

الفصل الخامس أولاً: تمهيد حول المصرفية الالكترونية • يقصد بعبارة المصرفية الالكترونية الخدمات المصرفية التي تقدمها المصارف او ممثلوها عبر أجهزة تعمل تحت رقابة وإدارة مباشرة من المصرف او بموجب اتفاقية اسناد هذه المهمة لجهة اخرى تعتبر المصرفية الالكترونية مصطلح عام لعملية يمكن بواسطتها للعميل القيام بعمليات مصرفية الكترونية بدون زيارة الفرع • يشمل هذا المصطلح الأنظمة التي تمكن عملاء المصارف سواء افراد او شركات من الوصول الي حساباتهم او تنفيذ عملياتهم او الحصول علي معلومات تتعلق بمنتجات وخدمات مالية عبر شبكة عامة او خاصة بما في ذلك شبكات الانترنت • تواجه المصارف تحدي التكيف والابتكار والتعامل مع الفرص التي تقدمها التطورات التقنية فقد استفادت المصارف وعملائها الي حد كبير من نمو المصرفية الالكترونية اذا اتاحت المصرفية الالكترونية للمصارف التوسع في تقديم الخدمات الي من يتعذر عليهم الوصول اليها وتقليص تكاليف العمليات وتحسين الفاعلية وتقديم خدمات مصرفية مباشرة • علي الجانب الاخر استفاد العملاء من الخدمات المصرفية الفعالة بتكاليف اقل نسبيا مع اتاحة خيار الاختيار من القنوات البديلة لتقديم الخدمات كما سهلت المصارف للالكترونية الانتقال السريع للاموال محليا وعبر الحدود نظرا لاهمية الموضوع أصدرت لجنة بازل للرقابة المصرفية في عام 2003 مبادي ادارته المخاطر المصرفية الالكترونية والتي تتكون من 14 مبدا تتناول الاشراف الفعال علي المخاطر المصاحبة لنشاطات المصرفية الالكترونية والضوابط الأمنية وادار المخاطر القانونية ومخاطر السمعة • مخاطر المصرفية الالكترونية • أنواع التهديدات المرتبطة بالقنوات الالكترونية • طرق التصدي • دور المصارف المركزية والتنسيق مع السلطات الأخرى

ثانيا: مخاطر المصارف الالكترونية لتحديد ماهية المخاطر من المفيد تحديد أنواع وخدمات المصرفية والالكترونية وتتمثل اهم الخدمات المصرفية الالكترونية وفقا للمواقع الالكترونية بما يلي: أ- المواقع الالكترونية للحصول علي المعلومات فقط تعرف هذه المواقع بانها تلك التي تتيح الدخول لغرض الحصول علي معلومات عن التسويق بشكل عام ومعلومات اخرى متاحة للجمهور او لارسال رسائل بريدية الكترونية غير حساسة ويجب علي المصارف ضمان تحذير العملاء من المخاطر المحتملة المرتبطة بالرسائل البريدية الالكترونية غير المشفرة عبر وسيله كهذه ب- المواقع الالكترونية لنقل المعلومات تعد هذ المواقع تفاعلية من حيث انها تمكن من ارسال الرسائل او الوثائق او الملفات الحساسة فيما بين مجموعة من المستخدمين مثل موقع الكتروني لمصرف يتيح للعميل تقديم طلب الحصول علي قرض او حساب ايداع عن طريق الانترنت وبما ان المخاطر الامنيه المتعلقة بالاتصال والانظمه تشمل خصوصيه وسريه البيانات وسلامه البيانات وعدم الانكار وتصميم نظام الدخول لذا من الضروري وضع بعض الطرق للتخفيف من حده المخاطر ج - المواقع الالكترونيه لاتمام تنفيذ العمليات تمثل هذه المواقع اعلي درجه للطاقة التشغيليه كما انها تنطوي علي مستويات مرتفعه من المخاطر المتحملة فهذه الانظمه توفر الإمكانيات اللازمه للتقدم بطلب الحصول علي المعلومات وانظمه التحويل المعلومات الكترونيا بالاضافه الي الحصول علي الخدمات المصرفيه لتنفيذ العمليات عبر الانترنت وتوفر هذه الإمكانيات عن طريق الارتباط التفاعلي بين اجهزه العملاء وبين الانظمه الداخليه للمصرف كما ان العديد من الانظمه تشمل من هذه الإمكانيات علي ضوء ما تقدم فقد اوجدت الخدمات المصرفيه الالكترونيه تحديات لاداره المخاطر بالنسبه للمصارف وبالطبع تتاثر جميع المخاطر المرتبطه بالخدمات و المنتجات المصرفيه التقليديه بتطبيق تلك الخدمات وعلاوه علي ذلك هنالك فئات من المخاطر ذات صله بشكل خاص بالخدمات المصرفيه الالكترونيه تتمثل اهم المخاطر المصاحبه للخدمات المصرفيه الالكترونيه في مخاطر استراتيجيه وتشغيليه (عمليات ومخاطر تقنيه ومخاطر احتيال عبر الانترنت ومخاطر سمعه ومخاطر قانونيه) وفقا لما يلي : هي المخاطر الناتجه عن قرارات عما غير ملائمه وتطبيق خاطئ للقرارات او قصور او عدم الاستجابه للتغيرات الحاصله في الصناعات المصرفيه ويجب ان تتوافق الخدمة المصرفيه مع استراتيجيه المصرف الكليه ان تركز عمليه التخطيط اتخاذ القرارات علي كيفيه تصميم المصرفيه الالكترونيه وعمليه تطبيقها ومتابعتها ب - مخاطر تشغيليه (العمليات) تنشأ المخاطر التشغيليه من الاحتيال واطء المعالجه وتوقف النظام وعدم القدره علي تقديم المنتجات والخدمات والمحافظة علي الوضع التنافسي واداره المعلومات ولتقديم الخدمات المصرفيه الالكترونيه قد تعتمد المصارف علي اسناد مهام لشركات وبرمجيات خارجيه وتتطلب المصارف انظمه ملائمه لاداره المعلومات والسعه المناسبه لخدمات عملائها وانه من الضروري بالنسبه للمصارف تخطيط حالات الطوارئ واستئناف العمل لضمان قدرتها علي تقديم المنتجات والخدمات في الأحوال والظروف ج - مخاطر تقنيه هي المخاطر المتعلقة بتوقف العمل او خلل او تعطل النظام ناجم عن استخدام او اعتماد اجهزه الكمبيوتر والبرمجيات والاجهزه الالكترونيه وشبكات الانترنت بالاضافه الي انظمه الاتصال وان مثل هذه المخاطر قد ترتبط أيضا بتوقف النظام واطء المعالجه وخلل في البرمجيات واطء التشغيل وتعطل النظام وعدم ملاءمه السعه وضعف المراقبه

وقصور في حمايه والهجمات بقصد الحاق الضرر و حوادث الاختراق واعمال الاحتيال ويجب علي المصارف مراقبه كل عنصر و عمله تتعلق بانظمتها المصرفيه الالكترونيه ويمثل كل عنصر نقطه للمراقبه تؤخذ بعين الاعتبار وكذلك العناصر المتحملة التي يجب تقييمها بطريقه مناسبه قبل تطبيقها في بيئه المصرفيه الالكترونيه ويتاثر مستوي مخاطر العمليات بهيكل بيئه المعالجه للمصرف د - مخاطر الاحتيال عبر الانترنت يجب اخذ مخاطر الاحتيال المباشره عبر الانترنت بعين الاعتبار فالتخطيط غير القانوني للتحايل مثل هجمات المواقع المزوره والرسائل الالكترونيه وتزوير العناوين التي تتطلب افشاء معلومات شخصيه سريه وسرقه بيانات الهوية وتعرض المصرف لمخاطر عاليه له ولعملائه ويجب علي المصرف اتخاذ الإجراءات المناسبه لمنع حدوث خسائر نتيجة التعرض للاحتيال عبر الانترنت و القيام بالاجراء المناسب لحمايه عملائه ه - مخاطر السمععه تنشأ مخاطر السمععه نتيجة لراي الجمهور السلبي ويمكن ان تتضرر سمعه المصرف بواسطه الخدمات المصرفيه الالكترونيه التي تنفذ بشكل سيئ والتي تنسب بطريقه او اخري في نفور العملاء ومن المهم ان يفهم العملاء ما يمكن ان يتوقعوه بشكل معقول من المنتج او الخدمه وما هي المخاطر والفوائد الخاصه التي تترتب عليهم استخدامهم لهذه المنتجات او الخدمات ويمكن ان تساعد رفع مستوي تثقيف العميل وتقليل مخاطر السمععه للمصرف وبطلب من المصارف التواصل بطريقه شفافه وواضحه مع عملائه وعلي المصرف وضع استراتيجيه فعاله للتواصل و- مخاطر قانونيه هي مخاطر تنشأ من الانتهاكات او عدم الالتزام بالقوانين والانظمه واللوائح والمعايير وتزيد الحاجه لضمان التوافق بين الإعلانات الورقيه الالكترونيه والافصاحات والاشعارات من احتمال حدوث مخالفه قانونيه وتساعد عمليه المتابعه المنتظمه لمواقع المصرف الالكترونيه علي ضمان الالتزام بالقوانين والانظمه . المصرف هو المسؤول عن اداره المخاطر المذكورة أعلاه ويجب عليه ضمان ان اداره مخاطر المصرفيه الالكترونيه جزء لا يتجزأ من مخاطر المصرف بشكل عام ونتيجته لذلك يجب تعزيز وتنفيذ السياسات وإجراءات اداره المخاطر بشكل يناسب خدمات المصرفيه الالكترونيه علاوه علي ذلك يجب علي المصرف ضمان ان انظمه وضوابط اداره مخاطر المصرف يتم تحديثها حسب ما هو ضروري لكي تواجه المشاكل المصاحبه للمصرفيه الالكترونيه تعتبر الطبيعه المعقده لتقنيه المعلومات خصوصا المستخدمه بواسطه الانترنت مثال(مخاطر مصاحبه الاستخدام الانترنت مخاطر ذات صله بالشركاء في سلسله تقديم الخدمات مثل مزودي الاتصالات بائعي ومقدمي الانظمه ومقدمي المنتجات والخدمات) ومن اهم الأسباب الرئيسيه التي توجب علي المصرفي انشاء اطار عمل سليما لاداره المخاطر ويجب تغطيه جميع الاعمال ذات صله ومجالات التشغيل والدعم التي لديه مسؤوليات الاداره مخاطر التقنيه علي الخطوط اوالمستويات الوظيفيه من خلال تقديم وتحديد الاولويه للمخاطر لكي يتسني اعداد استراتيجيه للتعامل مع هذه المخاطر والتخفيف من حدتها ان المخاطر المصاحبه لخدمات المصرفيه لخدمات الالكترونيه لسيت في الحقيقه جديده لكن الطرق المختلفهالتي تنشأ من خلالها وحجمها واثارها المحتملته تتخذ ابعادا جديده ومن ناحيه اخري فان المخاطر الامنيه مثل تلك الي تتجلي في عمليات الهجوم لقطع الخدمه عن المستخدمين ليس لها سابقه او مقابل في الطريقه التقليديه لتنفيذ الاعمال قد تسبب انقطاعا حادا في عمليات المصرف مما يؤدي لخسائر فادحه لجميع الأطراف المتضررة يجب ان تغطي عمليه تحديد المخاطر تعين جميع أنواع التهديدات ونقاط الضعف والانكشاف الكامنه في هيكل المصرفيه الالكترونيه وجميع مكونات مثل الشبكات الداخليه والخارجيه والاجهزه والبرامج التطبيقات البرمجيه والعمليات والعناصر البشريه وخصوصا اثر سوء التصرف البشري وعلاوه علي ذلك يجب ان تغطي عمليه تحديد المخاطر بيئه المصرف الالكترونيه المباشره بالاضافه الي انظمه الدعم والمهام والاعتماد الفردي والمتبادل من اجل الحصول علي تقرير ملائم لحجم المخاطر يجب تقييم وحل المخاطر ذات الصله بعملية اطلاق منتجات او خدمات جديده او إجراءات تعديلات اساسيه للمنتجات والخدمات الموجوده خلال مراحل عمليه وضع التصورات والتطوير ويجب ان تكون إجراءات التحكم بالمخاطر واجراءات امنيه قبل او خلال مرحله التطبيق يجب علي المصرف تحديد وتصنيف المخاطر ذات الصله بعمليات المصرف علي سبيل المثال اعتماد صيغه لتصنيف المخاطر وتحديد خطه تشمل السياسات والممارسات والإجراءات لمعالجه هذه المخاطر ومدى فعاليه الخطه علي أساس مستمر وتحديد عمليات لعمل اختبارات منتظمه وتحديث الخطه لمراعاة التغيرات التي تحدث في التقنيه والتطورات القانونيه وبيئه العمل (وتشمل التهديدات الخارجيه والداخليه لامن المعلومات) ب - تحليل المخاطر و تحديد حجمها كما يجب موازانه تكاليف التحكم بالمخاطر والتخفيف من حدتها مقابل فوائد التي يمكن تحقيقها ويجب ان تتخذ المصارف قراراً يتعلق بالموارد التي تخصص لمهمه المراقبه انه من المهم التأكد من فعاليه الضوابط الداخليه بما في ذلك فصل المهام والرقابه الثنائيه والمطابقه حيث ان ضوابط امن المعلومات بشكل خاص أصبحت اكثر اهميه اذ تتطلب وجود إجراءات اضافيه أدوات وخبرات واختبارات ويجب علي المصارف تحديد

مستوي الضوابط الامنيه بناء علي تقييمها للخدمة التي تقدمها علي حساسيه المعلومات بالنسبه للعميل والمصرف ومستوي تحمل المخاطر القائم للمصرف د - متابعه المخاطر كما يجب القيام باختبارات مستمرة و مراجعه كفاءه و فعاليه اجراءات ادارة المخاطر و الضوابط المصاحبة و الاجراءات الامنيه الساريه . وينصح كثيرا بان يقوم المصرف باجراءات برنامج تقييم شامل للمخاطر بواسطه طرف ثالث سنويا أ- استهداف البنيه التحتيه : استهدفت ابرز الهجمات الالكترونيه تعطيل البنيه التحتيه للمصرف ومن اشهر أنواع التهديدات الاتي : 1- البرمجيات الخبيثه وتعطيل الخدمة الخدمات الخبيثه (malware) هي اختصار لكلمتين هما malicious software والبرمجيه الماكره او الخبيثه هي برمجيه تضمينها او ادراجها عمدا في نظام الحاسوب لأغراض ضاره فقد تستخدم لعرقلة تشغيل الحاسوب جمع معلومات حساسه او الوصول الي انظمه الكمبيوتر الخاصه وعندما يتم تثبيت البرمجيه الخبيثه فقد يكون من الصعب جدا ازلتها وبحسب درجه خطوره البرمجيه من الممكن ان يتراوح اذاها من ازعاج بسيط (بعض النوافذ الاعلانيه غير المرغوب فيها خلال عمل المستخدم علي الحاسوب سواء كان متصلا ام غير متصل بشبكته حواسيب) الي اذي غير قابل للإصلاح يتطلب اعاده تهيئه القرص الصلب علي سبيل المثال من الامثله علي البرمجيات الخبيثه الفيروسات واحصنه طرواده 2- استغلال الثغرات ويسمي أيضا بالهجوم دون انتظار zero day attack وهو عبارة عن استغلال نقاط الضعف في برمجيات وثغراتها الأمنية خاصه غير المعروفة منها للعامة او حتي مطوريها في شن هجمات الكترونيه وغالبا ما يتم استغلال هذه الثغرات بل وتشاركها بين القراصنة (hackers) بل ان تكتشفها الجهات المطوره للبرمجيات المصايبه وتسمح المعرفة بالثغرة الأمنية من قبل المطورين لمستغليها الحصول علي فترة زمنية ينشر فيها ادواته الخبيثه لتحديث ضررا كبيرا لانه متي ما اكتشفت الثغرة الأمنية يسارع المطورون لسدها من خلال نشر برامج تصحيحيه ويأتي مصطلح (zero day attack) من كون ان مستغل الثغرة الأمنية غير المعروفة لا يترك أي يوم يمر لبدء هجومه كونه في سباق مع الزمن وكلما تأخر اكتشاف الثغره منح ذلك مزيد من الوقت للمهاجمين في توسيع نطاق الهجوم واضافه ضحايا جدد - اغلب المستخدمين لا يلم بصفه عامه المخاطر الأمنية للهواتف الذكية ج- الرسائل المزيفه عبر وسائل الاتصال المختلفه (الاستدراج الالكتروني) : ان الاستدراج هو هجوم علي هوية شخص قد يكون عميلا لاحد المصارف ولقد جرت العاده علي اطلاق مصطلح "سرقة الهوية" علي هذا النوع من الهجمات لان غرض المهاجم هو الحصول علي البيانات الشخصية باستخدام تقنيات مختلفه كالمواقع الوهميه والرسائل الالكترونيه المزيفه. الخ فالاستدراج الالكتروني هو عبارة عن نشاط اجرامي ينطوي علي محاوله الحصول علي معلومات حساسه كهوية المستخدم وكلمة السر وبيانات الحسابات عن طريق الاحتيال من خلال انتحال هوية صديق موثوق او شركة او مصرف في رساله الكترونيه او موقع وهمي وتعتبر الشركات التي تقدم خدمات استثماريه علي الانترنت او المصارف الالكترونيه مواقع مستهدفه لعمليات الاستدراج اما اكثر وسائل الاتدراج شيوعا فهي الرسائل الالكترونيه وغالبا ما تنطوي علي طلب للمستخدمين بالكشف علي تفاصيل شخصيه عبر موقع وهمي وعلي الشبكه العنكبوتيه وكذلك تتم عمليات الاستدراج باستخدام المكالمات الهاتفية والرسائل النصية خامسا: طرق التصدي تشمل اهم طرق التصدي ما يلي :