الفصل الخامس أولا: 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 لجهةاخري تعتبرالمصرفية الالكترونية مصطلح عام لعملية يمكن بواسطتها للعميل القيام بعمليات مصرفية الكترونية بدون زيارة الفرع ● يشمل هذا المصطلح الأنظمة التى 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 اوخاصة 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 اداره 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 اخري 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 المتعلقه 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 للطاقه التشغيليه كما انها تنطوي علي مستويات مرتفعه من المخاطر المتحمله فهذه الانظمه توفر الإمكانات اللازمه للتقدم بطلب الحصول علي المعلومات وانظمه التحويل المعلومات الكترونيا بالاضافه الي الحصول علي الخدمات المصرفيه لتنفيذ العمليات عبر الانترنت وتوفر هذه الإمكانات عن طريق الارتباط التفاعلي بين اجهزه العملاء وبين الانظمه الداخليه للمصرف كما ان العديد من الانظمه تشمل من هذه الإمكانات 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 الصناعه المصرفيه ويجب ان تتوافق الخدمة المصرفيه مع استراتيجه المصرف الكليه ان تركز عمليه التخطيط اتخاذ القرارات علي كيفيه تصميم المصرفيه الالكترونيه وعمليه تطبيقها ومتابعتها ب ـ مخاطر تشغيليه (العمليات) تنشا المخاطر التشغيليه من الاحتيال واخطاء المعالجه وتوقف النظام وعدم القدره علي تقديم المنتجات والخدمات والمحافظه علي الوضع التنافسي وادراه المعلومات ولتقديم الخدمات المصرفيه الالكترونيه قد تعتمد المصارف علي اسناد مهام لشركات وبرمجيات خارجيه وتتطلب المصارف انظمه ملائمه الاداره 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 ـ مخاطره تقنيه هي المخاطر المتعلقه 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 واخطاء المعالجه وخلل في البرمجيات واخطاء 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 عمليه تتعلق بانظمتها المصرفيه الالكترونيه ويمثل كل عنصر نقطه للمراقبه تؤخذ بعين الاعتبار وكذلك العناصر المتحمله التي يجب تقييمها بطريقه مناسبه قبل تطبيقها في بيئه المصرفيه الالكترونيه ويتاثر مستوي مخاطر العمليات بهيكل بيئه المعالجه للمصرف د ـ مخاطر الاحتيال عبر الانترنت يجب اخذ مخاطر الاحتيال البماشره عبر الانترنت بعين الاعتبار فالتخطيط غير القانوني للتحايل مثل هجمات المواقع المزوره والرسائل الالكترونيه وتزوير العناوين التي تتطلب افشاء معلومات شخصيه سريه وسرقه بيانات الهويه 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 ـ مخاطر السمعه تنشا مخاطر السمعه نتيجه لراي الجمهور السلبي ويمكن ان تتضرر سمعه المصرف بواسطه الخدمات المصرفيه الالكترونيه التي تنفذ بشكل سيئ والتي تتسب 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 السمعه للمصرف وبطلب من المصارف التواصل بطريقه شفافه وواضحه مع عملائه وعلي المصرف وضع استراتيجيه فعاله للتواصل و ـ مخاطره قانونيه هي مخاطر تنشا 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 الالكتروني علي ضمان الالتزام بالقوانين والانظمه . المصرف هو المسؤول عن اداره المخاطر المذكورة أعلاه ويجب عليه ضمان ان اداره مخاطر المصرفيه الالكترونيه جزء لا يتجزا من مخاطر المصرف بشكل عام ونتيجه 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 ومقدمى 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 تنشا من خلالها وحجمها واثارها المحتمله 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 و العناصر 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 بعمليه اطلاق منتجات او خدمات جديده او إجراءات تعديلات اساسيه للمنتجات والخدمات الموجوده خلال مراحل عمليه وضع التصورات والتطوير ويجب ان تكون إجراءات التحكم بالمخاطرواجراءات 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 ومدي فعاليه الخطه علي أساس مستمر وتحديد عمليات لعمل اختبارات منتظمه وتحديث الخطه لمراعاه التغيرات التي تحدث في التقنيه والتطورات القانونيه وبيئه العمل (وتشمل التهديدات الخارجيه والداخليه لامن المعلومات) ب ـ 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 للخدمه التي تقدمها علي حساسيه المعلومات بالنسبه للعميل والمصرف ومستوي تحمل المخاطر القائمه للمصرف د ـ متابعه المخاطر كما يجب القيام باختبارات مستمرة و مراجعه كفاءه و فعالية اجراءات ادارة المخاطر و الضوابط المصاحبة و الاجراءات الامنيه الساريه . وينصح كثيرا بان يقوم المصرف باجراءات برنامج تقييم شامل للمخاطر بواسطه طرف ثالث سنويا أـ استهداف البنيه التحتيه : استهدفت ابرز الهجمات الالكترونيه تعطيل البنيه التحتيه هي اختصار malware) (للمصرف ومن اشهر أنواع التهديدات الاتي : 1ـ البرمجات الخبيثه وتعطيل الخدمه الخدمات الخبيه والبرمجيه الماكره او الخبيثه هي برمجيه تضمينها او ادراجها عمدا في نظام الحاسوب malicious software لكلمتين هما لأغراض ضاره فقد تستخدم لعرقله تشغيل الحاسوب جمع معلومات حساسه او الوصول الي انظمه الكمبيوتر الخاصه وعندما يتم تثبيت البرمجيه الخيثه فقد يكون من الصعب جدا ازالتها 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 بشبكه حواسيب) الي اذي غير قابل للإصلاح يتطلب اعاده تهيئه القرص الصلب علي سبيل المثال من الامثله علي البرمجيات الخبيثه وهوعبارة عن استغلال zero day attack الفيروسات واحصنه طرواده 2 ـاستغلال الثغرات ويسمي أيضا بالهجوم دون انتظار نقاط الضعف في برمجيات وثغراتها الأمنية خاصه غير المعروفة منها للعامة او حتي مطوريها في شن هجمات الكترونية وغالبا ما بل ان تكتشفها الجهات المطورة للبرمجيات المصابة وتسمح(hackers) يتم استغلال هذه الثغرات بل وتشاركها بين القراصنة المعرفة بالثغرة الأمنية من قبل المطورين لمستغليها الحصول علي فترة زمنية ينشر فيها ادواته الخبيثة لتحدث ضررا كبيرا لانه من(zero day attack) متي ما اكتشفت الثغرة الأمنية يسارع المطورون لسدها منخلال نشر برامج تصحيحيه وياتي مصطلح 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 واضافة ضحايا جدد ـاغلب المستخدمين لا يلم بصفه عامة المخاطر الأمنية للهواتف الذكية جـالرسائل المزيفة عبر وسائل الاتصال المختلفة (الاستدراج الالكتروني) :ان الاستدراج هو هجوم علي هوية شخص قد يكون عميلا لاحد المصارف ولقد جرت العادة علي اطلاق مصطلح"سرقة الهوية" علي هذا النوع من الهجمات لان غرض المهاجم هو الحصول علي البيانات الشخصية باستخدام تقنيات مختلفة كالمواقع الوهمية والرسائل الالكترونية المزيفة. الخ فالاستدراج الالكتروني هو عبارة عن نشاط اجرامي ينطوي علي محاولة الحصول علي معلومات حساسة كهوية المستخدم وكلمة السر وبيانات الحسابات عن طريق الاحتيال من خلال انتحال هوية صديق موثوق او شركة او مصرف في رسالة الكترونيه او موقع وهمي وتعبتر الشركات التي تقدم خدمات استثمارية علي الانترنت او المصارف الالكترونية مواقع مستهدفه لعمليات الاستدراج اما اكثر وسائل الاتدراج شيوعا فهي الرسائل الالكترونيه وغالبا ما تنطوي علي طلب للمستخدمين بالكشف علي تفاصيل شخصية عبر موقع وهمي وعلي الشبكه العنكوبتية وكذلك تتم عمليات الاستدراج باستخدام المكالمات الهاتفية والرسائل النصية خامسا: طرق التصدي تشمل اهم طرق التصدي ما يلي :