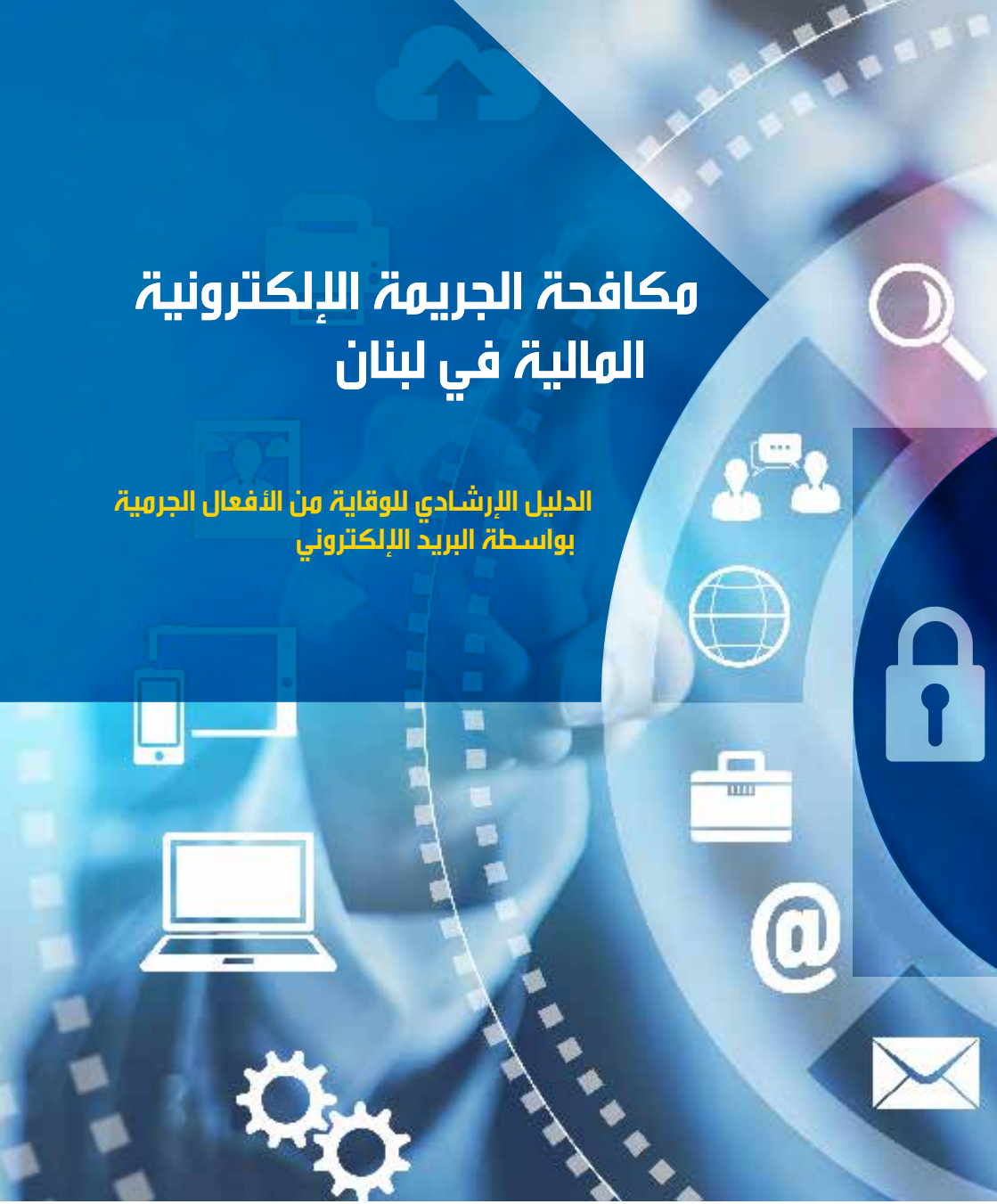
مكافحة الجريمة الإلكترونية المالية في لبنان

الدليل الإرشادي للوقاية من الأفعال الجرمية بواسطة البريد الإلكتروني



جمعية المصارف في لبنان

مصرف لبنان
BANQUE DU LIBAN

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.

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.