2010

التجارة الالكترونية
الخدمات المصرفية الالكترونية و تأمينها

اعداد : فوزي سيتاي

ASK PC Academy

5/20/2010

المحتويات

بسم الله الرحمن الرحيم

لشكر و الإهداء

الشكر لله سبحانه و تعالى الذي علم الإنسان ما لم يعلم ..

ثم أشكر كل الذين ساهموا معي في إعداد هذا البحث المتواضع ..

و أشكر القائمين على ASK PC Academy على إتاحتهم لي الفرصة في المشاركة في هذه المسابقة الرائع و أهدي لهم هذا العمل المتواضع ..

فوزي سيتاي

ملخص البحث

شهدت السنوات القليلة الأخيرة تحولا جذريا في التجارة , و تطور التقنية المعلومات و الاتصالات و تجلى ذلك فيما يعرف بـ (التجارة الالكترونية) , إذ حققت الكثير من المنظمات التي تحولت من التجارة التقليدية إلى التجارة الالكترونية إنجازات باهرة , فإن ذلك قد بدأ يحفز المنظمات الأخرى للتحول نحو التجارة الالكترونية . بالرغم من الاجابيات و مزايا التجارة الالكترونية مثل الراحة و السعر و الاختيار فإن التهديدات الأمنية و الإختراق غير أخلاقية تقف أمام التجارة الالكترونية , و أينما وجدت المشكلة فإن الحلول موجودة بلا شك , لذلك فإن التجارة الالكترونية ستشق الطريقها إلى الريادة , لذلك تناولت في المبحث الأول عن مفهوم التجارة الإلكترونية و أهميتها و فوائدها في دفع عجلة الاقصاد العالمي , و مبينا الأرقام و مؤشرات التي تدل على تطور و تقدم التجارة الالكترونية , مع إستشهاد بأنجح الشركة العالمية في مجال التجارة الالكترونية . مع ولادة التجارة الالكترونية ظهرت طرق الدفع الالكتروني لشراء من المتاجر الالكترونية , و لتكامل دائرة التجارة الالكترونية قامت البنوك بتدشين الخدمات المصرفية الالكترونية لتسهيل على العملاء إجراء معاملاتهم البنكية كتحويل المال و كشف الحسابات و غيرها , لذلك قمت بمناقشة هذا الموضوع في المبحث الثاني موضحا مفهوم الخدمات المصرفية الالكترونية , المخاطر التي تأثر عليها و الأهداف من التحكم و الضبط في عمليات المصرفية الالكترونية , و في ختام المبحث عرضت الحلول المبتكرة لتأمين الخدمات المصرفية الالكترونية , و من تلك الحلول التحقق من الهوية ثنائي العناصر أو المعيار , مع ذكر البنوك التي طبقت هذه الحلول .

المبحث الأول : التجارة الإلكترونية

1-1 مفهوم التجارة الإلكترونية

تعتبر التجارة الإلكترونية واحدة من التعابير الحديثة والتي أخذت بالدخول إلى حياتنا اليومية حتى أنها أصبحت تستخدم في العديد من الأنشطة الحياتية والتي هي ذات ارتباط بثورة تكنولوجيا المعلومات والاتصالات. التجارة الإلكترونية تعبير يمكن أن نقسمه إلى مقطعين، حيث أن الأول، وهو "التجارة"، والتي تشير إلى نشاط اقتصادي يتم من خلال تداول السلع والخدمات بين الحكومات والمؤسسات والأفراد وتحكمه عدة قواعد وأنظمة يمكن القول بأنه معترف بها دولياً، أما المقطع الثاني "الإلكترونية" فهو يشير إلى وصف لمجال أداء التجارة، ويقصد به أداء النشاط التجاري باستخدام الوسائط والأساليب الإلكترونية مثل الإنترنت.

لا يوجد تعريف يمكن القول عنه على أنه تعريف متفق عليه دولياً للتجارة الإلكترونية، ولكن اجتهد المعنيون في هذا الشأن في إدراج العديد من التعاريف حول أدبيات موضوع التجارة الإلكترونية، محاولين الوصول إلى تعريف شامل وعام يقوم على خدمة المتعاملين في التجارة الإلكترونية، ومن هذه التعاريف:

1. منهج حديث في الأعمال موجه إلى السلع والخدمات وسرعة الأداء، ويتضمن استخدام شبكة الاتصالات في البحث واسترجاع المعلومات من أجل دعم اتخاذ قرار الأفراد والمنظمات
2. مزيج من التكنولوجيا والخدمات من أجل الإسراع بأداء التبادل التجاري وإيجاد آلية لتبادل المعلومات داخل مؤسسة الأعمال وبين مؤسسات الأعمال، وبين مؤسسات الأعمال والعملاء، أي عمليات البيع والشراء
3. إنتاج، وترويج، وبيع، وتوزيع المنتجات بواسطة شبكة اتصالات
4. عمليات تبادل باستخدام نظام تبادل البيانات إلكترونياً (بالإنجليزية: Electronic Data Interchange) والبريد الإلكتروني والنشرات الإلكترونية والفاكس وتحويل الأموال بواسطة الوسائط الإلكترونية (بالإنجليزية: Electronic Funds Transfer) وكذلك كافة الوسائط الإلكترونية المشابهة
5. بنية أساسية تكنولوجية تهدف إلى ضغط سلسلة الوسائط استجابة لطلبات السوق وأداء الأعمال في الوقت المناسب
6. نوع من تبادل الأعمال حيث يتعامل أطرافه بطريقة أو وسيلة إلكترونية عوضاً عن استخدامهم لوسائط مادية أخرى بما في ذلك الاتصال المباشر
7. شكل من أشكال التبادل التجاري من خلال استخدام شبكة الاتصالات بين مؤسسات الأعمال مع بعضها البعض، ومؤسسات الأعمال وزبائنها، أو بين مؤسسات الأعمال والإدارة العامة
8. استخدام تكنولوجيا المعلومات لإيجاد روابط فعاله بين مؤسسات الأعمال في العمليات التجارية
9. نوع من عمليات البيع والشراء ما بين المنتجين والمستهلكين، أو بين مؤسسات الأعمال وبعضها البعض من خلال استخدام تكنولوجيا المعلومات والاتصالات
10. أداء العملية التجارية بين شركاء تجاريين باستخدام تكنولوجيا معلومات متطورة من أجل رفع كفاءة وفاعلية الأداء

ويمكن أن نخلص إلى تعريف يجمع بين التعاريف سالفة الذكر على النحو التالي: التجارة الإلكترونية هي "تنفيذ كل ما يتصل بعمليات بيع وشراء السلع والخدمات والمعلومات باستخدام شبكة الإنترنت، بالإضافة إلى الشبكات التجارية العالمية الأخرى"، ويشمل ذلك:

1. عمليات توزيع وتسليم السلع ومتابعة الإجراءات
2. سداد الالتزامات المالية ودفعها
3. إبرام العقود وعقد الصفقات
4. التفاوض والتفاعل بين المشتري والبائع
5. علاقات العملاء التي تدعم عمليات البيع والشراء وخدمات ما بعد البيع
6. المعلومات عن السلع والبضائع والخدمات
7. الإعلان عن السلع والبضائع والخدمات
8. الدعم الفني للسلع التي يشتريها الزبائن
9. تبادل البيانات إلكترونياً (Electronic Data Interchange) بما في ذلك:
    1. التعاملات المصرفية
    2. الفواتير الإلكترونية
    3. الاستعلام عن السلع
    4. كتالوجات الأسعار
    5. المراسلات الآلية المرتبطة بعمليات البيع والشراء

1- 2 التجارة الإلكترونية أهميتها و فوائدها

يعكس النمو المتسارع للتجارة الإلكترونية جانبا كبيرا من أهميتها وفوائدها، وستتم الإشارة إليها

من خلال محاور ثلاثة:

أولا / للمستهلكين

1 . الحصول على منتوجات وخدمات اقل كلفة من خلال التسوق في أماكن عديدة والمقارنة السريعة عبر الشبكة.
2 . وجود خيارات اكثر حيث يمكن الاختيار من بين بائعين عديدين، والعديد من المنتوجات الأكثر مقارنة بأي أسلوب آخر.
3 . التسوق وعقد عمليات تجارية أخرى 24 ساعة باليوم وعلى مدار السنة.
4 . نقل المعلومات التفصيلية ذوات الصلة خلال ثوان وليس بأيام أو أسابيع.
5 . الحصول على منتوجات وخدمات تحقق المتطلبات الخاصة، من الحواسيب الشخصية إلى السيارات، وبأسعار منافسة.
6 . من الممكن قيام الأفراد بالعمل والدراسة وهم في المنزل.
7 . من الممكن القيام بمزادات علنية فعلية يتمكن المستهلكون من خلالها الحصول على منتوجات فريدة والتي لا يمكن الحصول عليها تقليديا إلا بالسفر إلى مسافات بعيدة للوصول إلى مزادات معينة بوقت محدد.
8 . تفاعل المستهلكين مع مستهلكين آخرين في المجتمعات الإلكترونية، وتبادل الأفكار، إضافة إلى مقارنة الخبرات.
9 . ازعاجات اقل، فلن يلتقي المستهلكون برجال البيع ويتعرضوا للاستغلال والإقناع، ولن ينتظروا في صفوف.
10 . الحصول على كم هائل من المعلومات المقارنة حول الشركات والمنتوجات والمنافسين والأسعار دون مغادرة المكتب أو البيت.

ثانيا / لمنظمات الأعمال

1 . تغيير صورة الشركات وتحويلها من شركات ضخمة مترهلة تعاني من هياكل تنظيمية قد تكون معقدة، ويعمل فيها أعداد كبيرة، إلى شركات صغيرة الحجم يعمل فيها عدد قليل من العاملين.
2 . توسيع سوق الشركة محليا ودوليا، واختراق أسواق جديدة، واكتشاف أو خلق قنوات بيعية جديدة.
3 . تصبح الشركات اكثر قربا من زبائنها وشركائها في العمل من خلال قنوات الاتصالات.
4 . التكيف السريع وفقا لظروف السوق، فالشركات تتمكن بسرعة من إضافة منتوجات إلى عروضها، وتغيير الأسعار والمواصفات.
5 . كلف اقل من خلال تجنب نفقات الاحتفاظ بمخازن وكلف الإيجار والتأمين والمنافع، وبالإمكان أعداد كتالوجات رقمية وتفادي كلف الطبع والإرسال والبريد.
6 . حجم الجمهور، فبالإمكان معرفة عدد الأشخاص الزائرين للمواقع على الشبكة، وتوقفهم في أماكن معينة بما يؤدي إلى تحسين العروض والإعلانات.
7 . بناء علاقات مع الجمهور من خلال الحوار معه.
8 .التجارة الإلكترونية متاحة أمام الشركات الصغيرة والكبيرة على حد سواء.
9 . ليس هناك تحديد حقيقي لمساحة الإعلان مقابل الطبع والنشر في الوسائل التقليدية.
10 . يمكن زيارة المواقع على الشبكة من قبل أي شخص في أي مكان في العالم وفي أي وقت.
11 . تقصير بل وحتى إزالة قنوات التوزيع مما يجعل المنتوج ارخص، وأرباح الباعة أعلى.
12 . تقليل حوالي % 90 من كلفة إنشاء ومعالجة وتوزيع وخزن واسترداد المعلومات القائمة على أساس ورقي.

ثالثا / للمجتمع

1 . تمكن أفراد اكثر من العمل في المنزل، والقيام بتنقلات اقل، مما يؤدي إلى تقليل الازدحام في الطرق، وتلوث هواء اقل.
2 . طالما أن هناك إمكانية لأن تباع سلع وخدمات بأسعار اقل فأن ذلك يؤدي إلى أن الأفراد الأقل غنى يمكنهم الشراء اكثر وبالتالي زيادة مستوى معيشتهم.
3 . تمكن الأفراد في الأقطار الأقل تطورا والأماكن الريفية من التمتع بالمنتوجات والخدمات التي لا يمكن أن تتوفر لهم بأسلوب آخر .ويشمل ذلك الفرص في تعلم المهن والحصول على درجات جامعية أو الحصول على رعاية طبية افضل.
4 . تسهيل تقديم الخدمات العامة بكلف توزيع اقل، وتحسين نوعية الخدمات الاجتماعية، وعمل الشرطة، والرعاية الصحية، والتعليم.

1 - 3 أرقام و مؤشرات على مدى تطور التجارة الإلكترونية

يتوقع الخبراء أن مبيعات التجارة الإلكترونية ستنمو نموا قويا على مدى السنوات القادمة , لما تتمتع بمزايا عديدة منها , الراحة و الإختيار و السعر , و كذلك الشركات في مجال التجارة الإلكترونية ستنمو نموا سريعا كشركة أمازون .

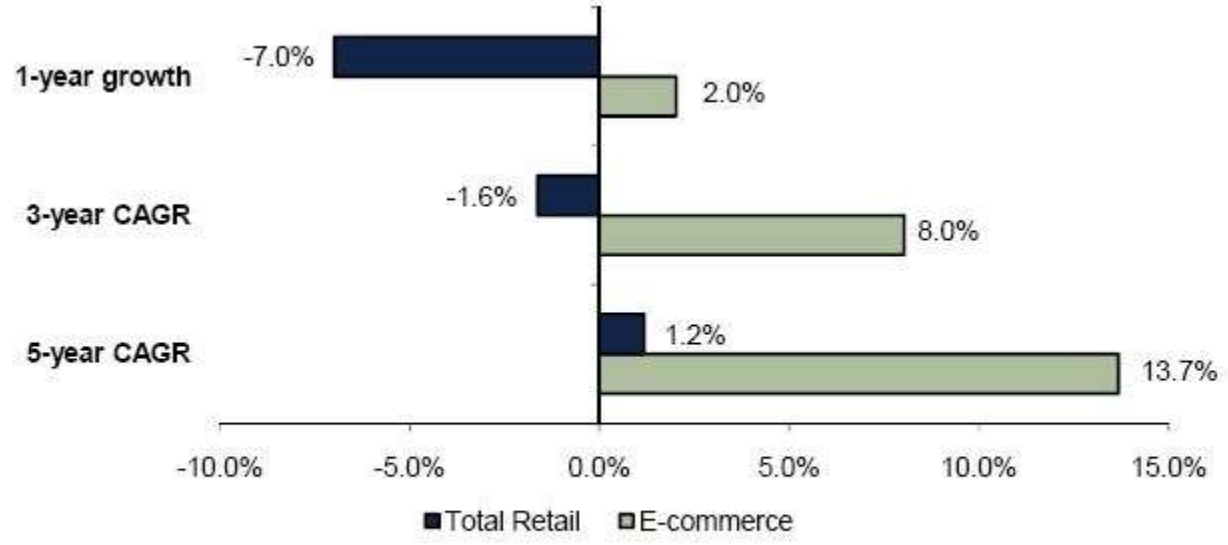
تتمتع التجارة الإلكترونية بفرصة كبيرة في سرعة النمو على المدى البعيد خصوصا في مجال المبيعات التجزئة ما لا يقل عن 10 السنوات المقبلة , و وفقا لمكتب الإحصاء الإمريكي , أن التجارة الإلكترونية بلغ مجموع مبيعات التجزئة حوالي 135 مليار دولار في عام 2009 بزيادة % 2.0 عن عام 2008 و بزيادة في المتوسط 13.7% عن السنوات الخمس الماضية . في حين تباطئ نسبة نمو مبيعات التجارة الإلكترونية من % 18.4 في 2007 إلى نمو بنسبة 4.4 % في 2008 إلى 2.0% في 2009 نتيجة لضغوط إقصادي على الإنفاق الإستهلاكي . و مبيعات التجارة الإلكترونية تسارع في النمو بنسبة % 2.0 في الربع الثالث من 2009 و بنسبة نمو % 14.6 في الربع الرابع من نفس العام ثلاث مرات متتالية بعد إنخفاضات الفصلية , و توقع الخبراء أن الولايات المتحدة نمو مبيعات التجارة الإلكترونية سنة كاملة و إسترداد نحو 10% في عام 2010 و الحفاظ على هذا المستوى خلال فترة 2011 إلى 2014 . في هذه المعادلات من النمو , فإن الخبراء قدروا حصة التجارة الإلكترونية مبيعات التجزئة تصل إلى 5.5% في عام 2014 إرتفاعا من 3.7% في عام 2009 .

الشكل (1) U.S. E-commerce Retail Sales, 2002-2014E

Sources: U.S. Census Bureau, William Blair & Company estimates

تحول إنفاق المستهلكين من خلال إنترنت , زاد نسبة التجارة الإلكترونية مبيعات التجزئة نحو 1.4 ٪ من اجمالى مبيعات التجزئة في عام 2002 إلى 3.7 ٪ في عام 2009. خلال فترة خمس سنوات الأخيرة ، وزادت مبيعات التجارة الإلكترونية في الولايات المتحدة بمعدل سنوي مركب بلغ 13.7 ٪ ، في حين أن نمو مبيعات التجزئة قد ارتفعت بمعدل سنوي مركب 1.2 ٪ خلال نفس الفترة. ونحن نتوقع نمو حجم انفاق المستهلكين و مواصلة التحول نحو التجارة الإلكترونية نتيجة مزاياها في الراحة , و إختيار , و السعر .

الشكل (2) E-commerce Versus Retail Sales Growth, 2004-2009



Source: U.S. Census Bureau

الجدول التالي يوضح نسبة المبيعات عبر الإنترنت في عام 2009 و المتوقعة في عام 2014:

U.S. Online Sales by Category (3) الشكل

Category	% of Sales Online 2009	2014E	Category	% of Sales Online 2009	2014E
PCs	57%	57%	Apparel and accessories	9%	13%
Software	52%	66%	Jewelry	9%	15%
Music	40%	73%	Auto parts	9%	14%
Peripherals	38%	40%	Large appliances	8%	12%
Videogames	27%	39%	Footwear	8%	10%
Event tickets	23%	26%	Pets	6%	11%
Books	22%	30%	Art and collectibles	6%	11%
Housewares/small appliances	16%	24%	Nutraceuticals	5%	7%
Office products	14%	18%	Medical supplies	5%	7%
Consumer electronics	14%	19%	Personal care	5%	8%
Videos	13%	19%	Over-the-counter drugs	4%	6%
Flowers	13%	19%	Garden supplies	4%	6%
Toys	12%	17%	Furniture	2%	5%
Movie tickets	11%	14%	Home improvement	2%	2%
Sporting goods	11%	14%	Grocery	1%	2%

Source: Forrester

الأعلى فئات نموا : مجموعة واسعة من فئات المنتجات تتمتع بنمو قوي في مبيعات التجارة الإلكترونية , في حين الإلكترونيات و البرمجيات من الفئات الأكثر مباعا على الإنترنت , و وفقا لفوريستر شهدت فئة الإلكترونيات الإستهلاكية نموا 17% و البرمجيات 12% و فئة الكمبيوتر 5% في عام 2009 . و كذلك الفئات الأخرى شهدت نموا قويا مثل التغذية و الأحذية , بينما فئات المجوهرات و تذاكر الحدث و الفن و المقتنيات شهدت نموا ضعيفا نتيجة البيئة الصعبة للمستهلك . و على مدى خمس السنوات القادمة من المتوقع نموا قويا لهذه الفئات .

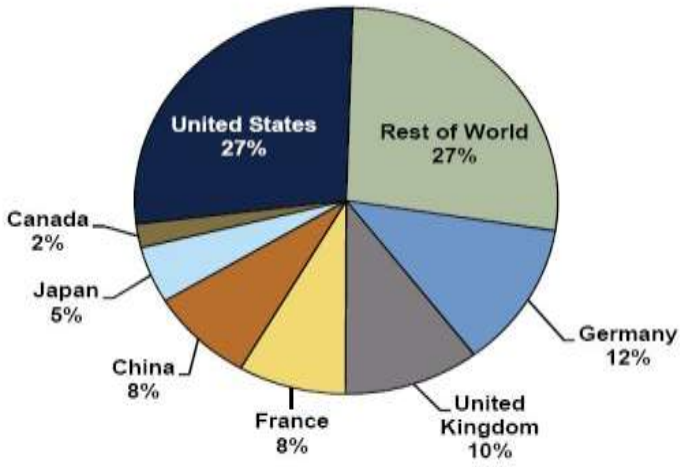
الشكل (4) U.S. Online Sales Growth by Category

Category	2009 Y/Y Growth	2009-2014E CAGR	Category	2009 Y/Y Growth	2009-2014E CAGR
Nutraceuticals	23%	13%	Office products	9%	9%
Footwear	20%	9%	Garden supplies	8%	11%
Grocery	19%	13%	Music	7%	10%
Consumer electronics	17%	12%	Videos	6%	9%
Apparel and accessories	16%	11%	Peripherals	6%	5%
Personal care	16%	14%	Movie tickets	6%	10%
Toys	16%	9%	PCs	5%	5%
Auto parts	15%	13%	Furniture	5%	15%
Over-the-counter drugs	15%	8%	Sporting goods	5%	9%
Pets	14%	17%	Videogames	4%	14%
Medical supplies	13%	12%	Home improvement	3%	8%
Software	12%	8%	Jewelry	2%	13%
Housewares/small appliances	12%	11%	Event tickets	2%	7%
Books	11%	8%	Art and collectibles	2%	16%
Flowers	9%	11%	Large appliances	-4%	10%

Note: Forrester estimates total e-commerce sales growth of 10.6% in 2009 compared with the Census Bureau growth estimate of 2.0%. The Forrester data is skewed to large e-commerce retailers, which experienced higher growth rates in 2009.
Source: Forrester

في الرسم البياني التالي يشير على أن الولايات المتحدة هي أكبر سوق التجارة الإلكترونية بنسبة 27% مقارنة بدول أخرى وفقا لمؤسسة آي دي سي . و ثاني أكبر أسواق التجارة الإلكترونية هي ألمانيا , و التي تمثل حوالي 12% مقارنة بدول أخرى , ثم المملكة المتحدة و تمثل حوالي 10% . و يتوقع الخبراء أن معظم الأسواق التجارة الإلكترونية ستنمو بمعدل أسرع من الولايات المتحدة خلال السنوات الخمس القادمة , مع نمو قوي في تطوير التجارة الإلكترونية بشكل خاص في أسواق الصين . في حين توقع الخبراء أن الولايات المتحدة تتمتع نمو صحي على مدى السنوات القليلة القادمة .

الشكل (5) Global E-commerce Sales, 2008

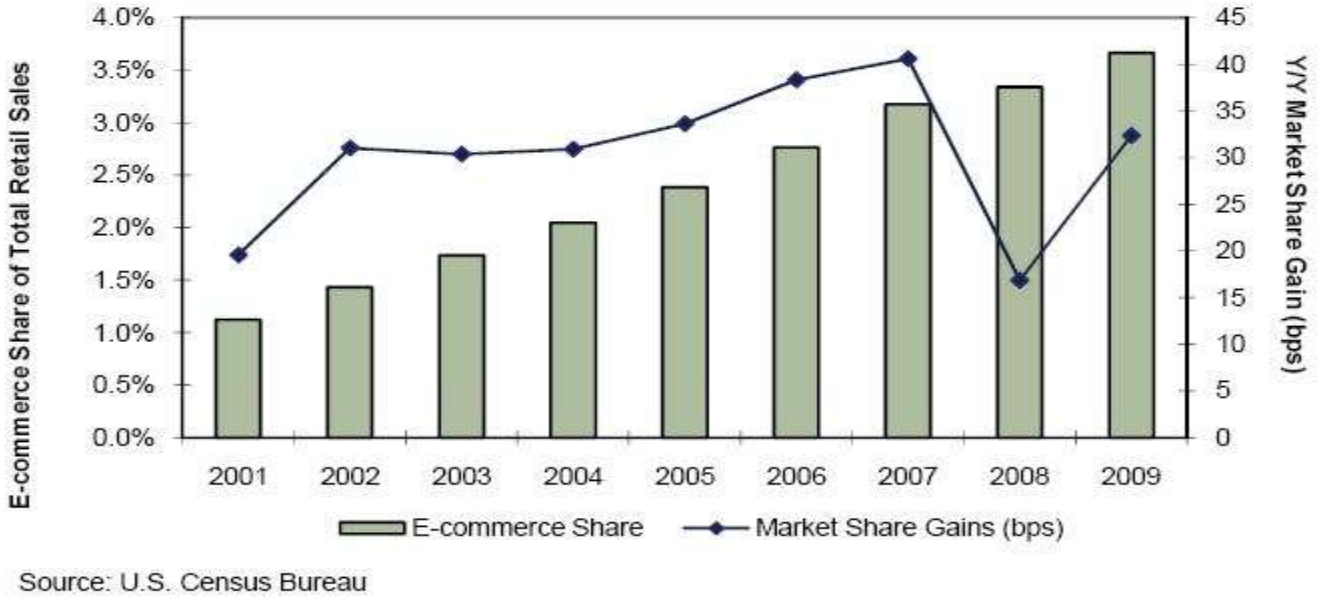


Source: International Data Corporation

تزايد حصة الإنفاق الإستهلاكي

تحول إنفاق المستهلكون عبر الانترنت أصبح أمر شائع الآن , و يتوقع الخبراء بأن نمو حجم إنفاق المستهلكون عبر التجارة الالكترونية متزايدة في السنوات القادمة نتيجة مزايا التجارة الالكترونية في الراحة , و الاختيار , و السعر . مبيعات التجزئة خلال التجارة الالكترونية أرتفعت 0.9% من إجمالي مبيعات التجزئة الامريكية في عام 2000 إلى 3.7% في عام 2009. و خلال فترة نفسها , زادت مبيعات التجارة الالكترونية في الولايات المتحدة بمعدل نمو قدره 19% , من 27.7 مليار دولار في عام 2000 إلى 134.9 مليار دولار في 2009 . في حين أن مبيعات التجارة الالكترونية في نمو متباطئ من مستويات 4.4% في عام 2008 و 2.0% في 2009, واصلت زيادة حصة التجارة الالكترونية من إجمالي مبيعات التجزئة . مع ذلك تباطأ مكاسب حصة التجارة الالكترونية إلى 17 نقطة في 2008 بعد مكاسب 38 نقطة في 2006 و 41 نقطة في 2007 . و رغم تباطأ المكاسب في 2008 , فإنها تتسارع إلى 32 نقطة في 2009 .

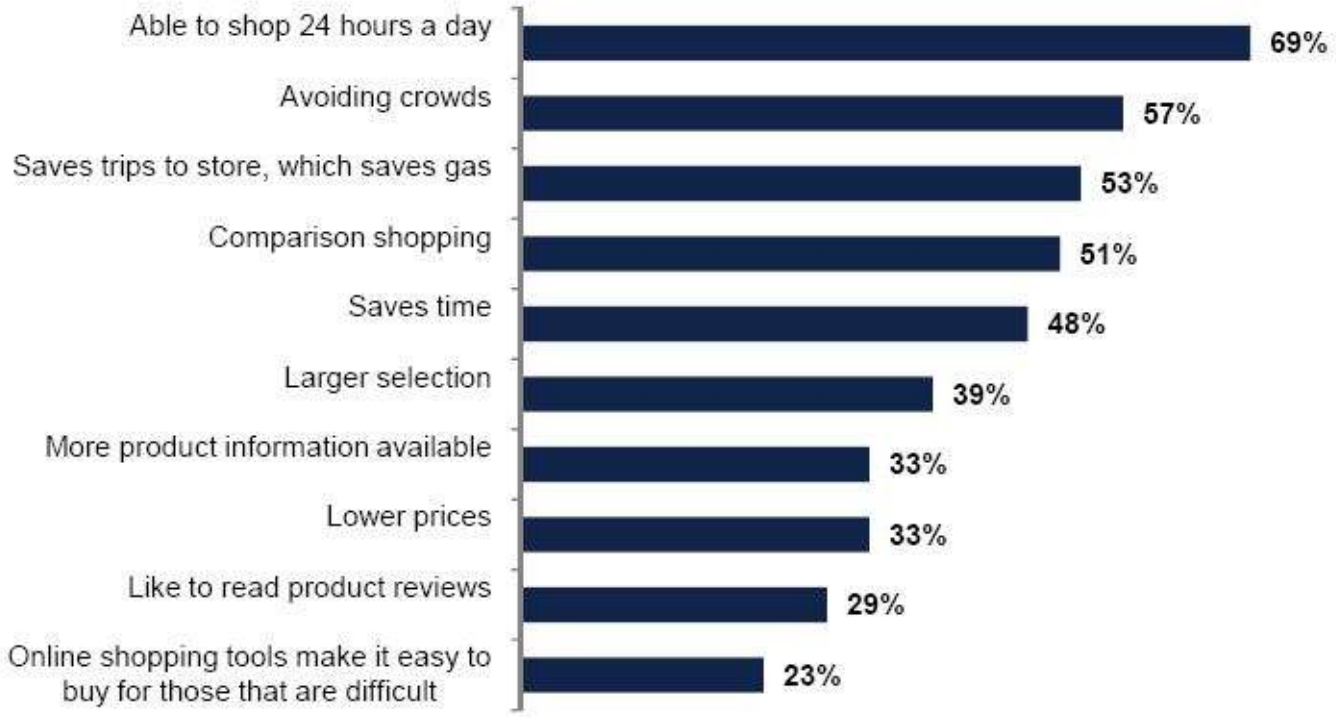
الشكل (6)E-commerce Retail Sales and Share, 2001-2009



Source: U.S. Census Bureau

الدراسات الإستقصائية التي أجريت من قبل Nielsen Online و Harris Interactive تبين أن الراحة , و الاختيار , و مزايا السعر , هي الأسباب التي أدت إلى الإقبال المتزايد على التجارة الالكترونية من بين المتسوقين .

Top 10 Reasons Consumers Purchase Online (7) الشكل



Source: Nielsen Online

Reasons to Purchase Online (8) الشكل

	% of Respondents	
Reason	**Female**	**Male**
I purchase online because it's easier to find the product I'm looking for	76%	71%
Generally, there is a broader choice of products online than in my local stores	75%	72%
Generally, there is a broader choice of retailers online than are available in my local market	73%	69%
I purchase online because it takes less time than going to a store	72%	61%
Online retailers are more likely to have my product in stock as compared with the stores	68%	65%
I feel paying for a product online is just as secure as in the store	65%	61%
Generally, prices are lower online than at the store	51%	60%
I purchase online to save money on gas	50%	36%

Source: Harris Interactive

1 – 4 دراسة حالة : أمازون الرائد في مجال التجارة الإلكترونية

أمازون شركة أمريكية مختصة بالتجارة الإلكترونية يقع مقرها في سياتل بولاية واشنطن . كانت أمازون أولى الشركات الكبرى التي تقدم على بيع السلع عبر شبكة الإنترنت حتى أصبحت رمزا لازدهار شركات تقنية المعلومات في أواخر التسعينات . و في أعقاب تفجر فقاعة الإنترنت واجهت أمازون شكوكا قوية بشأن إمكانية استمرارها إلا أنها سرعان ما عادت بقوة لتعلن عن تحقيق أول أرباح سنوية لها في عام 2003 .
تأسست الشركة في عام 1994 من قبل جيف بيزوز لتبدأ أول نشاط لها في عام 1995 من خلال العمل بمثابة مخزن لبيع الكتب عبر الإنترنت و أستطاعت بعد فترة وجيزة أن تنوع خطوط نشاطها لتشمل بالإضافة تأسست الشركة في عام 1994 من قبل جيف بيزوز لتبدأ أول نشاط لها في عام 1995 من خلال العمل بمثابة مخزن لبيع الكتب عبر الإنترنت و أستطاعت بعد فترة وجيزة أن تنوع خطوط نشاطها لتشمل بالإضافة إلى الكتب أشرطة و أقراص الفيديو و أقراص الموسيقي و برامج الكمبيوتر و ألعاب الفيديو و الأجهزة الإلكترونية و الألبسة و الأثاث و المواد الغذائية و ألعاب الأطفال و سلع أخرى . و قد أسست الشركة مواقع منفصلة على الإنترنت في كندا و المملكة المتحدة و ألمانيا و النمسا و فرنسا و الصين و اليابان .
الإستحواذ و التوسع
في إبريل 1998 أقدمت أمازون على شراء شركة إنترنت موقي داتابيز .
في أغسطس 1998 أشترت الشركة بلانيت أول مقابل 800 ألف سهم من أسهمها .
في يونيو 1999 أشترت أمازون أكسيبت دوت كوم و إكستشينج دوت كوم ضمن صفقة لتبادل الأسهم قيمتها 645 مليون دولار .
في عام 2004 أشترت أمازون جويو دوت كوم و هي عبارة عن موقع تجاري صيني . كما بدأت الشركة العمل بـ أي ناين و هي شركة تركز أعمالها على البحث و بناء تكنولوجيا جديدة .
في مارس 2005 أستحوذت أمازون على شركة بوك سيرج و هي شركة للطباعة حسب الطلب و على شركة موبي بوكيت دوت كوم و إي بووك المصنعتين للبرامج .
في يوليو 2005 أشترت أمازون شركة كريبيت سبيس لتوزيع أقراص الفيديو الرقمية .
في فبراير 2006 أستحوذت أمازون على شوب بوب المتخصصة ببيع الألبسة الراقية .
في مايو 2007 أستحوذت أمازون على شركة دي بي ريفيوز كوم البريطانية للدراسات الخاصة بالتصوير و التي أسسها فيل أسكي .

الأمازون سوف يطيل ريادتها في مجال التجارة الإلكترونية

تشير الدراسات بأن قبل عام 2020 و أمازون قد تصل إلى 100 مليار دولار في المبيعات , و تتنافس في الحجم أمثال Carrefour و Home Depot و Tesco . مكاسب سهم أمازون تجبر تجار التجزئة التقليدية لتغيير نماذج الأعمال نحو التجارة الإلكترونية .
الأمازون هي أكبر متاجر التجزئة على الإنترنت في الولايات المتحدة و العالم , بلغت مبيعات الأمازون في شمال أمريكا (مبيعات التجزئة) إلى 12.3 مليار دولار , أو 9.1% من إجمالي السوق و التجارة الإلكترونية في الولايات المتحدة في عام 2009 . بما في ذلك مبيعات خارجية , و يقدر الخبراء أن أمازون حصتها في السوق يبلغ حوالي 12% إلى 13% و يعتقدون أن منطقة أمازون قد وضعت واحدة من أقوى و أهم العلامات التجارية الموثوق بها على شبكة الانترنت , مبنية على تجربة إستخدام متميز و بدعم من مجموعة واسعة , و أسعار منخفضة , و الراحة , كما هو مبين في الشكل 9, و الأمازون في شمال إمريكا نمو المبيعات فاق بكثير مقارنة بمناطق أخرى على مدى السنوات الثلاث الماضية .

الشكل (9) Amazon N.A. Sales Growth Versus U.S. E-commerce Retail Sales Growth
(First Quarter 2007-Fourth Quarter 2009)

Sources: U.S. Census Bureau and company data

Amazon تتغلب على eBay

وصلت أسعار أسهم Amazon.com إلى أعلى معدلاتها خلال شهر أكتوبر 2009 حيث استمر في الارتفاع دون أن يعانى من الآثار السلبية للخسائر التي شهدتها مؤشرات الشركات التقنية في البورصة. ويرجع هذا النجاح لما توليه Amazon من رعاية كبيرة لرسالة المؤسسة المتمثلة في خدمة العميل والحصول على ثقته إلى جانب ما لديها من خبرات في علم الإدارة حيث يشهد محرك التصفية داخلها تحسناً مستمراً. وأخيراً فان Amazon تمثل منصة بيع فائقة تطلب من البائعين توفير بيانات ودرجة كفاءة أعلى من eBay والنتيجة هي أن Amazon توفر أمناً أكثر للمشتري عن إجراء تعاملاته معها.

المبحث الثاني : الخدمات المصرفية الالكترونية و سبل تأمينها

2 – 1 مقدمة

إستطاعت الخدمات والمنتجات المصرفية المتوافرة عن طريق الشبكة العالمية للمعلومات (الإنترنت) أن تقدم فرصاً هائلة للبنوك ، فهي تتيح لهذة البنوك التوسع وخلق فرص تنافسية كبيرة في أسواقها من خلال الإستمرارية في أنشطة جذب الودائع ومنح الائتمان بصورة أكبر ، كما تتيح لها تقديم خدمات ومنتجات مصرفية جديدة أو دعم وتقوية وضعها التنافسي في السوق عن طريق تقديمها واستخدامها لأنظمة المدفوعات المتاحة حالياً ، بالإضافة إلى أن الخدمات المصرفية المتاحة عن طريق الإنترنت بإستطاعتها أن توفر في تكاليف التشغيل الخاصة بالبنوك والمؤسسات المالية .

ومما لاشك فيه فإن الاستمرار في تطوير الخدمات المصرفية المتاحة عن طريق الإنترنت تساهم بشكل أو بآخر في تحسين كفاءة أنظمة المدفوعات والأنظمة البنكية وتساهم أيضاً في خفض تكلفة العمليات الخاصة بعملاء التجزئة في البنوك سواء على المستوى الإقليمي أو المستوى الدولي ، وكذلك يكون للعملاء والبنوك القدرة على رفع كفاءة عمل أو استلام مدفوعاتهم وبالشكل الذي يكونوا فيه مرتاحين جداً بأداء تلك الأعمال ، كما أن الخدمات المصرفية المتاحة عبر الانترنت يمكن أن تساعد المؤسسات المالية في توفير عدد من القنوات والمنافذ للعملاء الذين كانو يعانون سابقاً من محدودية هذه الأنظمة والمؤسسات .

وعلى القدر الذي يمكن الجزم به حيال التطورات التقنية والسوقية المستقبلية في الخدمات المصرفية المتاحة عبر الإنترنت فإنه من المهم جداً أن تتجنب الصلاحيات الإشرافية كل السياسات والممارسات التي يمكن أن تحول دون تحقيق الفوائد والمقاصد التي من أجلها تم تطوير تلك التقنيات والخدمات ، ولايخفى في ذات الوقت أن البنوك قد أدركت بأن تلك الفوائد والخدمات التي تتيحها الإنترنت قد تتضمن مخاطر عديدة ويجب أن يتم أخذها بالإعتبار ومحاولة الموازنة بين تلك الفوائد وهذه المخاطر .

2- 2 مفهوم الخدمات المصرفية الإلكترونية

يقصد بالخدمات المصرفية الالكترونية تقديم البنوك الخدمات المصرفية التقليدية أو المبتكرة من خلال شبكات إتصال الكترونية تقتصر صلاحية الدخول إليها على المشاركين فيها وفقا لشروط العضوية التى تحددها البنوك، وذلك من خلال أحد المنافذ على الشبكة كوسيلة لإتصال العملاء بها بهدف:-

(1) إتاحة معلومات عن الخدمات التى يؤديها البنك دون تقديم خدمات مصرفية على الشبكة.

(2) حصول العملاء على خدمات محدودة كالتعرف على معاملاتهم وأرصدة حساباتهم وتحديث بياناتهم وطلب الحصول على قروض.

(3) طلب العملاء تنفيذ عمليات مصرفية مثل تحويل الأموال.

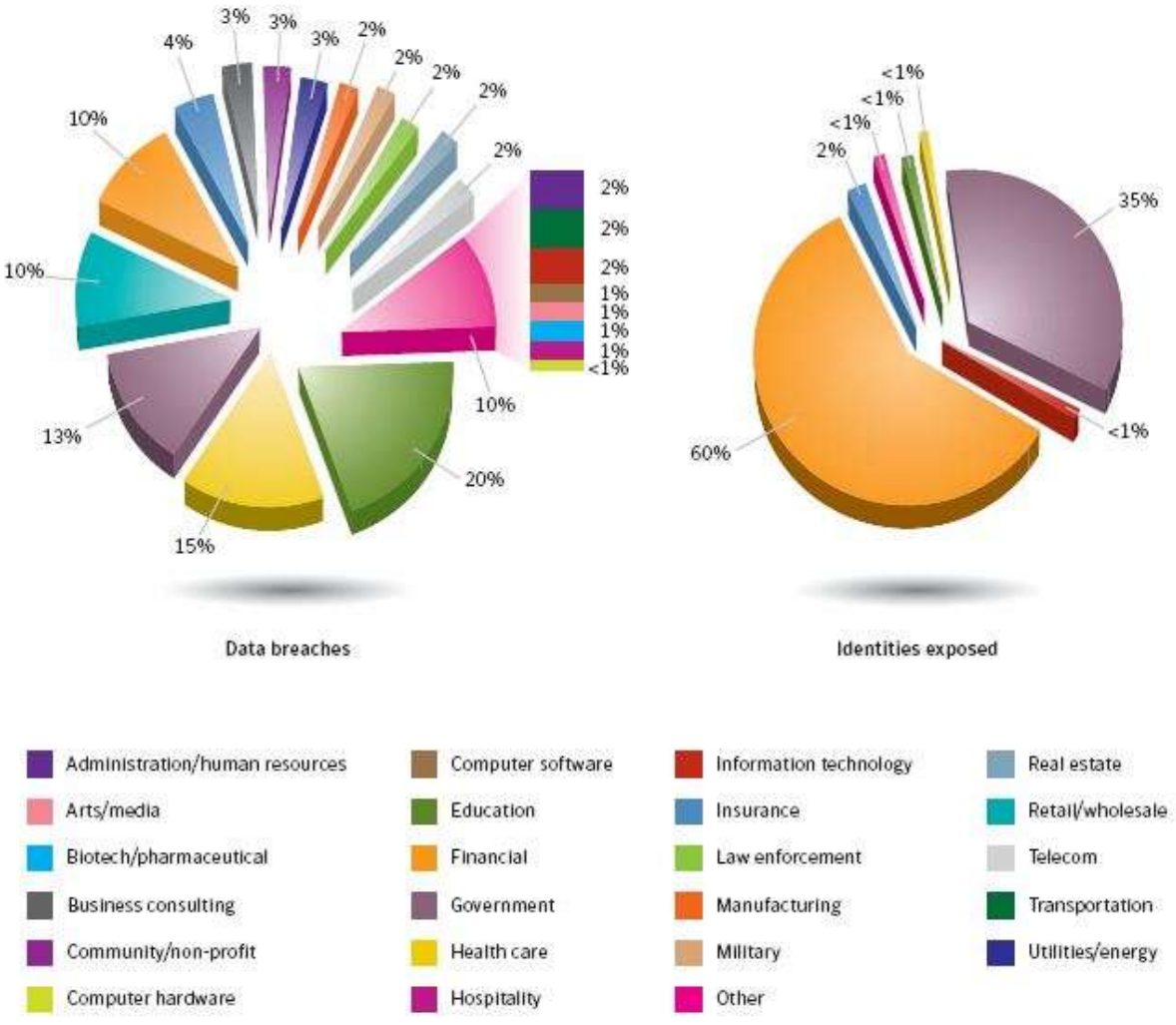
وتتمثل مزايا العمليات المصرفية الالكترونية فيما يلى:

- إمكان وصول البنوك إلى قاعدة أعرض من العملاء المودعين والمقترضين وطالبى الخدمات المصرفية.
- تقديم خدمات مصرفية جديدة.
- خفض تكاليف التشغيل بالبنوك وتكاليف إنجاز عمليات التجزئة محليا ودوليا.
- زيادة كفاءة أداء البنوك.

2- 3 المخاطر التي تأثر على الخدمات المصرفية الإلكترونية

إن إستمرارية التطورات المتقدمة في التقنية ودورها المتميز في التجارة ستقود المؤسسات والمنظمات المالية حتماً نحو الشبكة العالمية للمعلومات (الإنترنت) وذلك بشكل إضطرادي وإستـخدامات الإنترنت يمكن أن تنطوي على مـعلومـات فقط ، تبادل معلومات ، أو مواقع تداول معاملات بحتة على الوب , أو من خلال استطاعة الدخول على الإنترنت التي يمكن أن تتم إما من داخل أو خارج البنك أو المؤسسة المالية ، وبغض النظر عن ماهية الاستخدام لتلك الشبكة فإن عدد هائل من المخاطر تحتويه عملية الاستخدام تلك والتي يجب أخذها بعين الاعتبار في برنامج إدارة المخاطر للبنك ، إن الاختراقات الأمنية الناتجة عن أحد العوامل التالية قد تكون قليلة جداً ونادرة حالياً ، ولكن كبنوك تسعى لتوسيع ونشر دورها من خلال التجارة الإلكترونية فمن المحتمل جداً أن تصبح أهدافاً مرغوبة ومميزة لنشاطات وممارسات غير أخلاقية .

و تشير الدراسات التي أعدتها سمانتيك 2010 أن كشف الهوية المستخدم تمثل 60% في القطاع المالي , و هو الأعلى بين بقية القطاعات .



Data breaches that could lead to identity theft by sector and identities exposed by sector

Source: Based on data provided by OSF DataLoss DB

الشكل (10)

أ - الإختلاف في المخاطر طبقاً لمستوى الخدمة :

- خدمة المعلومات (مخاطرة قليلة)

هذا هو اكثر نموذج مبسط من خدمات الإنترنت الفورية التي تتيح الإتصال من جهة واحدة والتي عادة ما تغطي الإعلانات ، مواد التحفيز ... الخ ، وهذه النوعية من مواقع الإنترنت عادة ما تكون أهداف سهلة لتدميرها وإتلاف المعلومات الأساسية الخاصة بهذه المواقع مما قد ينتج عنها أو تتسبب في أذى لمستخدميها.

* تبادل المعلومات (مخاطرة متوسطة)

العملاء بإستطاعتهم الاتصال مع البنك الخاص بهم ، والإستفسار عن حساباتهم ، وتعبئة النماذج الخاصة بتلك الحسابات ..... الخ ، وبالتالي المخاطرة المترتبة على ذلك والخاصة بتلك المواقع تعتمد على توافر خدمة الاتصال المباشر لهؤلاء العملاء مع الشبكة الداخلية للبنوك .

- خدمة إنشاء وتداول معاملات (مخاطرة كبيرة)

إن خدمة وتمكين العملاء من إتمام معاملاتهم فوراً أو بشكل مباشر مع البنوك الخاصة بهم عن طريق مواقع على الإنترنت مثل تحويل الأموال ، دفع الفواتير ، التسوق الفوري والمباشر وبقية المعاملات ذات الطابع المالي ، فهي في الغالب تتضمن بيع وشراء أمانات ، وطبقاً لذلك فهي مصنفة إنها ذات مخاطرة كبيرة وتتطلب أقصى درجات التحكم بها .

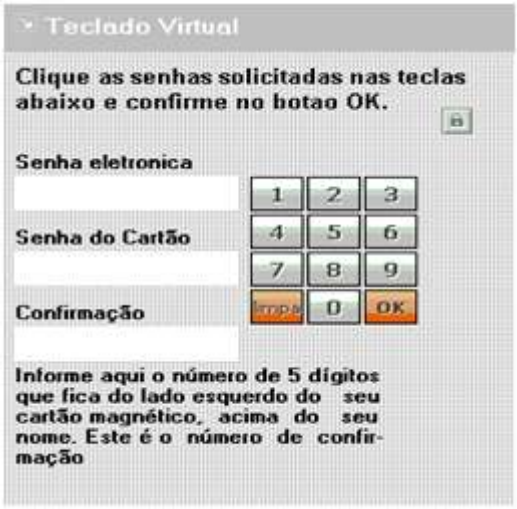
ب - بقية أنواع المخاطر :

الهجمات المحلية (الداخلية)

أحد المفاهيم المغلوطة لدى المستخدم المنزلي هو أن المعاملات البنكية التي تدعم قناة اتصال محمية ببروتوكول SSL/TLS (الذي يشير له رمز القفل في متصفح الانترنت) سوف توفر الحماية المثالية لهم ضد أي نوع من الهجمات. لكن هذا المفهوم خطأ لأن بروتوكول طبقة المقابس الآمنة SSL مصمم لحماية قناة الاتصال بين مستخدم الحاسوب وخادم المعاملات البنكية وليس حماية الأجهزة المثبتة على النهايات الطرفية لتلك القناة. لذلك إذا أصيب جهاز المستخدم قبل الشروع في فتح قناة الاتصال مع المعاملات البنكية عبر الانترنت فإن البرنامج الخبيث قد يسرق البيانات أو يغيرها وهذا خارج نطاق وظيفة بروتوكول SSL الذي يحمي فقط قناة الاتصال.

وقد استغلت العديد من البرمجيات الخبيثة هذه الحقيقة بطرق مختلفة لشن الهجمات أبسطها برمجيات التي تسجل نقرات لوحة المفاتيح Keylogger وترسلها إلى المهاجم. وقد استخدمت تلك البرمجيات في القيام بالعديد من المعاملات البنكية غير المشروعة وسرقة الحسابات مثل واقعة رجل الأعمال الذي رفع دعوة قضائية على بنك of America Bank بسبب خسارته لـ 90000 دولار. بعض الأنواع الأخرى من البرمجيات الخبيثة تسرق ما يجري كتابة في الاستمارات الإلكترونية web forms مثل الحصان الطروادي المعروف باسم PWSteal.Bankash الذي يلتقط المعلومات المكتوبة قبل تشفيرها بواسطة بروتوكول طبقة المقابس الآمنة SSL وإرسالها إلى المؤسسات المالية. قد يحدث ذلك باستخدام عدة طرق مثل غرس أحد مكتبات الوصلات الديناميكية داخل متصفح مايكروسوفت Internet Explorer كأحد العناصر المساعدة للمتصفح (BHO) أو حقن شفرة خبيثة إلى ذاكرة المتصفح أو اصطياد أحد الوصلات البينية لبرامج التطبيق API. لذلك يستطيع هذا النوع من التهديدات اعتراض أي معلومات يجري إدخالها إلى عند زيارة أي موقع إلكتروني باستخدام متصفح الانترنت وذلك قبل تشفيرها.

أنواع أخرى من البرمجيات الخبيثة يمكنها مراقبة تعامل المستخدم مع المتصفح وبمجرد دخول المستخدم على موقع البنك المستهدف يقوم الحصان الطروادي بفتح موقع يحاكي موقع مزيف يشبه موقع البنك فوق الموقع الأصلي ثم يغلقه بعد تقديم الاستمارة الالكترونية مستولياً بذلك على البيانات الموجودة فيها. يستخدم هذا الأسلوب الحصان الطروادي المعروف باسم PWSteal.Bancos.B.



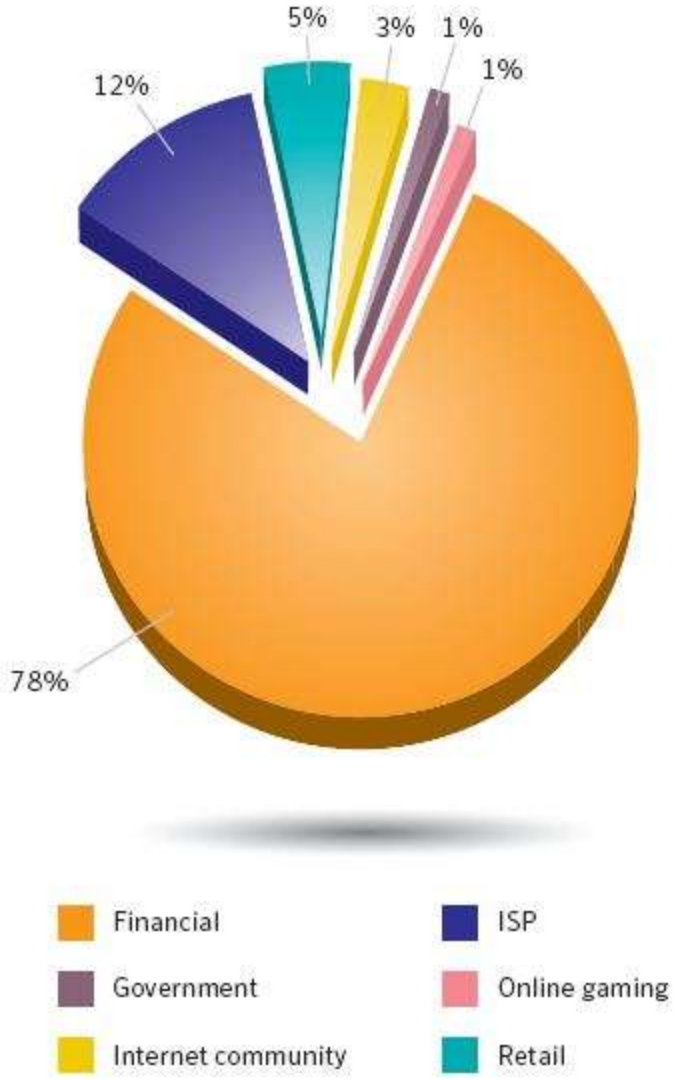
PWSteal.Bancos.B display this fake popup when user open “bankline” web site
الشكل (11)

و قد استخدمت بعض البنوك مؤخراً ما يعرف بتقنية لوحة المفاتيح الافتراضية virtual keyboard لحماية المستخدم من برمجيات تسجيل نقرات لوحة المفاتيح لكن ذلك مجرد تغير لوجه المشكلة دون حلها فالنوع الثاني من البرمجيات الخبيثة الذي يقوم بتشغيل سفرة خبيثة داخل متصفح الانترنت أو يظهر شاشات مزيفة للاستمارات الإلكترونية أو حتى برمجيات تسجيل نقر المفاتيح التي تخزن لقطات متتابعة من شاشة الجهاز لديها القدرة على القيام بنفس وظيفة مسجل نقرات لوحة المفاتيح العادي.
خطوة أخرى في اتجاه مستوي أفضل من الأمن هي استخدام العناصر غير الثابتة للتحقق من هوية المستخدم. لم يعد اسم المستخدم وكلمة المرور الثابتة كافية لحماية فترات التعامل مع البنوك عبر الشبكة. لذلك فرضت هيئة النقد في هونج كونج قانون ينص على أن كل التطبيقات المعاملات البنكية عبر الانترنت يجب أن تستخدم عناصر مزدوجة للتحقق من الهوية بداية من يونيو 2005. الأنواع الثلاثة الشائعة من عناصر التحقق المزدوجة التي تستخدمها البنوك في هونج كونج هي الشهادات الرقمية digital certificates وكلمات المرور التي تستخدم لمرة واحدة من خلال إرسالها عبر الرسائل النصية القصيرة SMS-based one-time passwords وأجهزة الرقم الأمني المميز security-token التي تعتمد كلمات مرور تستخدم لمرة واحدة. سوف يجري مناقشة كل منها فيما يلي من التقرير.

الهجمات عن بعد (الخارجية)

تمثل هجمات الاصطياد الالكتروني أكبر الهجمات التي تتعرض لها المعاملات البنكية عبر الانترنت حيث يرسل المهاجمون رسائل بريد الكترونية للعديد من المستخدمين ليخدعوهم بفتح موقع الكتروني مزيف للتعاملات البنكية أو موقع وهمي يقدم خدمات مفيدة حتى يقوم المستخدم بالكشف عن معلومات حسابه البنكي. يوجد العديد من الأساليب لخداع المستخدم وإنشاء صفحات الويب المزيفة بحيث لا يستطيع المستخدم التفريق بين المواقع الحقيقية والمواقع المزيفة. من هذه الأساليب استخدام نفس اسم الموقع مع تغيير حرف واحد أو إضافة أحد الرموز مثل الشرطة السفلي (_). بالإضافة إلى أساليب أخرى مثل كتابة عنوان بروتوكول الانترنت الخاص بموقع مزيف بدون النقطة (.) ثم إضافة اسم مستخدم وكلمة مرور في الموضع الخاص بالتحقق من هوية المستخدم كما يلي http://bank.com@233484731. هذا العنوان صحيح ويخدع الكثير من المستخدمين الذين يفتحونه. تصدر جميع المتصفحات حالياً رسائل إنذار حيال هذا النوع من عناوين بروتوكولات الانترنت أو تمنع كتابته من الأصل باستثناء متصفح Safari 4 الذي ما يزال لديه تلك الثغرة.

مؤشرات سمانتيك 2010 تبين نسبة عمليات تصيد المعلومات من خلال عناوين مواقع وهمية , و حسب الدراسات أن قطاع المال لها نصيب الأسد بنسبة 78% .



Phished sectors by volume of phishing URLs
الشكل (12)

تدعم أسماء النطاقات العالمية حالياً جداول الكود الموحد Unicode والحروف غير اللاتينية وهي خاصية يمكن استغلالها لإنشاء اسم نطاق جديد وليكن http://Citibank.com للنطاق الأصلي http://Citibank.com والتغيير هو استبدال حرف الـ (a) داخل النطاق الأصلي بحرف (a) من اللغة السريالية. يعرف هذا النوع من الهجوم باسم هجوم التشابه اللفظي على أسماء النطاقات العالمية وقد استطاعت شركة Symantec من اقتناص العديد من مواقع الاصطياد الالكتروني التي تستخدم هذا الأسلوب.

نوع أخر من الهجمات الموجهة إلى النطاق ولكنه يصيب الخوادم الموجودة لدى المستخدم ما يعرف باسم المزرعة أو تسميم الذاكرة المخبأة cache memory الخاصة بنظام أسماء النطاقات DNS. يقوم المهاجم بتغيير عنوان بروتوكول الانترنت IP للموقع المستهدف ليصبح عنوان الموقع المزيف و عندما يزور المستخدم الموقع المستهدف يقوم خادم أسماء النطاقات بالإشارة إلى الموقع المزيف ويجرى توجيه المستخدم مباشرة إليه.هذا النوع من الهجمات ليس جديداً وقد اثبت نجاحه خلال العديد من السنوات الماضية .

ومن هجمات الاصطياد الالكتروني أيضاً هجمات الوقت الفعلي على بروتوكول التوثيق باعتراض البيانات أو ما يعرف بهجمات man-in-the-middle وهو مصطلح تقليدي يشير إلى المهاجم التي تعترض يتدخل بين نهايتي قناة اتصال ليقوم بتوجيه الرسائل بينهما ذهاباً وإياباً وقد يغيرها.

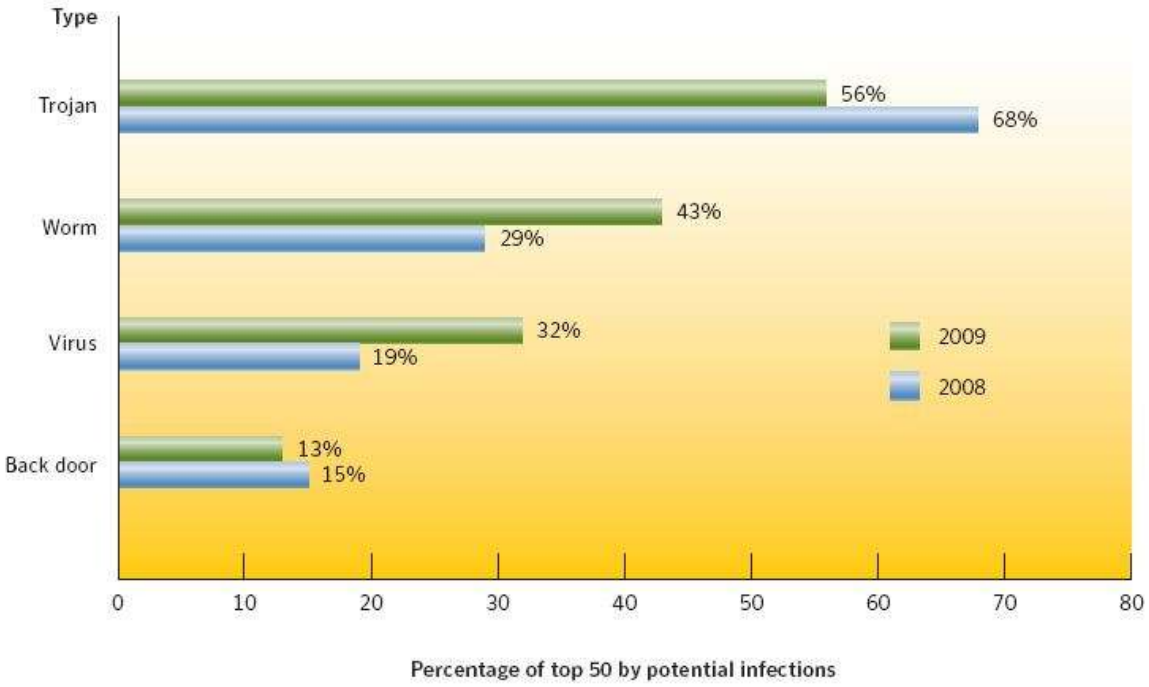
تتنوع الأساليب التي يحدث بها هذا النوع من التهديد ولكن الشكل النموذجي لها عندما يقوم المهاجم بإرسال طلب يبدو في الظاهر سليم من أحد المواقع الموثقة سائلاً المستخدم الدخول إلى أحد التطبيقات المألوفة كما في الشكل (3).

show MITM in general
الشكل (13)

الهجمات الهجينة

في الهجمات الهجينة يمزج المهاجم بين أساليب الهجمات المحلية (الداخلية) والهجمات عن بعد (الخارجية) ليكسب هجمته المزيد من القوة. أبسط أشكال هذه الهجمات هو إصابة جهاز المستخدم بحصان طروادي يبدل بعض عناوين الصفحات الالكترونية المحفوظة في سجل الصفحات المفضلة إلى عناوين مواقع مزيفة. لكن هناك بعض الهجمات الأكثر قوة حيث تغير ملف المستضيف الموجود في نظام التشغيل وإضافة عنوان بروتوكول الانترنت IP الخاص بموقع المعاملات البنكية المستهدف إلى الموقع المزيف بحيث يظهر الموقع المزيف عندما يبعث المستخدم طلب بفتح الموقع الحقيقي للبنك. العديد من البرمجيات الضارة لديها القدرة على القيام بهذا النوع من الهجمات مثل الحصان الطروادي المعروف باسم Trojan.Qhost الذي يضيف سطر بروجي في ملف المضيف لتحويل كافة المعلومات المتدفقة إلى موقع البنك المستهدف إلى موقع خبيث.

تشير الدراسات التي أعدتها سمانتيك 2010 تبين أن نسبة الهجمات بواسطة الحصان الطروادي أنخفض إلى 56% في عام 2009 مقارنة بعام 2008 التي كانت نسبتها 68% انظر الشكل (14) .



Prevalence of malicious code types by potential infections
الشكل (14)

2- 4 الأهداف من التحكم والضبط في الخدمات المصرفية الالكترونية :

إن التهديدات للجوانب الأمنية والمتمثلة في هجمات الذين ليس لديهم صلاحية ، أو المستخدمين لأساليب وهمية أو العابثين أو المدمرين أو بقية من لديهم نشاطات وممارسات غير قانونية تتطلب وضع سياسة أمنية تغطي أهداف التحكم التالية :

- التحكم والضبط في الاتصالات
- سرية البيانات
- موثوقية الرسائل والبيانات
- المصادقة للمستخدمين والوحدات
- عدم نكران (جحود) المعاملات
- التحكم والضبط في الدخول (المنافذ)
- أمن شبكة العمل
- متابعة الحركة والتدقيق
- توفير النظام ، القدرة على التكيف واحتواء الكوارث
- حماية العميل

سرية البيانات :

وهذا يعود إلى أن حماية معلومات البنوك الحساسة والأنظمة الفورية والمباشرة والتشفير الملائم والمطلوب لها يعتمد على نوعية المخاطرة المتاحة والمتواجدة على شبكة العمل والأنظمة التي يمارس ذلك البنك نشاطه من خلالها وذلك باختيار لوغارتيمات التشفير طبقاً للمواصفات والمعايير الدولية ، وبذلك فإن التسهيلات والإجراءات المناسبة تعتبر جوهرية لإدارة مفاتيح تشفير الرسائل والمعلومات من أجل عمليات أمنية ووثيقة لجميع الأنظمة الأمنية الخاصة بتشفير الرسائل والمعاملات .

وعدا البيانات المحمية بالطرق الملائمة ، فإن تحويل البيانات وبما يتضمنه من بريد إلكتروني ، ونظام التنقل المفتوح عبر الإنترنت من الممكن العبث والتعديل عليها وقراءتها من قبل الآخرين .

ومن خلال الحجم للبيانات المنتقلة عبر الإنترنت والمسارات العديدة التي يمكن أن تسلكها هذه البيانات في تنقلها ، ومن غير المتوقع أن تراقب هذه البيانات بطريقة عشوائية حسب مرورها في الإنترنت ولكن برامج الكشف (SNIFFER) من الممكن إعدادها ووضعها في المواقع المحتملة على شبكة العمل مثل خادم الموقع (كأن تكون حاسوبات توفر خدمات لحاسوبات أخرى على الإنترنت) وذلك ليتمكن من النظر وتجميع أنواع البيانات المطلوبة بسهولة ، والبيانات التي تم تجميعها من مثل تلك البرامج يمكن أن تتضمن أرقام حسابات (مثل بطاقات ائتمان ، ودائع ، قروض) أو الأرقام السرية ، وبعض برامج الكشف (SNIFFER) قد يكون أكثر تقدماً وتعقيداً بحيث يستطيع مثلاً الإطلاع على الأنشطة الخاصة بالتبادل التجاري وما يتعلق بها من ضمانات وذلك من أجل استخدامها في النصب والاحتيال على السوق .
وكما ذكر في حجب الخدمة فإن الهجمات التي تستخدم مواقع يعتقد أنها جيدة وصحيحة وهي على عكس ذلك ، أي أن المهاجم يبحث عن مستخدم اصلي وصحيح ولكنه يتسم بالغباء ويستخدم خدمة فورية وبذلك يبادر المهاجم فوراً باستخدام البيانات والمعلومات التي حصل عليها من ذلك المستخدم ولكن بإستخدام موقع مزيف بدلاً من الموقع الأصلي لذلك المستخدم ، ويمكن إعطاء المثل التالي كأن تسرق المعلومات الخاصة بحركة مستخدم أصلي بحسابه أو الاتصال الذي بين المستخدم والموقع المزيف يمكن تمريرها على مراحل إلى الموقع الحقيقي وبهذا يعرف هذا النموذج بهجوم الرجل الذي في الوسط أو (الرجل الوسيط) .

ومن أجل تصميم الإنترنت ، فإن خصوصية البيانات وقضايا السرية يجب أن تتجاوز تحويل البيانات ويجب أن تتضمن أنظمة تخزين البيانات المتصلة ، وتوجيه وقيادة شبكة العمل ، ويمكن لأي بيانات مخزنة على خادم الموقع أن تسمح أو أن تكون عرضة لسرقتها أو العبث بها عندما تتوافق مع نية أو أغراض أحد العابثين أو المدمرين إذا لم يتوخىالحذر حيالها ووضع الإحترازات الأمنية الملائمة لها .

موثوقية الرسائل والبيانات :

وهذا يعود بالدرجة الأولى إلى الدقة ، والإعتمادية ، والاكتمال ، والتوقيت للمعلومات الإجرائية المخزنة أو المنقولة بين البنك وعملاءه دون إغفال المخاطر الكبيرة المتمثلة في استطاعة أي شخص بالدخول من خلال الإنترنت على البنوك من أي مكان وفي أي وقت .

ومن المحتمل جداً وفي بيئة مفتوحة مثل الإنترنت يمكن لهؤلاء الأشخاص وبمعرفة وأدوات محددة أن يعدلوا ويغيروا في البيانات أثناء انتقالها أو حركتها ، كما إن بيانات الربط يُمكن أن تكون أيضا متاحة ومتوافقة من خلال نظام تخزين البيانات ذاته وعلى حدً سواء كانت لغرض معين أو بدون غرض إذا كانت الشروط الملائمة للدخول أو العبورلا يتم صيانتها كل فترة ، لذا يجب اتخاذ الخطوات اللازمة للتأكد من أن جميع البيانات يتم صيانتها وفقاً للنماذج الأساسية والأصلية أو الغرض الذي أنشأت من أجله .

المصادقة :

وبشكل جوهري أن يكون في التجارة الإلكترونية حاجة عند إجراء إتصال معين ، أومعاملة ، أو طلب صلاحية الدخول للمطابقة مع الأصل في كل ذلك ، ولشرح ذلك بالمثال التالي أنظمة الحاسوب على الإنترنت يتم تعريفها بواسطة التسجيل الرسمي على الإنترنت (رقم IP) والعنوان ، وهذا يمكن تشبيهه بالهاتف عندما يتم تعريفه برقم الهاتف .

ومن خلال عدة طرق وأساليب ، هناك طريقة تعرف (الإيهام بالتسجيل على الإنترنت)

(IP SPOOFING) وهي تتيح لأي حاسوب بأن يدعي فعلياً بأنه صاحب الحق ، وهذا ما يمكن أن يحدث بالضبط لتعريف المستخدم عندما يُساء استخدامه من قبل العابثين أو المدمرين.

وفي الحقيقة وبشكل ذو علاقة يمكن ببساطة إرسال رسالة بالبريد الإلكتروني وتظهر أو تقرأ على أنها من شخص آخر أو حتى إرسالها بدون معرفة المصدر ، إذن وبناءً على ماتقدم فإن إشتراطات وأحكام المصادقة ضرورية جداً لوضع وتأسيس التعريفات والهويات لجميع الأطراف التي ترغب في الإتصال فيما بينها .

عدم الإنكار (الجحود) :

عدم الإنكار(الجحود) ينطوي على خلق أو إبداع أدلة قاطعة على مصدر أو تسليم البيانات لحماية المرسل من عدم الإعتراض الغير صحيح من قبل المستلم (المستقبل) بعدم إستلام البيانات وبأنها أستلمت أيضاً لحماية المستلم (المستقبل) من عدم الإعتراض الغير صحيح من قبل المرسل بأن البيانات فعلاً قد تم إرسالها ولعل الأمر الأول أصعب في تحقيقه من الأمر الثاني .

اما عدم إنكار تعليمات الدفع فيجب ان تولى عناية خاصة من البنوك وذلك للتأكد من أن المعاملات تتم بالطريقة الصحيحة وأنه يتم إتخاذ الخطوات اللازمة لمنع النزاعات بين أطراف تلك المعاملات على صلاحية معينة و/ أو رفض الإعتراف بها و/ أو مصدر وصحة الإتصال بين الأطراف أو المعاملات التي بينهم .

إشتراطات وأحكام الدخول

إن الهجوم الفعلي (المادي) على المعدات والأجهزة يعتبر خطر حقيقي وربما ينطوي فقط على سرقة الرقم السري وإستخدامه على المعدات والأجهزة الأصلية والتي تكون في مكاتب ومواقع غير محمية ، وعلى الجانب الآخر يمكن أن يعني هجوم فعلي (مادي) مثل إعداد رقم تحديد هوية شخصي (PIN) على ورق معين وبإستخدام تقنيات درجة الحرارة المنخفضة في سبيل كسر وتحطيم أي أدلة ممكنة والدخول لمفاتيح التشفير المخزنة في المعدات والأجهزة الخاصة بها .

وفي كلتا الحالتين ، فإنه من الضروري التأكد من أن جميع المعدات والأجهزة لا يمكن الوصول إليها من قبل الأشخاص غير المخولين أو من قبل حتى الموظفين المخولين ولكن لديهم النية في التزوير والتلاعب .

إن الهدف من التحكم هنا هو للتأكد على أن من المتعارف عليه هو من لديه الصلاحية للدخول على معدات وأجهزة معينة بأن هذه الصلاحية تحت الملاحظة والسيطرة من قبل الأبواب الأمنية الفعلية وأنه يتم التوقيع في الدخول والخروج .....الخ .

وفيما وراء الهجوم الفعلي (المادي) قد يكون خادم البنك (SERVER) مرتبط بالإنترنت وقابل للتلف أو الهجوم عليه من قبل جهات متعددة ومختلفة غير مخولة .

وزيادة على ذلك ، إذا قامت أطراف غير مصرح لها بالدخول على خادم البنك فإن هذا من شأنه أن يضع أنظمة عملاء هذا البنك أيضاً في خطر كبير ، لذا فإن الهدف الأساسي من أحكام وإشتراطات الدخول على شبكة العمل هو لتقليل هذه المخاطر إلى أدنى درجة .

أمن شبكة العمل :

بشكل عام ، الأنظمة المصرفية تفترض أن شبكات الأعمال غير آمنة بذاتها ولذلك فإن تعريف ووضع مواصفات وضوابط أمنية بتحديد الأطراف المشاركة ووضعها على مستوى التطبيق ضروري جداً ، خاصةً وأن شبكة العمل ذات البيئة المفتوحة مثل الإنترنت من غير المحتمل بأن تكون المعدات والأجهزة الخاصة بالعميل (والتي ربما تكون مرتبطة عبر الانترنت بأنظمة البنك) محتوية على أجهزة أو معدات أمنية وبرامج لتحقيق ذلك .

وحالياً ، لايوجد على مستوى العالم آلية مقبولة لحل مثل هذه المشاكل وقد وضعت شركة فيزا ، ماستركارد ، مايكروسوفت وآخرين أحكام وإشتراطات أمن المعاملات الآلية (SET) ولكن لم يتم قبوله بشكل عام .

ونظام أمن خط نقاط التحمل (SSL) والذي يعتمد على أمن خط الاتصال باستخدام آلية الخط المشفر والتي تقوم بتأمين المعاملات من العابثين في أجهزة ومعدات العميل بإرتباطها ببرامج الإنترنت في النظام المركزي .

وفي الإصدارات الحالية من الـ (SSL) بعض المطابقات تم توفيرها مستندةً على شهادات رقمية ومن المحتمل أن يكون هذا أفضل ماتم تحقيقه في آلية أمن شبكة العمل للمعاملات عبر الإنترنت في الوقت الحاضر .

متابعة الحركة والتدقيق :

إن متابعة حركة المعاملات والتغيرات المتعددة بين أجهزة الحاسوب خلال القيام بها أمر جوهري لتوفير سجل عن ماهية البيانات التي تم تمريرها فعلاً بين أجهزة الحاسوب من خلال ارتباط بعضها بالبعض الآخر وبمعنى آخر هي وسلية للتدقيق .

ومن أفضل الوسائل هنا إستخدام طريقة (WORM) إختصاراً لـ (تكتب مرة وتقرأ عدة مرات) وهي عبارة عن متابعة حركة الجزء المالي من المعاملة حيث أن هذا الجزء ليس من السهولة العبث فيه ولأجل قراءته فهو يتطلب صلاحية الدخول والبحث بطرق ووسائل غير إعتيادية .

وبهذا فإن إكتمال وإتمام عملية صلاحية الدخول الخاصة بمتابعة حركة التدقيق هي المفتاح لإستخدامها بالشكل المطلوب كأداة للكشف والبحث في أنشطة التزوير وحتى الأخطاء التي تقع.

توفر النظام :

إن مستخدمي الخدمات المصرفية عبرالإنترنت يتوقعون أن بإستطاعتهم الدخول الفوري والمباشر على الأنظمة خلال الـ 24ساعة يومياً وأي يوم على مدار السنة ، كذلك من بين الإعتبارات الأخرى المرتبطة مع توافر النظام هي القدرة على التحمل ، ومتابعة الأداء ، ميزة الأنظمة المتوازية بحيث يستمر العمل مع تعطل أحد المكونات ، والقدرة على إستمرارية العمل حتى بعد الإنقطاع لأمر طارىء ، لذا على البنوك المحلية وموردیهم المسئولين عن توفير المنتجات والخدمات المصرفية عبر الإنترنت التأكد من أن لديهم القدرة على تأمين وتركيب المعدات والأجهزة والبرامج التي تستطيع أن تقدم خدمة على أعلى مستوى ، كما أن مزودي الخدمات الفورية والمباشرة يعتبرون على مستوي عالى من الأهمية حيث يجب عليهم الأخذ بعين الاعتبار مدى مرونة التصميم ، إحتواء الكوارث وإستمرارية العمل والأنظمة الإحتياطية وخطط الطوارئ في حال الهجمات خصوصاً على الخدمات التي لا تحتاج إلى صلاحية .

بالإضافة إلى أن طرق وأساليب متابعة الأداء يمكن أن توفر للإدارة معلومات هامة مثل حجم وعدد المعاملات ، الوقت الذي يستغرقه إنجاز تلك المعاملات ومدى الوقت الذي يستنفذه العميل في الحصول على تلك الخدمة ، أما متابعة القدرة على التحمل للنظام ومتابعة الوقت بين إيقاف النظام وتشغيله و أداء هذه النظام وذلك بشكل منتظم فهو سيساعد الإدارة على التأكد من أن النظام دائماً جاهز ومتوافر على أرقى مستوى لأداء المطلوب منه في تقديم خدمات مصرفية عبر الإنترنت ، كذلك من المهم جداً أيضاً تقييم قابلية شبكة العمل وقدرتها على مواجهة الهجمات التدميرية والإتلافية وذلك لمنع أي إنقطاع للخدمة أثناء عملها المتواصل نتيجة لأي خلل أو مشكلة في عناصر تلك الأنظمة ، حيث أنه يمكن أن تصبح كامل شبكة العمل غير قادرة على العمل بسبب خلل بسيط جداً في أحد أجزاء أو عناصر الأجهزة والمعدات أو البرامج ، وبناء على ذلك فإنه على البنوك المحلية وموردیهم التأكد والحرص على وضع ونشر خطط الطوارىء في المناطق والمواقع الحساسة والحرجة أو أن تكون لديها القدرة على التحول الآلي والمباشر إلى المواقع والمناطق الإحتياطية .

حماية العميل :

إن عملية تحديد صلاحيات الدخول وإستخدام الأنظمة والمعلومات التي تحتويها لتشمل فقط الأطراف أو الأشخاص المخولين لأستلام تلك المعلومات ونقل البيانات وبالطريقة التي تضمن الخصوصية هي الخطوات الأولى لتحقيق النجاح في العملية الأمنية عند إستخدام الإنترنت ، وأكثر الطرق شيوعاً في تحديد صلاحية الدخول بصرامة للبيانات والإنترنت هو إستخدام طريقة تحديد هوية المستخدم ورمزه السري ، وحيث أن نمط الحياة الآن يتطلب الحماية ضد البرامج المعقدة التي تستطيع أن تعيد أي تحركات للمستخدم وممكن أن تستفيد وتستخدم الرموز الخاصة به بعد أن تقوم بتصميمها مرة أخرى لتتلائم وتؤدي الغرض منها بعد نزع الصلاحية الخاصة والمرتبطة بهوية المستخدم الأصلي ورمزه الشخصي ، ومثل هذا التهديد يمكن أن يكون أيضاً بسبب المواقع الوهمية أو التي يعتقد أنها جيدة ، لهذا فإن المواقع التي تعتمد أساساً على تطبيقات مالية يجب أن يكون لديها القدرة وتستخدم وسائل ومقاييس مثل تحديد عدد الحركات الغير صحيحة وتسجيل عدد المحاولات للدخول غير الناجحة والطرق التي أتبعت وذلك من أجل حماية سرية هوية المستخدم ورمزه السري ذاتهما .

وهناك العديد من الأساليب والطرق التي يمكن إستخدامها لإيقاف الهجمات الناجحة والتي من ضمنها تحذير المستخدمين من محاولات هجوم وذلك عن طريق إبلاغهم عن وقت وتاريخ آخر حركة ناجحة وعدد محاولات الحركات غير الناجحة منذ تلك العملية الناجحة وتفاصيل آخر معاملة للمستخدم .

خلال سير العمل فإنه على مزودي وموفري المعلومات المالية خلق وإبداع وتطبيق طرق وأساليب أمنية لإنتاج وإصدار الرموز الخاصة بالعملاء ، أما أحكام وإشتراطات تحديد هوية المستخدم ورمزه الشخصي فهي تصبح جزء من إجراءات التوثيق ، وتعليمات العمل ، وعلى كل مؤسسة أومنظمة مالية أن تقوم بالتدقيق والمراجعة والصيانة بين كل فترة وأخرى وبشكل أكبر من مجرد التسويق عبر الإنترنت الذي نراه حالياً .

أما على الجانب الآخر وبشكل منفصل يتم التدقيق والتحكم بشكل مزدوج أثناء سير العمليات وفي مواقعها وذلك من أجل التأكد وصيانة صلاحية دخول المستخدم للمعلومات و/أو الموقع ذاته ويجب صيانته والتأكد منه والتعامل معه بنفس درجة الخطورة التي يتعامل فيها مع خزائن النقد أو المفاتيح الخاصة بالمواقع والمناطق الحساسة جداً في المؤسسات والمنظمات المالية ، وبذا يمكن القول أن أكثر التقنيات أمناً قد تتأثر بالهجمات والعبث اذا لم تكون ادارتها جيدة.

2- 5 الحلول المبتكرة لتأمين الخدمات المصرفية الإلكترونية

حلول التحقق من الهوية

تبنت البنوك حول العالم تقنيات الانترنت والهاتف البنكي للقيام بعملها سواء مع المؤسسات أو الشركات الصغيرة مما سمح لها بخفض التكاليف وخدمة العملاء بطريقة أفضل. لكن الهجمات على مواقع المعاملات البنكية تكاثرت وأصبح لها الآن أسلوب إجرامي معروف. وكما سبق فإن هذه الهجمات تضم الاصطياد الالكتروني وأسلوب المزرعة والأحصنة الطروادية والهجمات على بروتوكول التوثيق باعتراض البيانات المعروفة باسم "الرجل في المنتصف" (الاصطياد الالكتروني في الوقت الفعلي لحركة البيانات). وقد جرى الاتفاق على ضرورة الاستثمار في تحسين التحقق من هوية العميل لمنع هذه الهجمات والاحتفاظ بثقة العملاء.

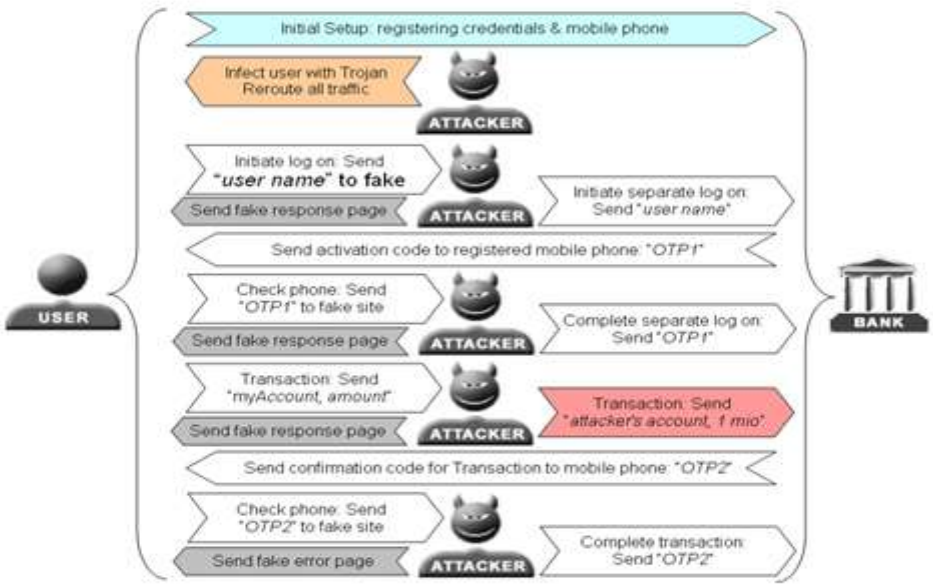
إن التحقق من هوية المستخدم هو الأساس الذي تقوم عليه المعاملات الإلكترونية لأنها تقيم الثقة من خلال التأكد أن هويات المُرسِل والمُستقبِل هي بالفعل هوياتهم الحقيقية. أكثر أنواع التحقق من الهوية شيوعاً هو كلمات المرور حيث تمثل الحد الأدنى من أشكال التحقق من الهوية لكنها عرضة للتخمين بسهولة وتكرار نسيانها وخطورة الاحتفاظ بها. كما أن كلمات المرور تتسم بالثبات وطول فترات استخدامها وعادة ما يُعاد استخدامها في أكثر من تطبيق مما يجعلها على وجه الخصوص هدفاً ثميناً لاصطياده. كلمات المرور عرضة لهجمات الاصطياد الالكتروني حيث يمكن الاحتيال على المستخدم لإدخال كلمة المرور في موقع أو تطبيق مخادع بعدها يستطيع المهاجمون بالاصطياد الالكتروني جمع المعلومات واستخدامها في التزوير والسرقة.
لذلك فإن القدرة على التحقق من الهوية بقوة ضرورة لحماية المعاملات والعملاء من هجمات الاصطياد الالكتروني.
يوفر التحقق المعتمد على عنصرين للتحقق من الهوية وسيلة حماية متطورة إلى حد كبير لأن المستخدمون يُدخلون شيء معروف لديهم مثل رقم الهوية الشخصية وشيء أخر يمتلكونه مثل الشفرة المتغيرة على جهاز للتوثيق في حجم سلسلة مفاتيح.

لذلك فإن التحقق القوي من الهوية باستخدام عنصرين حل مؤكد للأمن داخل المؤسسة لكنه مصمم لتوثيق المستخدم لدى التطبيق وليس من الضرورة توثيق التطبيق لدى المستخدم. ترفع أساليب التحقق من الهوية باستخدام عنصرين من العراقيل أمام المهاجم بشكل أعلى وتوفر الحماية ضد الهجمات الحالية لسرقة كلمات المرور دون الاتصال بالشبكة لكنها لا تستطيع التعامل مع الأنواع الأخرى من الهجمات مثل الهجمات على بروتوكول التوثيق باعتراض البيانات أو هجمات الأحصنة الطروادية.

التحقق من الهوية ثنائي العناصر باستخدام رسائل نصية قصيرة تحمل كلمات مرور فورية

في هذا السيناريو يرغب المستخدم في الدخول على موقع البنك من خلال كتابة اسم المستخدم الخاص به وكلمة مروره ثم يُرسل البنك كلمة مرور مؤقتة فورية لهاتف المستخدم المحمول بحيث يمكنه استخدامها لاستكمال الدخول إلى الموقع. يعمل التحقق من الهوية باستخدام عنصرين بكفاءة ويلاءم الكثير حيث أن أحد أهم مميزاته هو امتلاك معظم المستخدمين لهواتف محمولة مما ينفي الحاجة لشراء المزيد من أجهزة الرقم المميز وتركيبها ودعمها.

أسوء الحالات التي لا يستطيع هذا النوع من التحقق مواجهتها هي الهجمات على بروتوكول التوثيق باعتراض البيانات حيث يجري توجيه المستخدم إلى موقع مزيف. وبمجرد إدخال البيانات الخاصة بحسابه في الموقع المزيف يستخدم المهاجم بيانات اسم المستخدم في الدخول على الموقع الحقيقي للخدمة وينشئ طلب بالحصول على كلمات مرور مؤقتة فورية من خلال الرسائل النصية القصيرة. يستقبل المستخدم الشفرة على هاتفه المحمول ويقوم بإدخالها في الموقع المزيف معتقداً أنه ما يزال يتعامل مع الموقع الحقيقي. بعدها يستخدم المهاجم هذه الشفرة لتوثيق نفسه لدى الخدمة الحقيقية. وللتغلب على هجمات سرقة كلمات المرور أثناء عدم الاتصال بالشبكة جعلت البنوك تضع مطلباً هو التحقق من كل معاملة بكلمة مرور تُستخدم لمرة واحدة. تُستخرج كلمات المرور بنفس طريقة استخراجها عند عملية الدخول الأولى, ولهذه الحالة يقوم المهاجم بالإبقاء على فترة تعامل مزيفة منتظراً حتى يقوم المستخدم بإنشاء المعاملة الإلكترونية. يعمل المهاجم كجهاز وكيل بين البنك الإلكتروني الحقيقي والمستخدم النهائي ليقوم بتصفية المعلومات غير المرغوبة والتحذيرات. يظل الهجوم مستمر طالما المطلوب من المستخدم هو الرد باستخدام شفرة التحقق المرسلة عبر الرسالة النصية القصيرة بدلا من إدخالها عبر الموقع الالكتروني حيث يعتقد المستخدم أنه يوثق نفسه معاملته الالكترونية. الشكل (15) يوضح عمل هذا الهجوم.



show MITM against SMS-OTP 2FA
الشكل (15)

هناك حل أفضل لتقليل هجمات الاصطياد الالكتروني أو هجمات اعتراض البيانات وهو التحقق من المعاملات الالكترونية

نفسها بمعنى أنه يجب على البنك ضم تفاصيل المعاملة في الرسالة النصية القصيرة. بهذه الطريقة يعلم المستخدمون أي معاملة يقومون بها ويستطيعون إدراك ما إذا كان هناك اعتراض للبيانات قام بإضافة أي شيء للمعاملة الالكترونية. الشكل الذي سوف تظهر به الرسالة النصية القصيرة يوضحه الشكل (16)

transfer amount [xx] SR.
from account [first and last digits]
to account [first and last digits]
at [time and date]
Your one-time password is [8 digits].

show SMS that Authenticate the Transaction
الشكل (16)

لكن يوجد مشكلة أخرى في الأنظمة المعتمدة على الرسائل النصية القصيرة لإرسال كلمة المرور الفورية هي استخدام شبكات اتصالات الهواتف المحمولة GSM التي تعرضت للهجوم مؤخراً واستطاع المهاجمون التقاط كافة الرسائل النصية القصيرة وفك تشفيرها. تستخدم شبكات الهواتف المحمولة العديد من خوارزميات التشفير لتحقيق الأمن مثل خوارزميات التشفير A5/1 و A5/2 المُستخدمة للتأكد من سرية الموجات الصوتية المنقولة عبر الأثير وقد أعلن عن عدد من الهجمات التي تستهدف هاتين الخوارزميتين. بعض الخوارزميات تتطلب فترة معالجة تحضيرية طويلة بعدها يمكن مهاجمة تشفيرها و فكه في ثوان معدودة. يوجد على الأقل أربع أدوات تجارية تسمح بفك تشفير اتصالات شبكات الهواتف المحمولة. يتراوح سعر هذه الأدوات بين 100000 دولار و250000 دولار حسب السرعة التي تريد أن يعمل بها البرنامج.

حتى وقت قريب كانت نقاط الضعف تستغل من خلال الهجمات السالبة passive attacks باستخدام افتراض النص غير المشفر المعروف. شهد عام 2003 جوانب ضعف أكثر خطورة يمكن استغلالها في حالات النصوص المشفرة أو بواسطة مهاجم نشط. في عام 2006 قدم إلياد باركان وإلي بيهام وناثان كيلر عرضاً لهجمات على خوارزميات التشفير A5/1 و A5/3 و حتى شبكات اتصال الهواتف المحمولة سمحت للمهاجمين التصنت على محادثات الهاتف المحمول وفك تشفيرها إما في وقتها الفعلي أو في وقت لاحق.

في عام 2008 قامت مجموعة من المخترقين تدعى The Hackers Choice بإطلاق مشروع لتطوير هجوم عملي على خوارزمية A5/1. تتطلب الهجوم إقامة جدول بحث كبير يبلغ حجمه ما يقارب 3 تيرابايت. بالاتحاد مع إمكانيات الفحص التي جرى تطويرها كمشورع فرعي توقعت المجموعة أن تكون قادرة على تسجيل أي مكالمة تحدث عبر شبكات اتصال الهواتف المحمولة أو الرسائل النصية القصيرة المشفرة باستخدام A5/1 وفي خلال 3 إلى 5 دقائق تمكنت المجموعة من سحب مفتاح التشفير وبالتالي الاستماع إلى المكالمات وقراءة الرسائل النصية القصيرة بوضوح. لكن الجداول المستخدمة في هذا الاختراق لم يجري نشرها.

وفي جهد مماثل عام 2009 جرى الإعلان عن مشروع كسر خوارزمية A5/1 في مؤتمر Black Hat للأمن بواسطة المُشفّر كارستن نوهل الذي استخدم بطاقة رسوميات من شركة nVidia للقيام بعملية الحوسبة العامة على وحدات معالجة الرسوميات من خلال هيكلية حوسبة موزعة تعتمد مبدأ الند للند peer-to-peer distributed computing architecture. منذ بداية المشروع في سبتمبر عامم 2009 قام المشروع بتشغيل ما يعادل 12 بطاقة رسوميات من نوع

GeForce GTX 260 nVidia. وحسب المؤلفين فإن هذا الاسلوب يمكن استخدامه على أي نوع من أنواع التشفير ذات المفتاح 64 بت.

في ديسمبر 2009 أعلن كل من كريس لجيت وكارستن نوهل عن جداول الهجوم الخاصة بمشروع كسر خوارزمية A5/1. استخدمت الجداول خليط من أساليب الضغط بما فيها جداول التنقيب في الذاكرة بحثاً عن النصوص غير المشفرة لكلمات المرور وسلاسل نقاط مميزة. وقد امتدت فترة حسابها لثلاثة شهور باستخدام 40 نقطة في هيكلية من أجهزة الحوسبة الموزعة CUDA. جرى نشر الجداول عبر خوادم مشاركة الملفات المعروفة باسم BitTorrent.

ومع توالي ظهور الهجمات وجوانب الضعف الجديدة في شبكات اتصال الهواتف المحمولة صرح خبير التشفير نوهل بأنه يجب على تلك الشبكات الا تُستخدم لأنظمة الأمن خاصة الجديدة منها.

التحقق من الهوية ثنائي العناصر باستخدام جهاز الرقم المميز لكلمة المرور الفورية المؤقتة

جهاز الرقم المميز هو جهاز ملموس يتسلمه المستخدم لمساعدته في عملية التوثيق لذلك يشار له أيضاً بجهاز التوثيق أو جهاز الشفرة. تأتي الأرقام المميزة على شكل جهاز أو برنامج. في حالة الجهاز تكون على شكل قطع صغيرة سهلة الحمل. بعض هذه القطع يخزن مفاتيح تشفير أو بيانات قياس حيوي بينما البعض الأخر يعرض رقم تعريف شخصي يجري تغيره بمرور الوقت. وعندما يرغب المستخدم في الدخول إلى النظام بمعنى توثيق نفسه لدى النظام يستخدم رقم التعريف الشخصي المعروض في الجهاز بالإضافة إلى كلمة مروره العادية. أما في حالة البرنامج فإن برامج الرقم المميز تعمل على الحواسيب لتولد رقم تعريف شخصي يتغير بمرور الوقت. تطبق هذه بالبرامج خوارزمية كلمة المرور التي تُستخدم مرة واحدة فقط المعروفة باسم OTP. هذا النوع من الخوارزميات يمثل خطورة للأنظمة التي تستخدمه طالما أنه لا يجب أن يمتلك المستخدمين غير المصرح لهم القدرة على تخمين كلمة المرور التالية. تستخدم أجهزة SecurID التي تنتجها شركة RSA أرقام مميزة (يمكن أن تكون على أجهزة أو برامج) حيث يجري مزامنة ساعتها الداخلية مع الخادم الرئيسي. لكل جهاز منشأ فريد يستخدم في توليد رقم عشوائي وهمي. يجري تحميل هذا المنشأ للخادم عند شراء الجهاز واستعماله في التعرف على المستخدم. يولد الجهاز كلمة مرور تستخدم مرة واحدة كل 60 ثانية يستعملها المستخدم مع رقم التعريف الشخصي الذي لا يعرفه أحد غيره لتوثيق نفسه والتحقق من صحة هويته لدى الخادم. في حال مطابقة كلمة المرور التي تستخدم مرة واحدة و رقم التعريف الشخصي مع البيانات الموجودة في الخادم يجري توثيق المستخدم. يستلزم استخدام أجهزة الرمز المميز عدة خطوات تشمل تسجيل المستخدمين وانتاج الجهاز وتوزيعه ثم توثيق الجهاز و المستخدم وأخيراً إلغاء الجهاز والمستخدم. لذلك فإن أجهزة الرمز المميز بالغة التكلفة للمنظمات. على سبيل المثال فإن البنط الذي لديه مليون عميل

الشكل (17)

سوف يشتري ويعمل على تركيب وصيانة مليون جهاز من اجهزة الرمز المميز. بالإضافة إلي أن البنك عليه أن يوفر دعم مستمر لتدريب العملاء على كيفية استخدام ذلك النوع من الأجهزة. ويجب على البنك أيضاً الاستعداد لاستبدال أي جهاز في حال كسره أو سرقته. وللعلم فإن تكلفة استبدال جهاز من أجهزة الرمز المميز اكبر بكثير من تكلفة استبدال بطاقة الصراف الآلي أو إعادة تخصيص كلمة مرور. من وجهة نظر العميل فإن امتلاك حساب في أكثر م بنك يعني الحاجة لحمل والاحتفاظ بعدة أجهزة للرمز المميز مما يمثل إزعاجاً كبيراً وقد يؤدي إلى فقد أحد تلك الأجهزة أو سرقتها أو كسرها. وفي أغلب الحالات يدفع العميل تكلفة كل منها.

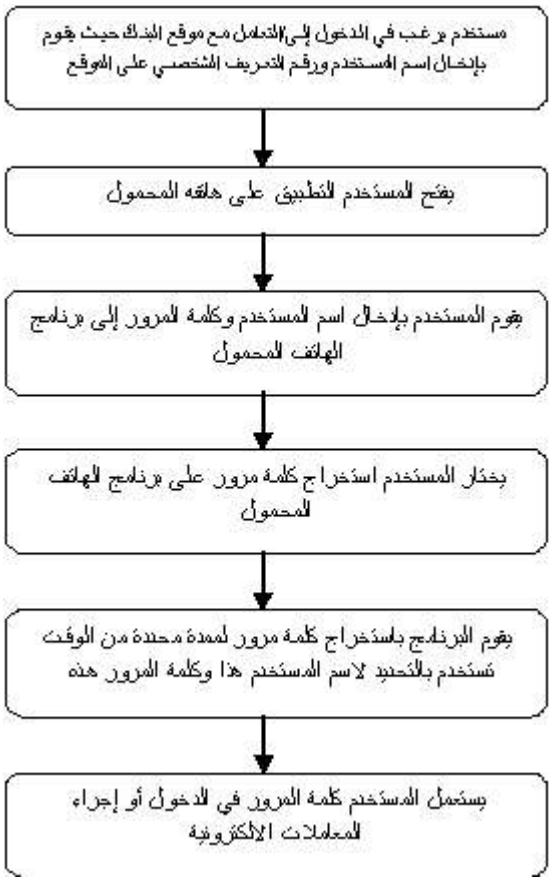
لسوء الحظ هذه الأساليب لا تحتمل الهجوم على بروتوكول التوثيق باعتراض البيانات حيث يستطيع المهاجم سرقة كلمة المرور بعد استخراج المستخدم لها من جهاز الرمز المميز وكتابتها في الموقع المزيف.

التحقق من الهوية ثنائي العناصر ببرنامج الرمز المميز على الهاتف المحمول – كلمة مرور تستخدم مرة واحدة

في هذه الحالة يجري استخراج كلمة مرور تستخدم مرة واحدة من خلال جهاز الهاتف المحمول مباشرة دون استخدام أي أجهزة رمز مميز أو انتظار موقع إلكتروني يرسل بكلمة المرور. يوجد في هذا الأسلوب برنامج مثبت على الهاتف المحمول حيث يستقبل اسم المستخدم ورقم التعريف الشخصي من المستخدم ثم يقوم بعدها باستخراج كلمة المرور التي تستخدم مرة واحدة دون الحاجة إلى تخزين اسم المستخدم ورقم تعريفه الشخصي. لذلك لا توجد أي خطورة في حال سرقة الهاتف المحمول أو تعطله. عند مقارنته بأسلوب التحقق من الهوية باستخدام الرسائل النصية القصيرة فإن أحد مميزات هذا الأسلوب هي رخص التكلفة وسهولة الاستخدام وعدم تقيده بالمكان مثل مشكلة التجوال في أنظمة كلمة المرور التي تستخدم مرة واحدة عبر الرسائل النصية القصيرة.

تعتمد خوارزميات توليد كلمة المرور التي تستخدم لمرة واحدة على عامل معين هو أن خادم الموقع الالكتروني قادر على استخراج نفس كلمة المرور عندما يريد المستخدم الدخول بمعنى أن الخادم على معرفة بمدى صحة كلمة المرور المستخدمة. ولتأمين النظام فإن كلمة المرور المستخرجة يجب أن تكون صعبة في تخمينها أو استرجعها أو تتبعها بواسطة المخترقين. لذلك من الممهم جداً تطوير خوارزمية آمنة لتوليد كلمات المرور التي تستخدم مرة واحدة.

النظام المقترح هنا يستلزم استخدام هاتف محمول وبرنامج رمز مميز لتوليد كلمة المرور التي تستخدم مرة واحدة التي تكون صالحة لمدة قصيرة يحددها المستخدم إضافة إلى أنها تستخرج باستخدام عناصر فريدة لكل من المستخدم وجهاز الهاتف المحمول نفسه. يبين المخطط التالي خطوات برنامج الهاتف المحمول لاستخراج كلمة المرور التي تستخدم لمرة واحدة.



عند مقارنة هذه الطريقة بأسلوب الرسائل النصية القصيرة لكلمات المرور التي تستخدم مرة واحدة الذي تطبقه بعض المصارف فإن طريقة البرنامج المثبت على الهاتف المحمول تؤدي نفس الخدمة مع تحمل البنك تكلفة أقل كما أنها أسهل في التعامل من جانب المستخدم وتحل مشكلة التجوال الموجودة في نظام الرسائل النصية القصيرة.

لسوء الحظ هذه الأساليب لا تحتمل الهجوم على بروتوكول التوثيق باعتراض البيانات حيث يستطيع المهاجم سرقة كلمة المرور بعد استخراج المستخدم لها من جهاز الرمز المميز وكتابتها في الموقع المزيف (كما في كل أنظمة كلمة المرور التي تستخدم لمرة واحدة التي عند استعمالها لمتصفح الويب للتعامل مع المواقع المزيفة).

البنوك المحلية تطبق المعيار الثنائي للتحقق من الهوية

مؤخراً قام بنك "سامبا" في السعودية برفع مستوى الأمن والحماية من خلال اجراءات أمنية جديدة ينفذها من خلال خدماتها المصرفية على شبكة الانترنت وبإطلاق مايُسميه "المعيار الثنائي للتحقق من الهوية"، لعل عملاء بنك "سامبا" يتذكرون شاشة الدخول إلى حسابهم المصرفي التي تظهر في شكل (18) والتي تسمح بكتابة بيانات الدخول من خلال لوحة مفاتيح افتراضية، فلقد تم إلغاء هذه الطريقة في الدخول منذ بدء شهر أبريل الحالي.

الشكل (18)

الآن لن يتم دخول عملاء بنك "سامبا" لحساباتهم الإلكترونية إلا باستخدام "المعيار الثنائي للتحقق من الهوية" و التي ابتكرها بنك "سامبا" لزيادة الحماية الآمنية لعملائه، وتقوم فكرة هذا المعيار الثنائي على أن تقوم بكتابة بيانات الدخول لحسابك كما في الشكل (19)، بعد أن تُحدد ما الخدمة التي تريد الدخول إليها، فهل هي الخدمات البنكية أو سداد الفواتير أو خدمات بطاقة الائتمان الخ .

الشكل (19) - صفحة الدخول الجديدة لموقع سامبا

بعدها سينقلك موقع ''سامبا'' إلى صفحة أخرى ومن خلالها سيطلب منك كتابة رقم سري مؤقت قام بإرساله إلى هاتفك الجوال لتقوم بإدخاله في هذه الصفحة كما في الشكل (20) لينقلك بعد ذلك إلى حسابك المصرفي و تُنجز معاملاتك المالية كالمعتاد.

شكل (20) - صفحة إدخال الرقم السري المؤقت الذي سيصلك عن طريق هاتفك الجوال

كذلك قام البنك الأهلي السعودي , و الراجحي المصرفية السعودية بتطبيق نفس المعيار لزيادة الأمان و بالتالي تعكس النظرة الإجابية حول التعامل مع الخدمات المصرفية عبر الإنترنت .

الخاتمة

كما لاحظنا من خلال البحث أن التجارة الإلكترونية في تطور متزايد , و تطوير تقنية المعلومات مستمرة في سبيل جعل الحياة أسهل , و كسب المستهلكين و العملاء و إقناعهم بأن التعاملات عبر الإنترنت آمنة , كما تشير الدراسات التي أعدتها William Blair & Company, L.L.C. بأن التجارة الإلكترونية ستشهد نموا قويا في السنوات القادمة , بالمقابل فإن التهديدات الأمنية في تزايد مستمر , لاحظنا من خلال التقارير التي أعدتها شركة Symantec بأن التورجينات و الفيروسات و وسائل الهجمات أخرى عبر الانترنت في تزايد و تطور مستمر , و أن قطاع المالي هو المستهدف الرئيسي بين القطاعات المختلفة بسبب الخدمات المصرفية الإلكترونية, إن هاجس حماية المعلومات البنكية الخاصة بعملاء البنوك على الانترنت يزداد يوما بعد يوم نظرا لتزايد الجرائم الالكترونية على الانترنت , و حيث أن البنوك تعتبر من الضرورة تأمين وصول عملائها إلى حساباتهم إلكترونيا لتنفيذ عملياتهم البنكية دون الحاجة لزيارة الفروع فإنها تعده استثمارا طويل الأجل و تدفع نحمه بشكل مستمر , إن اهتمام البنوك بزيادة مستوى الأمان لموقعها الالكتروني يعتبر معيار و دليلا على رقي مستوى خدماتها البنكية و مع ذلك فإن البنوك لم تقف موقف الاستسلام بل حاولت إجاد حلول أمنية مبتكرة للتصدى لمثل تلك الهجمات و الاختراقات غير قانونية , و من تلك الحلول التحقق من الهوية ثنائي العناصر , و سوف نشاهد حلول أخرى أكثر أمانا كنظام الذي يستخدم بطاقات الذكية تعتمد على البنية التحتية للمفتاح العام أو أجهزة المميز التي يمكن توصيلها عبر منفذ الـ USB . مع أن هذه الأنظمة مكلفة و قد تكون غير مناسبة للمستخدمين إلا أن تطوير أدوات و أنظمة الحماية مستمرة .

المراجع

المراجع العربية :

موجز الدليل الإرشادي لأمن الخدمات المصرفية عبر الانترنت – مؤسسة النقد العربي السعودي 2001 ver. 1.0 .

الضوابط الرقابية للعمليات المصرفية الالكترونية و إصدار وسائل دفع لنقود الالكترونية – البنك المركزي المصري 2002 .

التحقق من الهوية في المعاملات البنكية عبر الانترنت – مقالة علمية – مركز التميز لأمن المعلومات – جامعة الملك سعود .

التجارة الالكترونية من منظور الادارة الاستراتيجية:فرص وتهديدات لصناعة التأمين - د .جمال الدباغ-جامعة فيلادلفيا- الاردن 2005 .

المراجع الأجنبية :

Symantec Global Internet Security Threat Report Trends for 2009 Volume XV, Published April 2010

E-commerce Annual Report - William Blair & Company, L.L.C.2010

Secure Internet Banking Authentication - PUBLISHED BY THE IEEE COMPUTER SOCIETY 2006

المواقع الانترنت :

أموالي www.amoaly.com

مركز التميز لأمن المعلومات – جامعة الملك سعود http://coeia.edu.sa

موسوعة ويكيبيديا الحرة ar.wikipedia.org