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 والتجسّس بالوسائل الإلكترونية.

يتناول هذا الدليل الإرشادي بشكل خاص الجرائم الالكترونية المالية المرتكبة بواسطة البريد الالكتروني والتي تطال عمليات التحاويل المصرفية. ان الارشادات الواردة فيه سوف تساعد الافراد والمؤسسات غير المالية في اتخاذ الاجراءات اللازمة لحماية التعامل بالبريد الالكتروني. يتطرق الدليل الى المواضيع التالية:

المؤشرات على الأفعال الجرمية بواسطة البريد الإلكتروني

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

1. اي بريد الكتروني يختلف عن البريد الالكتروني العائد «للمورّد» (أي الشركة المورّدة أو المستوردة أو التاجر أو أي من مقدمي الخدمات الذين يجري التعامل معهم).
2. اختلاف في عنوان البريد الالكتروني المنسوب إلى «المورّد» لجهة حرف أو رقم أو رمز أو إشارة بحيث يتمّ مثلاً استبدال حرف «g» بحرف «q» إلخ.

الدليل الإرشادي الخاص بالأفراد والمؤسسات غير المالية

جمعية المصارف في لبنان

بالتعاون مع
الاقتصاد والاعمال
Al-Iktissad Wal-Aamal

E. التنبّه للمُراسلات الواردة والمتضمنة مرفقات (Attachments) مشبوهة مثل: scr, dll, cox com, exe, bat, vbs, dif, shs, pif لإمكانية إحتوائها برامج خبيثة.
F. تحديث المتصفّح (Update Browser) المستعمل على الاجهزة الالكترونية بشكل منتظم.
G. استعمال برنامج أصلي لمكافحة الفيروسات (Antivirus) وتحديثه باستمرار.
H. تفعيل خاصية النشاط الحديث (Recent Activity) للبريد الالكتروني وفي حال وجود اي شك حول هذا النشاط يقتضي على الفور تغيير كلمة المرور.
I. عدم تصفّح البريد الالكتروني المخصص للمُراسلات المرتبطة بالتحاويل المالية مع المصرف من خلال (Public WIFI).
J. الإحتفاظ بالمعلومات المخزنة على(Mail server) لأكثر من ثلاثة اشهر إذا أمكن.
K. التنبه من البريد الالكتروني الذي يرد فيه طلب تنفيذ فوريّ للتحويل (Real Time Transfer).

الاجراءات التصحيحية عند اكتشاف عملية قرصنة أو محاولة تنفيذ عملية قرصنة

لدى اكتشاف او تبلّغ وقوع او محاولة وقوع أفعال جرمية بالوسائل الإلكترونية فانه يتوجب فوراً **ابلاغ المصرف الذي نفذ عملية التحويل وتزويده على وجه السرعة بالمعلومات كافة ذات الصلة لكي يتسنى له إجراء المقتضى.**

كما يقتضي أيضاً:

1. التواصل مع «المورّد» على أرقامه المعتمدة لابلاغه بحصول او محاولة حصول أفعال جرمية بالوسائل الإلكترونية ولفت نظره إلى ضرورة مراجعة عملائه هاتفياً وإعلامهم باحتمال تعرضهم لأفعال قرصنة إلكترونية.
2. التقدّم بشكوى امام المراجع القضائية المختصة والمحافظة على جميع الأدلة الرقميّة والمُراسلات الجارية على البريد الالكتروني دون إلغائها او إجراء اي تعديل عليها لإمكانية استخدامها في اية تحقيقات.
3. تغيير فوري لكلمة المرور.
4. مراجعة العمليات كافة مع «المورّد» للتأكد من عدم التعرض سابقاً لأفعال جرمية أخرى بالوسائل الالكترونية وإبلاغ المصرف المعني بنتيجة هذه المراجعة.

3. اي بريد الكتروني منسوب «للمورّد» يدعي فيه المُرسِل (المُقرصن) 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 (قد يكون مصرفاً أو مؤسسة مالية أو مؤسسة وساطة مالية) السابق بسبب العمولات المرتفعة.
4. اي بريد الكتروني يتضمن تعليمات بإرسال تحاويل إلى حساب مفتوح في الخارج بإسم مُشابه أو مُطابق لإسم «المورّد»، وانما برقم حساب جديد مختلف عن رقم حساب «المورّد» المُعتمد بحسب المستندات المحفوظة لدى الفرد او لدى الشركة المعنية.
5. اي بريد الكتروني منسوب «للمورّد» يطلب فيه المرسل (المُقرصن) عدم الاتصال به («المورّد») هاتفياً للتأكد من اي تعديل أو تغيير لجهة اسم المصرف المستفيد أو اسم المستفيد او رقم حسابه.
6. اي بريد الكتروني او اتصال هاتفي منسوب للمصرف او «للمورّد» او لغيره يطلب فيه المُرسِل معلومات محدّدة عن حسابات مصرفية او معلومات حسّاسة اخرى.
7. اي بريد الكتروني منسوب «للمورّد» ينطوي على:
- اخطاء لغوية غير عادية أو فاضحة.
- 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 مُشابهاً (مزوّراً) لتوقيع «المورّد».
10. اي بريد الكتروني منسوب «للمورّد» موجه الى الشركة المُتلقية بشكل عام وليس الى الموظف الذي يتلقى عادة التعليمات من المورّد لتنفيذها.
11. اي بريد الكتروني منسوب «للمورّد» يتضمن تعليمات غير مشابهة للتعليمات السابقة.
12. اي بريد الكتروني منسوب «للمورّد» ومُوجّه إلى طرف ثالث لا علاقة له بالتحويل المطلوب تنفيذه.
13. عنوان المصرف المستفيد يقع في دولة تختلف عن تلك التي يعمل فيها «المورّد».
14. عنوان «المورّد» (المزعوم، الوارد في تعليمات الدفع) يقع في دولة تختلف عن تلك التي يعمل فيها «المورّد»
15. اي بريد الكتروني يتضمن رابط (Link) إلى موقع الكتروني

السياسات والاجراءات الوقائية من الأفعال الجرمية

1. يقتضي، عند القيام بعمليات تجارية، اتباع الخطوات الوقائية التالية:

i. تحديد أكثر من وسيلة تواصل مع «المورّد» للتأكد من التعليمات الواردة منه قبل تنفيذها (رقم الهاتف، رقم الفاكس، البريد الالكتروني، اسم الشخص الذي يمكن التواصل معه...).
ii. التواصل هاتفياً مع «المورّد» على الارقام المحدّدة من قبله وليس على الأرقام الواردة في البريد الالكتروني وذلك للتثبت من مكوّنات التحويل لجهة اسم المصرف المستفيد واسم المستفيد ورقم حسابه والمستندات المرفقة.
iii. عدم تزويد «المورّد» او اي طرف آخر عبر البريد الالكتروني بأية معلومات مالية خاصة (اسم المصرف، رقم الحساب ورصيده، العمليات الجارية عليه...)
iv. في حال تعذّر الاتصال «بالمورّد» بأية وسيلة من وسائل الاتصال المتفق عليها فانه يقتضي الامتناع عن الطلب من المصرف اجراء التحويل لحين تأكيد صحّة التعليمات الواردة او المُرسلة بالبريد الالكتروني.
v. أخذ العلم بأن المصرف سيمتنع عن اجراء التحويل او تنفيذ اية تعليمات اخرى عندما يتعذر عليه الاتصال بعميله بأية وسيلة من وسائل الاتصال المتفق عليها لتأكيد طلب إجراء التحويل الوارد عبر البريد الإلكتروني.
vi. التنبه إلى عدم شحن السلع الى الشركات المستوردة في الخارج قبل تأكيد صحة تعليمات الدفع، هاتفياً، بإحدى طرق الاتصال المتفق عليها.
vii. التأكد من ان بوالص التأمين تغطي المخاطر المرتبطة بتنفيذ عمليات مالية ومصرفية عبر البريد الإلكتروني.

2. كما يستحسن، في اطار ممارسة العمليات اليومية اتباع الإجراءات الوقائية الروتينية التالية:

A. ضرورة إستخدام حسابَيْن الكترونيَيْن على الاقل:
- الأول لجميع المُراسلات المرتبطة بالتحاويل المالية مع المصرف والتأكد من عدم ذكره على بطاقة التعريف (Business Card).
- الثاني مُخصّص لمواقع التواصل الاجتماعي.

B. الامتناع عن الردّ على اية مُراسلة واردة بواسطة البريد الالكتروني عبر الضغط على اختيار (Reply) واستبداله بالضغط على اختيار (Forward) لانتقاء عنوان البريد الالكتروني من قائمة العناوين (Mailing list) لأن اسم المُرسِل الظاهر في البريد الالكتروني قد لا يعود فعلياً له، بل لأحد المُقرصنين الذي أنشأ بريداً الكترونياً مُشابهاً. كما يمكن كشف أي تلاعب في عنوان البريد الإلكتروني من خلال فتح نافذة الاختيار (Reply) (دون استعمالها) والتأكد من هوية مُرسِل البريد الالكتروني.

C. عند ارسال رسائل إلكترونية لعدة أشخاص يجب وضع عناوين البريد الإلكتروني في خانة BCC لكي لا يطّلع عليها الغير ويحاول إختراقها.

D. 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)