مكافحة الجريمة الإلكترونية المالية في لبنان

الدليل الإرشادي للوقاية من الأفعال الجرمية بواسطة البريد الإلكتروني

جمعية المصارف في لبنان

مصرف لبنان
BANQUE DU LIBAN

بالتعاون مع
الإقتصاد والأعمال
Al-Iktissad Wal-Aamal

المقدمة

إن الجريمة الإلكترونية المالية، هي فعل أو محاولة فعل أو أفعال، محلية أو عابرة للحدود، صادرة بإرادة جرمية عن أفراد أو مجموعات منظمة بهدف إنتهاك الحسابات المصرفية أو المعلومات المالية والشخصية عبر إستخدام وسائل الكترونية وتقنية عدة. يدخل ضمن نطاق هذه الجريمة مثلاً عمليات الإحتيال والسرقة والإختلاس والإبتزاز والتخريب والتجسّس بالوسائل الإلكترونية.

وتتميز كل جريمة بخصائص وعناصر محددة مما يوجب على المعنيين التنبه للمؤشرات التي تدل عليها وتطبيق إجراءات العناية الواجبة بغية التعرف إليها وتجنب حدوثها واتخاذ التدابير اللازمة لمكافحتها.

ونعرض فيما يلي، وبشكل مختصر وعلى سبيل المثال لا الحصر، نماذج عن الأفعال الجرمية بواسطة البريد الالكتروني التي قد تتعرض لها المصارف أو المؤسسات المالية أو مؤسسات الوساطة المالية "القطاع المالي" (النوع الأول) أو الأشخاص وسائر المؤسسات والهيئات غير المالية (النوع الثاني).

نماذج أفعال جرمية واقعة على "القطاع المالي"

لغاية هذا العرض يُعنى بعبارة Bank Email Compromise اختراق البريد الإلكتروني العائد لإحدى مؤسسات "القطاع المالي". يتضمن هذا النوع الحالات الموصوفة التالية (Typology):

- انتهاك البريد الإلكتروني للمصرف(Bank Email Compromise - BEC1):
يقوم شخص مجهول الهوية (المُقرصن) بالولوج غير المصرح به الى البريد الالكتروني العائد لعميل "القطاع المالي" او يقوم بانشاء بريد الكتروني مشابه له (يحمل نفس الاسم أو إسماً مشابهاً) وبإستخدام أي منهما في مراسلة المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية المفتوح لديها حساب العميل لطلب اجراء عملية مصرفية أو مالية عبر هذا الحساب كعملية تحويل الى حساب آخر في الخارج او في لبنان (يفترض المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية انها للعميل او لجهة يتعامل معها العميل).

من جهته يقوم المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية بإجراءات العناية الواجبة الاعتيادية وينفّذ التحويل المطلوب ويتبين لاحقاً ان المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية و/او العميل وقعوا (أو وقع أي منهم) ضحية أفعال جرمية بالوسائل الإلكترونية.

- انتهاك البريد الإلكتروني للمصرف(Bank Email Compromise - BEC2):
يقوم شخص مجهول الهوية (المُقرصن) بالولوج غير المصرح به إلى البريد الالكتروني لمدير تنفيذي في المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية أو يقوم بإنشاء بريد الكتروني مشابه له وبإستخدام أي منهما في مراسلة مدراء فروع أو إدارات مالية لتنفيذ عمليات مصرفية أو مالية مشبوهة. من جهته يقوم المدير المعني بتنفيذ العملية المصرفية او المالية ويتبيّن لاحقاً انه وقع ضحية أفعال جرمية بالوسائل الالكترونية.

- انتهاك البريد الإلكتروني للمصرف(Bank Email Compromise – BEC3):
يقوم شخص مجهول الهوية (المُقرصن) بالولوج غير المصرح به إلى البريد الالكتروني لمدير تنفيذي في المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية أو يقوم بإنشاء بريد الكتروني مشابه له وبإستخدام أي منهما في مراسلة أحد عملاء المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية مدعياً أنه بصدد تحديث ملف العميل ويطلب منه معلومات محدّدة بهذا الخصوص، سيما عن حسابه أو حساباته.

نماذج أفعال جرمية واقعة على الاشخاص وسائر المؤسسات والهيئات غير المالية

لغاية هذا العرض يُعنى بعبارة Company Email Compromise اختراق البريد الإلكتروني العائد لأحد الأشخاص أو المؤسسات والهيئات غير المالية. يتضمن هذا النوع الحالات الموصوفة التالية (Typology):

- انتهاك البريد الإلكتروني للشركة (Company Email Compromise - CEC1):
يقوم شخص مجهول الهوية (المقرصن) بالولوج غير المصرح به الى البريد الالكتروني "للمورّد" (أي الشركة "المورّدة" أو التاجر أو أي من مقدمي الخدمات الذين يتعامل معهم عميل "القطاع المالي") او يقوم بإنشاء بريد الكتروني مشابه له وباستخدام أي منهما في مراسلة العميل لطلب اجراء تحويل الى حساب في الخارج او في لبنان يفترض أنه مقابل بضاعة او خدمةمقدمة من "المورّد" أو من شركة مرتبطة به أو تعمل لحسابه.
من جهته يقوم العميل اما بمراسلة المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية التي يتعامل مع أي منها لطلب اجراء التحويل من حسابه الى الحساب المحدد في المراسلة المنسوبة "للمورّد" أو بالتوجه شخصياً الى المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية لطلب تعبئة الاستمارة الخاصة بالتحاويل ويتبيّن لاحقاً ان العميل وقع ضحية أفعال جرمية بالوسائل الإلكترونية.

- انتهاك البريد الإلكتروني للشركة (Company Email Compromise - CEC2):
يقوم شخص مجهول الهوية (المُقرصن) بالولوج غير المصرح به الى البريد الالكتروني للعميل او يقوم بإنشاء بريد الكتروني مشابه له وباستخدام أي منهما في مراسلة أحد "الموردين" الذي يتعامل مع العميل لطلب اجراء تحويل من حسابه الى حساب في الخارج او في لبنان يُفترض انه عائد للعميل او لشركته.
من جهته يقوم "المورّد" اما بمراسلة المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية الذي يتعامل مع أي منها لطلب اجراء التحويل من أحد الحسابات العائدة له الى الحساب المحدد في المراسلة المنسوبة للعميل، واما بقيام احد مندوبيه بالتوجه شخصياً الى المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية لطلب تعبئة الاستمارة الخاصة بالتحاويل ويتبيّن لاحقاً ان "المورّد" وقع ضحية أفعال جرمية بالوسائل الإلكترونية.

نماذج أفعال جرمية واقعة على الاشخاص والمؤسسات غير المالية

- انتهاك البريد الإلكتروني للشركة (Company Email Compromise - CEC3):
يقوم شخص مجهول الهوية (المُقرصن) بالولوج غير المصرح به إلى البريد الالكتروني لمدير تنفيذي في احدى الشركات، أو يقوم بإنشاء بريد الكتروني مشابه له (بالأخص عند غياب هذا المدير بداعي السفر) وبإستخدام أي منهما في مراسلة مدراء فروع أو مسؤولين ماليين لطلب تنفيذ عمليات مالية أو مصرفية مشبوهة.
من جهته يقوم المدير المعني بتنفيذ العملية المصرفية او المالية ويتبيّن لاحقاً انه وقع ضحية أفعال جرمية بالوسائل الالكترونية.

- انتهاك البريد الالكتروني عن طريق الهندسة الاجتماعية (Social Engineering – SE):
على سبيل المثال، يقوم شخص مجهول الهوية (المُقرصن) بالولوج غير المصرح به الى البريد الالكتروني العائد لشخص طبيعي او بإنشاء بريد الكتروني مشابه له وبإستخدام أي منهما في مراسلة معارف الشخص الطبيعي او اصدقائه او اقربائه او آخرين مع تحديد حساب لكل من يرغب بدعم حاجات الشخص بسبب ضيق مالي. يقوم المعنيون بإجراء التحاويل من حساباتهم الى الحساب المحدد ليتبيّن لاحقاً انهم وقعوا ضحية أفعال جرمية بالوسائل الإلكترونية.

إن هذا الدليل الارشادي يتناول بشكل خاص الجرائم الالكترونية المالية المُرتكبة بواسطة البريد الالكتروني والتي تطال عمليات التحاويل المصرفية. ولهذه الغاية يقسم الدليل إلى جزئين:

1. الجزء الاول: إرشادات "للقطاع المالي" (المصارف والمؤسسات المالية ومؤسسات الوساطة المالية)
2. الجزء الثاني: إرشادات للأشخاص وسائر المؤسسات والهيئات غير المالية

ويتناول في جزئيه العناوين التالية:

1. المؤشرات على الأفعال الجرمية بواسطة البريد الإلكتروني
2. السياسات والإجراءات الوقائية من الأفعال الجرمية
3. الاجراءات التصحيحية

الجزء الاول:
إرشادات للقطاع المالي (المصارف والمؤسسات المالية ومؤسسات الوساطة المالية)

1. المؤشرات على الأفعال الجرمية بواسطة البريد الإلكتروني

إن الأفعال الجرمية بواسطة البريد الإلكتروني قد تتخذ أشكالاً عدة، ويتوجب التنبه إلى المؤشرات التالية، على سبيل المثال لا الحصر، التي قد تساعد في اكتشاف هذه الأفعال:

1. بريد الكتروني منسوب للعميل يدّعي فيه المُرسل انه على عجلة من امره او لديه حالة طارئة وهو بحاجة لمبلغ من المال وانه لا يمكن الاتصال به عبر الهاتف او الفاكس او بأية وسيلة اخرى.
2. بريد الكتروني منسوب للعميل يطلب فيه المُرسل عدم الاتصال به هاتفياً لتأكيد طلب التحويل ويعطي أسباباً واهيةً لهذا الأمر.
3. بريد الكتروني منسوب للعميل يدّعي فيه المُرسل انه تم تغيير رقم حساب «المورّد» لأسباب وحجج مختلفة، منها، على سبيل الذكر، إجراءات تدقيق تقوم بها السلطات الرقابية او الضريبية على حسابات "المورّد"، أو تدهور العلاقة السابقة مع المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية بسبب العمولات المرتفعة.
4. بريد الكتروني منسوب للعميل يطلب فيه المُرسل تغيير او تعديل اسم المستفيد أو المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة او رقم حساب المستفيد او عنوانه بحسب شروحات مختلفة واردة في البريد الالكتروني.
5. بريد الكتروني منسوب للعميل او لغيره يطلب فيه المُرسل معلومات عن حساب العميل و\او رصيده و\او معلومات حساسة تتعلق بالعميل.
6. ريد الكتروني منسوب للمصرف أو للمؤسسة المالية أو لمؤسسة الوساطة المالية أو للعميل أو لغيره يطلب فيه المرسل معلومات حساسة (كلمة السر، رقم حساب...)
7. بريد الكتروني يتضمن رابط (Link) إلى موقع الكتروني يُطلب فيه معلومات مالية أو شخصية عن العميل.
8. بريد الكتروني منسوب للعميل ينطوي على أخطاء لغوية متعدّدة غير عادية أو فاضحة.
9. بريد الكتروني منسوب للعميل ينطوي على صياغة ولغة تختلفان عن مُراسلات العميل المعتادة.
10. بريد الكتروني منسوب للعميل يكون فيه عنوان البريد الإلكتروني غير صحيح (يختلف بحرف أو برقم أو برمز أو بإشارة...)

11. بريد الكتروني منسوب للعميل مرفق به مستندات تدعو إلى الشك بصحة مضمونها، مثلاً: فواتير جرى التلاعب بأرقامها أو تواريخها، طلب تحويل يتبيّن فيه أن الاحرف والارقام الواردة غير متناسقة من حيث الشكل أو الحجم أو اللّون، مستندات تحمل توقيعاً مزوراً عن توقيع العميل.
12. بريد الكتروني منسوب للعميل يتضمن تعليمات غير مشابهة لتعليمات سابقة من العميل.
13. بريد الكتروني منسوب للعميل موجّه الى المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية بشكل عام وليس الى الموظف الذي يتلقى عادة التعليمات من العميل لتنفيذها.
14. بريد الكتروني يختلف عن البريد الالكتروني المصرّح عنه في العقد الموقع مع العميل.
15. بريد الكتروني منسوب لعميل لم يسبق له ان استخدم بريده الالكتروني في مراسلاته.
16. عدم قيام العميل سابقاً بتحاويل ذات طابع تجاري.
17. عدم وضوح الغاية من التحويل المطلوب تنفيذه.
18. عدم وجود رصيد كاف في حساب العميل لإجراء التحويل المطلوب.
19. عدم ملاءمة التحويل المالي لطبيعة نشاط العميل (موضوع التحويل، وجهته، قيمته والعملة).
20. المستفيد بحسب المستندات المرفقة بالبريد الالكتروني المشبوه يقيم او يعمل في دولة تختلف عن تلك التي يعمل فيها المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة.
21. عدم اشتراك المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة في نظام السويفت.
22. امتناع المصرف المُراسل عن تنفيذ التحويل والتبليغ عن احتمال وقوع أفعال احتيالية.
23. امتناع المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة عن قيد التحويل في حساب العميل (رقم الحساب غير صحيح او لا يعود لصاحب الحساب...)
24. بريد الكتروني منسوب للعميل أو لغيره يدّعي وجود حساب مفتوح في الخارج بإسم مُشابه لإسم العميل او بإسم مُطابق لإسمه، سيما عندما يتبيّن للمصرف أو للمؤسسة المالية أو لمؤسسة الوساطة المالية من واقع المعلومات المصرّح عنها ان العميل لا يقيم في الخارج او ليس لديه حساباً في الخارج.
25. بريد الكتروني منسوب للعميل موجّه الى المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية والى طرف ثالث لا علاقة له بالتحويل المطلوب تنفيذه.
26. التنبّه لأية محاولة فتح حساب من نوع (Mule Account) سيّما اذا صرّح الشخص المعني انه ينوي فتح حساب لتلقي تحاويل بناءً لطلب جهة خارجية او طرف ثالث.
27. بريد الكتروني منسوب للعميل يطلب فيه إجراء تحويل بعملات مختلفة عن عملياته السابقة او بعملات غير معتمدة في البلد المرسل إليه أو عمليات خارجة عن إطار الأعراف التجارية السائدة.
28. بريد الكتروني وارد من العميل ولكنه مبني على معلومات وشروحات واهية ومضلّلة تلقاها هذا الأخير على بريده الإلكتروني، بحيث يطلب فيه تغيير او تعديل اسم المستفيد أو المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة او رقم حساب المستفيد.

2. السياسات والاجراءات الوقائية من الأفعال الجرمية

يقتضي اتباع الخطوات الوقائية التالية:

1 - مراقبة العمليات المنوي تنفيذها عملاً بالموجبات المفروضة قانوناً ونظاماً وبحسب مندرجات العقد الموقع مع العميل بهذا الخصوص ومقارنتها مع طبيعة نشاط العميل المصرّح عنه في بيان "إعرف عميلك" (KYC).

2 - مراقبة موضوع التحويل ووجهته لجهة الدول المُرسل اليها والوسطاء الماليين أو المصرفيين المعتمدين ومراجعة اسماء المستفيدين النهائيين وارقام حساباتهم مقارنة مع تعاملات العميل السابقة.

3 - التنبّه لأي طلب تحويل مشبوه عبر البريد الإلكتروني خاصة اذا تبين انه لا يتلاءم مع النشاط الاعتيادي للعميل أو مع العمليات التي تجري عادةً على حساب العميل لجهة قيمتها وموضوعها ووجهتها.

4 - الاتصال بالعميل بواسطة وسيلة موثوقة اخرى متفّق عليها غير البريد الالكتروني للتأكد من صحّة التعليمات الواردة بواسطة البريد الإلكتروني، وعدم تلف المعلومات والمُراسلات والأدلّة كافة المُثبتة للاتصال أو محاولة الاتصال بالعميل وحفظها في مكان آمن بحوزة الموظفين المعنيين حصراً.

5 - اعتماد سياسة تفرض على المسؤولين في المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية قبل تنفيذ أي تحويل تفوق قيمته مبلغاً معيناً (يحدده المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية)، التأكد بوسائل معزّزة من صحة التعليمات الواردة بواسطة البريد الإلكتروني.

6 - كما يقتضي على المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية وضع عقد أو أحكام خاصة في عقد فتح الحساب ووضع أنظمة وإجراءات داخلية مخصّصة لتنفيذ طلبات تحويل الاموال بواسطة البريد الالكتروني.

تشمل هذه الاحكام الخاصة، على الاقل، ما يلي:

أ - موجبات العميل لجهة:

1 - تحديد بشكلٍ واضحٍ وبارزٍ في العقد:

- وسائل الاتصال (عناوين البريد الكتروني وأرقام الهاتف) الخاصة بالعميل التي سيعتمدها المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية لتأكيد صحّة الطلبات المُرسلة بالبريد الالكتروني وتعهّد العميل بعدم اجراء اي تعديل على هذه المعلومات الا بعد اخذ موافقة المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية الخطيّة وفق الآلية التي يجري الاتفاق عليها.
- أخذ العلم انه وفي حال تعذر على المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية الاتصال بالعميل لتأكيد طلب التحويل، فإن المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية لن ينفذ التحويل ولا تقع عليه أي مسؤولية تجاه أي كان من جراء ذلك.

2 - وجوب قيام العميل بإبلاغ المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية فور علمه او

اكتشافه او تبلغه ارتكاب او محاولة ارتكاب أية أفعال جرمية بالوسائل الالكترونية وذلك تجنباً لإمكانية المسّ بحقوقه المادية والقانونية في لبنان والخارج.

3 - التنبُّه والتأكد من صحّة أي تعديل يطرأ على إسم أو رقم الحساب أو اسم المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية المطلوب تحويل الأموال إليها.

4 - التنبّه لاستعمال كلمة سرّ متينة لبريده الإلكتروني (Strong Password) وتغييرها دورياً.

ب - موجبات المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية لجهة:

1 - اعلام العميل عن المخاطر الناتجة عن استخدام بريده الالكتروني لإجراء التحاويل المالية وتوجيهه لاستعمال وسائل اخرى اكثر اماناً، والاستحصال على موافقته الخطية على تحمّل هذه المخاطر وتزويده **بالدليل الإرشادي الخاص بالأفراد والمؤسسات غير المالية**.

2 - التنبّه لطلبات تحويل الاموال المُقدّمة من العميل شخصياً او المُرسلة من بريده الالكتروني التي تتضمن رقم حساب جديد ومختلف منسوب لمستفيد قام عميل المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية بالتعامل معه سابقاً والطلب من هذا العميل الاتصال بالمستفيد هاتفياً لتأكيد صحة تعليمات الدفع.

3 - التنبّه لطلبات تحويل الاموال المُقدّمة من العميل شخصياً او المُرسلة من بريده الالكتروني التي تتضمن اسم مستفيد جديد ينوي عميل المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية التعامل معه لأول مرة والطلب من هذا العميل الاتصال بالمستفيد هاتفياً لتأكيد صحة تعليمات الدفع.

4 - التأكد من ان البريد الالكتروني الذي ورد منه طلب التحويل عائد فعلاً للعميل وأنه لم يتم تحريفه بإضافة حرف او رقم او رمز او اشارة، وفي هذه الحالة يقتضي ابلاغ العميل بواسطة وسائل الاتصال المتفق عليها والمحددة في العقد.

5 - عدم تنفيذ طلبات تحويل الاموال الواردة إلى المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية بواسطة البريد الالكتروني، وعلى كامل مسؤولية العميل، إلا بعد الاتصال بهذا الأخير على الرقم المحدّد من قبله او بأية وسيلة من وسائل الاتصال المتّفق عليها في العقد على أن تكون جميع الادلة والبراهين على الاتصالات أو محاولة الاتصال محفوظة لدى المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية. كما يجب على المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية إعادة الإتصال بالعميل حتى ولو بادر هذا العميل بالاتصال، وذلك لتلافي المخاطر المترتبة على استعمال المُقرصن تطبيقاً يظهر رقم العميل المذكور المدون في سجلات المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية.

كما يجب على المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية الطلب من عميله الاجابة على جميع التفاصيل التالية المتعلقة بالتحاويل المطلوب تنفيذها بواسطة البريد الإلكتروني:

- المبلغ والعملة.
- رقم حساب المستفيد.
- الاسم الكامل للمستفيد.
- البلد المُرسل اليه.
- المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية المُرسل اليه.

6 - قيامه، فور علمه بوقوع أفعال جرمية بالوسائل الالكترونية تطال العميل ، بالاتصال بالمصرف المُراسل بالوسائل كافة المتّفق عليها بينهما (الهاتف، البريد الالكتروني او الـ SWIFT) وتزويده بوقائع القضية والطلب اليه تجميد قيمة التحويل وإعادته في حال كان لا يزال في حساباته. وفي حال تعذّر القيام بذلك فيقتضي عندها ابلاغ المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة بوقائع القضية والطلب اليه إعادة قيمة التحويل الى المصرف المُراسل تمهيداً لإعادته الى حساب العميل الذي تعرض للفعل الجرمي.

7 - إرسال رسالة نصية SMS إلى هاتف العميل الجوال لإبلاغه بتنفيذ التحويل، أو إبلاغه بأن المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية حاول الاتصال به لتأكيد عملية التحويل بغية تنفيذها.

8 - كما يقتضي على المصرف او المؤسسة المالية او مؤسسة الوساطة المالية التنبّه إلى الأمور التالية:

أ. لفت نظر العميل اثناء حضوره لتعبئة الاستمارة الخاصة بالتحويل الى اي تعديل لجهة اسم المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة او اسم المستفيد او رقم حسابه والطلب من العميل قبل تعبئة الاستمارة المذكورة او قبل اجراء التحويل مراجعة "المورّد" هاتفياً على الرقم المحدد من قبله والمدوّن في سجلات العميل وذلك للتثبت من مكونات التحويل لجهة اسم المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة او اسم المستفيد او رقم حسابه.

ب. في حال تعذّر الاتصال بالعميل بأية وسيلة من وسائل الاتصال المتفق عليها فانه يقتضي الامتناع عن اجراء التحويل على مسؤولية العميل، تطبيقاً لأحكام العقد الموقع مع هذا الأخير، لحين تأكيد صحة التعليمات الواردة او المرسلة بالبريد الالكتروني. يقع على عاتق المصرف أوالمؤسسة المالية ومؤسسة الوساطة المالية في هذه الحالة توثيق الاتصال أو محاولات الاتصال بالعميل بالوسائل كافة وعدم تلف هذه الإثباتات.

ج. مراجعة العميل عند وجود أدنى شك في المستندات المرفقة بالبريد الالكتروني وذلك قبل اجراء التحويل المطلوب.

د. تطبيق اجراءات العناية الواجبة المعزّزة فيما خصّ التحاويل الإلكترونية وبالأخص في حال وجود شك بارتكاب أفعال جرمية بالوسائل الالكترونية والطلب من العميل مراجعة "المورّد" هاتفياً على الرقم المحدد من قبله والمدوّن في سجلات العميل وليس على الرقم الوارد في البريد الالكتروني وذلك للتثبّت من مكوّنات التحويل لجهة اسم المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة واسم المستفيد ورقم حسابه .

ه. الامتناع عن إعطاء أية معلومات عبر البريد الالكتروني عن اسماء العملاء وارقام حساباتهم وارصدتها.

و. الامتناع عن الرد على اية مراسلة واردة بالبريد الالكتروني وذلك عبر الضغط على الاختيار (Reply) إنما يقتضي الضغط على الاختيار (Forward) وإعادة كتابة الاسم والعنوان الإلكتروني المُبلّغ للمصرف أو للمؤسسة المالية أو لمؤسسة الوساطة المالية من قبل العميل.

ز. التنبه عند مراسلة العميل بالبريد الالكتروني الى توجيه نسخة عن المراسلة الى شخص آخر مسؤول في المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية لضمان ازدواجية المراقبة.

ح. التأكد من ان بوالص التأمين تغطّي المخاطر المرتبطة بالتحاويل المالية بواسطة البريد الإلكتروني.

ط. الاحتفاظ بنسخة إلكترونية سليمة واحدة على الأقل، ونسخة ورقية، عن المراسلات الالكترونية والاتصالات الهاتفية أو محاولات الاتصال بأية وسيلة أخرى وتفاصيل العمليات المالية بالوسائل الالكترونية كافة التي يجريها العميل مع المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية.

ي. في حال الشكّ بمصدر البريد الإلكتروني، يقتضي مراجعة الجهة المسؤولة عن أمان المعلومات في المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية، أو أي جهة أخرى تقوم بهذا الدور، بهدف التحقق التقني من البريد الإلكتروني المشبوه وبالأخص لمقارنته مع لوائح العناوين الإلكترونية المشتبه بأنها سبقت واستعملت لارتكاب أفعال جرمية. في حال عدم وجود جهة مسؤولة عن أمان المعلومات في المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية تتمتع بالمقدرات التقنية والبشرية اللازمة، فإنه يقتضي على المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية اتخاذ الخطوات الضرورية كافة لتصحيح هذا النقص على وجه السرعة.

3. الاجراءات التصحيحية

لدى اكتشاف او علم او تبلّغ المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية بأن عميله وقع ضحية أفعال جرمية بالوسائل الإلكترونية فانه يقتضي اتخاذ إجراءات سريعة وفعّالة تشمل على الأقل ما يلي:

1. تزويد كل من المصرف المراسل والمصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة بالمعلومات كافة ذات الصلة وطلب الغاء التحويل واعادة قيمته الى عميل المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية، فضلاً عن تزويد هيئة التحقيق الخاصة بهذه المعلومات وبالمستندات وبالمراسلات ذات الصلة بالإضافة الى اسم المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة واسم المستفيد ورقم حسابه وقيمة التحويل وتاريخ تنفيذه.
2. طلب استرداد الأموال موضوع الأفعال الجرمية بالوسائل الإلكترونية أو الناتجة عنها.
3. إبلاغ المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة بأن الحساب المفتوح لديه يُستعمل لتلقي أموالاً ناتجة عن أفعال جرمية بالوسائل الإلكترونية.
4. مراجعة العميل عبر وسائل الاتصال المتفق عليها تعاقدياً، وفي حال الضرورة، ودون مخالفة ما ذكر سابقاً من شروط متعلقة بتنفيذ التحويل الالكتروني، على أرقامه المعتمدة والمدوّنة في سجلات المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية وليس على الأرقام الواردة في البريد الالكتروني.
5. الطلب من العميل مراجعة جميع العمليات المنفّذة على حساباته لدى المصارف أو المؤسسات المالية أو مؤسسات الوساطة المالية التي يتعامل معها والتأكّد من صحتها.
6. توجيه العميل لتقديم إبلاغ وشكوى قضائية الى الجهات المختصة.
7. توعية الموظفين والعملاء على كيفية تطبيق اجراءات العناية الواجبة للوقاية من الأفعال الجرمية بالوسائل الإلكترونية.
8. إدراج اسم أو رقم حساب المستفيد (وفق الحالة) على لائحة الأسماء المشبوهة ضمن (Filtering System) الموضوع لدى المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية لتفادي تنفيذ تحاويل مماثلة في المستقبل. كما يقتضي تحديث قاعدة بيانات المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية لتتضمن المعلومات كافة المتعلقة بالأفعال الجرمية.
9. إبلاغ شركات التأمين عند الضرورة.
10. إخضاع المعلومات المشبوهة للمراقبة من قبل أكثر من شخص في المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية.

الجزء الثاني:
إرشادات للأشخاص وسائر المؤسسات والهيئات غير المالية

1. المؤشرات على الأفعال الجرمية بواسطة البريد الإلكتروني

إن الأفعال الجرمية بواسطة البريد الإلكتروني قد تتخذ أشكالاً عدة، ويتوجب التنبه إلى المؤشرات التالية، على سبيل المثال لا الحصر، التي قد تساعد في اكتشاف هذه الأفعال:

1. اختلاف في عنوان البريد الالكتروني المنسوب إلى «المورّد» لجهة حرف أو رقم أو رمز أو إشارة بحيث يتمّ مثلاً استبدال حرف «g» بحرف «q».
2. بريد الكتروني منسوب «للمورّد» يدعي فيه المرسل انه تم تغيير رقم حساب «المورّد» لأسباب وحجج غير مقنعة، منها، على سبيل الذكر، إجراءات تدقيق تقوم بها السلطات الرقابية او الضريبية على حسابات «المورّد»، أو تدهور العلاقة مع المصرف السابق بسبب العمولات المصرفية المرتفعة.
3. بريد الكتروني يتضمن تعليمات بإرسال تحاويل إلى حساب مفتوح في الخارج باسم مشابه أو مطابق لاسم «المورّد»، وانما برقم حساب جديد مختلف عن رقم حساب «المورّد» المعتمد بحسب المستندات المحفوظة لدى الفرد او لدى الشركة المعنية.
4. بريد الكتروني منسوب «للمورّد» يطلب فيه المرسل عدم الاتصال «بالمورّد» هاتفيا للتأكد من اي تعديل أو تغيير لجهة اسم المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة أو اسم المستفيد او رقم حسابه.
5. بريد الكتروني منسوب لمصرف أو لمؤسسة مالية أو لمؤسسة وساطة مالية يدّعي فيه المُرسل ان المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية بصدد تحديث ملف احد عملائه ويطلب معلومات محدّدة بهذا الخصوص.
6. بريد الكتروني منسوب «للمورّد» ينطوي على اخطاء لغوية غير عادية أو فاضحة.
7. بريد الكتروني منسوب «للمورّد» ينطوي على صياغة ولغة تختلفان عن المُراسلات السابقة.
8. الاحرف والارقام الواردة في الفاتورة المرفقة بالبريد الالكتروني المشبوه غير متناسقة من حيث الشكل والحجم واللون.
9. طلب التحويل المرفق بالبريد الالكتروني المشبوه يحمل توقيعاً مشابهاً لتوقيع «المورّد».
10. بريد الكتروني منسوب «للمورّد» موجه الى الشركة المُتلقية بشكل عام وليس الى الموظف الذي يتلقى عادة التعليمات من «المورّد» لتنفيذها.

11. بريد الكتروني يختلف عن البريد الالكتروني العائد «للمورّد».
12. بريد الكتروني منسوب «للمورّد» يتضمن تعليمات غير مشابهة للتعليمات السابقة.
13. بريد الكتروني منسوب «للمورّد» ومُوجّه الى الفرد/الشركة بالإضافة إلى طرف ثالث لا علاقة له بالتحويل المطلوب تنفيذه.
14. عنوان «المورّد» يقع في دولة تختلف عن تلك التي يعمل فيها المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة.
15. بريد الكتروني منسوب «للمورّد» او لغيره يطلب فيه المُرسل معلومات عن حسابات مصرفية ومالية و/او أي معلومات حساسة أخرى.
16. بريد الكتروني يتضمن رابط (Link) إلى موقع الكتروني يطلب معلومات مالية أو شخصية.

2. السياسات والاجراءات الوقائية من الافعال الجرمية

يقتضي اتباع الخطوات الوقائية التالية :

1. تحديد العميل لاكثر من وسيلة تواصل مع «مورّديه» كافة للتأكد من التعليمات الواردة منهم قبل تنفيذها (رقم الهاتف، رقم الفاكس، البريد الالكتروني، اسم الشخص الذي يمكن التواصل معه).
2. التواصل هاتفياً مع «المورّد» على الارقام المحدّدة من قبله والمدونة في سجلات الفرد/الشركة وليس على الأرقام الواردة في البريد الالكتروني وذلك للتثبت من مكوّنات التحويل لجهة اسم المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة واسم المستفيد ورقم حسابه والمستندات المرفقة.
3. عدم تزويد «المورّد» او اي طرف آخر عبر البريد الالكتروني بأية معلومات مالية خاصة تتعلق باسم المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية الذي يتعامل معه الفرد/الشركة ورقم الحساب ورصيده والعمليات الجارية عليه.
4. التنبّه للاتصال الهاتفي او للبريد الالكتروني الذي يطلب معلومات مالية بحجّة تحديث الملفات الشخصية والمالية العائدة للفرد/الشركة.
5. الامتناع عن الردّ على اية مُراسلة واردة بالبريد الالكتروني عبر الضغط على اختيار (Reply) واستبداله بالضغط على اختيار (Forward) لانتقاء عنوان البريد الالكتروني من قائمة العناوين (Mailing list) لأن اسم المرسل الظاهر في البريد الالكتروني قد لا يعود فعلياً له، بل لأحد المُقرصنين الذي أنشأ بريداً الكترونياً مشابهاً. كما يمكن كشف أي تلاعب في عنوان البريد الإلكتروني من خلال فتح نافذة الاختيار (Reply) (دون استعمالها) والتأكد من هوية مرسل البريد الالكتروني.
6. التأكد من كامل تفاصيل عنوان البريد الالكتروني والانتباه إلى أي بريد الكتروني مشكوك وغير موثوق المصدر مشابه لبريد «المورّد».

7. عند ارسال رسائل إلكترونية لعدة أشخاص يجب وضع عناوين البريد الإلكتروني في خانة (BCC) لكي لا يطّلع عليها الغير ويحاول إختراقها.
8. في حال تعذّر الاتصال «بالمورّد» بأية وسيلة من وسائل الاتصال المتفق عليها فانه يقتضي الامتناع عن الطلب من المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية إجراء التحويل لحين تأكيد صحة التعليمات الواردة او المرسلة بالبريد الالكتروني.
9. أخذ العلم بأن المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية سيمتنع عن اجراء التحويل او تنفيذ اية تعليمات اخرى عندما يتعذر عليه الاتصال بالفرد/الشركة بأية وسيلة من وسائل الاتصال المتفق عليها لتأكيد طلب إجراء التحويل الوارد بواسطة البريد الإلكتروني.
10. ضرورة إستخدام حسابين الكترونيين على الاقل:
    - الأول لجميع المُراسلات المرتبطة بالتحاويل المالية مع المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية والتأكد من عدم ذكره على بطاقة التعريف (Business Card).
    - الثاني مخصّص لمواقع التواصل الاجتماعي.
11. عدم استخدام كلمة مرور (Password) موّحدة لأكثر من بريد أو موقع الكتروني. كما يجب استخدام كلمة مرور قوية وتغييرها بشكل دائم مع تفعيل خاصية الدخول بخطوتين (Two-Step Verification).
    لا يجب أن تتضمن كلمة السر، على سبيل المثال، ما يلي:
    - نماذج بسيطة على لوحة المفاتيح، سلسلة من أرقام وحروف أو حروف متكررة مثل (qwerty, abcdef, 1234, AAAa)
    - كلمات مطبوعة بالمقلوب مثل (sdrawkcab=backwards)
    - كلمات قصيرة، غير مكتملة أو مكتوبة بشكل خاطئ مثل (Helo)
    - كلمات قصيرة متتالية مثل (Catcat)
    - كلمات يسبقها أو يليها رمز واحد مثل (Apple3, %hello)
    - معلومات شخصية (تاريخ الولادة، الاسم، الشهرة)
12. التنبّه للمُراسلات الواردة والمتضمنة مرفقات (Attachments) مشبوهة مثل:
    (scr, dll, cox, com, exe, bat, vbs, dif, shs, pif) لإمكانية إحتوائها برامج خبيثة.
13. تحديث المتصفّح (Update Browser) المستعمل على الاجهزة الالكترونية بشكل منتظم.
14. استعمال برنامج أصلي لمكافحة الفيروسات (Antivirus) وتحديثه باستمرار.
15. تفعيل خاصية النشاط الحديث (Recent Activity) للبريد الالكتروني. في حال وجود اي شك حول هذا النشاط، يجب على الفور تغيير كلمة المرور.

16. التنبّه من تصفّح البريد الالكتروني من خلال (Public WIFI).
17. الإحتفاظ بالمعلومات المخزنة على (Mail Server) لأكثر من ثلاثة اشهر إذا أمكن.
18. الامتناع عن شحن السلع الى الشركات المستوردة في الخارج قبل تأكيد صحة تعليمات الدفع هاتفياً بإحدى طرق الاتصال المتفق عليها.
19. التأكد من ان بوالص التأمين تغطّي المخاطر المرتبطة بتنفيذ عمليات مالية ومصرفية عبر البريد الإلكتروني.
20. التنبه من البريد الالكتروني الذي يرد فيه طلب تنفيذ فوريّ للتحويل (Real Time Transfer).

3. الاجراءات التصحيحية

لدى اكتشاف او علم او تبلّغ وقوع أفعال جرمية بالوسائل الإلكترونية فانه يقتضي اتخاذ إجراءات سريعة وفعّالة تشمل على الأقل ما يلي:

1. ابلاغ المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية المعني فوراً وتزويده على وجه السرعة بالمعلومات كافة ذات الصلة لإجراء المقتضى.
2. التواصل مع «المورّد» على أرقامه المُعتمدة لابلاغه بحصول أو محاولة حصول أفعال جرمية بالوسائل الإلكترونية ولفت نظره إلى ضرورة مراجعة عملائه هاتفياً وأعلامهم باحتمال تعرّضهم لأفعال قرصنة إلكترونية.
3. التقدّم بشكوى امام المراجع القضائية المختصة والمحافظة على الأدلة الرقميّة كافة.
4. تغيير فوري لكلمة المرور.
5. الحرص على الاحتفاظ بالمُراسلات الجارية على البريد الالكتروني دون إلغائها او إجراء اي تعديل عليها نظرا لإمكانية استخدامها في اية تحقيقات.
6. من المُستحسن أن تتم مراجعة العمليات كافة مع «المورّد» للتأكد من عدم تعرّضه سابقاً لأفعال جرمية أخرى بالوسائل الالكترونية وإبلاغ المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية المعنية بنتيجة هذه المراجعة.

وفي الختام، لا بد من لفت نظر جميع المعنيين بمكافحة الجريمة الالكترونية المالية الى ضرورة القيام دورياً بمتابعة التطورات والارشادات الدولية والممارسات الفضلى (Best practices) المتعلقة بهذا الموضوع وذلك بغية تحديث وتحسين الاجراءات المتبعة للحد من هذه الجريمة.

مكافحة الجريمة الإلكترونية المالية في لبنان

الدليل الإرشادي للوقاية من الأفعال الجرمية بواسطة البريد الإلكتروني