مصرف ليبيا المركزي

ص.ب 1103 العنوان البرقي : مصرفليبيا - طرابلس - ليبيا

المنشور إ ر م ن رقم (12 /2024)
التاريخ: 26 ذو القعدة 1445 هـ
الموافق: 2024/6/3

السادة/ رؤساء مجالس الإدارة بالمصارف

السادة / المدراء العامين بالمصارف

بعد التحية ،،،

الموضوع: " تعليمات خاصة بمكافحة قرصنة البريد الإلكتروني و الجريمة المالية الإلكترونية "

في إطار متابعة إدارة الرقابة على المصارف والنقد لأوضاع المصارف العاملة بليبيا وعلى الدور الإشرافي والرقابي الذي يُمَارِسهُ مصرف ليبيا المركزي على كافة المصارف العاملة بليبيا.

وتأسيساً على المنشور أ ر م ن رقم (2018/5) المؤرخ في 13 يونيو 2018، الذي أُحِيلَ بِمُوجَبِهِ منشور السيد/ مُحافظ مصرف ليبيا المركزي رقم (1) لسنة 2018، بشأن ضوابط تطبيق قانون مُكافحة غسل الأموال و تمويل الإرهاب.

وإلى المنشور أ ر م ن رقم (2021/02) المؤرخ في 08 سبتمبر 2021، بشأن تعميم دليل حوكمة عمل وحدات الامتثال بالمؤسسات المالية.

عليه نحيل إليكم التعليمات الخاصة بمكافحة قرصنة البريد الإلكتروني و الجريمة المالية الالكترونية ، للعمل بها و إعداد السياسات اللازمة وإتخاذ الإجراءات والتدابير الوقائية من الأفعال الإجرامية بالوسائل الالكترونية .

والسلام عليكم ،،،

ناجي محمد عيسى
مُدير إدارة الرقابة على المصارف والنقد

صورة للسيد/ المحافظ
صورة للسيد/ نائب المحافظ
صورة للسيد/ مدير وحدة المعلومات المالية الليبية – مصرف ليبيا المركزي
صورة للسيد/ مدير إدارة المدفوعات و التسويات – مصرف ليبيا المركزي
صورة للسيد/ مدير إدارة تقنية المعلومات – مصرف ليبيا المركزي
صورة للسيد/ مدير إدارة أمن المعلومات – مصرف ليبيا المركزي
صورة للسيد/ مدير إدارة العمليات المصرفية – مصرف ليبيا المركزي
صورة للسيد/ نائب مدير إدارة الرقابة على المصارف والنقد لشؤون الرقابة المكتبية ومتابعة الامتثال
صورة للسيد/ نائب مدير إدارة الرقابة على المصارف والنقد لشؤون التفتيش
صورة للسيد/ نائب مدير إدارة الرقابة على المصارف والنقد لشؤون الصيرفة الاسلامية
صورة للسيد/ نائب مدير إدارة الرقابة على المصارف والنقد للشؤون المصرفية - بنغازي
صورة للسادة مدراء وحدات الامتثال بالمصارف
قسم المتـــــــــابعة المصرفية ومراقبة الامتثال

ن . ايجاد / منشور 2024

مصرف ليبيا المركزي
إدارة الرقابة على المصارف والنقد

تعليمات خاصة بمُكافحة قرصنة البريد الإلكتروني والجريمة المالية الإلكترونية

تعريفات:

المصطلح	التعريف
الجريمة الإلكترونية المالية:	هي فعل أو مُحاولة فعل أو أفعال، محلية أو عابرة للحدود، صادرة بإرادة إجرامية عن أفراد أو مجموعات منظمة بهدف انتهاك الحسابات المصرفية أو المعلومات المالية والشخصية عبر إستخدام وسائل الكترونية وتقنية عدة. يدخل ضمن نطاق هذه الجريمة مثلاً عمليات الإحتيال والسرقة والإختلاس والإبتزاز والتخريب والتجسس بالوسائل الإلكترونية، وتتميز كل جريمة بخصائص وعناصر محددة مما يوجب على المعنيين التنبه للمؤشرات التي تدل عليها وتطبيق إجراءات العناية الواجبة للتعرف عليها وتجنب حدوثها واتخاذ التدابير اللازمة لمكافحتها.
قرصنة البريد الالكتروني:	هي عملية اختراق تستهدف حسابات المؤسسة المالية للوصول إلى المعلومات الشخصية من خلال استخدام تقنيات متطورة مثل الصيد الاحتيالي **(Phishing)** أو البرمجيات الخبيثة **(Malware)** ، مما يمكنهم من قراءة رسائل البريد الإلكتروني وسرقة المعلومات الحساسة أو إرسال طلبات تحويل أموال او تعديل ببيانات دون معرفة صاحب البريد الالكتروني.

على المؤسسة المالية الإلتزام بإعداد سياسات و إتخاذ تدابيروإجراءات وقائية من الافعال الإجرامية بالوسائل الإلكترونية على ان تتضمن بالحد الأدنى التدابيروالإجراءات المذكورة ادناه.

أ. الإجراءات الإحترازية: يقتضي اتباع الإجراءات الاحترازية التالية عند طلب العميل تنفيذ عملية تحويل من حساباته: -

1. مُراقبة العمليات المطلوب تنفيذها ومقارنتها مع طبيعة نشاط العميل المصرّح عنه في نموذج اعرف عميلك KYC وعلى الجهة التحقق من انها متطابقة مع ملف العميل وحركة نشاطه وعملياته.
2. مُراقبة موضوع التحويل ووجهته لجهة الدول المُرسل اليها ومراجعة اسماء المستفيدين من التحويل وارقام حساباتهم مقارنة مع تعاملات العميل السابقة ان وجدت.
3. الإنتباه لأي طلب تحويل مشبوه عبر البريد الإلكتروني خاصةً إذا تبين انه غير متوافق مع أنشطة العميل او مع العمليات التي تجري عادةً على حساب العميل للجهة (قيمتها وموضوعها ووجهتها).

4. إعتماد سياسة تفرض على المسؤولين في المؤسسة المالية عدم تنفيذ أي تحويل تفوق قيمته مبلغاً معيناً تحدده المؤسسة المالية، قبل التأكد بوسائل معزّزة من صحة التعليمات الواردة بواسطة البريد الإلكتروني.

5. يقتضي على المؤسسة المالية التحقق من ان نموذج فتح الحساب للعملاء يتضمن إجراءات التحقق من تنفيذ طلبات العملاء لتحويل الاموال بواسطة البريد الالكتروني.

6. على المصارف تنبيه العملاء بشكل دائم، وإعلامهم عن المخاطر الناتجة عن استخدام البريد الالكتروني لإجراء الحوالات وتوجيههم لاستعمال وسائل اخرى أكثر اماناً، والحصول على موافقة خطية من العميل على تحمّل هذه المخاطر.

7. اعتماد وسيلة تواصل موثوقة أخرى متفّق عليها غير البريد الالكتروني للتأكد من صحّة التعليمات الواردة بواسطة البريد الإلكتروني، والاحتفاظ بالمعلومات والمُراسلات والأدلّة كافة المُثبتة للاتصال أو محاولة الاتصال بالعميل.

8. على المؤسسات المالية التحقق من طلبات تحويل الاموال المُقدّمة من العميل سواء شخصيا او المُرسلة من بريده الالكتروني التي تتضمن رقم حساب جديد او تعليمات تحويل جديدة ومختلفة عن تعاملاته السابقة.

9. على المؤسسات المالية الانتباه لطلبات تحويل الاموال المُقدّمة من العميل شخصياً او المُرسلة من بريده الالكتروني التي تتضمن اسم مستفيد جديد ينوي عميل المؤسسة المالية التعامل معه لأول مرة.

10. على المؤسسات المالية التحقق من كل طلب تحويل وارد عبر البريد الالكتروني أنه عائد فعلاً للعميل وأنه لم يتم تحريفه بإضافة حرف او رقم او رمز او اشارة، وفي حال اكتشاف أي تغيير يقتضي عدم تنفيذ طلب التحويل وابلاغ العميل وفقا لوسائل التواصل المعتمدة.

11. على المؤسسة المالية إعادة الاتصال بالعميل في حال بادر من تلقاء نفسه لتأكيد التحويل وذلك لتفادي أي محاولات قرصنة تمت على رقم هاتف العميل، ويجب على المؤسسة المالية إرسال رسالة نصية SMS إلى هاتف العميل لإبلاغه بتنفيذ التحويل، أو إبلاغه بأنها حاولت الاتصال به لتأكيد عملية التحويل لغرض تنفيذها، وفي حال إستجابة العميل يجب على المؤسسة المالية مطالبة العميل بتزويدها بجميع التفاصيل التالية المتعلقة بالتحويل المطلوب تنفيذه بواسطة البريد الإلكتروني :.

- الرصيد الحالي لحساب العميل.
- رقم حساب المستفيد.
-الاسم الكامل للمستفيد.
- البلد المُرسل اليه.
- المصرف المُرسل اليه.

12. في حال تعذّرالإتصال بالعميل بأية وسيلة من وسائل الاتصال المتفق عليها فإنه يقتضي الامتناع عن اجراء التحويل وفقاً للتعليمات الواردة بنموذج فتح الحساب، لحين التأكد من صحة البيانات الواردة او المرسلة بالبريد الالكتروني، ويقع على عاتق المؤسسة المالية في هذه الحالة توثيق الاتصال أو محاولات الاتصال بالعميل بجميع الوسائل والاحتفاظ بها كإثبات.

13. على المؤسسة المالية عند علمها بوقوع احد عملائها ضحية احتيال مالي الكتروني القيام بالإجراءات التالية :.

- الاتصال بالمصرف المُراسل وتزويده بالتفاصيل الضرورية ومطالبته بتجميد قيمة التحويل وإعادته في حال كان لا يزال في حساباته ، وفي حال تعذّر القيام بذلك عليه ابلاغ المصرف المستفيد بواقعة الاحتيال ومطالبته بإعادة قيمة التحويل الى المصرف المُراسل تمهيداً لإعادته الى حساب العميل الذي تعرض لعملية الاحتيال.
- على المؤسسة المالية في هذه الحالة ارسال بلاغ الى وحدة المعلومات المالية يتضمن كافة الوقائع والمستندات اللازمة والإجراءات المتخذة من قبل المؤسسة المالية في هذا الشأن، على ان يتضمن البلاغ أيضا المعلومات التقنية المتعلقة بما يلي :.

- مصدر البريد الإلكتروني (IP Address) المنسوب للعميل أو الذي تم من خلاله ارسال طلبات الحوالات المشبوهة.
- اسم الشركة مقدمة خدمة الانترنت التي تم من خلالها ارسال طلبات الحوالات المشبوهة.
- اسم الشركة مقدمة خدمة الانترنت المستخدمة للدخول غير المصرح به الى حساب العميل عن طريق خدمة العمليات المصرفية الالكترونية (Electronic Banking) .

- توجيه العميل الى اتخاذ الإجراءات القضائية المناسبة وتقديم شكوى الى الجهات الأمنية.
- تصنيف حساب العميل على انه مرتفع المخاطر، وتطبيق إجراءات العناية المعززة على الحساب وعدم تنفيذ اية عمليات سحب او تحويل من الحساب قبل اتخاذ إجراءات التحقق من كافة التفاصيل والتواصل مع العميل وفقا لوسائل الاتصال المعتمدة.

14. على المؤسسة المالية التأكد من الجهة المسؤولة عن امن المعلومات في المؤسسة المالية وهل لديها خبرات كافية للتحقق من مصدر البريد الالكتروني الوارد من العميل واعتماد قاعدة بيانات بمصادر العناوين المشبوهة، وفي حال الشكّ بمصدر أي بريد إلكتروني، يقتضي مراجعة الجهة المسؤولة عن أمن المعلومات في المؤسسة المالية أو أية جهة أخرى تقوم بهذا الدور، بهدف التحقق التقني منه و لمقارنته مع العناوين الإلكترونية المشتبه بها بأنها سبق وأن أُستعملت لإرتكاب أفعال إجرامية .

15. على المؤسسات المالية تزويد إدارة الرقابة على المصارف والنقد سنويا بكافة الإجراءات والسياسات المتخذة من قبلها في سبيل مكافحة الجرائم المالية الالكترونية، بالإضافة الى تقييم المخاطر المعد من قبل هذه المؤسسات وإجراءات الحد من هذه المخاطر.

16. على المؤسسة المالية الإنتباه إلى الأمور الاتية :

. التأكيد على العميل عند حضورة وقبل تعبئة الاستمارة الخاصة بالتحويل الاتصال بالمورد او المستفيد من التحويل هاتفيا على الرقم المحدد من قبله و المدون في سجلاته للتأكد من تفاصيل التحويل فبل إجراء اي تعديل للجهة " سواء اسم المصرف المستفيد، أو المؤسسة المالية المستفيدة ،او اسم المستفيد، أو رقم حسابه.

- مراجعة العميل عند وجود أدنى شك في المستندات المرفقة بالبريد الإلكتروني وذلك قبل اجراء التحويل المطلوب.
- تطبيق اجراءات العناية الواجبة المعزّزة فيما يخص التحويلات الإلكترونية خاصة في حال وجود شك بارتكاب أفعال إجرامية بالوسائل الإلكترونية، ويطلب من العميل مراجعة المستفيد من التحويل هاتفياً على الرقم المحدد من قبله والمدوّن في سجلات العميل وليس على الرقم الوارد في البريد الإلكتروني وذلك للتثبّت من بيانات التحويل للمؤسسة المالية المستفيدة (اسم المستفيد ورقم حسابه) .
- الزام الموظفين بالامتناع عن إعطاء أية معلومات عن العملاء عبر البريد الالكتروني أوعن ارقام حساباتهم وارصدتها.
- الامتناع عن الرد على اية مراسلة واردة بالبريد الالكتروني وذلك عبر الضغط على الاختيار (**Reply**) إنما يقتضي الضغط على الاختيار (**Forward**) وإعادة كتابة الاسم والعنوان الإلكتروني المُبلّغ للمؤسسة المالية من قبل العميل.
- توجيه نسخة من المراسلة بين المؤسسة المالية والعميل الى شخص آخر مسؤول في المؤسسة المالية لضمان ازدواجية المراقبة.
- التأكد من ان بوالص التأمين تغطّي المخاطر المرتبطة بالتحويلات المالية بواسطة البريد الإلكتروني.
-

ب- **إجراءات وقائية:** يقتضي اتباع الإجراءات الوقائية التالية والتي تشمل :

1. اعتماد قواعد صارمة لجهة تفحص (**Filtering**) البريد الإلكتروني الوارد وضبط الوصول إلى البريد الإلكتروني من خارج المؤسسة المالية وحصره بموظفين معينين.
2. تحديث انظمة اجهزة الكمبيوتر والتحقق من أمان الأجهزة الموضوعة بتصرف الموظفين في حال تم استخدامها خارج المؤسسة المالية.
3. اجراء عمليات اختبار دورية للتحقق من كفاءة أنظمة الحماية من الاختراق لكشف أي نقاط ضعف محتملة.
4. مراقبة الحركة على شبكة المؤسسة المالية لكشف أي سلوك غير اعتيادي، سواء من خلال نوعية المراسلات الواردة أو عددها.
5. التحقق من سلامة البيانات ومراقبتها بهدف كشف أي تلاعب غير مشروع ، وتعقّب مصدر الوصول غير المشروع إليها.

ت- إجراءات عامة:

1. التحقق من ان الجهة المسؤولة عن امن المعلومات لديها تجهيزات وتدريبات كافية للتنبه لمؤشرات الاحتيال المالي الالكتروني وللتحقق تقنياً من مصدر البريد الالكتروني الوارد من العميل والذي يتضمن تعليمات التحويل، بالإضافة الى تخصيص جزء من ميزانية المؤسسة المالية لرفع من مستوى وكفاءة وتجهيزات الجهة المسؤولة عن مكافحة الاحتيال الالكتروني.
2. التعاقد مع شركات تأمين لتغطية مخاطر عمليات الاحتيال المالي الالكتروني.
3. وضع الخطط اللازمة للوقاية من الأفعال الإجرامية الالكترونية وتحديثها باستمرار.
4. توعية الموظفين حول الوقاية من الافعال الإجرامية الالكترونية ورفع مستوى كفائتهم للتنبه لمؤشرات الاشتباه بمحاولة ارتكاب جريمة مالية الكترونية.
5. اصدار نشرات توعوية وتثقيفية للعملاء للتنبه من مخاطر الجريمة المالية الالكترونية وتذكيرهم بضرورة التواصل مع المؤسسة المالية في حال شكهم بتعرضهم لعملية قرصنة بريد او جريمة مالية الكترونية.
6. مراقبة اي تغيرات في عادات وسلوك الموظفين، لا سيما الذين يتمتعون بصلاحية الدخول على الانظمة المعلوماتية.
7. اخد الحيطة والحدر عند التعاقد مع جهات خارجية لتكليفها بمهام تتعلق بالأنظمة الالكترونية والتأكد من ان هذه الجهات لا تقوم بالتعاقد مع جهات ثانوية لا تتمتع بالكفاءة اللازمة.
8. يجب على المؤسسة المالية تحليل مخاطر الجرائم الالكترونية المحتملة والاطلاع المستمر على آخر المستجدات في مجال تكنولوجيا أمن المعلومات.

إنتهى ،،،