مقتطف عن
الدليل الإرشادي
للوقاية من الأفعال الجرمية
بواسطة البريد الإلكتروني

إرشادات للأشخاص
وسائر المؤسسات والهيئات غير المالية

Creditbank S.A.L.

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 إكتشاف هذه الأفعال:

١. إختلاف في عنوان البريد الإلكتروني المنسوب إلى "المورّد" لجهة حرف أو رقم أو رمز أو إشارة بحيث يتمّ مثلاً إستبدال حرف "g" بحرف "q".

٢. بريد إلكتروني منسوب "للمورّد" يدّعي فيه المرسل أنه تم تغيير رقم حساب "المورّد" لأسباب وحجج غير مقنعة، منها، على سبيل الذكر، إجراءات تدقيق تقوم بها السلطات الرقابية أو الضريبية على حسابات "المورّد"، أو تدهور العلاقة مع المصرف السابق بسبب العمولات المصرفية المرتفعة.

٣. بريد إلكتروني يتضمن تعليمات بإرسال تحاويل إلى حساب مفتوح في الخارج بإسم مشابه أو مطابق لإسم "المورّد"، وإنما برقم حساب جديد مختلف عن رقم حساب "المورّد" المعتمد بحسب المستندات المحفوظة لدى الفرد أو لدى الشركة المعنيّة.

٤. بريد إلكتروني منسوب "للمورّد" يطلب فيه المرسل عدم الإتصال "بالمورّد" هاتفياً للتأكد من أي تعديل أو تغيير لجهة إسم المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة أو إسم المستفيد أو رقم حسابه.

٥. بريد إلكتروني منسوب لمصرف أو لمؤسسة مالية أو لمؤسسة وساطة مالية يدّعي فيه المُرسل ان المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية بصدد تحديث ملف أحد عملائه ويطلب معلومات محدّدة بهذا الخصوص.

٦. بريد إلكتروني منسوب "للمورّد" ينطوي على أخطاء لغوية غير عادية أو فاضحة.

٧. بريد إلكتروني منسوب "للمورّد" ينطوي على صياغة ولغة تختلفان عن المُراسلات السابقة.

٨. الأحرف والأرقام الواردة في الفاتورة المرفقة بالبريد الإلكتروني المشبوه غير متناسقة من حيث الشكل والحجم واللون.

٩. طلب التحويل المرفق بالبريد الإلكتروني المشبوه يحمل توقيعاً مشابهاً لتوقيع "المورّد".

١٠. بريد إلكتروني منسوب "للمورّد" موجه إلى الشركة المُتلقية بشكل عام وليس إلى الموظف الذي يتلقى عادة التعليمات من "المورّد" لتنفيذها.

١١. بريد إلكتروني يختلف عن البريد الإلكتروني العائد "للمورّد".

١٢. بريد إلكتروني منسوب "للمورّد" يتضمن تعليمات غير مشابهة للتعليمات السابقة.

١٣. بريد إلكتروني منسوب"للمورّد" ومُوجّه إلى الفرد/الشركة بالإضافة إلى طرف ثالث لا علاقة له بالتحويل المطلوب تنفيذه.

١٤. عنوان "المورّد" يقع في دولة تختلف عن تلك التي يعمل فيها المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة.

١٥. بريد إلكتروني منسوب"للمورّد" أو لغيره يطلب فيه المُرسل معلومات عن حسابات مصرفية ومالية و/أو أي معلومات حساسة أخرى.

١٦. بريد إلكتروني يتضمن رابط (Link) إلى موقع إلكتروني يطلب معلومات مالية أو شخصية.

السياسات والإجراءات الوقائية من الأفعال الجرمية

يقتضي إتباع الخطوات الوقائية التالية :

١. تحديد العميل لأكثر من وسيلة تواصل مع "مورّديه" كافة للتأكد من التعليمات الواردة منهم قبل تنفيذها (رقم الهاتف، رقم الفاكس، البريد الإلكتروني، إسم الشخص الذي يمكن التواصل معه).

٢. التواصل هاتفياً مع "المورّد" على الأرقام المحدّدة من قبله والمدونة في سجلات الفرد/الشركة وليس على الأرقام الواردة في البريد الإلكتروني وذلك للتثبت من مكوّنات التحويل لجهة إسم المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة وإسم المستفيد ورقم حسابه والمستندات المرفقة.

٣. عدم تزويد "المورّد" أو أي طرف آخر عبر البريد الإلكتروني بأية معلومات مالية خاصة تتعلق بإسم المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية الذي يتعامل معه الفرد/الشركة ورقم الحساب ورصيده والعمليات الجارية عليه.

٤. التنبّه للإتصال الهاتفي أو للبريد الإلكتروني الذي يطلب معلومات مالية بحجّة تحديث الملفات الشخصية والمالية العائدة للفرد/الشركة.

٥. الإمتناع عن الردّ على أية مُراسلة واردة بالبريد الإلكتروني عبر الضغط على إختيار (Reply) وإستبداله بالضغط على إختيار (Forward) لإنتقاء عنوان البريد الإلكتروني من قائمة العناوين (Mailing list) لأن إسم المرسل الظاهر في البريد الإلكتروني قد لا يعود فعلياً له، بل لأحد المُقرصنين الذي أنشأ بريداً إلكترونياً مشابهاً. كما يمكن كشف أي تلاعب في عنوان البريد الإلكتروني من خلال فتح نافذة الإختيار (Reply) دون إستعمالها والتأكد من هوية مرسل البريد الإلكتروني .

٦. التأكد من كامل تفاصيل عنوان البريد الإلكتروني والإنتباه إلى أي بريد إلكتروني مشكوك وغير موثوق المصدر مشابه لبريد "المورّد".

٧. عند إرسال رسائل إلكترونية لعدة أشخاص يجب وضع عناوين البريد الإلكتروني في خانة (BCC) لكي لا يطّلع عليها الغير ويحاول إختراقها.

٨. في حال تعذّر الإتصال "بالمورّد" بأية وسيلة من وسائل الإتصال المتفق عليها فانه يقتضي الإمتناع عن الطلب من المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية إجراء التحويل لحين تأكيد صحة التعليمات الواردة أو المرسلة بالبريد الإلكتروني .

٩. أخذ العلم بأن المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية سيمتنع عن إجراء التحويل أو تنفيذ أية تعليمات أخرى عندما يتعذر عليه الإتصال بالفرد/الشركة بأية وسيلة من وسائل الإتصال المتفق عليها لتأكيد طلب إجراء التحويل الوارد بواسطة البريد الإلكتروني.

١٠. ضرورة إستخدام حسابين إلكترونيين على الأقل:
• 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 الإجتماعي.

١١. عدم إستخدام كلمة مرور (Password) موحّدة لأكثر من بريد أو موقع إلكتروني. كما يجب إستخدام 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 (abcdef, 1234, AAAa qwerty).
• 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، الإسم، الشهرة).

١٢. التنبّه للمُراسلات الواردة والمتضمنة مرفقات (Attachments) مشبوهة مثل:shs, pif, scr, dll, cox, com exe, bat, vbs, dif لإمكانية إحتوائها برامج خبيثة.

١٣. تحديث المتصفّح (Update Browser) المستعمل على الأجهزة الإلكترونية بشكل منتظم.

١٤. إستعمال برنامج أصلي لمكافحة الفيروسات (Antivirus) وتحديثه بإستمرار.

١٥. تفعيل خاصية النشاط الحديث (Recent Activity) للبريد الإلكتروني. في حال وجود أي شك حول هذا النشاط، يجب على الفور تغيير كلمة المرور والمؤسسات غير المالية.

١٦. التنبّه من تصفّح البريد الإلكتروني من خلال (Public WIFI)

١٧. الإحتفاظ بالمعلومات المخزنة على (Mail Server) لأكثر من ثلاثة أشهر إذا أمكن.

١٨. الإمتناع عن شحن السلع إلى الشركات المستوردة في الخارج قبل تأكيد صحة تعليمات الدفع هاتفياً بإحدى طرق الإتصال المتفق عليها.

١٩. التأكد من أن بوالص التأمين تغطّي المخاطر المرتبطة بتنفيذ عمليات مالية ومصرفية عبر البريد الإلكتروني.

٢٠. التنبه من البريد الإلكتروني الذي يرد فيه طلب تنفيذ فوريّ للتحويل Real Time Transfer.

الإجراءات التصحيحية

لدى إكتشاف أو علم أو تبلّغ وقوع أفعال جرمية بالوسائل الإلكترونية فإنه يقتضي إتخاذ إجراءات سريعة وفعّالة تشمل على الأقل ما يلي:

١. إبلاغ المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية المعني فوراً وتزويده على وجه السرعة بالمعلومات كافة ذات الصلة لإجراء المقتضى.

٢. التواصل مع "المورّد" على أرقامه المُعتمدة لإبلاغه بحصول أو محاولة حصول أفعال جرمية بالوسائل الإلكترونية ولفت نظره إلى ضرورة مراجعة عملائه هاتفياً وإعلامهم بإحتمال تعرّضهم لأفعال قرصنة إلكترونية.

٣. التقدّم بشكوى أمام المراجع القضائية المختصة والمحافظة على الأدلة الرقميّة كافة وتزويد المصرف بنسخة عن الشكوى المقدمة أمام المراجع القضائية المختصة.

٤. تغيير فوري لكلمة المرور.

٥. الحرص على الإحتفاظ بالمُراسلات الجارية على البريد الإلكتروني دون إلغائها أو إجراء اي تعديل عليها نظرًا لإمكانية إستخدامها في أية تحقيقات.

٦. من المُستحسن أن تتم مراجعة العمليات كافة مع "المورّد" للتأكد من عدم تعرّضه سابقاً لأفعال جرمية أخرى بالوسائل الإلكترونية وإبلاغ المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية المعنية بنتيجة هذه المراجعة.

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