أمانة مجلس محافظي المصارف المركزية
ومؤسسات النقد العربية

سلامة وأمن المعلومات المصرفية الإلكترونية

اللجنة العربية للرقابة المصرفية

رقم
72
2017

صندوق النقد العربي
ARAB MONETARY FUND

أمانة
مجلس محافظي المصارف المركزية
ومؤسسات النقد العربية

سلامة وأمن المعلومات المصرفية الإلكترونية

اللجنة العربية للرقابة المصرفية

صندوق النقد العربي
أبوظبي- الامارات العربية المتحدة

تقديم

أرسى مجلس محافظي المصارف المركزية ومؤسسات النقد العربية تقليداً منذ عدة سنوات، بدعوة أحد أصحاب المعالي والسعادة المحافظين لتقديم ورقة عمل حول تجربة دولته في أحد المجالات ذات العلاقة بعمل المجلس. كما يصدر عن اللجان وفرق العمل المنبثقة عن المجلس، أوراق عمل تتناول الموضوعات والقضايا التي تناقشها هذه اللجان والفرق. إضافة إلى ذلك، يعد صندوق النقد العربي ضمن ممارسته لنشاطه كأمانة فنية لهذا المجلس، عدداً من التقارير والأوراق في مختلف الجوانب النقدية والمصرفية التي تتعلق بأنشطة المصارف المركزية ومؤسسات النقد العربية. وتعد هذه التقارير والأوراق من أجل تسهيل اتخاذ القرارات والتوصيات التي يصدرها المجلس. وفي ضوء ما تضمنته كل هذه الأوراق والتقارير من معلومات مفيدة عن موضوعات ذات صلة بأعمال المصارف المركزية، فقد رأى المجلس أنه من المناسب أن تتاح لها أكبر فرصة من النشر والتوزيع. ولذلك، فقد باشر الصندوق بنشر هذه السلسة التي تتضمن الأوراق التي يقدمها السادة المحافظين إلى جانب التقارير والأوراق التي تعدّها اللجان والصندوق حول القضايا النقدية والمصرفية ذات الأهمية. ويتمثل الغرض من النشر، في توفير المعلومات وزيادة الوعي بهذه القضايا. فالهدف الرئيسي منها هو تزويد القارئ بأكبر قدر من المعلومات المتاحة حول الموضوع. ونأمل أن تساعد هذه السلسة على تعميق الثقافة المالية والنقدية والمصرفية العربية.

والله ولي التوفيق،،

عبد الرحمن بن عبد الله الحميدي
المدير العام رئيس مجلس الإدارة
صندوق النقد العربي

المحتويات

الصفحة

الملاحق

أولاً: تمهيد حول المصرفية الإلكترونية

يقصد بعبارة المصرفية الإلكترونية الخدمات المصرفية التي تقدمها المصارف أو ممثلوها عبر أجهزة تعمل تحت رقابة وإدارة مباشرة من المصرف أو بموجب اتفاقية إسناد هذه المهمة لجهة أخرى. تعتبر المصرفية الإلكترونية، مصطلح عام لعملية يمكن بواسطتها للعميل القيام بعمليات مصرفية إلكترونياً بدون زيارة الفرع. يشمل هذا المصطلح، الأنظمة التي تمكن عملاء المصارف سواء أفراد أو شركات من الوصول إلى حساباتهم أو تنفيذ عملياتهم أو الحصول على معلومات تتعلق بمنتجات وخدمات مالية عبر شبكة عامة أو خاصة بما في ذلك شبكات الإنترنت.

ساهمت التطورات والابتكارات التقنية في التأثير الكبير على النشاط المصرفي، وتواجه المصارف تحدي التكيف والابتكار والتعامل مع الفرص التي تقدمها التطورات التقنية. فقد استفادت المصارف وعملائها إلى حد كبير من نمو المصرفية الإلكترونية، إذ اتاحت المصرفية الإلكترونية للمصارف التوسع في تقديم الخدمات إلى من يتعذر عليهم الوصول إليها، وتقليص تكاليف العمليات، وتحسين الفاعلية، وتقديم خدمات مصرفية مباشرة. وعلى الجانب الآخر استفاد العملاء من الخدمات المصرفية الفعالة بتكاليف أقل نسبياً مع إتاحة خيار الاختيار من القنوات البديلة لتقديم الخدمات. كما سهلت المصارف الإلكترونية الانتقال السريع للأموال محلياً وعبر الحدود.

لقد فرضت هذه البيئة المالية المتغيرة تحديات جديدة على المصارف والجهات الرقابية. فقد ازداد اعتماد المصارف على التقنية في بيئة عمل تنافسية بشكل متسارع، وبالتالي يجب عليها إدارة أمن تقنية المعلومات والمخاطر الأخرى المتعلقة بها. وتواجه المصارف المركزية والسلطات الرقابية تحديات جديدة في الرقابة المصرفية.

نظراً لأهمية الموضوع، أصدرت لجنة بازل للرقابة المصرفية في عام 2003 "مبادئ إدارة المخاطر المصرفية الالكترونية" والتي تتكون من 14 مبدأ، تتناول الإشراف الفعال على المخاطر المصاحبة لنشاطات المصرفية الإلكترونية والضوابط الامنية وإدارة المخاطر القانونية ومخاطر السمعة.

تشكر اللجنة العربية للرقابة المصرفية، مؤسسة النقد العربي السعودي على جهودها في إعداد المسودة الأولى من الورقة.

تهدف هذه الورقة إلى إلقاء الضوء على ما يتعلق بسلامة وأمن المعلومات المصرفية الإلكترونية والمخاطر والتهديدات المرتبطة بها وطرق الحد من تأثيرها من خلال التركيز على كل من النقاط التالية:

- مخاطر المصرفية الإلكترونية.
- طرق إدارة المخاطر.
- أنواع التهديدات المرتبطة بالقنوات الإلكترونية.
- طرق التصدي.
- دور المصارف المركزية والتنسيق مع السلطات الاخرى.

ثانياً: مخاطر المصرفية الإلكترونية

لتحديد ماهية المخاطر، من المفيد تحديد أنواع وخدمات المصرفية الإلكترونية. وتتمثل أهم **الخدمات المصرفية الإلكترونية** وفقاً للمواقع الإلكترونية، بما يلي:

أ. المواقع الإلكترونية للحصول على المعلومات فقط

تُعرف هذه المواقع بأنها تلك التي تتيح الدخول لغرض الحصول على معلومات عن التسويق بشكل عام ومعلومات أخرى متاحة للجمهور، أو لإرسال رسائل بريدية إلكترونية غير حساسة. ويجب على المصارف ضمان تحذير العملاء من المخاطر المحتملة المرتبطة بالرسائل البريدية الإلكترونية غير المشفرة عبر وسيلة كهذه.

ب. المواقع الإلكترونية لنقل المعلومات

تُعد هذه المواقع تفاعلية من حيث أنها تمكن من إرسال الرسائل أو الوثائق أو الملفات الحساسة فيما بين مجموعة من المستخدمين، مثل موقع إلكتروني لمصرف يتيح للعميل

تقديم طلب الحصول على قرض أو حساب إيداع عن طريق الإنترنت. وبما أن المخاطر الأمنية المتعلقة بالاتصال والأنظمة تشمل خصوصية وسرية البيانات وسلامة البيانات وعدم الإنكار وتصميم نظام الدخول، لذا من الضروري وضع بعض الطرق للتخفيف من حدة المخاطر.

ج. المواقع الإلكترونية لإتمام تنفيذ العمليات

تمثل هذه المواقع أعلى درجة للطاقة التشغيلية، كما أنها تنطوي على مستويات مرتفعة من المخاطر المحتملة، فهذه الأنظمة توفر الإمكانات اللازمة للتقدم بطلب الحصول على المعلومات وأنظمة تحويل المعلومات إلكترونياً، بالإضافة إلى الحصول على الخدمات المصرفية لتنفيذ العمليات عبر الإنترنت، وتوفر هذه الإمكانات عن طريق الارتباط التفاعلي بين أجهزة العملاء وبين الأنظمة الداخلية للمصرف، كما أن العديد من الأنظمة تشتمل على مزيج من هذه الإمكانات.

على ضوء ما تقدم، فقد أوجدت المصرفية الإلكترونية تحديات لإدارة المخاطر بالنسبة للمصارف. وبالطبع تتأثر جميع المخاطر المرتبطة بالخدمات والمنتجات المصرفية التقليدية بتطبيق المصرفية الإلكترونية، وعلاوة على ذلك هناك فئات من المخاطر ذات الصلة بشكل خاص بالمصرفية الإلكترونية. تتمثل **أهم المخاطر المصاحبة للمصرفية الإلكترونية**، في مخاطر استراتيجية وتشغيلية (عمليات ومخاطر تقنية ومخاطر احتيال عبر الإنترنت ومخاطر سمعة ومخاطر قانونية) وفقاً لما يلي:

أ. **مخاطر استراتيجية:** هي المخاطر الناتجة عن قرارات عمل غير ملائمة وتطبيق خاطئ للقرارات أو قصور أو عدم الاستجابة للتغيرات الحاصلة في الصناعة المصرفية. ويجب أن تتوافق الخدمة المصرفية الإلكترونية مع استراتيجية المصرف الكلية. وأن تركز عملية التخطيط واتخاذ القرارات على كيفية تلبية حاجات العمل وتعزيز المصرفية الإلكترونية. وأن تحدد الرؤية الاستراتيجية كيفية تصميم المصرفية الإلكترونية وعملية تطبيقها ومتابعتها.

ب. **مخاطر تشغيلية (العمليات):** تنشأ المخاطر التشغيلية من الاحتيال وأخطاء المعالجة وتوقف النظام وعدم القدرة على تقديم المنتجات والخدمات والمحافظة على الوضع التنافسي، وإدارة المعلومات. ولتقديم الخدمات المصرفية الإلكترونية قد تعتمد المصارف على إسناد مهام لشركات برمجيات خارجية. وتتطلب المصارف أنظمة ملائمة لإدارة المعلومات والسعة المناسبة لخدمة عملائها، وأنه من الضروري بالنسبة للمصارف تخطيط حالات الطوارئ واستئناف العمل لضمان قدرتها على تقديم المنتجات والخدمات في الأحوال والظروف.

ج. **مخاطر تقنية:** هي المخاطر المتعلقة بتوقف العمل أو خلل أو تعطل النظام، ناجم عن استخدام أو اعتماد أجهزة كمبيوتر والبرمجيات والأجهزة الإلكترونية وشبكات الإنترنت بالإضافة إلى أنظمة الاتصال. وأن مثل هذه المخاطر قد ترتبط أيضاً بتوقف النظام وأخطاء المعالجة وخلل في البرمجيات وأخطاء التشغيل وتعطل النظام وعدم ملاءمة السعة وضعف المراقبة وقصور في الحماية والهجمات بقصد إلحاق الضرر وحوادث الاختراق وأعمال الاحتيال. ويجب على المصارف مراقبة كل عنصر وعملية تتعلق بأنظمتها المصرفية الإلكترونية. ويمثل كل عنصر نقطة للمراقبة تؤخذ بعين الاعتبار. وكذلك العناصر المحتملة التي يجب تقييمها بطريقة مناسبة قبل تطبيقها في بيئة المصرفية الإلكترونية. ويتأثر مستوى مخاطر العمليات بهيكل بيئة المعالجة للمصرف.

د. **مخاطر الاحتيال عبر الإنترنت:** يجب أخذ مخاطر الاحتيال المباشرة عبر الإنترنت بعين الاعتبار. فالتخطيط غير القانوني للتحايل مثل هجمات المواقع المزورة والرسائل الإلكترونية وتزوير العناوين التي تتطلب إفشاء معلومات شخصية سرية، وسرقة بيانات الهوية، تعرض المصرف لمخاطر عالية له ولعملائه. ويجب على المصرف اتخاذ الإجراءات المناسبة لمنع حدوث خسائر نتيجة التعرض للاحتيال عبر الإنترنت والقيام بالأجراء المناسب لحماية عملائه.

ه. **مخاطر السمعة:** تنشأ مخاطر السمعة نتيجة لرأي الجمهور السلبي. ويمكن أن تتضرر سمعة المصرف بواسطة الخدمات المصرفية الإلكترونية التي تنفذ بشكل سيئ والتي تتسبب بطريقة أو أخرى في نفور العملاء. ومن المهم أن يفهم العملاء ما يمكن أن يتوقعوه بشكل معقول من المنتج أو الخدمة، وما هي المخاطر والفوائد الخاصة التي

تترتب عليهم عند استخدامهم لهذه المنتجات أو الخدمات. ويمكن أن يساعد رفع مستوى تثقيف العميل على تقليل مخاطر السمعة للمصرف. ويطلب من المصارف التواصل بطريقة شفافة وواضحة مع عملائه. وعلى المصرف وضع استراتيجية فعاله للتواصل.

و. **مخاطر قانونية:** هي مخاطر تنشأ من الانتهاكات أو عدم الالتزام بالقوانين والأنظمة واللوائح والمعايير. وتزيد الحاجة لضمان التوافق بين الإعلانات الورقية والإلكترونية والإفصاحات والإشعارات من احتمال حدوث مخالفة قانونية. وتساعد عملية المتابعة المنتظمة لمواقع المصرف الإلكتروني على ضمان الالتزام بالقوانين والأنظمة. المصرف هو المسؤول عن إدارة المخاطر المذكورة أعلاه، ويجب عليه ضمان أن إدارة مخاطر المصرفية الإلكترونية جزء لا يتجزأ من مخاطر المصرف بشكل عام. ونتيجة لذلك يجب تعزيز وتنفيذ السياسات وإجراءات إدارة المخاطر والضوابط الداخلية والمراجعة الداخلية وفق ما يتطلبه نظام إدارة مخاطر المصرف بشكل يناسب خدمات المصرفية الإلكترونية، علاوة على ذلك يجب على المصرف ضمان أن أنظمة وضوابط إدارة مخاطر المصرف يتم تحديثها حسب ما هو ضروري لكي تواجه المشاكل المصاحبة للمصرفية الإلكترونية.

ثالثاً: طرق إدارة المخاطر

تعتبر الطبيعة المعقدة لتقنية المعلومات خصوصاً المستخدمة بواسطة الإنترنت (مثال: مخاطر مصاحبة لاستخدام الإنترنت، مخاطر ذات صلة بالشركاء في سلسلة تقديم الخدمات مثل مزودي الاتصالات، بائعي ومقدمي الأنظمة، ومقدمي المنتجات والخدمات)، من أهم الأسباب الرئيسة التي توجب على المصرف إنشاء إطار عمل سليم لإدارة المخاطر. ويجب تغطية جميع الأعمال ذات الصلة ومجالات التشغيل والدعم التي لديها مسؤوليات لإدارة مخاطر التقنية على الخطوط أو المستويات الوظيفية، من خلال تقويم وتحديد الأولوية للمخاطر، لكي يتسنى إعداد استراتيجية للتعامل مع هذه المخاطر والتخفيف من حدتها.

أ. **تحديد المخاطر:** إن المخاطر المصاحبة لخدمات المصرفية الإلكترونية ليست في الحقيقة جديدة، ولكن الطرق المختلفة التي تنشأ من خلالها وحجمها وآثارها المحتملة تتخذ أبعاداً جديدة. ومن ناحية أخرى فإن المخاطر الأمنية مثل تلك التي تتجلى في

عمليات الهجوم لقطع الخدمة عن المستخدمين، ليس لها سابقة أو مقابل في الطريقة التقليدية لتنفيذ الأعمال، قد تسبب انقطاعاً حاداً في عمليات المصرف مما يؤدي لخسائر فادحة لجميع الأطراف المتضررة.

يجب أن تغطي عملية تحديد المخاطر تعيين جميع أنواع التهديدات ونقاط الضعف والانكشاف الكامنة في هيكل المصرفية الإلكترونية وجميع المكونات مثل الشبكات الداخلية والخارجية، والأجهزة والبرامج والتطبيقات البرمجية والعمليات والعناصر البشرية وخصوصاً أثر سوء التصرف البشري. وعلاوة على ذلك يجب أن تغطي عملية تحديد المخاطر بيئة المصرف الإلكترونية المباشرة بالإضافة إلى أنظمة الدعم والمهام والاعتماد الفردي والمتبادل من أجل الحصول على تقرير ملائم لحجم المخاطر.

يجب تقييم وحل المخاطر ذات الصلة بعملية إطلاق منتجات أو خدمات جديدة أو إجراء تعديلات أساسية للمنتجات والخدمات الموجودة خلال مراحل عملية وضع التصورات والتطوير. ويجب أن تكون هناك إجراءات التحكم بالمخاطر وإجراءات أمنية قبل أو خلال مرحلة التطبيق.

يجب على المصرف تحديد وتصنيف المخاطر ذات الصلة بعمليات المصرف على سبيل المثال: اعتماد صيغة لتصنيف المخاطر وتحديد خطة تشمل السياسات والممارسات والإجراءات لمعالجة هذه المخاطر والتحكم بها، تنفيذ الخطة، متابعة المخاطر ومدى فعالية الخطة على أساس مستمر وتحديد عمليات لعمل اختبارات منتظمة وتحديث الخطة لمراعاة التغيرات التي تحدث في التقنية والتطورات القانونية وبيئة العمل (وتشمل التهديدات الخارجية والداخلية لأمن المعلومات).

ب. **تحليل المخاطر وتحديد حجمها:** إن هذه المرحلة عبارة عن تحليل وفهم وتحديد حجم الأثر المحتمل وتبعات المخاطر التي تم تحديدها على العمل والعمليات بشكل عام، وتحديد الأولوية للمخاطر والقيام بتحليل تكلفة المنفعة واتخاذ قرارات لتخفيف حدة المخاطر.

ج. **معالجة المخاطر:** يجب على المصارف تقييم حجم الأضرار والخسائر التي قد يتحملها المصرف عند وقوع مخاطر معينة ذات صلة. ويجب على المصارف تحمل الخسائر التي قد تحدث من دون تعريض سلامتها المالية واستقرارها للخطر.

كما يجب موازنة تكاليف التحكم بالمخاطر والتخفيف من حدتها مقابل الفوائد التي يمكن تحقيقها. ويجب أن تتخذ المصارف قراراً يتعلق بالموارد التي تخصص لمهمة المراقبة.

أنه من المهم التأكد من فعالية الضوابط الداخلية بما في ذلك فصل المهام والرقابة الثنائية والمطابقة. حيث أن ضوابط أمن المعلومات بشكل خاص أصبحت أكثر أهمية إذ تتطلب وجود إجراءات إضافية وأدوات وخبرات واختبارات، ويجب على المصارف تحديد مستوى الضوابط الأمنية بناء على تقييمها للخدمة التي تقدمها، وعلى حساسية المعلومات بالنسبة للعميل والمصرف ومستوى تحمل المخاطر القائمة للمصرف.

د. **متابعة المخاطر:** لمواجهة التغير المستمر الحاصل في بيئة المصرفية الإلكترونية يجب على المصرف إنشاء إطار عمل لمتابعة المخاطر والالتزام على أساس مستمر للتأكد من أداء وفعالية وإجراءات إدارة المخاطر، ويجب تحديث إجراءات المخاطر وتعزيزها، كما يجب القيام باختبارات مستمرة ومراجعة كفاءة وفعالية إجراءات إدارة المخاطر والضوابط المصاحبة والإجراءات الامنية السارية. وينصح كثيراً بأن يقوم المصرف بإجراء برنامج تقييم شامل للمخاطر بواسطة طرف ثالث سنوياً.

رابعاً: أنواع التهديدات المرتبطة بالقنوات الإلكترونية

تتمثل أبرز أنواع التهديدات المرتبطة بالقنوات الإلكترونية، على القطاع المصرفي، بما يلي:

أ. **استهداف البنية التحتية:** استهدفت أبرز الهجمات الإلكترونية تعطيل عمل البنية التحتية للمصرف، ومن أشهر أنواع التهديدات الآتي:

1. **البرمجيات الخبيثة وتعطيل الخدمة:** البرمجيات الخبيثة (Malware) هي اختصار لكلمتين هما "malicious software" والبرمجية الماكرة أو الخبيثة هي برمجية

تضمينها أو إدراجها عمداً في نظام الحاسوب لأغراض ضارة. فقد تستخدم لعرقلة تشغيل الحاسوب، جمع معلومات حساسة، أو الوصول إلى أنظمة الكمبيوتر الخاصة، وعندما يتم تثبيت البرمجية الخبيثة فقد يكون من الصعب جداً إزالتها. وبحسب درجة خطورة البرمجية، من الممكن ن يتراوح أذاها من إزعاج بسيط (بعض النوافذ الإعلانية غير المرغوب فيها خلال عمل المستخدم على الحاسوب سواء كان متصلاً أم غير متصل بشبكة حواسيب) إلى أذى غير قابل للإصلاح يتطلب إعادة تهيئة القرص الصلب على سبيل المثال ومن الأمثلة على البرمجيات الخبيثة الفيروسات وأحصنة طروادة[1].

ويستخدم قراصنة الإنترنت أساليب عديدة لاختراق أو تعطيل شبكات الحاسوب المستهدفة، وقد يكون ضرر بعض هذه الأساليب محدوداً يقتصر على سرقة معلومات محددة من حاسوب مستهدف، وقد يكون مدمراً يؤدي إلى تعطيل شبكة بأكملها وتسريب بيانات مستخدميها وبريدهم الإلكتروني. ومن أبرز أساليب القراصنة لتعطيل شبكات الحاسوب ما يعرف بهجوم الحرمان من الخدمة (Denial-of-Service) وهي هجمات تستهدف مؤسسات حكومية أو شركات كبرى كالمصارف مثلاً، وهدفها جعل جهاز أو شبكة حاسوب غير متاحة للمستخدمين المستهدفين. أي حرمانهم من الخدمة التي تستضيفها خوادم الشبكة[2].

2. **استغلال الثغرات:** ويسمى أيضاً بالهجوم دون انتظار Zero Day Attack وهو عبارة عن استغلال نقاط الضعف في برمجيات وثغراتها الأمنية خاصة غير المعروفة منها للعامة أو حتى مطوريها في شن هجمات إلكترونية. وغالباً ما يتم استغلال هذه الثغرات بل وتشاركها ما بين القراصنة (Hackers) قبل أن تكتشفها الجهات المطورة للبرمجيات المصابة وتسمح المعرفة بالثغرة الأمنية من قبل المطورين لمستغليها الحصول على فترة زمنية ينشر فيها أدواته الخبيثة لتحدث ضرراً كبيراً. لأنه متى ما اكتشفت الثغرة الأمنية، يسارع المطورون لسدها من خلال نشر برامج تصحيحية.

(1) ويكيبديا الموسوعة الحرة، برمجيات خبيثة.
(2) الموقع الجزيرة نت، البرمجيات الخبيثة وأساليب القرصنة http://www.aljazeera.net

ويأتي مصطلح Zero Day Attack من كون أن مستغل الثغرة الأمنية غير المعروفة لا يترك أي يوم يمر لبدء هجومه كونه في سباق مع الزمن، وكلما تأخر اكتشاف الثغرة، منح ذلك مزيد من الوقت للمهاجمين في توسيع نطاق الهجوم وإضافة ضحايا جدد[3].

ب. **استهداف الهواتف الذكية:** بعد أن أصبحت الهواتف الذكية والأجهزة اللوحية هي الطريقة الشائعة للمستخدمين للاتصال بالإنترنت والتواصل مع بعضهم البعض ودخول الكثير من العملاء على حساباتهم المصرفية أو إجراء عمليات البيع والشراء من خلال الهواتف الذكية والأجهزة اللوحية، بدأ القراصنة والمهاجمون يركزون اهتمامهم على اختراق هذه الأجهزة، ويرتبط بهذا التهديد مجموعة من الحقائق التالية:

- أغلب المستخدمين لا يلم بصفة عامة بالمخاطر الأمنية للهواتف الذكية.
- انتشار استخدام الهواتف الذكية أدى إلى زيادة لجوء القراصنة لبرمجة التطبيقات الخبيثة.
- يلجأ قراصنة المعلومات الى التحايل على مالكي الهواتف لتوجيههم على تحميل تطبيق خاضع لسيطرتهم.
- ويكمن خطر تهديدات الهواتف الذكية في تطبيقاتها الخاصة بدخول العملاء من خلالها لحساباتهم المصرفية مما يتيح الفرصة لقراصنة المعلومات المصرفية من الدخول على تلك الحسابات أو إصابة النظام الإلكتروني للمصرف بالفيروسات التي تسبب عطل النظام أو بعض أجزاؤه.

ج. **الرسائل المزيفة عبر وسائل الاتصال المختلفة (الاستدراج الإلكتروني):** إن الاستدراج هو هجوم على هوية شخص قد يكون عميلاً لأحد المصارف، ولقد جرت العادة على إطلاق مصطلح " سرقة الهوية" على هذا النوع من الهجمات لأن غرض المهاجم هو الحصول على البيانات الشخصية باستخدام تقنيات مختلفة كالمواقع الوهمية والرسائل الإلكترونية المزيفة.. إلخ[4].

(3) ويكيبديا الموسوعة الحرة، هجوم دون انتظار
(4) شركة العربي الوطني للاستثمار، أمن المعلومات المصرفية

فالاستدراج الإلكتروني هو عبارة عن نشاط إجرامي ينطوي على محاولة للحصول على معلومات حساسة كهوية المستخدم وكلمة السر وبيانات الحسابات عن طريق الاحتيال من خلال انتحال هوية صديق موثوق أو شركة أو مصرف في رسالة إلكترونية أو موقع وهمي. وتعتبر الشركات التي تقدم خدمات استثمارية على الإنترنت والمصارف الإلكترونية مواقع مستهدفة لعمليات الاستدراج. أما أكثر وسائل الاستدراج شيوعاً فهي الرسائل الإلكترونية، وغالباً ما تنطوي على طلب للمستخدمين بالكشف عن تفاصيل شخصية عبر موقع وهمي على الشبكة العنكبوتية، وكذلك تتم عمليات الاستدراج باستخدام المكالمات الهاتفية والرسائل النصية.

خامساً: طرق التصدي

تشمل أهم طرق التصدي، ما يلي:

أ. **التوعية بأمن المعلومات المصرفية:** تتمثل المهمة الأولى في أمن المعلومات المصرفية في زيادة الوعي بأمن المعلومات لدى كافة مستويات المجتمع، في الأجهزة الحكومية والمؤسسات العامة والخاصة وكل الأفراد المستخدمين والمتعاملين مع نظم المعلومات المصرفية، والتعرف على أهمية أهداف وأمن المعلومات المصرفية والممارسات السليمة[5].

يجب على المصارف أن تضع وتنفذ برامج توعوية مناسبة حول منتجاتها وخدماتها المصرفية الالكترونية لضمان التعرف على هوية العميل وتوثيقه قبل الدخول وتنفيذ عمليات مصرفية عن طريق الانترنت. ولهذا الغرض تستطيع المصارف استخدام قنوات متعددة مثل المواقع الالكترونية على الشبكة أو الرسائل المطبوعة على كشوفات العميل أو المنشورات الترويجية أو الاتصال المباشر بالموظفين من خلال مراكز الاتصال الهاتفية للمصارف.

ب. **كفاءة أمن المعلومات cyber threat Intelligence:** أمن المعلومات، هو عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح

(5) منتديات اليسير للمكتبات وتقنية المعلومات المصرفية http:// alyaseer.net

وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين من المخاطر في الفضاء السيبراني.

ج. **اكتشاف وصد المواقع والرسائل المزيفة:** للحد من هجمات المواقع والرسائل المزيفة[6] على المصارف توعية عملائها و موظفيها بأهمية الإجراءات التالية:

- مراجعة إعدادات بوابات البريد الالكتروني (email gateway) للتصدي لرسائل البريد الالكتروني غير المرغوبة (phishing spam).
- عدم مشاركة عنوان البريد الإلكتروني إلا مع الأشخاص الموثوق بهم فقط.
- عدم الرد على رسائل البريد العشوائي التي تصل إلى صندوق الوارد.
- يجب الحذر عند ملء النماذج الموجودة على الانترنت، خاصة خانات الاختيار مثل (نعم، أريد تلقي معلومات عن ... في علبة الوارد).
- عدم مناقشة أية معلومات شخصية مهمة عبر المكالمات الهاتفية أو رسائل البريد الإلكتروني غير المرغوب فيها دون التحقق من مصداقية المرسل.
- يجب أن تكون على دراية بأن المصارف لن تطلب منك أية معلومات مهمة عن حسابك المصرفي عبر البريد الإلكتروني.
- التأكد من أن جهازك مزود بأحدث برامج التصحيح المصدرة لتصحيح الثغرات الأمنية في التطبيقات وأنظمة التشغيل المثبتة على جهازك.
- توعية المستخدمين بعدم فتح رسائل تحتوي على روابط أو مرفقات من أشخاص غير معروفين.
- استخدام أنظمة التشغيل المعتمدة والمحددة.

د. **اختبار الثغرات بشكل دوري:** يعتبر القيام بأعمال الكشف الدوري لاختبار الثغرات من أهم وسائل حماية أمن المعلومات المصرفية، وتعتبر أحد الوسائل الأساسية للقيام بذلك هي عملية الترقيع وهي عبارة عن عملية تقليل نقاط الضعف في الأنظمة وإغلاق المداخل على المخترقين. بحيث تكون البرامج معدة بصفة متقنة وجيدة ومحدثة بآخر

(6) إرشادات حول الأمان، تعرف على الجديد في بيئة التهديدات الديناميكية، http://www.eset.com/me

الرقع والنسخ وتشمل التطبيقات والشبكات وأنظمة التشغيل التي تدير تلك الشبكات، بحيث تكون التحديثات بشكل دوري ومستمر[7].

1. **الرقع الأمنية Security Patch:** هي برامج حاسوبية الهدف منها هو إصلاح منتج معين وحمايته من الناحية الأمنية وسد الثغرات الأمنية.

2. **إدارة الرقع وسد الثغرات Patch Management:** هي عملية التحكم وإدارة البرامج والرقع الحاسوبية المثبتة وطريقة تثبيتها والمتابعة المستمرة لآخر إصداراتها وطريقة إنزالها على الأنظمة الموجودة ويجب على مسئولي الأمن عند إدارة الرقع وسد الثغرات التأكد من عدم إتاحة فرص للمتطفلين في اختراق الأنظمة والتي تشمل الاتي:

- تحديد الأنظمة التي تحتاج إلى رقع وعمل تحديثات معينة.
- الاشتراك في الاستشارات وقوائم التنبيه والتحذيرات، وهذه تبقيك على اتصال بكل تحديث جديد أو سد ثغرات لبرنامج معين.
- مواقع منتجي الأنظمة والموردين.
- القيام بالتوثيق.
- تحديد وتقييم الثغرات الأمنية في كل برنامج.
- اختبار الرقع المصممة والتعديلات قبل إنزالها ومن ثم استشعار واكتشاف الثغرات الجديدة والتي تكون هدفاً للمهاجمين.

إن عمليات الترقيع والترقية من أهم العناصر الأمنية التي يجب على المؤسسة المصرفية أخذها بعين الاعتبار وأن تكون ذات أولوية لمسئولي الأمن.

ه. **اكتشاف الثغرات:** تقوم استراتيجية حماية البيانات في البيئة المصرفية على أن أول الخطوات لمستخدمي التقنية، هي تحصين النظام داخلياً (الحاسوب الشخصي أو الخوادم Servers) وذلك من خلال[8]:

(7) منتدى أمن المواقع والمنتديات http://www.starimes.com/laspx?t=33718990.websecurity
(8) http://www.kantakji.com/media/174535/e-banking.doc

- اغلاق الثغرات الموجودة في النظام، عن طريق اختبارات فعالة للثغرات الأمنية.
- التأكد من تحديث الأنظمة المستخدمة ومتابعة ما تصدره الشركات من تعديلات لسد الثغرات التي تظهر في النظم المستخدمة، ويمكن ذلك عبر مواقع الشركات المعنية على الأنترنت.
- متابعة المواقع التي تكشف عن ثغرات البرمجيات وأنظمة التشغيل وتعالج المشاكل الأمنية.
- استخدام البرامج المضادة للفيروسات مع دوام تطويرها وكذلك التأكيد من تقسيم الشبكة (Net segmentation) بشكل فعّال.
- عدم تشغيل برامج غير معروفة المصدر والغرض، مما يرد ضمن البريد الالكتروني أو مواقع الانترنت، لاحتمال أن تتضمن أبواب خلفية (Back Doors) تسهل الاختراق.
- إيجاد حلول تقنية للبنية التحتية التي تقوم بتحليل أنشطة البيانات (Traffic) واكتشاف الأنشطة المشبوهة في الشبكة.

سادساً: دور المصارف المركزية

يعتبر أمن وسلامة المعلومات المصرفية، ذو أهمية بالغة للمصارف المركزية المسؤولة عن الاستقرار المالي، وحيث يمثل التهديد الإلكتروني أبرز التحديات التي تواجه النظام المالي مما يستوجب سن التشريعات النظامية والرقابية وحث المصارف على تأمين معلوماتها وبنيتها الالكترونية، وإجراء تقييم لأنظمة المعلومات في المصارف واتخاذ الاجراءات الاحترازية للتقليل من الاختراقات الإلكترونية للمعلومات المصرفية. وفي هذا الإطار، يستلزم على المصارف المركزية مراجعة ومراقبة تطبيق تلك التشريعات ومنها على سبيل المثال:

- إصدار التعليمات بتحديد الحد الادنى لمتطلبات أمن المعلومات المصرفية (مثل: حوكمة أمن المعلومات، مخاطر أمن المعلومات، ومتطلبات تقنية للبنية التحتية، الخ). بحيث تستند على أفضل الممارسات الصادرة من الجهات الرقابية والجهات الدولية ذات العلاقة مثل لجنة بازل.

- وضع إطار اشرافي على المصارف يتم التأكد من خلاله بالتزام المصارف بمتطلبات الحد الادنى لأمن المعلومات.
- وحيث ان مجال امن المعلومات متغير بشكل متسارع فلابد من عمل التدقيق والمراجعة وتقييم البنية التحتية بشكل مستمر.
- تكوين اللجان وفرق العمل المختصة بين المصارف وتحت اشراف المصرف المركزي، لتبادل المعرفة والأفكار، ورسم إطار مشترك ومعالجة القضايا والتحديات الشائعة المتعلقة بأمن المعلومات.
- إدارة الاعتماد على الأطراف الأخرى الموفرة للخدمات وتقييم مخاطر الاعتماد على تلك الاطراف، بما في ذلك وضع ضوابط للإسناد لطرف ثالث (outsourcing) بما يكفل توفير الحماية اللاّزمة لأمن وسلامة المعلومات المصرفية.

سابعاً: العلاقة بين السلطات الاشرافية والسلطات الأخرى

إن سلامة القطاع المالي والمصرفي تعتمد على سن القوانين والتشريعات التي تحد من التهديدات الخارجية والداخلية. هذا وفي ضوء ما تم تناوله عن التهديدات المرتبطة بالقنوات الإلكترونية، فإن ذلك يستدعي التنسيق بين المصارف المركزية والسلطات التشريعية والتنفيذية الأخرى، لإصدار التشريعات القضائية وتحديد العقوبات المقررة للجرائم المعلوماتية لتساعد على تحقيق الامن المعلوماتي.

ثامناً: الخلاصة والتوصيات

تمثل العمليات الإلكترونية جانباً مهماً من جوانب التجديد والتطوير في تقديم الخدمات المالية والمصرفية. ويعتبر القطاع المصرفي في هذا الصدد، أكثر القطاعات الاقتصادية تعرضاً للمخاطر، لاسيما المخاطر المستقبلية، على ضوء تطورات العمل المصرفي وتنامي استخدام أدوات مصرفية إلكترونية جديدة، ساعد على خلقها التقدم التكنولوجي. بناءً عليه، يكتسب موضوع سلامة وأمن المصرفية الالكترونية أهمية عالية.

وفي ضوء ما تم تناوله من أهمية سلامة وأمن المعلومات المصرفية وفي ضوء المخاطر والتهديدات المعلوماتية التي تتعرض لها المصارف، من الأهمية تطوير الأنشطة القضائية

والتشريعية والرقابية، المتعلقة بأمن وسلامة المعلومات والعمليات المصرفية، والسعي لتحديد العقوبات المقررة للجرائم المعلوماتية بما يساعد على تحقيق الأمن المعلوماتي.

وإضافة لتقوية التشريعات القضائية، فإن هناك مجموعة من الإجراءات على مستوى المؤسسات المصرفية والسلطات الإشرافية، التي يجب اتخاذها لسلامة وأمن المعلومات المصرفية والتي من ضمنها الآتي:

- وجود استراتيجية واضحة لأمن المعلومات تتوافق مع استراتيجية قطاع الاعمال لدى المصرف وتعنى بحفظ المعلومات والقدرة على استمرارية الاعمال، وتطوير خططاً للاستجابة للحوادث العرضية التي تظهر فجأة من حوادث غير متوقعة متضمنه الهجوم الداخلي والخارجي الذي قد يعيق تقديم الخدمات والمنتجات المصرفية.
- وضع إطار تنظيمي للاختبارات الدورية والتأكد من كفاءة الانظمة الموجودة لمواجهة أي نوع جديد من الاختراقات.
- الاهتمام بحوكمة أمن المعلومات للتأكد من سلامة الاجراءات في المصرف.
- على المصرف إعادة تقييم وتحديث طرق مراقبة المخاطر لتأخذ بعين الاعتبار الظروف المختلفة والتغيرات.
- استقلالية إدارة أمن المعلومات في المصرف للقيام بواجباتها على أكمل وجه، والدعم من المصرف.
- تعزيز دور الرقابة على الشبكة الداخلية والخارجية للمصرف من خلال تطبيق أفضل الممارسات في هذا المجال.
- إيجاد العاملين الماهرين في مجال أمن المعلومات للقيام بالاختبارات اللازمة بشكل دوري.
- تأسيس رقابة إدارية فعالة على المخاطر المرتبطة بالأعمال المصرفية الإلكترونية، ووضع المفاهيم الأساسية لعملية ضبط الأمن الإلكتروني ومتابعة عملية تطوير وصيانة البنية التحتية لضوابط الأمن التي تحمي الأنظمة والبيانات من أي تهديد داخلي أو خارجي.
- يجب على المصارف أن تتخذ الإجراءات المناسبة للتحقق من هوية العملاء عند استخدام القنوات الإلكترونية لإجراء العمليات المصرفية، من خلال وضع ضوابط التيقن وامتيازات العبور المناسبة ضمن أنظمة الأعمال وقواعد البيانات والتطبيقات.

- وضع مقاييس تدقيق واضحة لجميع تعاملات وحركات الأعمال المصرفية الإلكترونية لحماية سلامة معطيات التعامل والملفات والمعلومات، وأن تكون مناسبة لحماية خصوصية المعلومات الهامة والأساسية للأعمال المصرفية الإلكترونية، بحيث تتناسب مع حساسية المعلومات التي ترسل إلى قواعد البيانات أو تسحب منها.
- تفعيل دور الإعلام المصرفي فيما يتعلق بضرورة رفع مستوى الوعي بأمن المعلومات المصرفية الإلكترونية للأطراف الداخلية والخارجية.
- إيجاد آلية من خلال البنك المركزي لمشاركة المعلومات حول حوادث أمن المعلومات للقطاع المصرفي.
- إصدار التشريعات القضائية وتحديد العقوبات المقررة للجرائم المعلوماتية لتساعد على تحقيق الأمن المعلوماتي.
- التعاون مع الجهات المختصة للإبلاغ وحفظ الادلة وتسليمها للجهات المختصة.

في ضوء ما تقدم، وبالنظر للتطور الكبير والمتسارع في جرائم الاحتيال المصرفي المستندة للخدمات الإلكترونية، فإن اللجنة العربية للرقابة المصرفية، تدعو السلطات الإشرافية، إلى تكثيف جهودها لمتابعة هذه الظاهرة والعمل على وضع القواعد والتشريعات والتعليمات لمواجهتها، بالتنسيق مع السلطات القضائية بما يعزز من سلامة وأمن العمليات المصرفية الإلكترونية. كما تدعو اللجنة، السلطات الإشرافية في الوقت نفسه، لتطوير الإطار الرقابي المتعلق بالخدمات المصرفية الإلكترونية وبناء قدراتها في هذا الشأن، وحثّ المؤسسات المصرفية على تطوير الأنظمة وضوابط المراقبة لديها، لمواجهة مختلف الجرائم المصرفية الإلكترونية، للحد من المخاطر التي قد تنتج عن تقديمها للخدمات المصرفية. كذلك يتعين على السلطات الإشرافية، تضمين الرقابة المصرفية الاعتيادية، لجوانب التحقق من كفاءة وفعالية منظومة الضوابط المتاحة لدى المؤسسات المصرفية في هذا الشأن.

الملحق (1)
تجربة مصرف البحرين المركزي حول الأنظمة والتعليمات الخاصة بسلامة وأمن المعلومات المصرفية الالكترونية في المملكة

أصدر مصرف البحرين تعليمات حول قضايا أمن الإنترنت وحماية المستهلك:

- يجب على جميع البنوك التي تقدم الخدمات البنكية الإلكترونية أن تقوم بشكل منتظم باختبار أنظمتها ضد الاختراقات الأمنية والتحقق من متانة إجراءات الرقابة الأمنية المطبقة لديها. ويجب أن يتم إجراء هذه الاختبارات من قبل خبراء في مجال الأمن الإلكتروني، مثل الهاكر الأخلاقي الذي يقوم بتقديم خدمات فحص الاختراق وتقييم الثغرات في النظام.
- يجب إجراء اختبار الاختراق المشار إليه في الفقرة السابقة كل سنة في شهري يونيو وديسمبر.
- يجب على البنك الاحتفاظ بتقارير تقييم الثغرات بالإضافة إلى الإجراءات التي يتم اتخاذها للحد من المخاطر ذات الصلة لمدة خمس سنوات من تاريخ الاختبار. كما يجب تزويد مصرف البحرين المركزي بنسخة منها خلال شهرين من نهاية الشهر الذي تم فيه إجراء الاختبار، أي في 31 أغسطس كحد أقصى بالنسبة للاختبار الذي يتم في شهر يونيو، وفي 28 فبراير بالنسبة للاختبار الذي يتم في شهر ديسمبر، (أنظر القسم BR-4A.2).

كما أصدر مصرف البحرين المركزي، خلال عام 2016 توجيهات جديدة تتعلق بأمن أجهزة الصراف الآلي حيث تتماشى مع أفضل الممارسات الدولية والمتطلبات الأمنية بهذا الخصوص، حيث تتطلب التوجيهات الجديدة أن تضمن البنوك توافق جميع أجهزة الصراف الآلي الخاصة بها مع معايير أمن البيانات لقطاع بطاقات الدفع PCI-DSS.

ويتمثل الهدف الأساسي من إصدار تلك التوجيهات هو إلزام البنوك بتطبيق إجراءات حماية إضافية لبيانات العملاء عند استخدامهم لأجهزة الصراف الآلي من خلال توفير وسائل حماية إضافية للأجهزة والبرمجيات الخاصة بأجهزة الصراف الآلي لمنع حدوث أي اختراقات أمنية للبيانات الهامة للعميل ومنها عمليات نسخ البيانات الموجودة في بطاقة الصراف الآلي (data skimming) مثل الرمز السري لبطاقة الصراف الآلي.

الملحق (2)
تجربة مؤسسة النقد العربي السعودي فيما يتعلق بالتعليمات والضوابط الصادرة حول المصرفية الإلكترونية

أصدرت المملكة العربية السعودية نظام مكافحة جرائم المعلوماتية، حيث يأتي صدور هذه الأنظمة للحد من وقوع الجرائم المعلوماتية وتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة او مخالفة وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات بما يؤدى إلى تحقيق الامن المعلوماتي وزيادة استخدامات الحاسب وشبكاته وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات والشبكات. كما أصدرت مؤسسة النقد العربي السعودي عدد من التعليمات فيما يخص أمن وسلامة المعلومات المصرفية الإلكترونية منها على سبيل المثال:

- إرشادات أمن المصرفية عبر الانترنت الصادرة عام 2001.
- تعليمات إسناد مهام لطرف ثالث 2008.
- دليل مكافحة الاختلاس والاحتيال المالي 2008.
- قواعد الخدمات المصرفية الإلكترونية الصادرة في إبريل 2010.
- تحديث تعميم/ استقلالية إدارة أمن المعلومات 2014.
- خدمة الإشعار الآلي الفوري عبر تقنية رسائل الجوال النصية القصيرة 2010.
- القرصنة الإلكترونية لأجهزة الصراف الآلي 2014.
- تطبيق أكثر من معيار من معايير التحقق من الهوية عند التحويل من الحسابات الجارية إلى الحسابات الاستثمارية 2013.
- الضوابط المتعلقة بتطبيق خدمة الجوال المصرفي 2013.
- إجراء تقييم لأنظمة الحماية وأمن المعلومات لجميع المصارف العاملة في المملكة 2012.
- متطلبات للحد من هجمات تعطيل أو حجب الخدمات الإلكترونية 2015.
- اتخاذ الحيطة والحذر بشأن عمليات الاحتيال الإلكتروني 2011.
- مبادئ حماية عملاء المصارف 2013.

من جانب آخر، وعلى ضوء النمو الكبير في ظاهرة الاحتيال المالي والمصرفي الآخذة في التزايد على المستوى العالمي والمسجلة لمعدلات قياسية متزايدة باتت تشكل تهديداً فعلياً لمجمل التعاملات الإلكترونية، تقوم المصارف السعودية من خلال لجنة الإعلام والتوعية المصرفية المنبثقة عن المصارف السعودية بحملات توعوية ضد عمليات الاحتيال المالي والمصرفي تهدف إلى رفع مستوى وعي أفراد المجتمع عامة وعملاء المصارف خاصة بالأسس السليمة لاستخدام البطاقات المصرفية والائتمانية والقنوات المصرفية الإلكترونية للحد من احتمالات التعرض لمحاولة الاحتيال.

وعلى سبيل المثال خصصت المصارف السعودية 60 مليون رسالة نصية توعوية للنصف الثاني من 2015 تتضمن نصائح وتوجيهات تتعلق بتوعية جمهور العملاء بالأسس السليمة لاستخدام القنوات المصرفية الإلكترونية والبطاقات الائتمانية بغرض الحفاظ على سرية وخصوصية بياناتهم الشخصية والمصرفية وكإجراء وقائي للحماية من تعرضهم للاحتيال. ويأتي بث هذه الرسائل كإحدى القنوات التوعوية التي تتبناها المصارف السعودية ضمن حملتها التوعوية بعمليات الاحتيال المالي والمصرفي والتي انطلقت نسختها السابعة في منتصف عام 2015 تحت عنوان (ينقال - ما ينقال)، واستمرت حتى نهايته، لغرض تعزيز مستوى الوعي لدى عملاء المصارف وأفراد المجتمع حيال وسائل التحايل وكيفية الوقاية منها. ومن بين أبرز الرسائل النصية للحملة دعوة عملاء المصرف إلى تجاهل الرسائل النصية الإلكترونية التي تزعم فوزهم بالجوائز النقدية أو العينية وحذفها من جوّالاتهم وبريدهم الإلكتروني على الفور وتجنب مساعدة الغرباء عند استخدام أجهزة الصراف الآلي والتأكيد على حصر عملية تحديث البيانات المصرفية من خلال فروع المصرف مباشرة فقط وتجنب الإعلانات المشبوهة لسداد المديونيات والقروض وأهمية الحفظ على الأرقام السرية وعدم الكشف عنها وتغييرها بصورة دورية وخاصة عند العودة من السفر.

سلسلة الكتيبات الصادرة عن أمانة مجلس محافظي المصارف المركزية و مؤسسات النقد العربية

1. التوجهات الدولية و الإجراءات و الجهود العربية لمكافحة غسل الأموال – 2002.
2. قضايا و مواضيع في الرقابة المصرفية – 2002.
3. تجربة السودان في مجال السياسة النقدية – 2003.
4. تطورات السياسة النقدية في جمهورية مصر العربية – 2003.
5. الوضعية النقدية و سير السياسة النقدية في الجزائر – 2003.
6. تطوير أسواق الأوراق المالية الحكومية في الدول العربية و دور السلطات النقدية- 2004.
7. الملامح الأساسية لاتفاق بازل II و الدول النامية – 2004.
8. تجربة السياسة النقدية في المملكة المغربية -2004.
9. إدارة المخاطر التشغيلية و كيفية احتساب المتطلبات الرأسمالية لها – 2004.
10. التقييم الداخلي للمخاطر الائتمانية وفقاً لمتطلبات (بازل II) – 2005.
11. تجربة السياسة النقدية و إصلاح القطاع المصرفي في الجمهورية اليمنية– 2005.
12. ضوابط عمليات الإسناد الخارجي للمؤسسات المصرفية – 2005.
13. مراقبة الامتثال للقوانين و التعليمات في المصارف – 2005.
14. أنظمة تحويلات العاملين – قضايا و توجهات – 2005.
15. المبادئ الأساسية لنظم الدفع الهامة نظامياً ومسؤوليات المصارف المركزية – 2006.
16. الدعامة الثالثة لاتفاق (بازلII) " انضباط السوق " – 2006.
17. تجربة مؤسسات نقد البحرين كجهاز رقابي موحد – 2006.
18. ترتيبات الإعداد لتطبيق مقترح كفاية رأس المال (بازل II) – 2006.
19. Payments and Securities Clearance Settlement System in Egypt -2007
20. مصطلحات نظم الدفع و التسوية – 2007.
21. ملامح السياسة النقدية في العراق – 2007.
22. تجربة تونس في مجال السياسة النقدية و التوجهات المستقبلية – 2007.
23. الدعامة الثانية لاتفاق بازل II – المراجعة الرقابية 2007.
24. ضوابط العلاقة بين السلطات الرقابية في الدولة الأم و الدول المضيفة – 2007.
25. الإرشادات العامة لتطوير نظم الدفع و التسوية – 2007.

26. تطوير أنظمة الاستعلام الائتماني ومركزيات المخاطر – 2008.
27. استمرارية الأعمال في مواجهة الطوارئ – 2008.
28. نظم الدفع الخاصة بعرض وسداد الفواتير الكترونياً – 2008.
29. مبادئ الإشراف على أنظمة الدفع والتسوية ومسؤوليات المصارف المركزية- 2008.
30. مقاصة الشيكات في الدول العربية – 2008.
31. برنامج إصلاح إدارة سوق الصرف و السياسة النقدية في مصر – 2008.
32. Information Sharing and Credit Reporting System in Lebanon
33. أنظمة الإنذار المبكر للمؤسسات المالية – 2009.
34. تنميط أرقام الحسابات المصرفية – 2009.
35. التمويل متناهي الصغر ودور البنوك المركزية في الرقابة والإشراف عليه – 2009.
36. برنامج الاستقرار المالي لمواجهة تداعيات الأزمة المالية في دولة الكويت – 2009.
37. تطوير السياسة النقدية والمصرفية في ليبيا 2010.
38. Information Sharing and Credit Reporting System in Syria-2010
39. Information Sharing and Credit Reporting System in Yemen-2010
40. Information Sharing and Credit Reporting System in Oman-2010
41. Information Sharing and Credit Reporting System in Tunisia-2010
42. مبادئ إدارة مخاطر الائتمان - 2011.
43. قواعد ممارسات منح المكافآت المالية - 2011.
44. الإدارة السليمة لمخاطر السيولة والرقابة عليها - 2011.
45. إطار ربط محولات الدفع الوطنية في الدول العربية - 2011.
46. الإطار القانوني لنظم الدفع وتسوية الأوراق المالية - 2012.
47. تجربة البنك المركزي التونسي في التعامل مع التداعيات الاقتصادية للتطورات السياسية الأخيرة - 2012.
48. السياسات النقدية والمصرفية لمصرف قطر المركزي في مواجهة تداعيات الأزمة العالمية - 2012.
49. توسيع فرص الوصول للتمويل والخدمات المالية في الدول العربية ودور المصارف المركزية - 2013.
50. مبادئ اختبارات الجهد للمؤسسات المصرفية - 2013.
51. نظم الدفع عبر الهاتف المحمول- الأبعاد والقواعد المطلوبة - 2013.
52. تجربة بنك المغرب في مجال تعزيز الولوج إلى الخدمات المالية - 2013.
53. قضايا تطوير نظم الحفظ المركزي للأوراق المالية ودور المصارف المركزية.
54. أهمية ودور مجلس المدفوعات الوطني – تجارب الدول العربية.

55. حماية المستهلك (العميل) في الخدمات المصرفية.
56. مبادئ حوكمة المؤسسات المصرفية.
57. التجربة الفلسطينية في مجال تطوير البنية التحتية للقطاع المالي والمصرفي.
58. الترجمة العربية للمبادئ الأساسية للرقابة المصرفية الفعّالة – 2014.
59. التعامل مع المؤسسات المصرفية ذات المخاطر النظامية محلياً ودور المصارف المركزية – 2014.
60. الرقابة على صيرفة الظل – 2014.
61. تطبيق آلية الوسيط المركزي لتسوية معاملات الأسواق المالية – تجربة بنك المغرب – 2014.
62. مبادئ البنية التحتية لأسواق المال وإطار الإفصاح ومنهجية التقييم لهذه المبادئ – 2014.
63. إصلاح القطاع المصرفي والاستقرار المالي في الجزائر – 2014.
64. قاموس مصطلحات الرقابة المصرفية – 2015.
65. المستجدات الرقابية في مكافحة عمليات غسل الأموال وتمويل الإرهاب وأهمية الاستعداد للجولة الثانية من عملية التقييم المتبادل – 2015.
66. التعامل مع مخاطر التعرضات الكبيرة وتجارب الدول العربية – 2015.
67. العلاقة المتداخلة بين الاستقرار المالي والشمول المالي – 2015.
68. متطلبات تبني استراتيجية وطنية شاملة لتعزيز الشمول المالي في الدول العربية – 2015.
69. متطلبات رأس المال الإضافي للحد من مخاطر التقلبات في دورات الأعمال ومنح الائتمان – 2015.
70. احتياجات الارتقاء بنظم الدفع صغيرة القيمة – 2015.
71. المعايير الدولية للتقارير المالية وانعكاساتها على الرقابة المصرفية – تطبيق المعيار رقم تسعة – 2017.
72. **سلامة وأمن المعلومات المصرفية الإلكترونية – 2017.**
73. مبادئ حوكمة المؤسسات المصرفية (ورقة محدثة) – 2017.
74. Financial Inclusion Measurement in the Arab World - 2017.
75. تطوير خدمات نظم الاستعلام والتصنيف الائتماني لقطاع المنشآت الصغيرة والمتوسطة في الدول العربية– 2017.
76. Financial Education Initiatives in the Arab Region -2017.
77. نشرة تعريفية بمفاهيم الشمول المالي – 2017.
78. كتيب تعريفي بمجلس محافظي المصارف المركزية ومؤسسات النقد العربية – 2017.
79. إدارة مخاطر السيولة في نظم الدفع والتسوية اللحظية – تجربة مؤسسة النقد العربي السعودي – 2017.
80. الإطار القانوني لحماية مستهلكي الخدمات المالية – 2017.
81. توافق السياسات الاحترازية والسياسات الاقتصادية الكلية – 2017.
82. Payments and Securities Settlement Systems in Lebanon - 2017

للحصول على مطبوعات صندوق النقد العربي

يرجى الاتصال بالعنوان التالي:

صندوق النقد العربي

ص.ب. 2818

أبوظبي - الإمارات العربية المتحدة

هاتف رقم: 6215000 (9712+)

فاكس رقم: 6326454 (9712+)

البريد الإلكتروني: centralmail@amfad.org.ae

موقع الصندوق على الإنترنت: http://www.amf.org.ae

http://www.amf.org.ae

صندوق النقد العربي
ARAB MONETARY FUND

أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية