Information Security Awareness Guidelines

Cyber security is the common responsibility of each and every stakeholder, including our clients. You play a key role in safeguarding the sensitive information related to our services.

The following Table helps to remind us of the action we must take to remain vigilant.

DO's	DON'Ts
Do: - Use hard to guess passwords or phrases. - Use a strong password that should have at least 8 characters using combination of alphanumeric, uppercases, lowercases letters, and special characters. - Use different passwords for different accounts. - Keep your passwords confidential - Use two factors authentication (2FA) when available (Password + SMS) to login into your electronic accounts.	**Do not:** - Use easy passwords like: Numbers from 1 to 8, your birthday, your name, (wife / husband/ children names). - Share your passwords with other people, including your colleagues or employees. - Use the same password across all your platforms and services (e.g. Email / Social Media / Online Banking).
Do: Pay attention to phishing traps in emails like: - Fake emails: Changing similar letters in the email address to trick the user (I / L) (g /q) (0 /O). - Rogue attachment (infected) - Fake email Links to un-trusted websites	**Do not:** - Open email attachment from un-trusted sources. - Open email attachments: scr, dll, com, exe - Do not click on links from unknown or un-trusted sources, attackers use them to trick you into visiting malicious websites.
Do: - Make sure that you have a reputable working and updated antivirus installed on your computer. - Make sure that you install the latest updates for your operating system and your browser to avoid being vulnerable to attacks. - Retain email Data for more than 3 months for reference and evidence.	**Do not:** - Install unauthorized programs on your PC - Install Pirated / Cracked Applications (software) because it might contain malicious codes. - Use the "SAVE Password" option provided by browsers to store your passwords. - Use the Wireless internet provided in coffee shops etc... to access your confidential accounts. - Turn on auto delete messages older than 3 months
Do: - provide the bank with more than one way to contact you (e.g. telephone: mobile and landline) - Allow the bank to confirm transfer requests via phone conversations. **Note that the bank will refrain from executing instructions if they fail in contacting the client and validating the information received.**	**Do not:** - Act so sure, always double check with the bank's related officers about the details of the transaction. - Hackers tend to modify instructions in the request you sent to the bank to redirect the transactions to another beneficiary.
Be smart on social media, what you post on social media can give cybercriminals information about your behavior, your preferences, your location and the activities which can be easily abused.	**Do not:** Use the same email address for social media and for formal business transactions

If you discover an actual or even an attempt of a cybercrime, you should:

1. Directly and promptly, inform the bank enabling the initiation of a corrective action. (followed by Written Claim)
2. Present a legal case as per Lebanese law. (Cyber Crimes Repression and Intellectual Property Protection Bureau)
3. Don't delete the evidence (Digital evidences: email, chat communications and logs)
4. Change your password.

01-957857

فينيسيا بنك

الدليل الارشادي للوقاية من الأفعال الجرمية الإلكترونية

الأمن السيبراني هو مسؤولية تقع على عاتق الجميع، بما في ذلك عملائنا، وإن إخلال اي طرف بدوره قد يعرض الجميع للخطر. فيما يلي جدولا» بأهم الإجراءات التي يمكن إتخاذها للوقاية من الوقوع ضحية للأفعال الجرمية الإلكترونية

الالتزام:	الامتناع:
ـ استخدم كلمة مرور قوية يصعب إكتشافها - يجب ألا تقل كلمة مرور عن ثمانية رموز: من احرف وارقام ، مستخدماً الأحرف اللاتينية (الكبرى والصغرى) بالإضافة الى الرموز # $ ٪. - استعمل كلمات مرور مغايرة لمختلف الحسابات، والحفاظ على سريتها. - اعتمد تقنية تعتمد على وسيلتين للمصادقة على كلمة السر (كلمة المرور + رسالة قصيرة على هاتفك)، للولوج الى حسابك الإلكتروني.	ـ عدم استخدام كلمة مرور بسيطة مثالا»: معلومات شخصية (اسمك، تاريخ ميلادك) - لا تفصح بكلمة المرور الخاصة بك لأي شخص آخر بما في ذلك زملاءك في العمل. - لا تستعمل كلمة السر نفسها للولوج الى عدة حسابات (بريد الإلكتروني، وسائل التواصل الاجتماعي، الخدمة المصرفية الإلكترونية)
ضرورة التيقظ للرسائل الوهمية التي تهدف للتضليل والحصول على بياناتك الخاصة مثال : - اختلاف في عنوان البريد الإلكتروني لجهة حرف فقط أو رقم مثلا: (٠ مكان o / 1 l L) لغاية استنساخ شخصية الجهة المرسلة. ـ الضغط على مرفقات تحتوي على فيروسات. ـ الولوج الى مواقع الكترونية الغير موثوق بها.	ـ تجنب فتح المرفقات المشبوهة المستلمة بواسطة البريد الإلكتروني من أشخاص غير موثوق بهم. - التنبّه للمُراسلات الواردة والمتضمنة مرفقات مشبوهة مثل: scr, dll, com, exe, لإمكانية احتوائها برامج خبيثة. - عدم الضغط على الروابط الواردة عبر البريد الالكتروني من أشخاص غير موثوقين.
ـ قم بتحديث مكافحة الفيروسات المثبتة على جهاز الكمبيوتر الخاص بك بشكل مستمر. - استعمل برنامج أصلي لمكافحة الفيروسات (غير مقرصن) - قم بتحديث المتصفح (Browser) المستعمل على جهازك ونظام التشغيل الخاص بك، لتجنب التعرض للهجمات. - احتفظ بالمعلومات المخزنة على (Mail Server) لأكثر من ثلاثة أشهر إذا أمكن لغاية استخدامها كمرجع ودليل قانوني.	ـ عدم تنزيل أو استخدام برامج مقرصنة أو غير موثوقة لإمكانية احتواءها على فيروسات تعطي المقرصن إمكانية التحكم بالحاسوب. - عدم الاستفادة من خاصية حفظ كلمة المرور التي يقترحها المتصفح. - تجنب استعمال (Public Wi-Fi) شبكات الإنترنت العامة للولوج الى حساباتك الخاصة. - عدم استخدام خاصية المسح التلقائي للرسائل الالكترونية.
-. الحرص على توافر أكثر من وسيلة للاتصال مع المصرف. - أطلب من المصرف تأكيد طلبات التحويل عبر المحادثة الهاتفية. **ملاحظة: سيمتنع المصرف عن إجراء التحويل أو تنفيذ اية تعليمات اخرى عندما يتعذر الاتصال بالعميل بأية وسيلة من وسائل الاتصال المتفق عليها لتأكيد طلب إجراء التحويل الوارد عبر البريد الإلكتروني.**	ـ عدم الأخذ بالمعلومات الواردة عبر الوسائل الالكترونية حول العملية المراد تنفيذها وإعادة التأكد من صحتها قبل طلب تنفيذها (عبر الهاتف مثلا») على سبيل المثال: «المقرصن قد يتمكن من تغيير المستفيد من الحوالة دون تغير المعطيات الأخرى كي لا يثير الشك بصحة العملية.»
ـ كن حذر على مواقع التواصل الاجتماعي، فالمعلومات التي يتم تداولها قد يتم استغلالها وإساءة استعمالها من قبل الجهات المتربصة.	ـ عدم استخدام البريد الإلكتروني الخاص بعملك، للولوج الى مواقع التواصل الاجتماعي، او لأي تطبيقات أخرى غير مهنية.

لدى اكتشافك أو علمك أو تبلغك بوقوع أفعال جرمية بالوسائل الإلكترونية فإنه يقتضي اتخاذ إجراءات سريعة وفعّالة تشمل التالي:

١. إبلاغ المصرف أو المؤسسة المالية المعنية فورا» وتزويده على وجه السرعة بالمعلومات كافة ذات الصلة لإجراء المقتضى.

٢. التقدم بشكوى أمام المراجع القضائية المختصة (مكتب مكافحة الجرائم الإلكترونية).

٣. الحرص على الاحتفاظ بالمراسلات الجارية على البريد الإلكتروني دون إلغائها أو إجراء أي تعديل عليها نظرا» لإمكانية استخدامها في أية تحقيقات.

٤. تغيير فوري لكلمة المرور.

01-957857

مكافحة الجريمة الإلكترونية المالية في لبنان

الدليل الإرشادي للوقاية من الأفعال الجرمية بواسطة البريد الإلكتروني

جمعية المصارف في لبنان

مصرف لبنان
BANQUE DU LIBAN

بالتعاون مع
الاقتصاد والأعمال
Al-Iktissad Wal-Aamal

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 الكترونية 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 الالكتروني 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).

الجزء الثاني:
إرشادات للأشخاص وسائر المؤسسات والهيئات غير المالية

1. 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:

1. اختلاف في عنوان البريد الالكتروني المنسوب إلى «المورّد» لجهة حرف أو رقم أو رمز أو إشارة بحيث يتمّ مثلاً استبدال حرف «g» بحرف «q».
2. 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.
3. 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.
4. 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.
5. 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.
6. بريد الكتروني منسوب «للمورّد» ينطوي على اخطاء لغوية غير عادية أو فاضحة.
7. بريد الكتروني منسوب «للمورّد» ينطوي على 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 مشابهاً لتوقيع «المورّد».
10. بريد الكتروني منسوب «للمورّد» موجه الى الشركة المُتلقية بشكل عام وليس الى الموظف الذي يتلقى عادة التعليمات من «المورّد» لتنفيذها.

11. بريد الكتروني يختلف عن البريد الالكتروني العائد «للمورّد».
12. بريد الكتروني منسوب «للمورّد» يتضمن تعليمات غير مشابهة للتعليمات السابقة.
13. بريد الكتروني منسوب «للمورّد» ومُوجّه الى الفرد/الشركة بالإضافة إلى طرف ثالث لا علاقة له بالتحويل المطلوب تنفيذه.
14. عنوان «المورّد» يقع في دولة تختلف عن تلك التي يعمل فيها المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة.
15. بريد الكتروني منسوب «للمورّد» او لغيره يطلب فيه المُرسل معلومات عن حسابات مصرفية ومالية و/او أي معلومات حساسة أخرى.
16. بريد الكتروني يتضمن رابط (Link) إلى موقع الكتروني يطلب معلومات مالية أو شخصية.

2. السياسات والاجراءات الوقائية من الافعال الجرمية

يقتضي اتباع الخطوات الوقائية التالية :

1. تحديد العميل لاكثر من وسيلة تواصل مع «مورّديه» كافة للتأكد من التعليمات الواردة منهم قبل تنفيذها (رقم الهاتف، رقم الفاكس، البريد الالكتروني، اسم الشخص الذي يمكن التواصل معه).
2. التواصل هاتفياً مع «المورّد» على الارقام المحدّدة من قبله والمدونة في سجلات الفرد/الشركة وليس على الأرقام الواردة في البريد الالكتروني وذلك للتثبت من مكوّنات التحويل لجهة اسم المصرف المستفيد أو المؤسسة المالية المستفيدة أو مؤسسة الوساطة المالية المستفيدة واسم المستفيد ورقم حسابه والمستندات المرفقة.
3. عدم تزويد «المورّد» او اي طرف آخر عبر البريد الالكتروني 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.
4. التنبّه للاتصال الهاتفي او للبريد الالكتروني الذي يطلب معلومات مالية بحجّة تحديث الملفات الشخصية والمالية العائدة للفرد/الشركة.
5. الامتناع عن الردّ على اية مُراسلة واردة بالبريد الالكتروني عبر الضغط على اختيار (Reply) واستبداله بالضغط على اختيار (Forward) لانتقاء عنوان البريد الالكتروني من قائمة العناوين (Mailing list) لأن اسم المرسل الظاهر في البريد الالكتروني 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 الالكتروني.
6. التأكد من كامل تفاصيل عنوان البريد الالكتروني والانتباه إلى أي بريد الكتروني مشكوك وغير موثوق المصدر مشابه لبريد «المورّد».

7. عند ارسال رسائل إلكترونية لعدة أشخاص يجب وضع عناوين البريد الإلكتروني في خانة (BCC) لكي لا يطّلع عليها الغير ويحاول إختراقها.
8. 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 الالكتروني.
9. 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.
10. 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.
11. 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)
12. التنبّه للمُراسلات الواردة والمتضمنة مرفقات (Attachments) مشبوهة مثل:
    (scr, dll, cox, com, exe, bat, vbs, dif, shs, pif) لإمكانية إحتوائها برامج خبيثة.
13. تحديث المتصفّح (Update Browser) المستعمل على الاجهزة الالكترونية بشكل منتظم.
14. استعمال برنامج أصلي لمكافحة الفيروسات (Antivirus) وتحديثه باستمرار.
15. تفعيل خاصية النشاط الحديث (Recent Activity) للبريد الالكتروني. في حال وجود اي شك حول هذا النشاط، يجب على الفور تغيير كلمة المرور.

16. التنبّه من تصفّح البريد الالكتروني من خلال (Public WIFI).
17. الإحتفاظ بالمعلومات المخزنة على (Mail Server) لأكثر من ثلاثة اشهر إذا أمكن.
18. الامتناع عن شحن السلع الى الشركات المستوردة في الخارج قبل تأكيد صحة تعليمات الدفع هاتفياً بإحدى طرق الاتصال المتفق عليها.
19. التأكد من ان بوالص التأمين تغطّي المخاطر المرتبطة بتنفيذ عمليات مالية ومصرفية عبر البريد الإلكتروني.
20. التنبه من البريد الالكتروني الذي يرد فيه طلب تنفيذ فوريّ للتحويل (Real Time Transfer).

3. الاجراءات التصحيحية

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

1. ابلاغ المصرف أو المؤسسة المالية أو مؤسسة الوساطة المالية المعني فوراً وتزويده على وجه السرعة بالمعلومات كافة ذات الصلة لإجراء المقتضى.
2. 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.
3. التقدّم بشكوى امام المراجع القضائية المختصة والمحافظة على الأدلة الرقميّة كافة.
4. تغيير فوري لكلمة المرور.
5. الحرص على الاحتفاظ بالمُراسلات الجارية على البريد الالكتروني دون إلغائها او إجراء اي تعديل عليها نظرا لإمكانية استخدامها في اية تحقيقات.
6. 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.

مكافحة الجريمة الإلكترونية المالية في لبنان

الدليل الإرشادي للوقاية من الأفعال الجرمية بواسطة البريد الإلكتروني