مجموعة إجمونت لوحدات المعلومات المالية

نشرة مجموعة إجمونت

الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال

فريق العمل المعني بتبادل المعلومات

يوليو 2019

"نسخة للنشر"

مجموعة إجمونت لوحدات المعلومات المالية

نشرة عامة: الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال

تهدف هذه النشرة إلى تحذير السلطات المختصة والجهات المبلّغة من أنماط ومخاطر غسل الأموال المرتبطة بمخططات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال. ينبغي أن تساعد المعلومات الواردة في هذه النشرة السلطات المختصة والجهات المبلّغة على كشف وتحديد مخططات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال والإبلاغ عنها والتحقيق فيها على النحو الأفضل وتعطيل شبكات التمويل غير المشروعة.

نشرة عن الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال

رقم التعريف: EG-Bulletin-01/2019

التاريخ: 30 يوليو 2019

الجهات المعنية: السلطات المختصة (الجهات التنظيمية والرقابية وجهات إنفاذ القانون) والجهات المبلّغة.

المقدمة

تولي مجموعة إجمونت والدول الأعضاء فيها أولوية رئيسية لمنع مرتكبي الجرائم الإلكترونية من استغلال النظام المالي العالمي. وقد وضعت مجموعة إجمونت هذه النشرة لتوعية وحدات المعلومات المالية الأعضاء والدول المعنية من التهديد المتزايد الذي تشكله مخططات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال. تُعدّ هذه المخططات من الجرائم الإلكترونية الأسرع نمواً والتي تؤثر سلباً على المؤسسات المالية، مما يعرّض القطاع المالي في جميع أنحاء العالم لخسائر تُقدّر بمليارات الدولارات. على سبيل المثال، قدّرت احدى الدول خسائر

محتملة تجاوزت قيمتها 12 مليار دولار ناتجة عن اكثر من 78000 حالة احتيال تم الإبلاغ عنها خلال فترة الخمس سنوات الأخيرة، والتي استهدفت ضحايا محليين ودوليين.[1] تستهدف هذه المخططات المؤسسات التجارية وأصحاب المهن والأفراد عن طريق انتهاك حساب البريد الإلكتروني الخاص أو المخصص للأعمال لإرسال (أو التسبب في إرسال) تعليمات دفع مغلوطة ومعلومات أخرى يتم استخدامها لارتكاب الاحتيال المالي.

الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال

يشمل ذلك مخططات يمكن من خلالها لمرتكبي الجرائم انتهاك حسابات البريد الإلكتروني الخاصة بالضحايا من خلال (1) إرسال تعليمات دفع احتيالية إلى المؤسسات المالية أو الشركاء التجاريين الآخرين بهدف اختلاس الأموال؛ أو (2) إرسال بيانات عن طريق الاحتيال بهدف اجراء الاحتيال المالي.

بإمكان المؤسسات المالية أن تلعب دوراً مهماً في كشف مخططات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال، ومنعها والإبلاغ عنها من خلال تعزيز التواصل والتعاون بين وحداتها الداخلية المعنية بمكافحة غسل الأموال ومنع الاحتيال والأمن السيبراني.

لمواجهة التهديد المتزايد والخطير الذي تشكله عمليات الاحتيال عبر انتهاك البريد الإلكتروني الواقعة على المؤسسات المالية وعملائها، أطلقت 11 وحدة معلومات مالية مشروع فريق اجمونت المخصص لمكافحة الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال الذي يركز على تحليل الاتجاهات والمنهجيات المعتمدة في هذه المخططات. تهدف مجموعة إجمونت الى مشاركة النتائج الرئيسية لهذا التحليل مع وحدات المعلومات المالية، لتقوم بدورها بمشاركتها مع السلطات المختصة والجهات المبلّغة بالطريقة المناسبة. استناداً إلى هذه النتائج الرئيسية، تتضمن هذه النشرة مؤشرات مخططات الاحتيال عبر انتهاك البريد

[1] راجع إعلان الخدمة العامة لمكتب التحقيقات الفدرالي، "الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال، عملية احتيال بقيمة 12 مليار دولار"The 12 Billion Dollar Scam، 12 يوليو 2018 م على الموقع: https://www.ic3.gov/media/2018/180712.aspx

الإلكتروني المخصص للأعمال والعمليات المرتبطة بها الناتجة عن الاحتيال . يمكن للمؤسسات المبلغة التي تلقت هذه النشرة استخدامها لتحديد عمليات الاحتيال المحتملة عبر انتهاك البريد الإلكتروني المخصص للأعمال، والإبلاغ عنها إلى الجهات التنظيمية والرقابية وجهات إنفاذ القانون.

كيف يتم الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال

عامةً تتضمن مخططات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال انتحال هوية الضحايا بهدف ارسال تعليمات دفع تبدو مشروعة للمؤسسة المالية لكي تقوم بتنفيذها. بالرغم من أن هذه المخططات تختلف في بعض الجوانب ، إلا أنها تتمحور جميعها حول استخدام حسابات البريد الإلكتروني التي يتم انتهاكها لحثّ المؤسسات المالية و/أو عملائها على إجراء عمليات دفع غير مصرّح بها أو احتيالية، أو إرسال بيانات خاصة إلى جهة أخرى غير مصرح لها باستخدام هذه البيانات بهدف اجراء الاحتيال المالي.

يمكن تقسيم مخططات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال إلى ثلاث مراحل:

المرحلة 1 - انتهاك المعلومات الخاصة بالضحية و حسابات بريدها الإلكتروني:

يقوم مرتكب الجريمة (المُقرصن) بدايةً بالولوج غير المصرح به إلى البريد الإلكتروني للضحية، غالباً من خلال تقنيات الهندسة الاجتماعية[2] أو تقنيات انتهاك جهاز الكمبيوتر. يستغل مرتكبو الجريمة بعد ذلك حساب البريد الإلكتروني الذي تم انتهاكه للحصول على معلومات تتعلق بالمؤسسات المالية التي يتعامل معها الضحية وتفاصيل الحسابات المصرفية والاشخاص الذين يتواصل معهم وأية معلومات أخرى ذات صلة.

[2]تشير الهندسة الاجتماعية إلى أساليب التفاعل البشري المستخدمة لخداع الفرد وحثّه على الكشف عن المعلومات. يستخدم مرتكبو الجرائم الهندسة الاجتماعية بصفة أساسية لتسهيل مخططات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال.

المرحلة 2 - إرسال تعليمات الدفع الاحتيالية:

بعدها، يستخدم مرتكب الجريمة (المُقرصن) المعلومات المسروقة الخاصة بالضحية لإرسال تعليمات أو بيانات دفع احتيالية عبر البريد الإلكتروني إلى المؤسسة المالية لتبدو كأنها مُرسلة من قبل الضحية. تحقيقاً لهذه الغاية، يستخدم مرتكب الجريمة (المُقرصن) إما حساب البريد الإلكتروني الفعلي للضحية الذي تم انتهاكه، أو حساب بريد الكتروني مشابه مُنشأ لهذه الغاية. قد يقوم مرتكب الجريمة (المُقرصن) بتقديم مستندات داعمة مزيفة بهدف تعزيز تعليمات الدفع الصادرة عنه .

المرحلة 3 - تنفيذ العمليات غير المصرّح بها:

يقوم مرتكب الجريمة (المُقرصن) بخداع الموظف المسؤول لدى الضحية أو لدى المؤسسة المالية التي يتعامل معها الضحية للقيام بتحويلات مالية تبدو في الظاهر مشروعة، لكنها في الواقع غير مصرّح بها أو تمت بطريقة احتيالية. بنتيجة التعليمات الاحتيالية يتم تحويل الاموال إلى حسابات مصرفية يسيطر عليها مرتكب الجريمة (المُقرصن) سواء في ذات البلد او خارجه.
تعتبر المؤسسات المالية في شرق وجنوب شرق آسيا، وكذلك دول أوروبا الغربية والشرقية، وُجهات شائعة لهذه العمليات الاحتيالية. إلا أنه تجدر الإشارة إلى أن مرتكبي الجرائم يقومون في كثير من الأحيان بتعديل استراتيجياتهم، ويمكن أن تتغير دول الوجهة نتيجة لذلك.

نماذج أفعال الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال

غالبًا ما تستهدف مخططات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال المؤسسات المالية أو عملائها من الشركات والأفراد الذين يقومون باجراء عمليات كبيرة من خلال المؤسسات المالية وكيانات الإقراض والشركات العقارية وشركات المحاماة، تتم عادة هذه المخططات على النحو التالي:

نموذج 1 مرتكب الجريمة (المقرصن) ينتحل صفة عميل مؤسسة مالية:

يقوم مرتكب الجريمة (المُقرصن) باختراق حساب البريد الإلكتروني العائد لموظف في شركة (A) ويستخدمه لإرسال تعليمات تحويل مصرفي إلى المؤسسة المالية التي تتعاطى معها الشركة (A)،[3] والتي تقوم بناءً على هذا الطلب بإجراء تحويل مصرفي وإرسال الأموال إلى حساب يخضع لسيطرة مرتكب الجريمة (المُقرصن).

في هذا النموذج، يقوم مرتكب الجريمة (المقرصن) الذي ينتحل صفة عميل المؤسسة المالية، بطلب إجراء تحويل مصرفي غير مصرّح به.

نموذج 2 – مرتكب الجريمة (المقرصن) ينتحل صفة مسؤول تنفيذي (يُعرف باسم "CEO Fraud"):

يقوم مرتكب الجريمة (المُقرصن) باختراق حساب البريد الإلكتروني لأحد المسؤولين التنفيذيين في الشركة (B) ويستخدمه لإرسال تعليمات تحويل مصرفي إلى الموظف المسؤول عن تسوية وإصدار الدفعات في الشركة (B). يقوم الموظف، اعتقاداً منه بأنها تعليمات صادرة عن المسؤول التنفيذي للشركة (B) بالطلب من المؤسسة المالية التي تتعاطى معه الشركة (B) إجراء التحويل المصرفي.

في هذا النموذج ، يقوم مرتكب الجريمة (المُقرصن) الذي ينتحل صفة أحد المسؤولين التنفيذيين في الشركة بتضليل موظف الشركة ليقوم عن غير قصد بالسماح بالتحويل المصرفي الاحتيالي إلى الحساب الذي يخضع لسيطرة مرتكب الجريمة (المُقرصن). كما يمكن لمرتكب الجريمة (المُقرصن) ، ضمن هذا

[3] في كافة هذه المخططات، عوضا عن اختراق حساب البريد الالكتروني للضحية، قد يقوم مرتكب الجريمة (المُقرصن) بإنشاء حساب بريد إلكتروني مشابه لحساب البريد الإلكتروني الفعلي للضحية.

المخطط، انتحال صفة مسؤول تنفيذي في الشركة لتضليل موظف فيها وحثّه على إرسال كشوفات الرواتب أو معلومات خاصة يمكن لمرتكب الجريمة (المقرصن) استخدامها لاحقاً في الاحتيال المالي.

نموذج 3 - مرتكب الجريمة (المقرصن) ينتحل صفة أحد الموردين:

ينتحل مرتكب الجريمة (المُقرصن) صفة أحد مورّدي الشركة (C) أو أحد مزودي الخدمات المهنية (على سبيل المثال وكيل عقاري أو شركة ضمان أو محامي) ويقوم بإرسال رسالة بريد إلكتروني إلى الشركة (C) لإبلاغها بإرسال دفعات الفواتير أو الودائع مستقبلاً إلى حساب ومكان جديدين . بناءً على هذه التعليمات الاحتيالية، تقوم الشركة (C) بتحديث معلومات الدفع الخاصة بموردها وتزود المؤسسة المالية التي تتعامل معها بتعليمات التحويل المصرفي الجديدة، لتقوم المؤسسة المالية بعدها بإرسال الدفعات إلى الحساب الذي يسيطر عليه مرتكب الجريمة.

في هذا النموذج، يقوم مرتكب الجريمة (المُقرصن)، الذي ينتحل صفة مورد أو مزود خدمة، بإرسال تعليمات دفع احتيالية لتضليل موظف الشركة التي يتعامل معها المورّد وحثّه على إرسال التحويلات المصرفية إلى الحساب الذي يخضع لسيطرته.

نموذج 4 – مرتكب الجريمة (المقرصن) يستهدف الخدمات العقارية:

يقوم مرتكب الجريمة (المُقرصن) بانتهاك حساب البريد الإلكتروني العائد لوكيل عقاري أو لشخص يقوم بشراء أو بيع عقارات بهدف تغيير تعليمات الدفع وتحويل الأموال الناتجة عن معاملة عقارية (كعائدات البيع أو مدفوعات القرض أو الرسوم). كما يمكن أن يقوم مرتكب الجريمة (المُقرصن) بانتهاك حساب البريد الإلكتروني لوكيل عقاري ويستخدمه للاتصال بشركة الضمان ويطلب منها تحويل عائدات العمولات التي يكسبها إلى الحساب الذي يخضع لسيطرته.

في هذا النموذج، يقوم مرتكب الجريمة (المُقرصن) الذي ينتحل صفة *وكيل عقارات (أو شريك رئيسي آخر في المعاملة العقارية) بارسال تعليمات دفع احتيالية لتضليل الطرف المقابل وتوجيه الدفعات الأولية أو أي أموال أخرى مرتبطة بالمعاملة العقارية إلى الحساب الخاضع لسيطرته .*

مؤشرات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال

إن النجاح في كشف وإيقاف مخططات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال، يتطلب التحقق من التعليمات المرتبطة بالمعاملة الصادرة عن العميل ومراجعتها بعناية، والنظر في الظروف المحيطة بهذه التعليمات. ونظراً إلى أن بعض المؤشرات المرتبطة بالاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال قد تعكس في الواقع أنشطة مالية مشروعة، **ينبغي على المؤسسات المالية عدم الاعتماد على مؤشر واحد مرتبط بالمعاملة لتحديد ما إذا كانت المعاملة مشبوهة**. كما ينبغي على المؤسسات المالية النظر في مؤشرات إضافية بالإضافة الى الوقائع والظروف ذات الصلة، كمراجعة العمليات المالية السابقة للعميل وما إذا كان تنطبق عليه مؤشرات متعددة قبل تقرير ما إذا كانت العملية مشبوهة. كما ينبغي على المؤسسات المالية أيضاً إجراء المزيد من عمليات التحقق والاستفسار عند الاقتضاء.

قد تدلّ المؤشرات التالية على مخططات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال:

مؤشرات خاصة بحساب الضحية

أنماط العمليات المشبوهة العامة:

- يقوم العميل بإرسال تعليمات دفع عبر البريد الإلكتروني لصالح مستفيد معروف؛ إلا أن المعلومات الخاصة بحساب المستفيد تختلف عن تلك المستخدمة سابقاً.

- يقوم العميل بإرسال تعليمات دفع عبر البريد الإلكتروني إلى مستفيد ليس لديه تعامل مالي سابق معه أو علاقة تجارية موثقة، وتكون قيمة التحويل مساوية أو تتجاوز الدفعات المرسلة سابقاً الى مستفيدين آخرين .

- يقوم العميل بإرسال تعليمات دفع اضافية عبر البريد الإلكتروني مباشرة بعد اتمام عملية دفع ناجحة إلى حساب لم يُحَوّل اليه سابقًا لتسديد مستحقات الموردين/البائعين. قد يتسق هذا السلوك مع محاولة مرتكب الجريمة (المُقرصن) إصدار دفعات إضافية غير مصرّح بها عقب نجاح عملية احتيالية.

- قيام العميل بإرسال تعليمات دفع عبر البريد الإلكتروني تحمل صفة "عاجل" أو "سري".

- قيام العميل بإرسال تعليمات دفع عبر البريد الإلكتروني بطريقة لا تتيح للمؤسسة المالية الوقت الكافي للتأكد من صحة العملية المطلوبة.

- قيام العميل بإرسال تعليمات دفع عبر البريد الإلكتروني لإجراء تحاويل إلى حساب لدى مؤسسة مالية أجنبية ورد بحقه شكاوى سابقة من العميل كونه وُجهة مشتبه بها للعمليات الاحتيالية.

- أن تتضمن تعليمات الدفع المرسلة من البريد الإلكتروني للعميل، والتي تبدو مشروعة، لغة وتوقيت ومبالغ مختلفة عن تعليمات الدفع السابقة التي تم التدقيق فيها والتأكد من صحتها.

- أن تصدر تعليمات الدفع من بريد إلكتروني يشبه إلى حد كبير البريد الإلكتروني المعروف للعميل، مع وجود اختلاف طفيف من حيث إضافة أو تغيير أو حذف حرف واحد أو أكثر. على سبيل المثال:

البريد الإلكتروني الصحيح	البريد الإلكتروني الاحتيالي
John-doe@abc.com	John_doe@abc.com
John-doe@bcd.com	

- أن تتلقى المؤسسة المالية تعليمات دفع عبر البريد الإلكتروني من موظف لدى العميل مفوض حديثاً بالتصرف في الحساب، أو من موظف مفوض لم يسبق له أن أرسل تعليمات دفع من قبل.

- قيام موظف لدى العميل أو ممثل عنه بإرسال تعليمات دفع عبر البريد الإلكتروني إلى المؤسسة المالية بالنيابة عن العميل مستنداً فقط إلى مراسلات عبر البريد الإلكتروني صادرة من مديرين تنفيذيين أو محامين أو من ينوب عنهم. غير أن الموظف أو ممثل العميل يشير إلى أنه تعذر عليه التحقق من العمليات مع هؤلاء المديرين التنفيذيين أو المحامين أو من ينوب عنهم.

بلدان ذات مخاطر عالية من حيث الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال

- قد يعود حساب المستفيد الى شركة اوف شور او الى مؤسسة مالية تقع في بلد ذات مخاطر عالية، بناءً على ما تحدده المؤسسة المالية والجهات المختصة في البلد حيث توجد المؤسسة المالية.

استخدام المستندات أو الفواتير المزورة

- يقوم مرتكب الجريمة (المُقرصن) بإرسال مستندات أو فواتير مزورة إلى موظف لدى الضحية لتأكيد العملية. قد تكون المستندات والفواتير المزورة عالية الجودة وقد تتضمن مستندات أصلية تم تعديلها بهدف تحويل الأموال إلى الحساب التابع لمرتكب الجريمة.

المؤشرات المرتبطة بحساب المشتبه بهم بارتكاب الاحتيال عبر انتهاك البريد الالكتروني المخصص للأعمال.

الأنماط العامة للعمليات المشبوهة

• بعد عملية انتهاك حساب/شركة، يتم سحب الأموال على الفور من المؤسسة المالية، أو تحويلها فوراً إلى خارج المؤسسة المالية، أو إلى حسابات متعددة داخل المؤسسة المالية.

• تتلقى مؤسسة مالية تحويلاً مصرفياً لإيداعه في حساب، غير أن التحويل المصرفي يحدد مستفيداً ليس هو صاحب الحساب المسجل لديها. قد ينطبق ذلك على الحالات التي تقوم فيها الضحية بإرسال التحويلات المصرفية عن غير قصد إلى رقم حساب جديد يحدده مرتكب الجريمة (المقرصن) منتحلاً صفة مورّد معروف، وتعتقد الضحية بالتالي أن الحساب الجديد يعود للمورّد المعروف منها، كما هو مبيّن في النموذج (3) أعلاه. قد ينطبق هذا المؤشر على المؤسسة المالية التي تتلقى تحاويل مرسلة من قبل مؤسسة مالية أخرى نتيجة للاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال.

قيمة التحويل

• أن لا تتوافق قيمة التحويل المستلم في حساب المستفيد مع نشاطه.

استخدام ناقلي الأموال (Money Mules)

• يمكن أن تشير الزيادة المفاجئة في العمليات الكبيرة والأرصدة الخاصة بعميل وسيط إلى تورطه المحتمل كناقل للأموال ضمن مخطط الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال. يعتبر ناقلو الأموال [4] بمثابة وسيط لمرتكبي الجرائم والمنظمات الإجرامية. في بعض الحالات، لا يدرك الضحايا أنه تم استغلالهم لنقل الأموال إلى مرتكبي الجرائم الإلكترونية. يستخدم مرتكبو الجرائم عادة ناقلي الأموال لتنفيذ مخطط الاحتيال عبر انتهاك البريد الإلكتروني المخصص

[4] تستخدم هوية ناقلي الأموال لفتح حسابات لدى المؤسسات المالية، والحصول على بطاقات مصرفية مزودة برقم تعريف شخصي، وعلى رموز شخصية، والوصول إلى تسهيلات الدفع عبر الإنترنت. يتوجب على ناقلي الأموال تسليم هذه المعلومات أو تمريرها إلى أعضاء آخرين ضمن جماعة الجريمة المنظمة لاستخدامها في عمليات إجرامية. غالبا ما لا يكون لناقل المال أي فكرة عن الجريمة التي شارك فيها ولا يتلقى سوى مبلغ بسيط مقابل "الخدمة" التي قدمها.

للأعمال. تكون أرصدة ناقلي الأموال عموماً منخفضة أو نشاطهم المالي محدود قبل مشاركتهم في المخطط.

الحدّ من المخاطر

إن التحقق الشامل من العمليات يمكن ان يساعد في حماية المؤسسات المالية من عمليات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال. على سبيل المثال، قد تتحقق المؤسسات المالية من صحة تعليمات الدفع المشبوهة الواردة عبر البريد الإلكتروني من خلال التواصل مع العميل عبر وسائل متعددة (مثل الهاتف أو حسابات البريد الإلكتروني البديلة) أو عن طريق الاتصال بالأشخاص المصرّح لهم بإجراء العمليات في شركة العميل. يعتمد نجاح مخططات الاحتيال عبر انتهاك البريد الإلكتروني على قيام مرتكبي الجرائم بالطلب من المؤسسات المالية تنفيذ على وجه السرعة عمليات تبدو مشروعة وإنما غير مصرّح بها. غالباً ما تكون هذه العمليات غير قابلة للإلغاء، مما يجعل المؤسسات المالية والعملاء غير قادرين على إلغاء التحاويل أو استعادة الأموال. لذلك، من المهم كشف تعليمات الدفع الاحتيالية قبل إصدار أوامر الدفع وذلك لمنع العمليات غير المصرّح بها والحدّ منها.

الاستجابة لحوادث الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال واسترداد الأموال

تتعاون بعض وحدات المعلومات المالية في مجموعة إجمونت مع المؤسسات المالية وجهات إنفاذ القانون للمساعدة في استرداد أموال الضحايا من خلال التبادل السريع للمعلومات المتعلقة بالعمليات المالية المشبوهة المرتبطة بعملية الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال. من المهم للغاية اتخاذ إجراءات سريعة من جانب الضحايا والمؤسسات المالية وجهات إنفاذ القانون لنجاح استرداد الأموال. حيث أن معدل استرداد هذه الأموال ينخفض إلى حد كبير بعد مرور أول 24 ساعة.

للمساعدة في التحقيق في حوادث الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال واسترداد الأموال الناتجة عن هذه العمليات، ينبغي على المؤسسات المالية اتخاذ الخطوات التالية[5]:

1) الاتصال الفوري بجهات إنفاذ القانون والجهات الأخرى المختصة:

أ. **الإبلاغ عن الجريمة:** ينبغي أن تعمل الضحية والمؤسسات المالية وجهات إنفاذ القانون والجهات التنظيمية ووحدات المعلومات المالية المحلية والأجنبية بسرعة لمحاولة استرداد الأموال التي تم تحويلها. للقيام بذلك، ينبغي على الضحية أو المؤسسة المالية ذات الصلة بالضحية تقديم تقرير فوري عن الجريمة وطلب المساعدة من جهات إنفاذ القانون ووحدة المعلومات المالية.[6]

من المهم أيضًا أن تقوم المؤسسات المالية بالإبلاغ ليس فقط عن عمليات الاحتيال الناجحة وإنما أيضًا عن المحاولات الفاشلة، حيث أن المعلومات المرتبطة بمحاولات الاحتيال قد تكون مهمة لمساعدة الجهات المختصة في إجراءات التحقيق في النشاط غير المشروع والشبكات الإجرامية.

ب. **تنبيه المؤسسة المالية المستفيدة:** يجب على المؤسسة المالية التي نفذت التحويل الناتج عن عملية احتيالية من حساب الضحية، الاتصال على الفور بالمؤسسة المالية المستفيدة لإبلاغها عن عملية الاحتيال المشتبه بها.

ج. **الإبلاغ عن عملية واردة مشبوهة:** قد تشتبه المؤسسة المالية المتلقية للتحويل الاحتيالي بوقوع عملية احتيال في حال كان لديها شكوك حول المصدر المشروع للأموال. في هذه الحالة، ينبغي عليها الاتصال فوراً بالجهات التنظيمية وجهات

---

[5] لا تكون العناصر ذات الصلة بكل خطوة متسلسلة بطبيعتها، حيث أن العديد من هذه الأنشطة يمكن أن تحدث بشكل متزامن أو متتابع. كما هو مذكور أعلاه، تعدّ الاستجابة السريعة والتعاون مع الجهات المختصة، بما في ذلك جهات إنفاذ القانون ووحدات المعلومات المالية، عناصر أساسية في دعم عملية استرداد الأموال التي تم خسارتها نتيجة الاحتيال.

[6] تختلف صلاحيات وإجراءات جهات إنفاذ القانون ووحدات المعلومات المالية والجهات الأخرى المختصة بحسب البلد. وعلى الرغم من أن هذا القسم يسلط الضوء على أهمية إبلاغ جهات إنفاذ القانون ووحدات المعلومات المالية المحلية بحالات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال، إلا أنه ينبغي على الأشخاص والمؤسسات المالية المتضررة أن تاخذ بالاعتبار السلطات والجهات المعنية في لديها لتحديد الجهات المناسبة التي يجب إشراكها.

إنفاذ القانون ذات الصلة في البلد، وبوحدة المعلومات المالية لإبلاغها عن العملية المشبوهة.

يتوجب أيضاً على الجهة المبلغة تقديم ابلاغ عن العملية المشبوهة فوراً إلى وحدة المعلومات المالية ذات الصلة بحسب الاقتضاء. إذا تم تنفيذ عملية التحويل خلال الـ 72 ساعة الماضية، يتوجب على الشخص الذي قدم الابلاغ الإصرار على عجلة الحالة.

2) إيقاف حركة النقد

أ. عدم إجراء عمليات مشبوهة: على المؤسسة المالية المستفيدة التي لديها معلومات (على سبيل المثال، رسالة سويفت SWIFT تطلب ارجاع التحويل) عن تلقي عملية تحويل احتيالية إلى حساب أحد عملائها، أن تمتنع عن إجراء عمليات قد تؤدي إلى خسارة الأموال من الحساب موضوع الاشتباه. من أجل تقييم صحة التحويل الوارد، ينبغي على المؤسسة المالية المستفيدة الاتصال بجهات إنفاذ القانون ووحدة المعلومات المالية.

3) حجز/استرداد الأصول

أ. إبلاغ السلطات المختصة عن مكان الأصول: لتعزيز إمكانية استرداد الأصول، ينبغي أن تتعاون المؤسسات المالية مع جهات إنفاذ القانون ووحدة المعلومات المالية المحلية من خلال توفير جميع المعلومات المطلوبة. كما ينبغي على المؤسسات المالية إبلاغ وحدة المعلومات المالية وجهات إنفاذ القانون قبل تنفيذ أي عملية صادرة، إذا كانت الأموال لا تزال في الحساب، وكذلك تقديم معلومات عن الوجهة التالية للأموال التي جرى تحويلها من الحساب.

ب. أوامر التجميد: ينبغي أن تتعاون المؤسسات المالية مع وحدة المعلومات المالية و/أو جهات إنفاذ القانون في حال صدور أوامر التجميد عن السلطات المختصة.

الإبلاغ عن العمليات المشبوهة بناءً على هذه النشرة

مع مراعاة الإجراء المعمول به في البلد ذو الصلة، ينبغي على المؤسسات المبلغة الإشارة إلى هذه النشرة عند إبلاغ السلطات المختصة عن العمليات المحتملة المتعلقة بـالاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال بناءً على مؤشرات هذه النشرة. حيث أن الإشارة إلى هذه النشرة في تقارير العمليات المشبوهة سيتيح للسلطات المختصة تحديد واتخاذ الخطوات المناسبة للمساعدة في استرداد الأموال والتحقيق في حالات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال. ينبغي على الجهات المبلّغة، حيثما أمكن، مراعاة إدراج المصطلح الرئيسي التالي في تقاريرها عن العمليات المشبوهة، للإشارة إلى استنادها إلى هذه النشرة في تحديد العمليات المشبوهة التي قد تكون مرتبطة بمخططات الاحتيال عبر انتهاك البريد الإلكتروني المخصص للأعمال:

"نشرة مجموعة إجمونت حول انتهاك البريد الإلكتروني المخصص للأعمال"

ينبغي أن تحرص المؤسسات التي تقوم بالإبلاغ عن عمليات الاحتيال عبر انتهاك البريد الإلكتروني على تضمين جميع المعلومات التفصيلية في تقارير العمليات المشبوهة ذات الصلة، لا سيما:

<u>تفاصيل التحويل المصرفي:</u>

- تواريخ ومبالغ العمليات المشبوهة؛
- معلومات تعريف المرسل ورقم الحساب والمؤسسة المالية؛
- معلومات تعريف المستفيد ورقم الحساب والمؤسسة المالية؛ و
- معلومات تتعلق بالمؤسسات المالية المراسلة والوسيطة، إن وجدت.

<u>تفاصيل المخطط:</u>

- المؤشرات الإلكترونية، مثل عناوين البريد الإلكتروني ذات الصلة، ورأس البريد الإلكتروني (email header)، وعناوين بروتوكول الإنترنت المرتبطة بها (Internet Protocol)، مع الطوابع الزمنية الخاصة بكل منها؛ و
- وصف وتوقيت رسائل البريد الإلكتروني المشبوهة.