****

|  |  |
| --- | --- |
| [www.coe.int/cybercrime](http://www.coe.int/cybercrime) | قسم حماية البيانات ومكافحة الجريمة الإلكترونية  المديرية العامة لحقوق الإنسان وسيادة القانون  ستراسبورغ، فرنسا  إصدار، مارس 2018 |

الدورة التدريبية المتقدمة في مجال الجريمة الإلكترونية والأدلة الإلكترونية لفائدة القضاة والمدعين العامين

2018

*مدخل إلى دراسة الحالة المرتبطة بتمرين التحقيق*

*ودليل المدربين*



**فهرس المحتويات**

1. **المقدمة ..………………………………………………………………………………………………………. ………………… 3**
2. **التحقيق …………………………………………………………………………………………………………………………… 4**

**1.2 استجلاء وإثبات الوقائع الأولية**

**2.2 إنشاء شك معقول حول البداية الممكنة للجريمة**

1. **الإعدادات المالية .………………………………………………….………………………………………… …………………… 6**
2. **الشروع في الارتكاب الفعلي للجريمة وأهم نقطة في التحقيق …………………….………………..……………… 7**
3. **نهاية ارتكاب الجريمة وبداية القضية………………………………………………….……………………………………… 9**
4. **أهم خطوات التحقيق والأدلة الإلكترونية الأساسية…………………..……………………..…………………………… 11**
5. **الملاحق .………………………………………………….….……………………………………………… ……………………… 12**
6. المقدمة

**يرتبط سيناريو دراسة هذه الحالة بالخطط التي اشتهرت حديثًا، أو ما يُعرف باسم "احتيال البريد الإلكتروني الخاص بالأعمال"، أو حالات "BEC" (**Business E-mail Compromise**)، وهي مشتقة من عمليات الاحتيال التي تم اكتشافها سابقًا وكانت تدعى " احتيال الرئيس المدير العام" أو عمليات احتيال "الوسيط". ويعتبر نطاق وحجم عمليات الاحتيال هذه مدهشا.**

**وما فتئت الأضرار الجسيمة التي تلحق بالضحايا تتزايد رغم أن السلطات الحكومية والقطاع الخاص في عدد كبير من بلدان العالم، يحاولان باستمرار توعية المجتمعات العامة والخاصة. لسوء الحظ، فإن أحدث المعلومات حول الأضرار المالية المجمعة على مستوى العالم لا تدعم الرأي السائد بأنه تم إحراز تقدم في هذا المجال.**

**ملاحظة للمدربين:** يبدأ السيناريو بالإشارة إلى البنك الفدرالي لأتلانتيس (FBA) كبنك دولي معروف وذي سمعة طيبة. وينبغي أن يجلب وصف من هذا القبيل المتدربين إلى استنتاج أن هذا النوع من البنوك لا ينبغي أن يشارك في أي نوع من المشاكل، ناهيك عن المشاكل المشابهة لتلك التي سيتم وصفها لاحقًا في هذه الوثيقة.

**ومن ناحية أخرى، يعتبر حاليا هذا النوع من البنوك تحديدا أهداف منتظمة لخطط من هذا القبيل، ربما بسبب ترددها في تعديل إجراءات أمن العمل لمواجهة التحديات الجديدة أو بسبب شعور زائف بالأمن والأهمية والحضور على المستوى العالمي.**

عند نهاية التدريب، ينبغي أن يدرك المتدربون أنه حتى البنوك أو المؤسسات المالية مثل هذا البنك يمكن أن تكون أهدافًا وضحايا لعمليات الاحتيال. **كما سيكشف التحقيق، في هذه القضية، أن "احتيال البريد الإلكتروني الخاص بالأعمال" مرتكب بالتأثير الإضافي للتهديد المستمر والمتقدم (APT) وهندسة اجتماعية إلكترونية عكسية، بالإضافة إلى استخدام عملات مشفرة.**

**ملاحظة للمدربين:** تتمثل الفكرة من وراء هذا التمرين في تعزيز المقاربة القانونية للتحقيق والتي ينبغي أن تجلب المتدربين إلى عملية تدريجية باستخدام الأدوات القانونية الموضوعة رهن إشارتهم لإجراء تحقيق شبه حقيقي وبناء قضية جنائية. **ويعتبر هذا التمرين مزيجا من مواد في اتفاقية بودابست وأحكام قانونية محلية تساعد المتدربين في حل القضية بنجاح ابتداء بمرحلة التحقيق، ومرورا بمرحلة المتابعة القضائية إلى الدعوى الرئيسية وانتهاء بصدور الحكم النهائي. وسيشمل ذلك أيضا بعض الخطوات الهامة التي يمكن وينبغي اتخاذها خلال عملية المساعدة القانونية المتبادلة طبقا للاتفاقية.**

**لأغراض هذا التدريب، تم إنشاء بلدان وهمية، وهي: أتلانتيس، نورلاندا، أوستلاندا، ويستلاند وغيرها.** وفي إطار إعداد التمرين، صادقت جميع هذه البلدان على اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية ("اتفاقية بودابست"). **ينبغي أن تسمح هذه المقاربة بنقل التدريب بين الولايات القضائية، دون الحاجة إلى إدخال تغييرات كبيرة في مواد الدورة التدريبية مع مرور الوقت.**

**ملاحظة للمدربين:** في نهاية هذه الحصة، ينبغي أن يكون المشاركون قادرين على:

* تحديد الأشخاص القانونيين والطبيعيين المشاركين في السيناريو؛
* شرح تصميم الحالة ووضع الوقائع التمهيدية؛
* متابعة تدفق وتطور التحقيق في القضية وشرحه؛
* تحديد كيف وأين ينبغي أن يبدأ التحقيق الجنائي وما هي الموجهات الإجرائية التي ينبغي اتباعها.

1. التحقيق

1.2 استجلاء وإثبات الوقائع الأولية

**البنك الفيدرالي لأتلانتيس (FBA) بنك مشهور وناجح وجدير بالثقة في أوروبا، يتوفر على العديد من الفروع والشركات في العديد من البلدان المختلفة، ليس فقط في أوروبا، بل وفي جميع أنحاء العالم أيضا. ومن المعروف أن علاقاته البنكية والتجارية تحظى بسمعة طيبة وبالثقة. ويبدو أنه بفضل سياسات البنك، يميل الناس بشكل متزايد إلى فتح حسابات بنكية واستخدام منتجات مصرفية أخرى في هذا البنك أكثر من العديد من البنوك المنافسة الأخرى.**

**وقد أصدر مجلس إدارة البنك الفيدرالي لأتلانتيس قرارا بشأن إصدار سند خاص للاحتفاء بالذكرى المئوية على تأسيس البنك وعملياته الناجحة. ولهذا الغرض، فوض المجلس قسم اللوجستيك والعمليات (DLO) للقيام بالتحضيرات اللازمة لطباعة السندات، بما في ذلك إيجاد شريك مناسب لتزويد جميع العناصر الضرورية للطباعة.**

**حدد قسم اللوجستيك والعمليات شريكا معروفا في المجال يقدم منتوجات وخدمات الطباعة. ويوجد المقر الرئيسي للشريك المختار، البنك المتحد للطباعة (UBP)، في أتلانتيس، ولديه فرع أوروبي في نورلاندا ويدعى "البنك المتحد للطباعة". ثم اتصل قسم اللوجستيك والعمليات داخليا بإدارة الشؤون المالية لدى البنك الفيدرالي لأتلانتيس لإشراكها في المشروع.**

الوقائع الرئيسية هي كالآتي:

* **البنك الفيدرالي لأتلانتيس (FBA) بنك مشهور وناجح وجدير بالثقة؛**
* **البنك يرغب في إصدار سند خاص بالذكرى المئوية لتأسيسه؛**
* **قسم اللوجستيك والعمليات (**DLO**) مكلف بالترتيبات اللوجستية في هذا الشأن؛**
* **البنك المتحد للطباعة (UBP) شركة توفر معدات الطباعة؛**
* **إشراك قسم الشؤون المالية لدى البنك الفيدرالي لأتلانتيس من قبل قسم اللوجستيك والعمليات في الترتيبات اللوجستية.**

**ملاحظة للمدربين:** ينبغي أن يتعرف المتدربون على الوقائع الرئيسية وأهم الأقسام التجارية وصانعي القرار بغية التمكن من فهم نطاق وتصميم دائرة النشاط التجاري التي ستضاف إليها وقائع أخرى مرتبطة بالقضية.

معدات دراسة الحالة الواجب استخدامها:

**⮘ الملف "اليوم 2/2.2.2 تقديم تمرين التحقيق/المواد المعدة للقراءة المسبقة":**

* **ملخص عن دراسة الحالة؛**
* **تقديم إلى عرض دراسة الحالة ودليل المدربين للتحقيق في دراسة الحالة.**

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/الخصائص":**

* **خصائص شركة البنك الفيدرالي لأتلانتيس؛**
* **خصائص شركة البنك المتحد للطباعة؛**
* **خصائص شركة "دوكلاندس سكيوريتيز – بنك نورلاندا".**

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/الوثائق والتقارير":**

* **إعلان البنك الفيدرالي لأتلانتس عن إصدار سند الذكرى المئوية لتأسيس البنك؛**
* **سند البنك الفيدرالي لأتلانتس.**

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/رسائل البريد الإلكتروني":**

* **أول رسالة إلكترونية؛**
* **ثاني رسالة إلكترونية.**

بعض الأسئلة التي يمكن طرحها على المتدربين:

* **ما هي السلطات وما نوع الأدوات القانونية التي سيتم استخدامها على المستوى المحلي لإثبات أهم الحقائق المشار إليها أعلاه؟**
* **كيف ستؤثر هذه الحقائق على تطور التحقيقات اللاحقة؟**
  1. إنشاء شك معقول حول البداية الممكنة للجريمة

**"بسبب فترة الإجازة الصيفية، كان قسم اللوجستيك والعمليات يسجل خصاصا في عدد الموظفين. لذلك، استعان نائب رئيس القسم موظفين مبتدئين وآخرين تم تجنيدهم مؤخرا للعمل على هذا المشروع، وإجراء المكالمات والتواصل مع الزملاء من قسم المالية".**

**ملاحظة للمدربين:** ينبغيأن يثير تقديم مسألة إشراك موظفين مبتدئين وموظفين جدد في هذه العملية المهمة، بسبب فترة الإجازة الصيفية، الشكوك بين المتدربين على الفور. **ويتمثل العنصر الرئيسي في أن أحد الموظفين المبتدئين منخرط في الواقع في مجموعة للجريمة المنظمة وتقدم بطلب للحصول على منصب في أدنى مستوى بقسم اللوجستيك والعمليات حتى يتمكن من الحصول على أي نوع من النفاذ المباشر إلى أجهزة الكمبيوتر الخاصة بالبنك الفيدرالي لأتلانتيس (FBA) وذلك بهدف زرع برمجية محددة للتجسس على البريد الإلكتروني قادرة على إرسال نسخ من المراسلات بالبريد الإلكتروني بين البنك الفيدرالي لأتلانتيس (FBA) وقسم اللوجستيك والعمليات، وقسم الشؤون المالية والأنشطة التجارية الخارجية إلى كمبيوتر ومستخدم معين، وفي هذه الحال إلى الموظف المبتدئ / المشتبه به الرئيسي. وبفضل هذا النوع من النفاذ، والمراقبة الوثيقة والكشف عن إمكانية إنجاز احتيال عبر البريد الإلكتروني الخاص بالأعمال، تم تصويب الهدف.**

معدات دراسة الحالة الواجب استخدامها:

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/رسائل البريد الإلكتروني":**

* **أول رسالة إلكترونية؛**
* **ثاني رسالة إلكترونية؛**
* **خامس رسالة إلكترونية؛**
* **سابع رسالة إلكترونية.**

بعض الأسئلة التي يمكن طرحها على المتدربين:

* **كيف يمكن تحديد نوع البرمجية الخبيثة التي تم استخدامها؟**
* **كيف يمكن تحديد تداعيات تلك البرمجية الخبيثة وآثار اتصال البرمجية الخبيثة مع نقاط اتصال خارجية، وما هي الوقائع الهامة الأخرى التي ينبغي أن يتبعها التحقيق في هذه المرحلة؟**

1. الإعدادات المالية

**" تقدم البنك الفيدرالي لأتلانتيس (FBA) بطلب لشراء 20.000 قطعة من المعدات الورقية المتخصصة من شركة البنك المتحد للطباعة (UBP) بسعر يعادل 300.000 يورو. وبدأت الأقسام ذات الصلة لدى " FBA" و"UBP" بإجراء الترتيبات اللوجستية والمالية الضرورية.**

**تبادلت شركتا "FBA" و"UBP" التفاصيل بشأن الفواتير والدفع بما في ذلك رقم حساب سويفت ورقم الحساب البنكي الدولي (IBAN) والرموز. طالب شركة "UBP" بدفعة مسبقة بقيمة 100.000 يورو من خلال تحويل على حسابها لدى "دوكلاندس سكيوريتيز – بنك نورلاندا" (DSBL). وتم التحويل في غضون 24 ساعة بعد قبول الطلبية. "**

**بالإضافة إلى تقديم الوقائع المالية، هنالك مجموعة من الإضافات إلى الوقائع الرئيسية:**

* **إدراج "دوكلاندس سكيوريتيز – بنك نورلاندا" في دائرة المعاملة التجارية باعتباره البنك حيث يوجد حساب شركة "UBP" من أجل تحويل الأموال؛**
* **الدفع الموفق للتحويل الأولي بمبلغ 100.000 يورو بين "FBA" و"UBP" على الحساب لدى بنك (DSBL)؛**
* **تقديم الوقائع التي تفيد أن رقم حساب السويفت ورقم الحساب البنكي الدولي (IBAN) مدرجان في المعاملة.**

**ملاحظة للمدربين:** ينبغيأن تشير هذه الإعدادات إلى أن التحويل البنكي الأولي للأموال تم دون أي مشاكل وأن الإشارة إلى رموز وحسابات السويفت ورقم الحساب البنكي الدولي تعني أن تحويل الأموال ذا طابع دولي وليس محلي. **وهكذا، ينبغي أن يبدأ المتدربون بالتفكير في استخدام مواد اتفاقية بودابست ذات الصلة بالمساعدة القانونية الدولية.**

معدات دراسة الحالة الواجب استخدامها:

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/الوثائق والتقارير":**

* **العقد المبرم بين شركتي "FBA" و"UBP"؛**

⮘ **الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/تصاريح البنوك":**

* **الفاتورة الأولية لشركة "UBP"؛**
* **تصريح بنك "FBA"؛**
* **تصريح بنك شركة "UBP".**

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/رسائل البريد الإلكتروني":**

* **ثالث رسالة إلكترونية؛**
* **رابع رسالة إلكترونية؛**
* **سادس رسالة إلكترونية؛**
* **سابع رسالة إلكترونية؛**
* **ثامن رسالة إلكترونية.**

بعض الأسئلة التي يمكن طرحها على المتدربين:

* **ما هي أهم المواد الموضوعية في العقد؟**
* **كيف ومتى تم تحويل الدفعة المسبقة؟**
* **هل تم التحويل دون أي مشاكل ولماذا؟**
* **هل كان هنالك أي احتمال لمراقبة التحويل من قبل طرف متطفل؟**
* **إذا كان الوضع كذلك، فكيف؟**

1. الشروع في الارتكاب الفعلي للجريمة وأهم نقطة في التحقيق

**" اشترط العقد طباعة 20.000 قطعة من المعدات الورقية في غضون سبعة أيام. واستوفت شركة البنك المتحد للطباعة (UBP) هذا الشرط قبل انتهاء الأجل بيوم واحد. وأخبرت شعبة الأعمال التجارية قسم الشؤون المالية لدى شركة "UBP" أن السلع جاهزة للشحن فور استلام الدفعة الأخيرة.**

قام قسم الشؤون المالية لدى شركة **"UBP" بمراسلة نظريه لدى شركة "FBA" عبر البريد الإلكتروني لإخباره أن الطلبية جاهزة للتسليم وأنه يجب تحويل الدفعة الأخيرة، أي مبلغ 200.000 يورو في غضون 48 ساعة. وفي مساء نفس اليوم، تلقت شركة "FBA" بريدا إلكترونيا من شركة "UBP" يخبرها أن الحساب البنكي للشركة في نورلاندا لن يكون متاحا طيلة الأيام الثلاثة الموالية بسبب إجازة العيد الوطني في البلد. وجاء في البريد الإلكتروني طلب بتحويل الرصيد المتبقي على حساب "UBP" لدى** لدى "دوكلاندس سكيوريتيز – بنك نورلاندا" (DSBN) / فرع أوستلاندا."

**ملاحظة للمدربين:** ينبغيالتعرف على هذه اللحظة باعتبارها نقطة الانطلاق لتنفيذ المخطط برمته. **لقد تمت الإشارة سابقا إلى أن عضوا في الجماعة الإجرامية المنظمة تمكن بفضل برمجية للتجسس من كشف وتتبع المراسلات التجارية بين شركتي "FBA" و"UBP". ولم يتبق سوى تحديد موعد الدفعة النهائية والرد على وجه السرعة. وهذا الموعد كان من المرتقب أن يحين فور إخبار شركة "UBP" شركة "FBA" باستكمال طباعة المواد الورقية المطلوبة.**

**وبمجرد أن أشعر قسم الشؤون المالية لدى شركة "UBP" نظيره لدى شركة "FBA" أن الدفع أصبح مستحقا، تمكن "الواشي/المخبر" من اعتراض البريد الإلكتروني وإخباري باقي أعضاء الجماعة الإجرامية. وبالتالي، أصبحوا مستعدين لإرسال فواتير مزيفة مجهزة من ذي قبل تحمل ترويسة بريد إلكترونية شبه مماثلة لترويسة قسم الشؤون المالية لدى شركة "UBP" باستخدام خدمات خادوم بروتوكول إرسال البريد البسيط المفتوح التي تم استئجارها قبل الشروع في ارتكاب الجريمة.**

**ينبغي استخدام** متغيرات في السيناريو**، بما في ذلك الإشارة إلى تغيير البريد الإلكتروني بإدخال بعض التغييرات الصغيرة في الاسم الفعلي لحساب البريد الإلكتروني الخاص بموظف القسم المالي لدى شركة "UBP" بدلاً من استخدام خادوم SMTP المجاني، في الحالات التي يلاحظ فيها المدربون أن مستوى المعرفة الفنية لدى المتدربين متدني مما قد يطرح بعض المشاكل تقوض نجاح تمرين التحقيق.**

**تم فتح حساب بنكي خاضع لمراقبة إجرامية بقصد إجرامي في البلد الآخر (أوستلاندا في هذا التمرين)، نيابة عن شركة "زائفة" تحمل اسمًا مشابهًا للحساب الأصلي ("UBP" في هذه القضية)، والذي سبق تسجيله لدى فرع البنك الرئيسي، بمعنى أنه تم فتح حساب بنكي احتيالي لدى فرع بنك "دوكلاندس سيكيوريتيز - بنك نورلاندا" في أوستلاندا. ولم يتم استخدام الحساب البنكي من قبل مع شركة "FBA" وتم فتحه باستخدام بيانات يعرفها المجرمون الرئيسيون ومساعدوهم. وقد تم تزوير البيانات المستخدمة أثناء عملية التسجيل وكانت شبه مطابقة للبيانات الأصلية بتفاصيل عن موظفي القسم المالي لدى شركة "FBA".**

**تمت إضافة عنصر الاستعجال إلى المخطط بأكمله بسبب عطلة العيد الوطني القادم في نورلاندا. وتم استخدام ذلك من قبل المجرمين كمبرر إضافي لتغيير رقم الحساب البنكي. وهكذا، أصبح الفخ، انطلاقا من هذه النقطة، جاهزا لوقوع الضحية في الشباك.**

أهم الوقائع:

* **تمت طباعة المعدات الورقية وأشعرت شركة "UBP" شركة "FBA" بذلك مطالِبة بأداء المبالغ المستحقة؛**
* **كشف عضو الجماعة الإجرامية المنظمة المتسلل باستخدام برمجية التجسس المواعيد النهائية لاستكمال الصفقة التجارية؛**
* **قامت الجماعة الإجرامية بتسجيل شركة "وهمية" في أوستلاندا وبفتح حساب بنكي للشركة في ذلك البلد لدى فرع للبنك الذي تتعامل معه شركة "UBP" لعملياتها المعتادة في نورلاندا؛**
* **تم إعداد وثائق مزورة، بما في ذلك أهم العناصر – فاتورة مزيفة، خادوم البريد الإلكتروني، رسائل البريد الإلكتروني؛**
* **تم استئجار خادوم بروتوكول إرسال البريد البسيط المفتوح واختباره لإرسال بريد إلكتروني مزيف (أو يمكن استخدام نموذج عن حساب بريد على الإنترنت مع إدخال بعض التغييرات الطفيفة على الاسم وحساب البريد الإلكتروني، بحسب مهارات المدرب)؛**
* **تم دفع رسوم خدمات خادوم بروتوكول إرسال البريد البسيط المفتوح بعملة البيتكوين (في حال استخدام نموذج البريد على الإنترنت، دون مقابل)؛**
* **تم إعداد بريد إلكتروني مزيف، بما في ذلك أسماء موظفين فعليين في قسم الشؤون المالية، وتفاصيل عن العقد واللغة المستخدمة من ذي قبل.**

معدات دراسة الحالة الواجب استخدامها:

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/تصريحات البنوك":**

* **الفاتورة المزيفة لشركة "UBP"؛**

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/الوثائق والتقارير":**

* **تسجيل الشركة الوهمية "UBP" في أوستلاندا؛**
* **تسجيل الحساب البنكي للشركة الوهمية "UBP" في أوستلاندا لدى "دوكلاندس سكيوريتيز – بنك نورلاندا" (DSBL) فرع أوستلاندا؛**
* **تقرير نتائج افتحاص البرمجية المضادة لبرمجيات التجسس؛**
* **تقرير تقفي شبكة خادوم بروتوكول إرسال البريد البسيط؛**
* **تقرير الدفع بعملة البيتكوين إلى شركة خادوم بروتوكول إرسال البريد البسيط.**

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/إفادات الشهود":**

* **تصريح قسم تكنولوجيا المعلومات لدى شركة "FBA".**

بعض الأسئلة التي يمكن طرحها على المتدربين:

* **كيف تم الحصول على المعلومات بشأن اكتمال الصفقة التجارية وكيف يمكن استرجاعها، إن كان ذلك ممكنا؟**
* **كيف يمكن الحصول على معلومات عن الشركة "الوهمية" وتفاصيل الحساب البنكي من أوستلاندا؟**
* **ما هو نوع المعلومات التي ينبغي المطالبة بها من أوستلاندا وبأي طريقة؟**
* **هل هنالك معلومات مطلوبة بشكل عاجل ويمكن تبرير طابعها المستعجل من أجل تفعيل نقاط الاتصال المتاحة 24/7 في شبكة مجلس أوروبا؟**
* **كيف يمكن الحصول على الأدلة بشأن الوثائق المزيفة/المزورة وكيف ينبغي تحليلها؟**
* **كيف يمكن الحصول على معلومات بشأن خادوم بروتوكول إرسال البريد البسيط المفتوح (أو معلومات من شركة البريد الإلكتروني المستند إلى الإنترنت) وما الذي يمكن أن تكشفه تلك المعلومات؟**
* **ما هي عملة "بيتكوين"؟ وكيف تم استخدامها وكيف يمكن استخدامها كدليل إلكتروني؟**
* **ما هو ملخص الأدلة الإلكترونية الذي يمكن الحصول عليه؟**

1. نهاية ارتكاب الجريمة وبداية القضية

**"** في يوم العمل الموالي، كان قسم الشؤون المالية لدى شركة "FBA" مستعدا لتحويل المبلغ المتبقي. وأذنت مديرة قسم الشؤون المالية بتحويل المبلغ المتبقي، أي 200.000 يورو، والذي تم تحويله على الحساب البنكي لشركة "UBP" في أوستلاندا.

وفي صباح يوم انتهاء الأجل المحدد في 48 ساعة، اتصل قسم الشؤون المالية لدى شركة "UBP" بنظيره لدى شركة "FBA" مطالبا بالدفع الفوري للرصيد المستحق. فأجابت لدى شركة "FBA" شركة "UBP" أن المبلغ قد تم تحويله بالفعل وأنها تنتظر تسليم البضائع. وكملاحظة جانبية، قدمت شركة "FBA" التهاني إلى شركة "UBP" بمناسبة العيد الوطني.

قام قسم الشؤون المالية لدى شركة "UBP" بالتأكد من الحساب البنكي للشركة ورد على شركة "FBA" أنه لم يتم استلام أي مبلغ منها، متسائلا أيضاً لماذا تهنئهم الشركة بالعيد الوطني، في حين أن المناسبة الوطنية المقبلة لن تحل قبل شهرين."

**ملاحظة للمدربين:** يسدل ستار المشهد الأخير من المخطط في اليوم الموالي عندما قامت مديرة الشؤون المالية لدى شركة "FBA" بترخيص التحويل البنكي على أساس الوثائق المقدمة مسبقا: البريد الإلكتروني المزيف لشركة "UBP" والذي تضمن معلومات عن حساب بنكي مزيف في بلد لا تعرفه لا شركة "FBA" ولا شركة "UBP".

**في هذه اللحظة بالذات، اكتملت عملية الاحتيال. فقد تم تحويل مبلغ 200.000 يورو على الحساب المزيف. ويمكن للمدربين، وفقا لتطور سيناريو الحالة، الخوض بشكل أعمق في المعاملات بين الحساب البنكي في أوستلاندا والحسابات البنكية الأخرى التابعة للدول الأطراف في اتفاقية بودابست أم لا، في إطار تمرين لتقفي آثار الأموال والمعاملات على الإنترنت من خلال تحقيقات مالية فعلية واختبار المعرفة لدى المتدربين بإجراء المساعدة القانونية المتبادلة.**

**وبحسب اختيار المدربين، يمكن إنهاء التحويلات البنكية في البلد الذي تطاله اتفاقية بودابست أم لا. وفي الحالة الثانية، من المحتمل أن تضيع الآثار والأدلة النهائية أو ألا يمكن استرجاعها للأبد. ومع ذلك، يمكن أن يستفيد المتدربون من النموذجين.**

أهم الوقائع:

* **قامت مديرة الشؤون المالية لدى شركة "FBA" بترخيص التحويل على أساس الوثائق المقدمة مسبقا؛**
* **تتمثل الوثائق في البريد الإلكتروني المزيف لشركة "UBP" الذي تضمن فاتورة مزيفة ومعلومات عن حساب بنكي مزيف؛**
* **تم تحويل مبلغ 200.000 يورو. وبحسب احتياجات الدورة التدريبية المحلية، يمكن مواصلة النقاش حول التحويلات البنكية إلى دول أخرى أو التوقف عند هذا المثال. ويمكن أيضا إنهاء مناقشة التحويل بالإشارة إلى البلد الطرف في اتفاقية بودابست أو غيره.**

معدات دراسة الحالة الواجب استخدامها:

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/رسائل البريد الإلكتروني":**

* **تاسع رسالة إلكترونية؛**
* **عاشر رسالة إلكترونية؛**
* **الرسالة الإلكترونية الحادية عشر.**

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/إفادات الشهود":**

* **تصريح قسم اللوجستيك والعمليات لدى شركة "FBA"؛**
* **تصريح قسم الشؤون المالية لدى شركة "FBA"؛**
* **تصريح قسم تكنولوجيا المعلومات لدى شركة "FBA"؛**
* تصريح قسم الحسابات لدى فرع بنك "دوكلاندس سيكيوريتيز - بنك نورلاندا" في أوستلاندا (DSBN)

**⮘ الملف "اليوم 2/3.2.2 تمرين التحقيق/الأدلة/تصريحات البنوك":**

* تصريح بنك "دوكلاندس سيكيوريتيز - بنك نورلاندا" فرع أوستلاندا (DSBN)

بعض الأسئلة التي يمكن طرحها على المتدربين:

* **لماذا أذنت مديرة الشؤون المالية بالتحويل؟**
* **إلى أي حساب تم تحويل المبلغ المالي؟**
* **بما أن أوستلاندا صادقت على اتفاقية بودابست، ما هي الخطوات التي ستتخذها سلطات إنفاذ القانون؟**
* **ما هي الوثائق التي ينبغي الحصول عليها من شركة "FBA" وفي أي صيغة؟**
* **ما هي الوثائق التي ينبغي الحصول عليها من شركة "UBP" وفي أي صيغة؟**
* **ما هو البنك الذي ينبغي الاتصال به وبأي طريقة وما نوع الطلب الذي ينبغي تقديمه خلال التحقيق؟**
* **كيف يمكن استرجاع المال، إن كان ذلك ممكنا؟**
* **ما نوع الطلبات و/أو الأوامر التي يمكن إصدارها وتوجيهها إلى كافة الهيئات التجارية والبنوك؟**
* **ما هي الأسس التي يمكن الاستناد إليها لهذا النوع من العمليات؟**
* **ما هي المواد في اتفاقية بودابست التي سيتم استخدامها؟**

6. أهم خطوات التحقيق والأدلة الإلكترونية الأساسية

**سيفترض المتدربون أن أول لحظة للاتصال بين البنك الفيدرالي لأتلانتيس وسلطات إنفاذ القانون تتمثل في يوم التحويل عندما وصل البريد الإلكتروني من شركة البنك المتحد للطباعة الذي تضمن سؤالا بشأن عدم التوصل بالتحويل المالي واستفسارا عن إجازة العيد الوطني. انطلاقا من تلك اللحظة، وبحسب الإطار القانوني المحلي، يبدأ التحقيق. النموذج متعدد الجوانب ويمكن أن يشمل الشرطة، والنيابة العامة، وقضاة التحقيق وغيرهم من الهيئات، عند الضرورة. ويمكن لجميع المؤسسات أن تضطلع بدور لأن عملياتها تسعى إلى تحقيق هدف مشترك وإن اختلفت المقاربات.**

**ومع ذلك،** ينبغي أن تتألف أهم خطوات التحقيق مما يلي:

* **تسجيل إفادات المشتبه بهم المحتملين؛**
* **تسجيل إفادات ممثلي البنك الفيدرالي لأتلانتس؛**
* **الحصول على الأدلة الإلكترونية وغيرها من الأدلة من البنك الفيدرالي لأتلانتس؛**
* **تلقي إفادات ممثلي البنك المتحد للطباعة؛**
* **الحصول على الأدلة الإلكترونية وغيرها من الأدلة من البنك المتحد للطباعة؛**
* **تسجيل إفادات ممثلي "دوكلاندس سكيوريتيز" بنك نورلاندا في نورلاندا وأوستلاندا؛**
* **الحصول على الأدلة الإلكترونية وغيرها من الأدلة من كلا البنكين؛**
* **الحصول على الأدلة من السلطة المختصة بتسجيل الشركات في أوستلاندا؛**
* **التعاون بين الشرطة والنيابة العامة وقضاة التحقيق، عند الاقتضاء؛**
* **تضمين المساعدة القانونية الدولية في أحكام اتفاقية بودابست؛**
* **إدماج المساعدة القانونية الدولية في أحكام اتفاقية بودابست؛**
* **غيرها من عمليات التحقيق الهامة والمعترف بها والمحددة من قبل المتدربين بدعم من المدربين.**

أهم الأدلة الإلكترونية:

* **سجلات كمبيوترات البنك الفيدرالي لأتلانتيس؛**
* **برمجية التجسس المستخدمة في البنك الفيدرالي لأتلانتيس؛**
* **خادوم بروتوكول إرسال البريد البسيط وسجل إرسال البريد الإلكتروني الزائف؛**
* **العملة المشفرة (بيتكوين)، سلسلة الكتلة، سجل سلسلة الكتلة؛**
* **البريد الإلكتروني المنتظم؛**
* **البريد الإلكتروني الزائف مع الترويسة الكاملة؛**
* **الفاتورة الزائفة؛**
* **سجلات كمبيوترات البنك المتحد للطباعة؛**
* **السجلات البنكية وسجلات الحسابات التابعة لـ"دوكلاندس سكيوريتيز بنك نورلاندا"؛**
* **سجلات تسجيل الشركات؛**
* **سجلات المراقبة؛**
* **أدلة إلكترونية أخرى.**

**لا تعتبر أي من القائمتين شاملة ومستوفية ويمكن تعديلهما أو تحديثهما بإضافة خطوات أخرى في التحقيق وأدلة إلكترونية حسب الحاجة.**

المواد الإضافية لدراسة الحالات الواجب استخدامها:

* **ملف "اليوم 2/3.2.2 تمرين التحقيق / مسرد المصطلحات":**
* **التهديد المستمر والمتقدم؛**
* **العملات المشفرة؛**
* **الهندسة الاجتماعية الإلكترونية؛**
* **برمجيات التجسس؛**
* **الخادوم بروتوكول إرسال البريد البسيط المفتوح ومحاكاة عنوان البريد الإلكتروني (E-mail spoofing).**

7. الملاحق