - عن الجرائم (مثل النصب والاحتيال) من جانب أفراد المجتمع والضحايا - إلى السلطات المختصة وعمليَّات المتابعة المركزيَّة والموحدة[6].
- إنشاء مراكز مخصَّصة لمكافحة الاحتيال، تقدِّم عددًا من الخدمات لمعالجة الأخطار الناجمة عن عمليَّات النصب والاحتيال بشكل أفضل، بما في ذلك إرسال إنذارات بالمواقع الإلكترونيَّة الاحتياليَّة والمحتوى الاحتيالي (مثل الإعلانات الاحتياليَّة) إلى الكيانات ذات الصلة (مثل مشغلي خدمة الإنترنت، ومنصَّات الإنترنت) وإطلاق آليَّات وإجراءات مناسبة لتعقُّب الأصول في الحالات العاجلة/ الخطيرة[7].
- إنشاء وكالات مخصَّصة لتعقُّب الأصول واستردادها، وإنشاء برنامج لتعقُّب الأصول (أي: الاستثمار في الموارد لتوظيف الخبراء، وتوفير التكنولوجيا الحديثة، وتوفير التدريب المستمر لإنشاء هيكل مستدام يساعد على تعقُّب الأصول تعقُّبًا روتينيًّا وفعَّالًا)[8].
- إعداد سلطات قضائيَّة مخصَّصة كنقطة اتصال واحدة (بالنسبة لوكالات إنفاذ القانون والجمهور العام) في حالات الجريمة السيبرانيَّة أو الاقتصاديَّة أو الماليَّة، بما يتضمَّن مسؤوليَّة تعقُّب الأصول وأوامر الاسترداد وإجراءاته.

---

[5] هذا أيضًا بالتوافُق مع ورقة فرقة العمل المعنيَّة بالإجراءات الماليَّة: «التحديات العملياتيَّة أمام استرداد الأموال.. تدابير لتحسين الفاعليَّة العالميَّة».

[6] على سبيل المثال: نموذج «أكشن فرود» في المملكة المتحدة.

[7] على سبيل المثال: نموذج مركز مكافحة النصب في سنغافورة، ونموذج مركز التنسيق لمكافحة الغش في هونج كونج (الصين)، وغير ذلك.

[8] على سبيل المثال: نموذج مكاتب استرداد الأصول (في دول الاتحاد الأوروبي)، ووكالة استرداد الأصول وإدارتها في أوكرانيا... إلخ.

- إعداد آليَّات لضمان التعاون والتنسيق المحليين الفعَّالين عبر مجموعة من أصحاب المصلحة المشاركين في عمليَّات استرداد الأصول (مثل: قطاع الخدمات القضائيَّة، وقطاع خدمات الشرطة، وقطاع الخدمات الماليَّة)، وهذا أمر حيوي لدعم قضايا استرداد الأصول المحليَّة، فضلًا عن القضايا العابرة للحدود التي تستجيب السلطات لطلباتها من ولايات قضائيَّة أخرى أو تسترد أصولًا في الخارج بشأنها. ويشمل ذلك عمليَّات التمكين من التنفيذ المباشر للأوامر الأجنبيَّة والطلبات الثنائيَّة العابرة للحدود.
- مشاركة وكالات إنفاذ القانون الإقليميَّة والدوليَّة أو أيٍّ منهما، والتزامها بمساعدة شبكات تعقُّب الأصول واستردادها. وعلى سبيل المثال: يمكن أن يكون ذلك بمنزلة تنشيط للمنتدى العربي لاسترداد الأصول، وإنشاء الشبكات القائمة بالفعل واستخدامها (مثل شبكة كارين) أو أيهما.
- اعتماد إطار عمل قانوني يسمح بالتدابير (الإداريَّة أو القضائيَّة) وتنفيذه للمساعدة على التجميد السريع للأصول أو المعاملات الماليَّة التابعة لمصدر غير مشروع - (نابع من عمليَّات النصب والاحتيال، بما في ذلك حالات التعدِّي والجرائم الأصليَّة والضحايا في الخارج) التي قد تكون عرضة لخطر التبديد - ومصادرتها أو تأجيلها[9].
- اعتماد إطار عمل قانوني يضمن تسريع وتيرة توفير المعلومات لوكالات إنفاذ القانون وتنفيذه، وتُعد هذه نقطة حاسمة بالنسبة لفعالية وسرعة تعقُّب الأصول تعقُّبًا روتينيًّا (للحالات الداخليَّة والاستجابة للطلبات العابرة للحدود). ويجب أن تشمل هذه المعلومات جميع معلومات ملكيَّة الحساب المصرفي الأساسيَّة والنشاط المالي (أي: التحويلات الجارية والصادرة... إلخ). ويجب أن تكون هذه المعلومات متاحة بسرعة (في غضون ساعات) دون أمر من المحكمة أو اتفاق أو ترتيب مع أي كيان أو مؤسَّسة أخرى. ويتفق ذلك أيضًا مع إحصائية «فاتف» بعنوان «التحديات التنفيذيَّة لاسترداد الأصول.. إجراءات تحسين الفاعليَّة العالميَّة». ويطبِّق مركز مكافحة النصب بسنغافورة آليَّة فعَّالة جدًّا من حيث الوصول إلى المعلومات وتوفيرها بسرعة، ويتعاون كذلك مع المصارف المحليَّة.
- إنشاء منصَّات وشراكات محليَّة بين القطاعين العام والخاص لمعالجة الجرائم الممكَّنة عبر الإنترنت والجرائم الماليَّة. ويُفضَّل أن تشمل هذه الشراكات أصحاب المصلحة المعنيين من قطاع الخدمات الماليَّة (مثل: المصارف، وشركات التكنولوجيا الماليَّة، ومقدِّمي خدمات الأصول الافتراضيَّة، ومقدِّمي خدمات الدفع... إلخ) والسلطات الحكوميَّة (مثل: وحدة الاستخبارات الماليَّة، وسلطات السلوك المالي والهيئات الإشرافيَّة ووكالات إنفاذ القانون... إلخ).

[9] ويتفق ذلك أيضًا مع إحصائيَّة «فاتف» بعنوان «التحديات التنفيذيَّة لاسترداد الأصول.. إجراءات تحسين الفاعليَّة العالميَّة».

4.2 الجوانب التحقيقيَّة والتنفيذيَّة والتكتيكيَّة

قد تنظر البلدان الأعضاء والسلطات المختصة فيما يلي:

- إنشاء منصَّة مشتركة تعتمد على تقنيات تصنف البيانات التي جُمِعت لرفع كفاءة عمليَّات الإنذار التي تخص المواقع الاحتياليَّة أو غير المشروعة عبر الإنترنت (على سبيل المثال: حملات النصب والاحتيال والإعلانات الاحتياليَّة... إلخ)، وتضمن معالجتها بسرعة وإحالتها إلى السلطات وكيانات القطاع الخاص المختصة، وتضمن أيضًا السعي إلى إغلاق هذه المواقع، وإزالة المحتوى الاحتيالي غير المشروع أو حجبه من نطاق الإنترنت المحلي.
- إنشاء قواعد بيانات تسهل تبادُل المعلومات بين مختلف سلطات الشرطة محليًّا، سعيًا إلى تحديد وتوحيد مختلف الشكاوى والتقارير والتحقيقات التي تستهدف مصدر الخطر نفسه وحملات النصب والاحتيال نفسها (على سبيل المثال: بسبب الموقع أو الرابط أو رقم الهاتف أو الحساب المصرفي نفسه الذي استخدمه المجرمون). ومن شأن هذه الآليَّة أن تساعد على مركزيَّة التحقيقات ودمجها، وإيجاد أوجه تآزر لها، ومنع ازدواجيَّة الجهود في التحقيقات والإجراءات القضائيَّة.
- تنفيذ آليَّة لتبادُل المعلومات بشأن التهديدات الماليَّة (مثل الحسابات المصرفيَّة المشتبه بها/ سيِّئة السمعة/ المشبوهة، المرجح/ المعروف أنها تتلقَّى عائدات عمليَّات النصب والاحتيال). ويمكن أن يطلق المصرف المركزي أو اتحاد المصارف منصَّات المعلومات ويديرها. وقد تنظر المصارف في الانضمام إلى منصَّات تبادُل المعلومات المتاحة والقائمة التي يديرها القطاع الخاص، والاستفادة منها.
- اعتماد الأدوات التقنية التي تضمن تعقُّب الأصول عبر مختلف المصارف والحسابات في الوقت المباشر. واعتمادًا على عدد المصارف المشاركة والملتزمة بهذه الأدوات، يمكن تعقُّب التدفُّقات غير المشروعة للأصول والأموال عبر مختلف المصارف، ما يضمن تقديم الإنذارات والإخطارات في الوقت المناسب لتعليق المعاملات الاحتياليَّة، ومنعها فيما بين المصارف المعنيَّة.
- تنفيذ آليَّة تضمن أن طلبات الحالات العاجلة أو المسائل الخطيرة المتعلقة بتعقُّب الأصول واعتراضها واستردادها (بما في ذلك العمليَّات العابرة للحدود) تُنفَّذ في الوقت المناسب ودون أي تأخير. ويتطلَّب ذلك إجراء اتصالات استباقيَّة ومنتظمة وبنَّاءة بين الجهات القضائيَّة المقدِّمة

للطلبات والسلطات القضائيَّة المستقبِلة للطلبات طوال عمليَّة تعقُّب الأصول واستردادها. ولاتخاذ الإجراءات الفوريَّة دور أساسي في الاستفادة من الزخم وتحقيق النتائج في عمليَّات اعتراض التدفُّقات الماليَّة غير المشروعة في الوقت المناسب[10].

- إنشاء سجل داخلي لوكالات إنفاذ القانون على الإنترنت، ويُفضَّل أن يشمل هذا السجلُّ مجموعةً من جهات الاتصال من القطاع الخاص (أي: من قطاع الخدمات الماليَّة، والمصارف، وشركات التكنولوجيا الماليَّة، ومقدمي خدمات الإنترنت، ومنصَّات الإنترنت، وشركات الاتصالات السلكيَّة واللاسلكيَّة... إلخ)، فضلًا عن التوجيهات والتعليمات المتعلقة بتقديم الإنذارات والطلبات من وكالات إنفاذ القانون إلى القطاع الخاص في سياق التحقيقات في الجريمة، ومنعها.

4.3 أدوات «الإنتربول» وخدماتها ومساعداتها:

- الاستخدام المستمر لشبكة «الإنتربول» I-24/7 في الحالات الخطيرة/ العاجلة لطلب أو تقديم معلومات إلى البلدان الأخرى الأعضاء في الشبكة (داخل المنطقة وحتى خارجها).
- النظر في تبادُل البيانات والمعلومات الاستخباراتيَّة المتعلِّقة بالقضايا مع الأمانة العامَّة لـ«الإنتربول»، والسعي إلى إجراء عمليَّات بحث متبادَلة والإخطار بحالات التطابُق التي تظهر في نهاية المطاف في قواعد بيانات «الإنتربول».
- طلب الدعم والمساعدة من «الإنتربول» في جهود تنسيق القضايا عبر الحدود.
- استخدام لوحة المتابعة الخاصَّة بـ«الإنتربول» ومنصَّة التعاون الآمن؛ إذ توفر كيانات القطاع الخاص التوجيهات وقوائم جهات الاتصال والكتيبات للمكاتب المركزيَّة الوطنيَّة في البلدان الأعضاء ووكالات إنفاذ القانون.

[10] تُعد المراكز المخصَّصة لمكافحة النصب وتعقُّب الأصول أو أحدهما، ومكاتب استرداد الأصول، في وضع جيِّد لتنفيذ آليَّة تضمن اتخاذ إجراءات فوريَّة، بما يتضمَّن الإنذارات وطلبات تعقُّب الأصول عبر الحدود. ويوفر منشور منظمة الإنتربول «تيك أكشن» مجموعة أدوات تضم القنوات والأنظمة الخاصَّة بتقديم الإنذارات الفوريَّة وطلبات إيقاف الدفع. وقد تنظر وحدات الاستخبارات الماليَّة في الدول الأعضاء في الانضمام إلى برنامج الاستجابة السريعة لوحدة الاستخبارات الماليَّة في مجموعة «إيجمونت».

4.4 النموذج المقترَح للحدِّ من جريمة الاحتيال المالي

عند الرجوع إلى التحديات التي تواجه الجهات المعنيَّة في الدول العربيَّة (إنفاذ القانون، والمؤسَّسات الماليَّة، والبنك المركزي، والنيابة العامَّة) التي حُدِّدت في اجتماع مجموعة التركيز، نجدها تتعلق بما يلي:

- بطء التواصُل بين الجهات المعنيَّة.
- استغراق وقت طويل في الإجراءات الإداريَّة في التحريات والتحقيق.
- ضعف تبادُل البيانات بين الجهات المعنيَّة (إنفاذ القانون، والنيابة العامَّة، والبنك المركزي).
- عدم وجود ربط بين البلاغات المتلقاة بالاحتيال المالي للتعرُّف إلى الأساليب الإجراميَّة.
- قصور البنوك في متابعة أنماط الاحتيال المتعددة التي يستخدمها المحتالون لمحاولة استباقها وتوعية عملائها.
- نقص في تأهيل جهات التحرِّي والتحقيق للتعرُّف إلى أنماط جرائم الاحتيال المالي وأساليبها.
- عدم تعاوُن بعض الدول في توفير البيانات أو مشاركتها.

ولتفعيل التوصيات، يمكن تقسيمها إلى ما يلي:

4.4.1 إنشاء مركز متخصِّص للاحتيال المالي

من أهم التوصيات المقترحة: إنشاء مركز متخصِّص للاحتيال المالي على المستوى الوطني ليُسهِم في الحفاظ على الاقتصاد الوطني للدول ويساعد الجهات المعنيَّة في حل كثيرٍ من قضاياها. الجدول رقم «10» يُبرز ملخصًا لأهم النماذج الدوليَّة في الحدِّ من جريمة الاحتيال المالي.

الجدول رقم «10»: أهم النماذج الدوليَّة للمراكز

الدولة	المراكز المتخصِّصة	البداية	الإدارة
سنغافورة	مركز مكافحة النصب	2019م	الشرطة السنغافورية
المملكة المتَّحدة	المركز الوطني للجرائم الاقتصاديَّة	2018م	
الولايات المتَّحدة	مركز شكاوى جرائم الإنترنت التابع لمكتب التحقيقات الفيدرالي	2018م	مكتب التحقيقات الفيدرالي (FBI)
هونج كونج	مركز التنسيق لمكافحة الغش	2017م	شرطة هونج كونج

المتخصِّصة للحدِّ من جريمة الاحتيال المالي

الهدف	المهام	المزايا في النموذج
منع النصب وردعه والكشف عنه	- معالجة المعلومات. - التدخل (بنهج التعطيل: التجميد المركزي للحسابات المصرفيَّة، ووقف خطوط الهاتف، وإزالة إعلانات الإنترنت المشتبه بها). - التحقيق والاستخبارات. - المبادرات والابتكار. - التعاون الدولي.	- استقبال البلاغات من جهات إنفاذ القانون وليس من الضحايا. - العمل بين جهات إنفاذ القانون والمؤسَّسات الماليَّة - خلال السنة الأولى، ساعد المركز في استعادة 21 مليون دولار أمريكي، وجمَّد على الأقل 6100 حساب مصرفي مشتبه به، وأقام شراكات حيويَّة مع كثير من شركاء المجال.
العمل على خفض معدل الجريمة الاقتصاديَّة المنظَّمة والخطيرة، وحماية العامَّة وضمان ازدهار المملكة المتَّحدة وسمعتها؛ كونها مركزًا ماليًّا.	- اقتفاء أثر المتهمين بالاحتيال على المواطنين البريطانيين، ومهاجمة الصناعة في المملكة المتَّحدة، وإساءة استخدام الخدمات الماليَّة بالمملكة المتَّحدة. - ضمان تثقيف الصناعات المختلفة والأجهزة الحكوميَّة في المملكة المتَّحدة بكيفيَّة الحماية من الجرائم الاقتصاديَّة. - تكثيف حماية مواطني المملكة المتَّحدة.	الجمع بين وكالات إنفاذ القانون وهيئات العدالة، والإدارات الحكوميَّة، والهيئات التنظيميَّة، والقطاع الخاص.
التحقيق في جرائم الإنترنت واسترجاع الأموال	- توفير آليَّة إبلاغ موثوق بها ومريحة لإرسال المعلومات إلى مكتب التحقيقات الفيدرالي فيما يخص أنشطة الجريمة المشتبه بها والميسرة بالإنترنت. - المساعدة على تحديد الحسابات الاحتياليَّة المحتملة في جميع أنحاء القطاع. - البقاء في طليعة الاتجاهات الناشئة فيما يخص مخططات عمليَّات الاحتيال المالي الجديدة. - تعزيز علاقة تكافليَّة تتشارك فيها المعلومات بشكل مناسب.	- استقبال البلاغات مباشرة من الضحايا. - تجميد الحسابات البنكيَّة. - جمع الجهات المعنيَّة.
توحيد الجهود المعنيَّة للشرطة في مكافحة الجريمة ومنعها	- وضع التوجُّهات الإستراتيجيَّة وتطبيقها لمكافحة الغش. - تقديم خدمة المشورة الفوريَّة إلى العامَّة عبر التليفون فيما يخص مكافحة الغش من أجل تقديم المساعدة في الوقت المناسب إلى من يحتاج إليها. - تحسين التعاون بين الشرطة والإدارات الحكوميَّة الأخرى وأصحاب المصلحة بالداخل والخارج لمكافحة الغش ومنعه. - تنظيم مواد الإعلان عن مكافحة الغش وحملات التثقيف المقدَّمة من وحدات الشرطة المختلفة، وتقديم الدعم الفوري إلى وحدات الخط الأمامي للشرطة. - متابعة اتجاهات الغش وتحليلها، وتوفير تقييم للأخطار، واتخاذ إجراءات في التوقيت المناسب.	معرفة أساليب الغش واتجاهاته وتحليلها، وتوفير تقييم للأخطار، واتخاذ إجراءات في التوقيت المناسب.

وبعد مراجعة النماذج الدوليَّة، نجد أنها تتكون من خمس ركائز رئيسة، هي:

4.4.1.1 البلاغات

توفر آليَّة بلاغات مستدامة ومخصَّصة لجرائم الاحتيال الموجَّهة ضد الاقتصاد الوطني، وتُسهم في الربط بين البلاغات المتلقاة بالاحتيال المالي للتعرُّف إلى الأساليب الإجراميَّة، وهناك نموذجان مختلفان لاستقبال البلاغات:

- استقبال البلاغات مباشرةً من الضحايا، وهذا النموذج سيكون الأسرع في اتخاذ الإجراء في تجميد الحساب، ولكن يحتاج إلى التحقُّق من صحة البلاغ.
- استقبال البلاغات من جهات إنفاذ القانون بعد التحقُّق من صحة البلاغ، وهذا النموذج سيخفف الضغط على المركز وعبء التحقُّق من صحة البلاغ، ولكنه سيكون أبطأ في اتخاذ الإجراء من حيث تجميد الحساب.

4.4.1.2 المعالجة

أيضًا هناك عدة نماذج تُسهِم في تقليل الوقت المستغرق للمعالجة ورفع سرعة الاستجابة والجاهزيَّة وتوافر البيانات، وهي:

- جمع الجهات المعنيَّة (على سبيل المثال: إنفاذ القانون، والنيابة العامَّة) في مكان واحد لتسريع التواصُل بين الجهات المعنيَّة.
- جهة إنفاذ القانون فقط.
- جمع القطاعين العام والخاص.

4.4.1.3 المبادرات والابتكارات

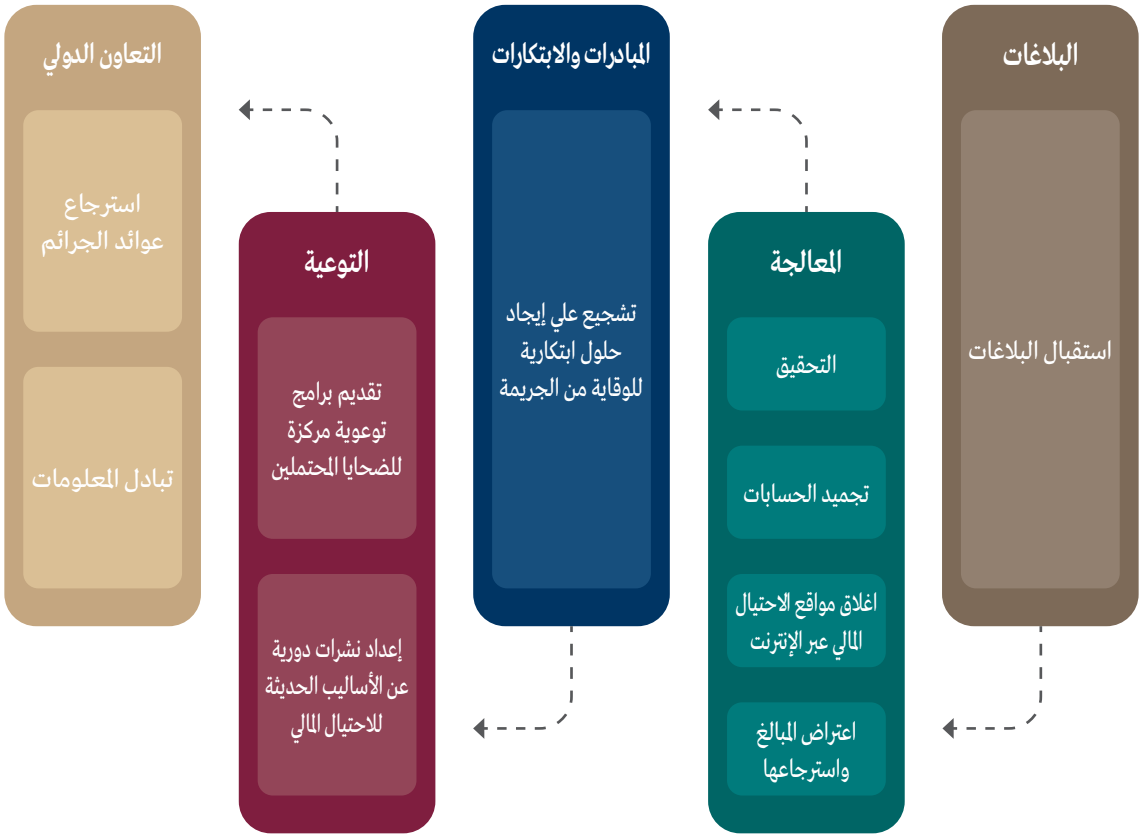
وهي أمر مهم في تشجيع المجتمع والمؤسَّسات غير الربحيَّة وغيرها لتقديم مبادرات تُسهِم في الوقاية من جريمة الاحتيال المالي. وقد حصل النموذج السنغافوري على ابتكارات أسهمت في الوقاية من الجريمة.

4.4.1.4 التوعية

نَشْرُ تقارير دوريَّة عن اتجاهات جريمة الاحتيال المالي والأساليب الناشئة، وتقديم برامج توعويَّة مركَّزة للضحايا المحتملين بالأساليب الإجراميَّة التي تستهدف مختلف فئات المجتمع، ككبار السن.

4.4.1.5 التعاون الدولي

هناك حاجة مُلحَّة إلى التعاون بين الدول والمراكز المشابهة، وبخاصَّةٍ أنَّ هذه الممارسة بدأت بالانتشار بين الدول. وستُسهم بتبادُل المعلومات الاستخباراتيَّة وإنشاء قوائم سوداء للمحتالين واعتراض الأموال واسترجاع عوائد الجرائم. الشكل التوضيحي رقم «29» يبيِّن مرتكزات النموذج المقترَح للحدِّ من جريمة الاحتيال المالي.



الشكل التوضيحي رقم «29»: مرتكزات النموذج المقترَح للحدِّ من جريمة الاحتيال المالي

4.4.2 نظام مقترَح للحدِّ من انتشار المواقع الاحتياليَّة ذات المحتوى العربي عبر الإنترنت

قد نرى من المناسب تأسيس نظامٍ للتحرِّي والتحقيق الرقمي في جرائم الاحتيال المالي عبر الإنترنت وتطويره من قِبَل فريق عمل بمركز الجرائم السيبرانيَّة والأدلَّة الرقميَّة بجامعة نايف العربيَّة للعلوم الأمنيَّة. وستساعد الجامعة وكالات إنفاذ القانون العربيَّة على التحقُّق من المواقع الاحتياليَّة/ تزويد الجهات بالأساليب الإجراميَّة الناشئة/ تزويد الجهات بروابط المواقع الاحتياليَّة التي تستهدف المنطقة العربيَّة لخداع مواطنيها والمقيمين فيها بالفرص الاستثماريَّة الوهميَّة. وستوفر قاعدة البيانات لعمليَّات الاحتيال المالية حلولًا تكتيكيَّة لتحديد مواقع الاستثمار الاحتياليَّة وآليَّات إغلاقها، والاستفادة من تطبيقات الذكاء الاصطناعي لتقصِّي الروابط المشبوهة، ويتم ذلك بدراسة الروابط التي ستُجمَع لإنشاء قاعدة بيانات مشتركة مع الجهات المعنيَّة والمجتمع الرقمي لتمكين عمليَّات تصنيف البيانات ورفع مستوى أداء التعقُّب باستمرار، وسيسمح للمؤسسات الماليَّة بالدخول إلى النظام لتزويده بالمواقع الاحتياليَّة والأساليب الإجراميَّة الحديثة. وهناك إمكانية بمشاركة المجتمع والمنظَّمات غير الربحية لتزويد النظام بالمواقع الاحتياليَّة لتشجيع المشاركة المجتمعيَّة للوقاية من الجريمة.

وسيوفِّر النظام للجهات الأمنيَّة ما يلي:

1. التحقُّق من الموقع عبر مطابقته بالمواقع الاحتياليَّة الموجودة في قاعدة البيانات.
2. تحميل رابط مشبوه إلى النظام، وبعد التحقُّق من المواقع المشبوهة، تُضاف السجلات الجديدة إلى قاعدة البيانات/ المستودع عبر الإنترنت.
3. التعرُّف إلى أفضل الممارسات للإبلاغ عن إساءة الاستخدام من قِبَل النطاقات المحتالة (على سبيل المثال: إجراءات الإبلاغ أو التصعيد للاتصال بمالكي النطاق أو المسجلين أو Verizon أو ICANN).
4. الحصول على تقارير إحصائيَّة نصف سنويَّة لجهات إنفاذ القانون عن مواقع الاحتيال المالي.
5. الحصول على نشرات عن الأساليب الإجراميَّة الناشئة.

4.4.3 إصدار مجموعة من الأدلَّة الاسترشاديَّة

العمل على إصدار مجموعة من الأدلَّة الاسترشاديَّة في المجال التقني، بالتعاون مع المنظَّمات الدوليَّة ذات العلاقة (مثل: الإنتربول، وآيكان) كاستخدام التقنيات وأدوات التحقيق الجنائي الرقمي المتقدِّم في الجرائم الماليَّة عبر الإنترنت.

4.4.4 تطوير القدرات البشريَّة

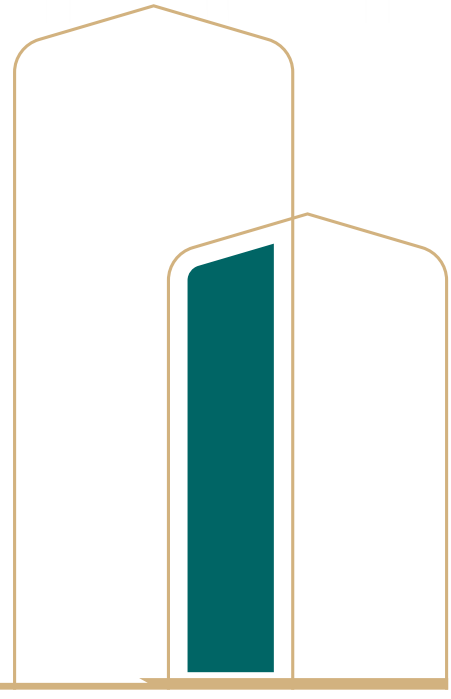
تطوير برامج تدريبية متخصِّصة في عدَّة مسارات تدريبيَّة تستهدف جهات إنفاذ القانون وأعضاء النيابة العامَّة والقضاء، باتباع أفضل الممارسات الدوليَّة في التحقيق الجنائي الرقمي للجرائم الماليَّة عبر الإنترنت.

4.4.5 إجراء بحوث ودراسات متخصِّصة

إجراء دراسات تتعلَّق بالسلوكات النفسيَّة لجميع الأطراف (الضحايا والمحتالين) لتطوير الأساليب والأدوات والتكتيكات الخاصَّة بالجرائم الماليَّة عبر الإنترنت للحدِّ من جريمة الاحتيال المالي، وإجراء البحوث في مجال تطوير السياسات للدول العربيَّة والأنظمة والقوانين المتعلِّقة بالحدِّ من جرائم الاحتيال المالي.

4.4.6 إنشاء مرصد ضحايا جريمة الاحتيال المالي عبر الإنترنت

إنشاء مرصد «open data» يمكِّن الضحايا من مشاركة تجربتهم عن جرائم الاحتيال التي تعرَّضوا لها، بحيث تكون هذه المعلومات متاحة للجميع للاطلاع عليها، وستكون مفيدة لتحذير المتابعين حتى لا يقعوا ضحايا لهذه الجرائم، وتكون مرجعًا للباحثين والجهات ذات العلاقة للوقاية من الجريمة والحد منها.



المراجع

أولًا: المراجع العربية

- حكومة المملكة المتَّحدة (2021م، 17 أغسطس). خطة الجريمة الاقتصاديَّة من 2019 إلى 2022. https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version

- ديلويت (2021م، 5 أغسطس). إطار العمل العالمي لمكافحة الجريمة المالية. https://www2.deloitte.com/global/en/pages/financial-services/articles/gx-global-framework-for-fighting-financial-crime.html

- الشياظمي، محمد (2020م، 29 يناير). لا تزال مصدر قلق عالمي.. مؤتمر بالدوحة يبحث تحديات الامتثال ومكافحة الجرائم الماليَّة. الجزيرة نت. https://bit.ly/3aBkVVK

- صحيفة سبق (2021م، 17 أبريل). الأمن العام يستعرض تفاصيل جرائم تم القبض على مرتكبيها. https://sabq.org/MN987P

- المفوضيَّة الأوروبيَّة (2020م). تقرير المفوضيَّة إلى البرلمان الأوروبي والمجلس - استرداد الأصول ومصادرتها - ضمان ألَّا تفيد الجريمة. https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200602_com-2020-217-commission-report_en.pdf

- مؤسسة النقد العربي السعودي (2008م). دليل مكافحة الاختلاس والاحتيال المالي وإرشادات الرقابة. https://www.sama.gov.sa/ar-sa/Laws/BankingRules/AntiFinancialFraudGuide.pdf

- وكالة الأنباء السعودية (2021م، 4 أغسطس). شرطة الرياض: القبض على 3 مواطنين و5 مقيمين ارتكبوا عددًا من جرائم النصب والاحتيال. https://www.spa.gov.sa/viewstory.php?lang=ar&newsid=2270371

- وكالة الأنباء السعودية (2021م، 16 أبريل). شرطة الرياض: القبض على شبكتين إجراميتين نفَّذتا عمليات احتيال. https://www.spa.gov.sa/2216449

ثانيًا: المراجع الإنجليزيَّة

- Abraham et al. (2020). The Global State of Scams 2020. Ecommerce Foundation. https://bit.ly/3k6zQKy

- Anti-Deception Coordination Center. (2021, July 25). Crime Matter. www.police.gov.hk/ppp_en/04_crime_matters/adcc/

- Australian Competition & Consumer Commission (2020). Targeting scams report 2020. https://www.accc.gov.au/sites/www.accc.gov.au/files/Targeting%20scams%20report%20infographic%202020.jpg
- Australian Cyber Security Center. (2021, July 25). ReportCyber. https://www.cyber.gov.au/acsc/report
- Bavarian State Ministry of Justice. (2021, August 04). Central Cybercrime Bavaria (ZCB). https://www.justiz.bayern.de/gerichte-und-behoerden/generalstaatsanwaltschaft/bamberg/spezial_1.php
- Bavarian State Ministry of Justice. (2021, August 11). Central Coordination Office for Asset Recovery in Bavaria (ZKV BY). https://www.justiz.bayern.de/gerichte-und-behoerden/generalstaatsanwaltschaft/muenchen/spezial_5.php
- BitcoinAbuse. (2021, August, 05). Bitcoin Abuse Datebase. https://www.bitcoinabuse.com/
- Buller, A. (2020, Dec 2020). Covid-19 sparks boom in Middle East digital payments sector. https://www.computerweekly.com/news/252493293/Covid-19-sparks-boom-in-Middle-East-digital-payments-sector
- Camden Asset Recovery Inter-agency Network. (2021, July 10). https://www.carin.network/
- Canadian Anti-Fraud Center. (2021, July 25) Recent Scams and Fraud. https://www.antifraudcentre-centreantifraude.ca/index-eng.htm
- Central Bank of Egypt. (2021, July 28). Financial Inclusion for the Unbanked Through Alternate Lending Methods. https://fintech-egypt.com/news/news_details.php?id=128
- Central Bank of Egypt. (2021. July 20). Financial Inclusion for the Unbanked Through Alternate Lending Methods. https://fintech-egypt.com/news/news_details.php?id=128
- CipherTrace. (2021, August, 10). Cryptocurrency Compliance Anti-Money Laundering, Financail Investigations and Fraud Detection. https://ciphertrace.com/
- City of London. (2021, July 20).General Guide to thr NFIB. https://www.actionfraud.police.uk/what-is-national-fraud-intelligence-bureau
- Comply Advantage. (2021, July 29). EU Anti Money landering Directives. https://complyadvantage.com/knowledgebase/eu-anti-money-laundering-directive/

- Cybera Global. (2021, August, 05). We use Technology to Disrupt Financially Motivated Cybercrime. https://cybera.io/solutions/

- DGCCRF (2021). The National Task Force Against Scams Publishes an Enriched Version of its Prevention Guide. https://www.economie.gouv.fr/dgccrf/la-task-force-nationale-de-lutte-contre-les-arnaques-publie-une-version-enrichie-de-son

- Ecommpay. (2021, July 24). Payment Systems in Middle East . https://ecommpay.com/products/payment-methods/payment-systems-in-middle-east/

- Europen Commission. 2020. Commission Adopts the Report "Asset Recovery and Confiscation: Ensuring that Crime does not Pay". https://ec.europa.eu/home-affairs/news/20200602_commission-adopts-report-asset-recovery-confiscation-ensuring-crime-does-not-pay_en

- Egmont Group. (2021, July 05). https://www.egmontgroup.org/

- Egmont Group. (2021, July 05). List of Members. https://www.egmontgroup.org/

- Egmont Group. (2021, July 05). New Publication: Egmont Group Bulletin – Business Email Compromise Fraud. https://www.egmontgroup.org/

- EUACI. (2021, July 20). Asset Recovery and Managemnt Agency. https://arma.gov.ua/en

- European Commission. (2021, July, 26). Migrantion and Home Affairs. https://ec.europa.eu/home-affairs/e-library/glossary/asset-recovery-office-aro_en

- European Commission. 2020. Report from The Commission to The European Parliament and The Council Asset Recovery and Confiscation: Ensuring that Crime does not pay. https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200602_com-2020-217-commission-report_en.pdf

- European Justice. (2021, August, 02). https://e-justice.europa.eu/home?action=home&plang=en

- EUROPOL. (2021, June 20). SIRIUS Project. https://www.europol.europa.eu/activities-services/sirius-project

- FS-ISAC. (2021, August 02). Intelligence. https://www.fsisac.com/what-we-do/intelligence

- GAFILAT. GAFILAT Asset Recovery Network (RRAG). (2021, June 17). https://www.gafilat.org/index.php/es/espanol/18-inicio/gafilat/49-red-de-recuperacion-de-activos-del-gafilat-rrag

- UK Government Digital Service. (2021). Policy Paper Economic Crime Plan, 2019 to 2022, Accessible Version. https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version

- Hong Kong Police Force. (2021, June, 28). Anti-Deception Coordination Center. https://www.police.gov.hk/ppp_en/04_crime_matters/adcc/about.html

- ICANN. (2021, July 28 (DAAR.نظام في البلدان لرموز الأعلى المستوى نطاقات https://www.icann.org/resources/pages/daar-cctld-2021-05-14-ar

- Internet Crime Complaint Centre. (2020). Internet Crime Report 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

- Internet Crime Complaint Center. (2021, July 20). https://www.ic3.gov/

- Interpol. (2021, July 27). Inside a French Police Crackdown on the Eurasian. https://www.interpol.int/

- Interpol. (2021, July 27). Returning Stolen Public Funds. https://www.interpol.int/Crimes/Corruption/Anti-corruption-and-asset-recovery#pt-1

- Interieur Gouv. 2016. Report Suspicious or Illegal Content with Pharos. https://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Signaler-un-contenu-suspect-ou-illicite-avec-PHAROS

- Mordor Intelligence. (2021, June 2021). Middle East & North Africa Digital Payments Market Growth, Trends, Covid-19 Impact, and Forecasts (2021 - 2026). https://www.mordorintelligence.com/industry-reports/middle-east-and-north-africa-digital-payments-market

- National Crime Agency. 2021. National Economic Crime Center. https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre

- National Fraud & Cyber Crime Reporting centre. (2021, July 20). https://www.actionfraud.police.uk/

- National Fraud & Cyber Crime Reporting centre. (2021, July 20). https://www.actionfraud.police.uk/what-is-national-fraud-intelligence-bureau

- Offcial Journal of the European Union. (2015). المبدأ التوجيهي للبرلمان الأوروبي، والمجلس

2015 مايو 20 ،2015/849 رقم الأوروبي. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=DE

- Phishtank. (2021, August 01). Stats. https://www.phishtank.com/stats.php

- Royal Canadian Mounted Police. (2021, July 25). New Cybercrime and Fraud Reporting System. https://www.rcmp-grc.gc.ca/en/new-cybercrime-and-fraud-reporting-system

- Royal Canadian Mounted Police. (2021, July 25). The National Cybercrime Coordination Unit (NC3). https://www.rcmp-grc.gc.ca/en/nc3

- Royal United Services Institue. 2020. Survey Report. Five Yaers of Growth in Public-Private Financial Information-Sharing Partnerships to tackle Crime. https://www.future-fis.com/uploads/3/7/9/4/3794525/five_years_of_ growth_of_public-private_partnerships_to_fight_financial_crime_-_18_aug_2020.pdf

- Stolen Asset Recovery Initiative. (2021, June 21).

- Stolen Asset Recovery Initiative. (2021, June 21). Arab Forum 2015. https://star.worldbank.org/events/arab-forum-2015

- Stolen Asset Recovery Initiative. (2021, June 21). StAR Supports international effort Arab Forum 2015. https://star.worldbank.org/events/arab-forum-2015

- Stolen Asset Recovery Initiative. 2021..دليل شبكات استرداد الأصول https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/workinggroup2/2018-June-6-7/V1803851e.pdf

- Singapore Police Force. (2021, August 11). Police Anti-Scam Center Marks First Year of Operationalisation. https://www.police.gov.sg/media-room/news/20200730_police-anti-scam-centre-marks-first-year-of-operationalisation

- The Advertising Standards Authority. (2021). Six Months Review of our Scam Ad Alert System. https://www.asa.org.uk/news/six-month-review-of-our-scam-ad-alert-system.html

- The Crown Prosecution Service. (2021, July 15). CPS Launches Ambitious Plan to Combat Economic Crime. https://www.cps.gov.uk/cps/news/cps-launches-ambitious-plan-combat-economic-crime

- TMNL. (2021, August, 02). What is TMNL?. https://tmnl.nl/summary-eng

- UK Finance. (2021, August 21). https://takefive-stopfraud.org.uk/

- VERISIGN. (2021, July 01). The Domain Name Industry Brief. https://www.verisign.com/en_US/domain-names/dnib/index.xhtml

- Vocalink. 2019. Trace and Alert Financial Crime. trace-and-alert-financial-crime%20(1).pdf; https://www.vocalink.com/services/financial-crime-solutions/

nauss.edu.sa nauss.sa +966 11 246 3444

info@nauss.edu.sa nauss_sa +966 11 245 0222