البنك اللبناني الفرنسي

الدليل الإرشادي للوقاية من قرصنة البريد الإلكتروني

١- الدليل الإرشادي الخاص بالأفراد والمؤسسات غير المالية للوقاية من قرصنة البريد الإلكتروني

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 إلكترونية وتقنية عدة، يدخل ضمن نطاق هذه الجريمة مثلاً عمليات الإحتيال والسرقة والإختلاس والإبتزاز والتخريب والتجسس بالوسائل الإلكترونية.

٢- السياسات والإجراءات الوقائية من الأفعال الجرمية

٢.١ يقتضي عند القيام بعمليات تجارية، إتباع الخطوات الوقائية التالية:

- تحديد أكثر من وسيلة تواصل مع المورد للتأكد من التعليمات الواردة منه (رقم الهاتف، رقم الفاكس، البريد الإلكتروني، إسم الشخص الذي يمكن التواصل معه ...).
- التواصل هاتفياً مع «المورد» على الأرقام المحددة من قبله وليس على الأرقام الواردة في البريد الإلكتروني وذلك للتثبت من مكونات التحويل لجهة إسم المصرف المستفيد وإسم المستفيد ورقم حسابه والمستندات المرفقة.
- عدم تزويد المورد أو أي طرف آخر عبر البريد الإلكتروني بأية معلومات مالية خاصة (إسم المصرف، رقم الحساب ورصيده، العمليات الجارية عليه ...).
- في حال تعذر الإتصال بالمورد بأية وسيلة من وسائل الإتصال المتفق عليها فإنه يقتضي الإمتناع عن الطلب من المصرف إجراء التحويل لحين تأكيد صحة التعليمات الواردة أو المرسلة بالبريد الإلكتروني.
- أخذ العلم بأن المصرف سيمتنع عن إجراء التحويل أو تنفيذ أية تعليمات أخرى عندما يتعذر عليه الإتصال بعميله بأية وسيلة من وسائل الإتصال المتفق عليها لتأكيد طلب إجراء التحويل الوارد عبرالبريد الإلكتروني.
- التنبه إلى عدم شحن السلع إلى الشركات المستوردة في الخارج قبل تأكيد صحة تعليمات الدفع، هاتفياً، بإحدى طرق الاتصال المتفق عليها.
- التأكد من أن بوالص التأمين تغطي المخاطر المرتبطة بتنفيذ عمليات مالية ومصرفية عبر البريد الالكتروني.

٢.٢ كما يستحسن في إطار ممارسة العمليات اليومية إتباع الاجراءات الوقائية الروتينية التالية:

ضرورة إستخدام حسابين الكترونيين على الأقل، الأول لجميع المراسلات المرتبطة بالتحاويل المالية مع المصرف والتأكد من عدم ذكره على بطاقة التعريف. الثاني مخصص لمواقع التواصل الإجتماعي.

- الإمتناع عن الرد على أية مراسلة واردة بواسطة البريد الإلكتروني عبر الضغط على إختيار Reply وإستبداله بالضغط على إختيار Forward لإنتقاء عنوان البريد الإلكتروني من قائمة العناوين لأن إسم المرسل الظاهر في البريد الإلكتروني قد لا يعود فعلياً له، بل لأحد المقرضين الذي أنشأ بريداً إلكترونياً مشابها. كما يمكن كشف أي تلاعب في عنوان البريد الالكتروني من خلال فتح نافذة الاختيار (دون استعمالها) والتأكد من هوية مرسل البريد الإلكتروني.
- عند إرسال رسائل إلكترونية لعدة أشخاص يجب وضع عناوين البريد الإلكتروني في خانة لكي لا يطلع عليها الغير ويحاول اختراقها.
- عدم إستخدام كلمة مرور موحدة لاكثر من بريد أو موقع إلكتروني. كما يجب إستخدام كلمات مرور قوية وتغييرها بشكل دائم مع تفعيل خاصية الدخول بخطوتين. 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، qwerty، ١٢٣٤، 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 (٪hello، apple3)

– معلومات شخصية (تاريخ الولادة، الاسم، الشهرة)

- التنبه للمراسلات الواردة والمتضمنة مرفقات مشبوهة («.bat»، «.vbs»، «.dif»، « .shs»، «.pif»، «.scr»، «.dll»، «.com»، «.cox»، «.exe») لإمكانية احتوائها برامج خبيثة.
- تحديث المتصفح المستعمل على الأجهزة الالكترونية بشكل منتظم.

- إستعمال برنامج أصلي لمكافحة الفيروسات وتحديثه بإستمرار.
- تفعيل خاصية النشاط الحديث للبريد الالكتروني وفي حال وجود أي شك حول هذا النشاط يقتضي على الفور تغيير كلمة المرور.
- عدم تصفح البريد الالكتروني المخصص للمراسلات المرتبطة بالتحاويل المالية مع المصرف من خلال public WIFI.
- الاحتفاظ بالمعلومات المخزنة على mail server لأكثر من ثلاثة أشهر إذا أمكن.
- التنبه من البريد الإلكتروني الذي يرد فيه طلب تنفيذ فوري للتحويل.

٣- الاجراءات التصحيحية عند إكتشاف عمليات قرصنة أو محاولة تنفيذ عملية قرصنة

لدى إكتشاف أو تبلغ وقوع أو محاولة وقوع أفعال جرمية بالوسائل الالكترونية فإنه يتوجب فوراً إبلاغ المصرف الذي نفذ عملية التحويل وتزويده على وجه السرعة بالمعلومات كافة ذات الصلة لكي يتسنى له إجراء المقتضى. كما يقتضي أيضاً:

٣.١ التواصل مع «المورد» على ارقامه المعتمدة لإبلاغه بحصول أو محاولة حصول أفعال جرمية بالوسائل الالكترونية ولفت نظره إلى ضرورة مراجعة عملائه هاتفياً واعلامهم بإحتمال تعرضهم لأفعال قرصنة إلكترونية.

٣.٢ التقدم بشكوى أمام المراجع القضائية المختصة والمحافظة على جميع الأدلة الرقمية والمراسلات الجارية على البريد الإلكتروني دون الغائها أو إجراء أي تعديل عليها لإمكانية استخدمها في أية تحقيقات.

٣.٣ تغيير فوري لكلمة المرور.

٣.٤ مراجعة العمليات كافة مع «المورد» للتأكد من عدم التعرض سابقاً لافعال جرمية أخرى بالوسائل الإلكترونية وإبلاغ المصرف المعني بنتيجة هذه المراجعة.

اضغط هنا لقراءة الدليل الكامل.