Guidelines against email-based Cybercrimes for Individuals and Non-Financial Institutions

A financial cybercrime is an act or attempt to commit local or transboundary act or acts, intentionally perpetrated by individuals or organized groups, in order to gain access to bank accounts or financial and personal information by using various electronic and technical means. The scope of this crime includes, for example, fraud, theft, embezzlement, extortion, sabotage and electronic espionage.

These guidelines specifically address financial cybercrimes that are committed through the use of electronic mails and that affect bank transfers. The enclosed guidelines assist individuals and non-financial institutions in taking the necessary measures to handle emails securely. The guidelines tackle the following topics:

Indicators of email-based criminal acts

Criminal acts committed through the use of emails may take many forms, and the following indicators that help detect such acts should be taken into consideration, including without limitation:

1. An email that differs from the email of the "Supplier" (i.e. Supplier, importer, merchant or any of the service providers being dealt with).
2. A difference in the email address attributed to the "Supplier" in terms of a character, number, symbol, or signal, such as replacing "g" with "q", etc.
3. An email attributed to the "Supplier" in which the sender (fraudster) claims that the "Supplier" account number has been changed for unpersuasive reasons and arguments, such as audit procedures by regulatory or tax authorities on the "Supplier's" accounts or deterioration of the relationship with the Bank (it could be a bank, a financial institution, or a financial intermediation company) because of high commissions.
4. An electronic mail containing instructions to send transactions to an account open abroad in a similar or identical name to that of the "Supplier", but in a new account number that is different from the "Supplier's" account number approved according to the documents held by the individual or the concerned company.
5. An email attributed to the "Supplier" in which the sender (fraudster) requests not to contact him ("Supplier") by phone to confirm any amendment or change to the name of the beneficiary bank or the name of the beneficiary or his account number.
6. An email or phone call attributed to the bank, the "Supplier", or others, in which the sender requests specific information about bank accounts or other sensitive information.
7. An email attributed to the "Supplier" that includes:
    - Unusual or obscene language errors.

- Formulation and language that differ from previous correspondence.

8. The letters and numbers in the invoice attached to the suspicious email are inconsistent in terms of shape, size and colour.
9. The request for transfer attached to the suspicious email is falsely signed by the "Supplier".
10. An email attributed to the "Supplier" and addressed to the recipient company in general and not to the employee who normally receives instructions from the Supplier for execution.
11. An email attributed to the "Supplier" and containing instructions that are not similar to the previous instructions.
12. An email attributed to the "Supplier" and addressed to a third party unrelated to the transfer to be executed.
13. The address of the beneficiary bank is located in a country different from the one in which the "Supplier" operates.
14. The "Supplier's" address (alleged in the payment instructions) is located in a country different from the one in which the "Supplier" operates.
15. An email that includes a link to a website.

Preventive Policies and Measures

1. In carrying out business operations, the following preventive steps are required:

i. Select more than one means of communication with the "Supplier" to confirm the instructions before executing them (phone number, fax number, email, contact person ...).
ii. Communicate with the "Supplier" by phone on the numbers specified by him and not the numbers mentioned in the email, in order to verify the transfer components regarding the name of the beneficiary bank, the name of the beneficiary, his account number and the attached documents.
iii. Abstain from providing the "Supplier" or any other party by email with any special financial information (bank name, account number and balance, current transactions ...)
iv. In the event of impossibility to contact the "Supplier" by means of any agreed means of communication, it is necessary to refrain from asking the bank to make the transfer until confirmation of the instructions received or sent by email.
v. Take note that the bank will refrain from making the transfer or implementing any other instructions when its client cannot be contacted by any means of communication agreed upon to confirm the request for transfer by email.
vi. Make sure not to ship goods to the importing companies abroad before the payment instructions are confirmed by telephone or by one of the agreed means of communication.

vii. Ensure that insurance policies cover the risks associated with performing financial and banking transactions via email.

2. It is advisable, within the framework of daily operations, to follow the standard preventive measures below:

A. Use at least two email accounts:
- The first for all correspondence related to financial transfers with the bank while making sure not to mention it on the Business Card.
- The second for social media sites.

B. Refrain from responding to any incoming messages by email by clicking Reply, instead, choose Forward to select the email address from the Mailing List, since the name of the sender that appears in the email might not be actually theirs, but that of the hackers who created a similar email account. Any manipulation of the email could be uncovered by opening the Reply window (without using it) and checking the identity of the email sender.

C. When sending an email to multiple users, insert their email addresses in the BCC checkbox to prevent others from seeing them and trying to penetrate them.

D. Do not use a unified Password for more than one email or website. Use a strong password and constantly change it, while activating the Two-Step Verification option. The password must not include for example:
    - Simple samples on the keyboard, a sequence of numbers and letters, or repetitive letters, such as: AAAa, 1234, abcdef, QWERTY.
    - Words typed backwards such as [sdrawkcab = backwards].
    - Short, incomplete, or misspelled words such as [helo].
    - Repetitive short words such as [catcat].
    - Words preceded or followed by one character such as [apple3, %hello].
    - Personal information such as [birth date, name, surname].

E. Be aware of incoming emails including dubious attachments such as: exe, cox com, dll, scr, pif, shs, dif, vbs, bat, for they might contain malware.

F. Regularly update browser used on electronic devices.

G. Use the genuine Antivirus and regularly update it.

H. Activate the Recent Activity option of your email. In case of any doubt about this activity, immediately change password.

I. Never navigate through email for correspondence related to financial transfers with the bank via Public WIFI.

J. Save the data stored on the Mail Server for more than three months if possible.

K. Be aware of emails in which Real Time Transfer requests appear.

Corrective Measures upon Discovery of any Cybercrime or Attempt of Cybercrime

Upon detecting or being notified of a cybercrime or a cybercrime attempt, **the bank that performed the transfer should be immediately notified and provided with all relevant information to do the necessary the soonest possible.**

The following is also advised:

1. Communicate with the "Supplier" on the agreed upon contact numbers to notify him of the perpetration or attempted perpetration of cybercrimes and draw his attention to the necessity of contacting his clients by phone and letting them know that they may be subject to electronic cybercrime.
2. File a lawsuit before the competent judicial authorities and preserve all digital evidence and correspondence without deleting or altering them for they may be used in any investigation.
3. Change the password immediately.
4. Review all transactions with the "Supplier" to make sure that he was not previously subject to other cybercrimes, and advise the concerned bank of the result of this review.

الدليل الإرشادي الخاص بالأفراد والمؤسسات غير المالية للوقاية من القرصنة بواسطة 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. أي بريد الكتروني يختلف عن البريد الالكتروني العائد «للموّرد» (أي الشركة الموّردة أو المستوردة أو التاجر أو أي من مقدمي الخدمات الذين يجري التعامل معهم.)
2. اختلاف في عنوان البريد الالكتروني المنسوب إلى «الموّرد» لجهة حرف أو رقم أو رمز أو إشارة بحيث يتمّ مثلاً استبدال حرف «g» بحرف «q» إلخ.
3. أي بريد الكتروني منسوب «للموّرد» يدعي فيه المُرسِل (المُقرصن) انه تم تغيير رقم حساب «الموّرد» لأسباب وحجج غير مقنعة، منها على سبيل الذكر، إجراءات تدقيق تقوم بها السلطات الرقابية او الضريبية على حسابات «الموّرد» أو تدهور العلاقة مع المصرف (قد يكون مصرفاً أو مؤسسة مالية أو مؤسسة وساطة مالية) السابق بسبب العمولات المرتفعة.
4. أي بريد الكتروني يتضمن تعليمات بإرسال تحاويل إلى حساب مفتوح في الخارج بإسم مُشابه أو مُطابق لإسم «الموّرد» وانما برقم حساب جديد مختلف عن رقم حساب «الموّرد» المُعتمد بحسب المستندات المحفوظة لدى الفرد او لدى الشركة المعنية.
5. أي بريد الكتروني منسوب «للموّرد» يطلب فيه المرسل (المُقرصن) عدم الاتصال به («الموّرد») هاتفياً للتأكد من أي تعديل أو تغيير لجهة اسم المصرف المستفيد أو اسم المستفيد او رقم حسابه.
6. أي بريد الكتروني او اتصال هاتفي منسوب للمصرف او «للموّرد» او لغيره يطلب فيه المُرسِل معلومات محدّدة عن حسابات مصرفية او معلومات حسّاسة اخرى.
7. أي بريد الكتروني منسوب «للموّرد» ينطوي على:

- أخطاء لغوية غير عادية أو فاضحة.
- صياغة ولغة تختلفان عن المُراسلات السابقة.

8. الأحرف والأرقام 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. أي بريد الكتروني منسوب «للمورّد» موجه الى الشركة المُتلقية بشكل عام وليس الى الموظف الذي يتلقى عادة التعليمات من المورّد لتنفيذها.
11. أي بريد الكتروني منسوب «للمورّد» يتضمن تعليمات غير مشابهة للتعليمات السابقة.
12. أي 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. أي بريد الكتروني يتضمن رابط (Link) إلى موقع الكتروني

السياسات والإجراءات 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 أي 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 حسابينَ الكترونيين 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)

E. التنبّه للمُراسلات الواردة والمتضمنة مرفقات (Attachments) مشبوخة 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 أي 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)

الإجراءات 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 «الموّرد» 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 أي تعديل عليها لإمكانية استخدامها في أية تحقيقات.
3. تغيير فوري لكلمة المرور.
4. مراجعة العمليات كافة مع «الموّرد» للتأكد من عدم التعرض سابقاً لأفعال جرمية أخرى بالوسائل الالكترونية وإبلاغ المصرف المعني بنتيجة هذه المراجعة.