GUIDELINES FOR FIGHTING **FINANCIAL CYBERCRIMES**

CEDRUS BANK

INTRODUCTION

Financial cybercrimes are acts, attempted acts or actions, whether local or cross-border, committed with criminal intent, by individuals or organized groups in an attempt to violate banking accounts or financial and personal information using various electronic and technological methods. This crime encompasses for example, acts of fraud, theft, embezzlement, blackmail, sabotage, and spying using electronic means.

Each crime has specific characteristics and elements, and the persons concerned should pay attention to its indications and implement due diligence to identify and prevent them and take the necessary measures to fight them.

Below is a summary, by means of enunciation without limitation, of examples of criminal acts committed using the e-mail and which banks, financial instructions, financial mediation institutions (financial sector" (first type) or individuals and other non-financial institutions and authorities (second type) are subject to.

EXAMPLES OF CRIMINAL ACTS COMMITTED AGAINST INDIVIDUALS AND OTHER NON-FINANCIAL INSTITUTIONS AND AUTHORITIES

For the purpose of this exposition, the expression: "Company E-mail Compromise" shall mean hacking into the email of an individual, or a non-financial institution or authority. This type includes the following events (typology):

- Company Email Compromise – CEC1:
An unknown person (hacker) has unauthorized access to the email of the "supplier" (the supplying company, trader or any of the service providers that the client of the "financial sector" deals with, or creates a similar email and uses any of them to correspond with the client to request making a transfer to an account abroad or inside Lebanon supposedly in exchange for merchandise or a service provided by the "supplier" : or a company connected to it or employed by it.

For his part, the client corresponds with the bank, financial institution or financial mediation institution that he deals with to request a transfer from his account to the account specified in the alleged "supplier's" email or heads in person to the bank, financial institution or financial mediation institution to request filling a transfer form, and it later appears that the client was victim of cybercrimes.

- Company Email Compromise – CEC2:
An unknown person (hacker) has unauthorized access to the email of the client or creates a similar email and uses any of them to correspond with one of the "suppliers" that the client deals with to make a transfer from his account to an account abroad or inside Lebanon supposedly pertaining to the client or his company.
On his part, the "supplier" either corresponds with the bank, financial institution or financial mediation institution that the supplier deals with to request a transfer from one of his accounts to the specific account mentioned in the alleged client's correspondence, or one of his delegates heads in person to the bank financial institution or financial mediation institution to request filling a transfer form, and it later appears that the "supplier" was victim of cybercrimes.

- Company Email Compromise – CEC3:
An unknown person (hacker) has unauthorized access to the email of an executive manager at a company or creates a similar email (especially when this manager is absent due to travel) and uses any of them to correspond with branch managers or financial officials to request suspicious financial or banking transactions.
On his part, the manager concerned executes the banking or financial transaction and later appears to have been a victim of cybercrimes.

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 إلكترونية 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.
ونعرض فيما يلي، وبشكل مختصر وعلى سبيل المثال لا الحصر، نماذج عن الأفعال الجرمية بواسطة البريد الإلكتروني التي قد تتعرض لها المصارف أو المؤسسات المالية أو مؤسسات الوساطة المالية "القطاع المالي" (النوع الأول) أو الأشخاص وسائر المؤسسات والهيئات غير المالية (النوع الثاني).

نماذج أفعال جرمية واقعة على الاشخاص وسائر المؤسسات والهيئات غير المالية

لغاية هذا العرض يُعنى بعبارة Company Email Compromise اختراق البريد الإلكتروني العائد لأحد الأشخاص أو المؤسسات والهيئات غير المالية. يتضمن هذا النوع الحالات الموصوفة التالية Typology :

- انتهاك البريد الإلكتروني للشركة Company Email Compromise - CEC1 :
يقوم شخص مجهول الهوية (المقرصن) بالولوج غير المصرح به الى البريد الإلكتروني "للمورّد" (أي الشركة "المورّدة" أو التاجر أو أي من مقدمي الخدمات الذين يتعامل معهم عميل "القطاع المالي") او يقوم بإنشاء بريد الكتروني مشابه له وباستخدام أي منهما في مراسلة العميل لطلب اجراء تحويل الى حساب في الخارج او في لبنان يفترض أنه مقابل بضاعة او خدمة مقدمة من "المورّد" أو من شركة مرتبطة به أو تعمل لحسابه.
من جهته يقوم العميل اما بمراسلة المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية التي يتعامل مع أي منها لطلب اجراء التحويل من حسابه الى الحساب المحدد في المراسلة المنسوبة "للمورّد" أو بالتوجه شخصياً الى المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية لطلب تعبئة الاستمارة الخاصة بالتحاويل ويتبيّن لاحقاً ان العميل وقع ضحية أفعال جرمية بالوسائل الإلكترونية.

- انتهاك البريد الإلكتروني للشركة Company Email Compromise - CEC2 :
يقوم شخص مجهول الهوية (المُقرصن) بالولوج غير المصرح به الى البريد الإلكتروني للعميل او يقوم بإنشاء بريد الكتروني مشابه له وباستخدام أي منهما في مراسلة أحد "الموردين" الذي يتعامل مع العميل لطلب اجراء تحويل من حسابه الى حساب في الخارج او في لبنان يُفترض انه عائد للعميل او لشركته.
من جهته يقوم "المورّد" اما بمراسلة المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية الذي يتعامل مع أي منها لطلب اجراء التحويل من أحد الحسابات العائدة له الى الحساب المحدد في المراسلة المنسوبة للعميل، واما بقيام احد مندوبيه بالتوجه شخصياً الى المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية لطلب تعبئة الاستمارة الخاصة بالتحاويل ويتب يّ لاحقاً ان "المورّد" وقع ضحية أفعال جرمية بالوسائل الإلكترونية.

- انتهاك البريد الإلكتروني للشركة Company Email Compromise - CEC3 :
يقوم شخص مجهول الهوية (المُقرصن) بالولوج غير المصرح به إلى البريد الإلكتروني لمدير تنفيذي في احدى الشركات، أو يقوم بإنشاء بريد الكتروني مشابه له (بالأخص عند غياب هذا المدير بداعي السفر) وبإستخدام أي منهما في مراسلة مدراء فروع أو مسؤولين ماليين لطلب تنفيذ عمليات مالية أو مصرفية مشبوهة.
من جهته يقوم المدير المعني بتنفيذ العملية المصرفية او المالية ويتبيّن لاحقاً انه وقع ضحية أفعال جرمية بالوسائل الالكترونية.

- Email Compromise by Social Engineering:
For example, an unknown person (hacker) has unauthorized access to the email of a physical person or creates a similar email and uses any of them to correspond with the acquaintances, friends or relatives of the physical person or other persons while specifying an account for whoever wishes to support the person's need due to financial difficulty. The persons concerned make the transfers from their accounts to the specified account, and it later appears that they have been victims of cybercrimes.

- انتهاك البريد الإلكتروني عن طريق الهندسة الاجتماعية Social Engineering :
على سبيل المثال، يقوم شخص مجهول الهوية (المُقرصن) بالولوج غير المصرح به الى البريد الإلكتروني العائد لشخص طبيعي او بإنشاء بريد الكتروني مشابه له وبإستخدام أي منهما في مراسلة معارف الشخص الطبيعي او اصدقائه او اقربائه او آخرين مع تحديد حساب لكل من يرغب بدعم حاجات الشخص بسبب ضيق مالي. يقوم المعنيون بإجراء التحاويل من حساباتهم الى الحساب المحدد ليتبيّن لاحقاً انهم وقعوا ضحية أفعال جرمية بالوسائل الإلكترونية.

INSTRUCTIONS FOR INDIVIDUALS AND OTHER INSTITUTIONS AND NON-FINANCIAL AUTHORITIES

1. INDICATIONS OF CYBERCRIMES

Cybercrimes may take on different forms. The following indications, by way of example without limitation that may assist in discovering such crimes should be taken into account:

1. Difference in the email attributed to the "supplier" in one letter, number, code or sign whereas, for example, the letter "g" is replaced with "q".
2. Email attributed to the "supplier" in which the sender claims that the "supplier's" account number changed for many unconvincing reasons and pretexts, including audit procedures conducted by control or taxation authorities on the "supplier's" accounts, or the deterioration of the relation with the previous bank due to high commissions.
3. Email that includes instructions to send transfers to an account opened abroad under a name similar or identical to the "supplier's" name, but with a new account number different from the "supplier's" account number adopted according to the documents filed by the individual or the company concerned.
4. Email attributed to the "supplier" in which the sender requests not to contact the "supplier" via phone to validate any amendment or change in the name of the beneficiary bank, beneficiary financial institution or beneficiary financial mediation institution, or the name or account number of the beneficiary.
5. Email attributed to a bank, financial institution or financial mediation institution, in which the sender claims that the bank, financial institution or financial mediation institution is updating the file of one of their clients, and requests specific information in this concern.
6. Email attributed to the "supplier" which involves unusual or flagrant grammatical errors.
7. Email attributed to the "supplier" involving syntax and language different from previous correspondence.
8. The letters and numbers in the invoice attached in the suspicious email are not consistent in terms of size, format and color.
9. The transfer request attached on the suspicious email has a signature similar to the "supplier's" signature.
10. Email attributed to the "supplier" addressed to the recipient company in general and not to the officer who usually receives instructions from the "supplier" to execute them.
11. Email different from the "supplier's" email.
12. Email attributed to the "supplier" which includes instructions not similar to the previous instructions.
13. Email attributed to the "supplier" addressed to the individual/company in addition to a third party who is not related to the requested transfer.
14. The "supplier's" address is located in a country different from the one in which the beneficiary bank, beneficiary financial institution or beneficiary financial mediation institution operates.
15. Email attributed to the "supplier" or another person in which the sender requests information of banking and financial account and/or any other sensitive information.
16. Email that includes a link to a website that requests financial or personal information.

إرشادات للأشخاص وسائر المؤسسات والهيئات غير المالية

١. 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:

١. اختلاف في عنوان البريد الإلكتروني المنسوب إلى «المورّد» لجهة حرف أو رقم أو رمز أو إشارة بحيث يتمّ مثلاً استبدال حرف «g» بحرف «q» .
٢. 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.
٣. 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.
٤. 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.
٥. 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.
٦. بريد الكتروني منسوب «للمورّد» ينطوي على اخطاء لغوية غير عادية أو فاضحة.
٧. بريد الكتروني منسوب «للمورّد» ينطوي على صياغة ولغة تختلفان عن المُراسلات السابقة.
٨. الاحرف والارقام 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 الكتروني منسوب «للمورّد» موجه الى الشركة المُتلقية بشكل عام وليس الى الموظف الذي يتلقى عادة التعليمات من «المورّد » لتنفيذها.
١١. . بريد الكتروني يختلف عن البريد الإلكتروني العائد «للمورّد»
١٢. بريد الكتروني منسوب «للمورّد» يتضمن تعليمات غير مشابهة للتعليمات السابقة.
١٣. بريد الكتروني منسوب «للمورّد» ومُوجّه الى 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 الكتروني منسوب «للمورّد» او لغيره يطلب فيه المُرسل معلومات عن حسابات مصرفية ومالية و/او أي معلومات حساسة أخرى.
١٦. بريد الكتروني يتضمن رابط Link إلى موقع الكتروني يطلب معلومات مالية أو شخصية.

2. CYBERCRIMES PREVENTION POLICIES AND PROCEDURES

The following prevention measures should be adopted:

1. The client specifying more than one method of communication with all his "suppliers" to confirm the instructions sent by them before executing them (tel, fax, email, name of contact persons).
2. Contacting the "supplier" by phone on the numbers specified by him and registered in the records of the individual/company and not on the numbers mentioned in the email, for the purpose of confirming the components of the transfers in terms of the name of the beneficiary bank, beneficiary financial institution or beneficiary financial mediation institution and the beneficiary's name and account number, and the attached documents.
3. Not providing the "supplier" or any other party by email of any private financial information related to the name of the bank, financial institution or financial mediation institution that the individual/company deals with, the account number and balance and the transactions executed on it.
4. Being wary of the phone call or email that requests financial information under the pretext of updating the individual/company's personal and financial files.
5. Abstaining from replying to any received email by clicking on the "Reply" option and instead clicking on the "Forward" option to choose the email from the mailing list because the name of the sender which appears in the email may not be effectively his but to a hacker who created a similar email. Any manipulation in the email address can be detected by opening the "reply" option (without using it) and checking the identity of the sender.
6. Confirming all the details of the email and paying attention to any suspicious email of untrustworthy source similar to the "supplier's" email
7. When sending emails to many persons, the email addresses should be put in the BCC section so that third parties don't see and try to hack them.
8. In the event of inability to contact the "supplier" using any of the agreed upon communication methods, there should be abstention from asking the bank, financial institution or financial mediation institution to make the transfer until confirmation of the validity of the instructions received or sent by email.
9. Taking note that the bank, financial institution or financial mediation institution will abstain from making the transfer or executing any other instructions in the event of failure to contact the individual/company using any of the agreed upon communication methods to confirm the transfer request received by email.
10. The necessity of using at least two emails:
    - The first for all correspondence related to money transfers with the bank, financial institution or financial mediation institution and making sure it doesn't mention the Business Card.
    - The second dedicated for social media sites.
11. Not to use a unified password for more than one email or website. In addition, a strong password should be used and changed constantly with activation of two-step verification. For example, the password cannot contain the following:
    - Simple samples from the keyboard, a series of numbers, letters or repeated letters such as AAAa, 1234, abcdef, qwerty)
    - Words printed backwards, such as backwards=sdrawkcab.
    - Short, incomplete or false words such as "Helo".
    - Short consecutive words such as "Catcat".
    - Words preceded or followed by one code such as "%hello, Apple3"
    - Personal information (date of birth, name, surname)
12. Being wary of incoming correspondence that include suspicious attachments such as: pif, shs, dif, vbs, bat, exe, com, cox, dll, scr, for containing potential malware.
13. Updating the browser used on electronic devices regularly.
14. Using the original version of the anti-virus and updating it constantly.
15. Activating the email's "Recent Activity" feature. In the event of any suspicion around this activity, the password should be changed immediately.
16. Being wary of browsing the email over a public Wi-Fi.
17. Keeping the information stored on a Mail Server for more than 3 months if possible.

٢. السياسات والاجراءات الوقائية من الافعال الجرمية

يقتضي اتباع الخطوات الوقائية التالية :

١. تحديد العميل لاكثر من وسيلة تواصل مع «مورّديه » كافة للتأكد من التعليمات الواردة منهم قبل تنفيذها رقم الهاتف، رقم الفاكس، البريد الإلكتروني، اسم الشخص الذي يمكن التواصل معه
٢. التواصل هاتفياً مع «المورّد» على الارقام المحدّدة من قبله والمدونة في سجلات الفرد/الشركة وليس على الأرقام الواردة في البريد الإلكتروني وذلك للتثبت من مكوّنات التحويل لجهة اسم المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة واسم المستفيد ورقم حسابه والمستندات المرفقة.
٣. عدم تزويد «المورّد» او اي طرف آخر عبر البريد الإلكتروني 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.
٤. التنبّه للاتصال الهاتفي او للبريد الإلكتروني الذي يطلب معلومات مالية بحجّة تحديث الملفات الشخصية والمالية العائدة للفرد/الشركة.
٥. الامتناع عن الردّ على اية مُراسلة واردة بالبريد الإلكتروني عبر الضغط على اختيار (Reply) واستبداله بالضغط على اختيار (Forward) لانتقاء عنوان البريد الإلكتروني من قائمة العناوين (Mailing list) لأن اسم المرسل الظاهر في البريد الإلكتروني 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 الإلكتروني.
٦. التأكد من كامل تفاصيل عنوان البريد الإلكتروني والانتباه إلى أي بريد الكتروني مشكوك وغير موثوق المصدر مشابه لبريد «المورّد»
٧. عند ارسال رسائل إلكترونية لعدة أشخاص يجب وضع عناوين البريد الإلكتروني في خانة (BCC) لكي لا يطّلع عليها الغير ويحاول إختراقها.
٨. 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 الإلكتروني.
٩. 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.
١٠. 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.
١١. عدم استخدام كلمة مرورPassword 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
١٢. التنبّه للمُراسلات الواردة والمتضمنة مرفقات Attachments مشبوهة مثل: scr, dll, cox, com, exe, bat, vbs, dif, shs, pif لإمكانية إحتوائها برامج خبيثة.
١٣. تحديث المتصفّح Update Browser المستعمل على الاجهزة الالكترونية بشكل منتظم.
١٤. استعمال برنامج أصلي لمكافحة الفيروسات Antivirus وتحديثه باستمرار.
١٥. تفعيل خاصية النشاط الحديث Recent Activity للبريد الإلكتروني. في حال وجود اي شك حول هذا النشاط، يجب على الفور تغيير كلمة المرور.
١٦. التنبّه من تصفّح البريد الإلكتروني من خلال Public WIFI
١٧. الإحتفاظ بالمعلومات المخزنة على Mail Server لأكثر من ثلاثة اشهر إذا أمكن.

18. Abstaining from shipping goods to importing companies abroad prior to confirming the validity of payment instructions by phone using one of the agreed upon communication methods.
19. Ensuring that insurance policies cover risks associated with the execution of financial and banking transactions via email.
20. Being wary of the email that contains a Real Time Transfer request.

3. CORRECTION MEASURES

Upon discovering, knowing or being informed of the occurrence of cybercrimes, fast and effective measures should be taken, including at least the following:

1. Advising the bank, financial institution or financial mediation institution concerned immediately and providing them quickly with all the relevant information to conduct the necessary.
2. Communicating with the "Supplier" on the adopted contact numbers to notify him of the perpetration or attempted perpetration of cybercrimes and drawing his attention to the necessity of contacting his clients by phone and letting them know that they may be subject to electronic hacking.
3. Filing a lawsuit before the competent judicial authorities and keeping all digital evidence.
4. Changing the password immediately.
5. Making sure to preserve email correspondence without deleting or altering them for the possibility of using them in any investigation.
6. It is better to go over all transactions with the "supplier" to make sure that he was not previously subject to other cybercrimes, and advising the bank, financial institution or financial mediation institution concerned of the result of this review.

In conclusion, all stakeholders in fighting cybercrimes should be advised to conduct periodic follow ups of the international developments and guidelines and Best Practices relevant to the matter for the purpose of updating and improving the adopted procedures to put an end to this crime

١٨. الامتناع عن شحن السلع الى الشركات المستوردة في الخارج قبل تأكيد صحة تعليمات الدفع هاتفياً بإحدى طرق الاتصال المتفق عليها.
١٩. التأكد من ان 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

٣. الاجراءات التصحيحية

لدى اكتشاف او علم او تبلّغ وقوع أفعال جرمية بالوسائل الإلكترونية فانه يقتضي اتخاذ إجراءات سريعة وفعّالة تشمل على الأقل ما يلي:

١. ابلاغ 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 لابلاغه بحصول أو محاولة حصول أفعال جرمية بالوسائل الإلكترونية ولفت نظره إلى ضرورة مراجعة عملائه هاتفياً وأعلامهم باحتمال تعرّضهم لأفعال قرصنة إلكترونية.
٣. التقدّم بشكوى امام المراجع القضائية المختصة والمحافظة على الأدلة الرقميّة كافة.
٤. تغيير فوري لكلمة المرور.
٥. الحرص على الاحتفاظ بالمُراسلات الجارية على البريد الإلكتروني دون إلغائها او إجراء اي تعديل عليها نظرا لإمكانية استخدامها في اية تحقيقات.
٦. 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.