

المعاملات التجارية والمالية عبر الانترنت وسبل تأمينها

الأستاذة بركان أمينة

م.ج. خميس مليانة

ملخص:

من أكثر موضوعات عصر المعلومات إثارة للجدل في وقتنا الحاضر موضوع التجارة الإلكترونية، ونسأل معاً، لماذا كان الحدث وآخر إفرازات عصر المعلومات - من بين موضوعاتها وتحدياتها وقطاعاتها - أكثرها إثارة للجدل وأكثرها محلاً للاهتمام، إن الخصوصية وحماية الحياة الخاصة من مخاطر التقنية كانت أول موضوعات الاهتمام في أواخر الستينات، ثم تبعها الاهتمام بجرائم الكمبيوتر ومن ثم الملكية الفكرية لمصنغات المعلوماتية وتحديد البرامج اعتباراً من النصف الثاني للستينات ومطلع الثمانينات، ومن ثم مسائل محتوى الموقع المعلوماتي مترافقة مع مسائل المعايير والمواصفات ومقاييس أمن المعلومات ومسائل الأتمتة المصرفية والمالية اعتباراً من مطلع التسعينات، أمن المعلومات ووسائل الدفع الإلكتروني والملكية الفكرية والتعاقد الإلكتروني والحجية والمعايير ...

الخ

وسنحول في مقالنا هذا التطرق إلى أهم المخاطر التي تتعرض لها المعاملات المالية والتجارية عبر الانترنت وكذا أهم الطرق المستخدمة لمواجهة هذه التهديدات.

لهذا فقد تم تقسيم هذا المقال إلى قسمين كالتالي:

أولاً: مخاطر وتهديدات المعاملات التجارية والمالية عبر الانترنت

ثانياً: نظم السرية وتأمين المعاملات التجارية والمالية والانترنت.

تمهيد :

بالرغم من المزايا الواضحة التي تحققها التجارة الالكترونية في الوقت الحالي وخاصة للدول المنتظمة إلا أنها ما زالت تعاني من قصور في مجالات امن التعاملات التجارية والمالية عبر الانترنت ،حيث يعتبر تأمين المعاملات التجارية وتأمين وسائل وطرق الدفع هو التطور التكنولوجي الأساسي المطلوب للانطلاق بالتجارة الالكترونية وتحقيق على مستوى للسرية والتأمين والخصوصية(*)

أولاً:مخاطر وتهديدات التعاملات التجارية والمالية عبر الانترنت

يعد امن وسرية المعلومات التي يجرى تبادلها بين البائع والمشتري (عند إبرام صفقة ما من صفقات الأعمال الالكترونية) من القضايا المهمة جدا والضرورية لنجاح هذه التجارة أو بقضايا مالية (مثل أرقام حسابات المشتريين أو البائعين وأرقام بطاقات الائتمان) إذ بالإمكان استغلال البيانات المالية للبائع أو للمشتري للقيام بعمليات نصب وسرقة واحتيال ولذلك قام مسالة امن وسرية البيانات (خصوصا المالية) هي من المسائل المهمة التي تتطلب جهودا كبيرة

فنجد برزت أهمية الأمن والسرية في تعاملات وتبادلات الأعمال والتجارة الالكترونية بسبب عمليات الاختراق والتخريب التي يمارسها لصوص الانترنت ، وهذه العمليات أدت إلى خسائر كبيرة لمنظمات الأعمال بسبب الفيروسات أو عمليات التخريب للموقع وغلقة ... وغيرها من المخاطر سنحاول انم نوحز أهم المخاطر والتهديدات التي تتعرض لها المعاملات التجارية والمالية عبر الانترنت فيما يلي:

(*) السرية: يقصد بها اخفاء محتوى الرسائل او البيانات بطريقة مناسبة تمنع التعرف على محتوياتها خلال تحريرها او حفظها او تداولها من شخصية كل من المرسل او المستقبل ، الخصوصية يقصد بها الاستخدام المعلومات والرسائل في صورتها الكلية او الجزئية في غير العرض المرخص به من صاحب المعلومة او الرسالة وان يقتصر ايضا على الشخص او الجهة المرسل اليها الرسالة ، وعدم اتاحة ما بها من بيانات لاي جهة الا بموافقة صاحب الشأن .

- تغيير محتوى الموقع: هي احد المخاطر البسيطة التي تتعرض كافة مواقع منظمات الأعمال بغض النظر عن حجم مقر المعلومات أو مكان بث معلومات المقر أو ارتباط المقر بالمنظمة الداخلية، ويتم تغيير المحتوى من خلال نوعين من الهجمات هما:

1- هجمات الصوت: يتم فيها تغيير لبعض المحتوى الذي يؤثر على شكل المقر ويجعل منه مدعات السخرية والاستخفاف.

2- هجمات المحترفين: هي هجمات تتم عن قصد من بعض الشركات المنافسة والتي تعتمد إلى تغيير بعض المعلومات بالمقر بما يسيء إلى المنظمة أو بما يؤدي إلى إساءة العلاقة بين المنظمة وعملائها نتيجة المعلومات التي تم تعديلها بمعرفة المهاجمين.

ب- إغلاق الموقع أمام المتصفحين: هو أيضا احد المخاطر العامة التي يمكن أن يتعرض لها أي موقع ، حيث يقوم المهاجم بشغل حاسب المقر الرئيسي **server** بسبل من الوسائل والاستفسارات التي تؤدي في النهاية إلى عدم قدرة الموقع على تلبية أي استفسارات من مستخدمين فعليين أو عدم قدرة أي مستخدم عادي على الدخول إلى مقر المعلومات من الصلف أو إبطاء ردود الموقع على أي استفسارات

ج- استخدام موقع معلومات المنظمة كقاعدة لتنفيذ أعمال هجومية خارجية:

تتعرض لهذا النوع من الهجمات المنظمات ذات المواقع الصغيرة ، وهذه الهجمات يمارسها هوات سوء الاستخدام، أو المجرمون المحترفون ، حيث يستخدم الموقع كنقطة انطلاق لتنفيذ أعمال هجومية على مواقع أخرى، حيث لا يستطيع هذه الأخيرة اكتشاف هوية المهاجم الحقيقي او موقعه الأساسي : كما قد يقوم المهاجمون بإخفاء ملفات تخص الموقع المهاجم.

د- تخريب موقع المنظمة: يتم تخريب الموقع بتغيير المحتوى أو وقف الخدمة من خلال التحميل الزائد بالاستفسارات أو الدخول على برامج إدارة الموقع وتغيير معاملاتهما مما يؤدي إلى توقف الموقع أو حدوث أخطاء في التشغيل ويكثر حدوثه للمنظمات الحكومية.

هـ- **الدخول على النظم الداخلية للمنظمة:** أعلى درجات التهديد التي تحدث عند ارتباط الموقع بالنظم الداخلية ، ويمكن دخول الأنظمة من أي جهاز يرتبط بالانترنت ومرتبطة في الوقت نفسه بالنظم الداخلية، ويعتبر دخول النظم الداخلية تهديدا حقيقيا حيث يتمكن الشخص الحصول على معلومات داخلية قد تؤدي إلى نتائج سلبية في أعمال المنظمة أو قد تؤدي إلى توقف العمل، أو يتمكن من حذف بعض أو كل المعلومات الداخلية .

و- **إخطار الوسائل الالكترونية:** تعد الوسائل الالكترونية أكثر مصادر الخطر التي تسمح للمصادر المجهولة بالدخول إلى الجهاز كما تعتبر أسرع وسيلة نشر برامج الفيروسات وبرامج الهجوم وتعطيل عمل الشبكات أو برامج التجسس ومن مصادر التهديد الأمني في الرسائل الالكترونية.

- الملفات المرفقة التي تحتاج فتحها خاصة إذا كانت بامتداد من الآتي بعد (مثل ملفات تنفيذية بامتداد لأنها تنفذ مباشرة، وامتداد ملفات الأوامر التي تعمل او ملفات الحزم التي تحتوي على مجموعة أوامر...)

- ملفات مرفقة ذاتية التشغيل تعمل فور فتح برنامج البريد دون حاجة لفتح المرفقات وتقوم إعادة تحميل نظام التشغيل ثم العمل في خفاء وإضافة نفسها في كل رسالة ترسلها دون علمك لتصيب المرسل إليه والطريقة الوحيدة للحماية من مثل هذا النوع هو إلغاء وحجب خاصية السماح بالنصوص البرمجية من التصفح.

- بقية نظام DOS يستطيع بها مرسل الرسالة أو الصفحة تخريب أو تعطيل الجهاز عند فتح الرسالة تستخدم لغة ترميز النص المتشعب لأنه يزرع تعليمات في نظام التشغيل لتعطيل نظام ويندوز المعتمد على نظام DOS يمنع نظام التشغيل من التعامل مع مكونات العتاد مثل الطابعة ، والقرص الصلب ..

- كما يمكن تقسيم التهديدات التي تواجهها مواقع المتاجر الالكترونية إلى ثلاثة أنواع نوجزها في:

أ- **تهديدات للبرنامج:** تتضمن:

- سرقة برنامج؛

- حذف برنامج عرضيا أو عن قصد؛
- تشويه برنامج أما نتيجة عطل في الاجهزة او نتيجة فيروس؛
- عيوب وعلل البرامج أو تصميم المواقع التي قد يكون تأثيرها عاجلا أو آجلا ؛
- ب- تهديدات للأجهزة : وتتضمن:
 - السرقة (الكمبيوتر أو المواد الأخرى)؛
 - العبث أو التدمير من موظف في عمل الأجهزة والمعدات أو قطع الكبلات؛
 - الاستخدام الخاطئ أو التصرف الغير سليم لحماية غير الجيدة بتعرض المعدات للتدمير بالنار أو المياه.
- ج- يدات للمعلومات: وتتضمن.

- الحذف أو النسخ أو السرقة؛
 - التشويه الناتج عن مشاكل الأجهزة أو من علة في برنامج.
- إما عن مصادر التهديدات التي تواجهها مواقع المتاجر الالكترونية فهي تكون مصادر داخلية وقد تكون مصادر خارجية ، فالمصادر الداخلية هي اغلب شيوعا ، نظرا لقرب المستخدمين من مستويات الأنظمة والأجهزة ، أما المصادر الخارجية للتهديدات فهي اخطر من الداخلية ليس بسبب عدم معرفة من الذي يحاول اختراق النظام بل لن يكون معروف مدى اختراقه للنظام ومدى خبرته في التخريب والسطو او هدفه من وراء ذلك ، فبعض الأشخاص يذهبون لى أقصى الحدود للوصول إلى الأنظمة والمعلومات.

ثانيا: نظم السرية وتأمين المعاملات التجارية والمالية والانترنت .

إن هجمات الهواة والمحترفين ومحاولتهم اختراق النظم الأمنية للمواقع المتاجر الالكترونية ونظم المعلومات، وتعددت مصادر هذه الهجمات والتهديدات (داخلية وخارجية) أصبح من اكبر عوائق التجارة الالكترونية لذى تم العمل والبحث عن عدة نظم لضمان السرية والتامين للمعاملات التجارية والمالية عبر الانترنت، واهم هذه النظم ما يلي:

أ. تشفير البيانات:

1- مفهوم التشفير (البيانات): التشفير هو احد وسائل تحقيق التامين والسرية ، ويعتمد على تغيير محتوى الرسالة باستخدام برامج مفتاح تشفير قبل إرسال الرسالة، وتكون لدى المستقبل قدرة استعادة الرسالة الأصلية بعملية عكسية لذلك التشفير، فالتشفير إذا عملية تستخدم للحفاظ على سرية المعلومات باستخدام غير محول لهم بذلك لا يتمكنون من فهمها بسبب ظهور خليط من الرموز و الأرقام والحروف العير مفهومة، وقد ساعدت الرغبة في دعم امن التجارة الالكترونية في زيادة توفير هذه النوعية من البرامج.

2- أنواع وأشكال تشفير البيانات: تختلف أنواع وأشكال برامج التشفير المتخصصة وتعتمد على مفهوم لكل معلومة مشفرة تحتاج إلى ثلاثة عناصر مجتمعة لإعادتها إلى أصلها وعلى هذا ظهرت ثلاثة أشكال لنظم التشفير وهي.

- نظام المفتاح العام: يعتمد هذا النظام على وجود مفتاحين لكل مستخدم هما: المفتاح العام والمفتاح الخاص.

المفتاح العام هو مفتاح معروف ويمكن استخدامه بواسطة أي شخص أو جهة يريد أو يرسل رسالة إلى شخص ولا يستخدم هذا المفتاح إلا في التشفير فقط، فهذا المفتاح العام إذا هو رقم يتم تداوله ونشره بين بقية المستخدمين لتشفير أي معلومة أو رسالة الكترونية ويعتبر المفتاح (الرقم) العام هو أساس التشفير ولا يستطيع احد أن يفك رموز المعلومات قبل صاحبها لأنها تحتاج إلى رقما سريا هو المفتاح الخاص

أما المفتاح الخاص هو النصف الآخر المكمل للمفتاح العام للوصول إلى رقم الأساس^(*) و إعادة المعلومة المشفرة لوضعها الطبيعي قبل التشفير، وهذا المفتاح الخاص يختلف لكل شخص عن غيره يجب الاحتفاظ بالمفتاح الخاص سرا.

- **نظام التشفير المتماثل:** يعتمد هذا النوع (النظام) من التشفير على استخدام مفتاح متماثل يتم به التشفير والحل، حيث تم التشفير الرسالة لدى المرسل باستخدام مفتاح خاص لينتج منها رسالة مشفرة ثم يقوم المرسل بإرسال الرسالة المشفرة إلى المستقبل باستخدام وسائل الاتصال العادية ويقوم بإرسال المفتاح بحل الشفرة والحصول على الرسالة الأصلية.

- **التشفير من خلال المزج بين نظام المفتاح المتماثل والمفتاح العام:** إن درجة التعقيد الموجود في نظام المفتاح العام وما تحتاجه ن قوة حساب عالية وقت في التشفير و في حل الشفرة تعد ميزة إضافية في توفير درجة أمان عالية وعيب بالنسبة لمتطلبات وتكلفة تنفيذ التشفير.

وإذا كان نظام المفتاح المتماثل بسيط في درجة تشفيره، وبالتالي لا يحتاج إلى قوة حاسبات كبيرة ولا إلى وقت طويل في فك شفرته، فإن ما يعيبه هو طريقة إرسال المفتاح الخاص و التي تحتاج إلى قناة اتصال مؤمنة .

لذا يوفر المزج بين النظامين وسيلة لتحقيق درجة تامين مناسبة في اقل وقت دون استخدام القدرات الكبيرة للحاسبات لتحقيق درجة التشفير المطلوبة وتتم الخطوات على النحو التالي:

- يتم تشفير الرسالة الأصلية بمفتاح متماثل؛
- يتم تشفير المفتاح بالمفتاح العام للمرسل إليه؛
- يتم إرسال الرسالة المشفرة بالمفتاح المتماثل والمفتاح المتماثل المشفر بالمفتاح المرسل إليه باستخدام أي شبكة اتصالات؛

(*) رقم الاساس تصدره هيئة مستقلة متخصصة من طريق برنامج متخصص بحيث يكون لكل مستخدم رقم اساس يتم تقسيمه الى مجموعتين اولها المفتاح العام، وثانيها المفتاح الخاص، بحيث ان ناتج حزب المفتاح العام في الخاص يساوي رقم الاساس وهو رقم خاص له حماية وتشفير

- يقوم المرسل إليه بتلقي المفتاح المتماثل المشفر بالمفتاح العام له ويقوم بحل شفرة هذا المفتاح باستخدام المفتاح الخاص به ليحصل على المفتاح المتماثل المشفر به الرسالة الأصلية ؛
- يقوم باستخدام المفتاح المتماثل (بعد فك تشفيره) في فك الرسالة الأصلية المشفرة ليحصل على الرسالة الأصلية .

ب - التوقيع الالكتروني:

- 1- تعريف التوقيع الالكتروني :** يقصد بالتوقيع الالكتروني اتخاذ وسيلة يتم من خلالها التحقق ن صاحب الرسالة أو المعاملة هو الشخص الذي قام فعلا بإرسالها أو تنفيذها .
- فالتوقيع الالكتروني هو مجموعة من الرموز أو الأرقام أو الحروف الالكترونية التي تدخل على شخصية الموقع دون غيره.

يستخدم التوقيع الالكتروني نظام التشفير بأسلوب المفتاح العام المزود وذلك على النحو التالي :

- يقوم المرسل إليه بتشفير الرسالة باستخدام المفتاح العام للمرسل إليه؛
- يتم إرسال الرسالة باستخدام المفتاح العام للمرسل إليه؛
- يتم إرسال الرسالة باستخدام شبكات مفتوحة؛
- يقوم المرسل إليه بحك بصمة المرسل منه باستخدام المفتاح العام للمرسل منه والتأكد من شخصية المرسل منه.

من خلال هذه العملية يتضح أن هناك درجتين من التشفير، الدرجة الأولى للتوقيع الخاص بالمرسل منه (أو البصمة) وتتم باستخدام مفتاحه الخاص ويتم فكها في آخر مرحلة باستخدام مفتاحه العام، وبذلك فهي خاصة بتحديد شخصية المرسل منه ولا يمكن ان يحدث فيها أي التباس حيث يتم تشفيرها بالمفتاح الخاص للشخص .

أما الدرجة الثانية من التشفير والخاصة بالرسالة والتي تتم لمحتوى الرسالة بالإضافة إلى التوقيع (بعد تشفيره بالمفتاح الخاص للمرسل منه)، وهذه تتم بالمفتاح العام للمرسل إليه.

أشكال التوقيع الإلكتروني : هناك أنواع التوقيع الإلكتروني منها:

- التوقيع باستخدام القلم الإلكتروني : معناه نقل التوقيع الإلكتروني المكتوب بخط اليد على المحور إلى الملف المراد نقل هذا المحور إليه باستخدام الجهاز اسكانير وعليه ينقل الدور موقعاً عليه من صاحبه إلى شخص آخر باستخدام الانترنت.
إلا أن تلك الطريقة تواجه الكثير من المعوقات تمثل في عدم الثقة حيث يمكن للمستقبل أن يحتفظ بهذا التوقيع الموجود على المحور، الذي استقبله عن طريق الانترنت عبر جهاز الاسكاتر ووضعه على أي مستند آخر ليده دون وجود أي طريقة يمكن من خلالها التأكد من أن صاحب هذا التوقيع هو الذي وضعه، فهذه الطريقة مأخوذ حذها انعدام الثقة ويقلل من حجية التوقيع الإلكتروني.

- التوقيع باستخدام الخواص الذاتية : هذا النوع من التوقيع يعتمد على الخواص الكيميائية والطبيعية للأفراد وتشمل تلك الطرق الآتي :

- البصمة الشخصية؛
 - مسح العين البشرية؛
 - التحقق من مستوى وثيرة الصوت؛
 - خواص اليد البشرية؛
 - التعرف على الوجه البشري؛
 - التوقيع الشخصي .
- وهو ما يعني أن يتم تعيين الخواص الذاتية للعين مثلاً عن طريق اخذ صورة دقيقة لها وتغذيتها في الحاسب الآلي لمنع أي استخدام من أي شخص آخر بخلاف الشخص المخزنة الخواص الذاتية لعينة ، وهكذا الحال بالنسبة لبصمة الأصابع أو خواص اليد البشرية ، وغيرها من الخواص الأخرى.

- التوقيع الرقمي: وتعني منظومة بيانات في صورة شفرة بحيث يتكون في إمكان المرسل إليه والتأكد من مصدرها ومضمونها، ولكن أكثرها شيوعا التوقيعات الرقمية القائمة على ترميز المفاتيح العامة والمفاتيح الخاصة.

3- نظام الحركات المالية الالكترونية (نظام المعاملات الالكترونية الآمنة) (SET^(*))

تم تطوير نظام المعاملات الالكترونية الآمنة SET بالتعاون أكبر شركات كروت الائتمان العالمية وهي شركة فيزا وماستركارد ، وذلك بغرض تأمين المعاملات المالية على شبكة الانترنت باستخدام بطاقة الائتمان، حيث صدر هذا النظام (SET) عام 1996. الغاية من هذا البروتوكول ضمان الحفاظ على امن البيانات (خصوصيتها وسلامتها) والتحقق من صولها إلى الجملة المطلوبة أثناء إجراء الحركات المالية عبر الانترنت، وكذا إضفاء الشرعية والموثوقية على أصحاب المتاجر الالكترونية وحملة البطاقات الائتمانية.

تتضمن عملية الشراء وفقا لبروتوكول الحركات المالية الآمنة (SET) خمسة أطراف هي:

- حامل البطاقة؛

- موفر المحفظة الالكترونية؛

- التاجر؛

- معالج عمليات الدفع؛

- بوابة الدفع.

ولإجراء الحركات المالية وفقا لبروتوكول الحركات المالية الآمنة يتطلب قيام الزبون في أول الأول بفتح حساب بطاقة ائتمانية في احد المصارف ثم يصدر المصرف إلى صاحب البطاقة برنامجا خاصا ببروتوكول الحركات المالية الآمنة SET يدعى برنامج المحفظة الالكترونية وتستخدم هذه المحفظة في الشراء وإجراء الحركات المالية عبر الانترنت.

(*) Secure Electronic Transaction

وتثبت المحفظة الالكترونية في كمبيوتر المستخدم حيث يمكن الولوج إليها في أي وقت للقيام بعملية الدفع عبر الانترنت، وتحمل هذه المحفظة الالكترونية على معلومات مثل رقم بطاقة الائتمان وشهادة بروتوكول الحركات المالية الآمنة، وتاريخ انتهاء البطاقة، ومن جهة أخرى تعد شهادة بروتوكول الحركات المالية الآمنة دليلاً على أن المصرف قد تحقق من هوية حامل البطاقة وللحصول على هذه الشهادة يحول الزبون إلى جهة مخولة بمنح الشهادات ومعتمدة لدى المصرف.

ويفتح التاجر حساباً لدى مصالح عمليات الدفع هو المؤسسة التي تزود التجار بالحسابات وتتولى التحقق من عمليات الدفع التي قام بها الزبائن بالإضافة إلى التعامل معها ومعالجتها) قد يكون مصرفاً ليحصل على ما يلزمه من برمجيات لاستخدام نظام **SET**، وتتضمن هذه البرمجيات شهادة نظام **SET** الممنوحة للتاجر والمفتاح العام لمعالج عمليات الدفع المختار، وتستخدم هذه البرمجيات لمعالجة الحركات المالية على الانترنت، ويمكن للزبون أن يسأل عن شهادة **SET** للتحقق من التاجر والاستفادة من مفتاحه العام، وعند إجراء طلب لشراء معين يستخدم الزبون المفتاح العام للتاجر في التوقيع على معلومات طلب الشراء، كما يستخدم المفتاح العام للمصرف في التوقيع على معلومات الدفع التي ستوجه لاحقاً إلى التاجر.

وبعد ذلك يعود التاجر بشهادة **SET** الخاصة به إلى المصرف أو معالج عمليات الدفع للتحقق من هوية الزبون والحصول على تحويل بالدفع وذلك استناداً إلى شهادة **SET** الزبون (أو وسائل الدفع)، ويتحقق المصرف أو معالج عمليات الدفع من هويتي التاجر والزبون ويعالج طلب الشراء ومعلومات الدفع وبعد التحقق يوقع المصرف (أو معالج عمليات الدفع) رقمياً على رسالة تحويل يرسلها إلى التاجر وبعد ذلك يرسل التاجر رسالة تأكيد إلى الزبون ثم تنفذ الخدمات المطلوبة في استمارة الطلبية ثم يولد السند أو الوصل ثم يشحن.

ويمكن للتاجر تلقي الدفعات من الزبائن دون شهادة **SET** وفي هذه الحالة ليس على التاجر سوى استخدام شهادة **SET** الخاصة به لتوثيق الحركات المالية مع المصرف أو معالج الحركات المالية

الذي يتعامل معه، وبعد التأكد من صحة الحركة المالية وقبولها يولد هذا التاجر السند ويشحن البضاعة الى الزبون.

بالرغم من تعقد الإجراءات التي تنفذ لإتمام المعاملات من خلال SET إلا أن هذه الإجراءات تتم في خلفية العمل و لا يشعر بها أي من المشتري أو البائع حيث تقوم البرامج المتاحة في كل من متصفح المشتري ونظام المشتري نظام إدارة مقر معلومات البائع بإجراء كافة العمليات بصورة آلية

4- بروتوكول طبقة الفتحات الآمنة (بروتوكول الطبقات الآمنة) SSL(*)

قامت شركة NETXEPE بتطوير بروتوكول SSL واستخدامه في متصفحات من اجل دعم الجانب الأمني للانترنت.

بروتوكول SSL هو برنامج به بروتوكول تشفير متخصص لنقل البيانات والمعلومات المشفرة بين جهازين عبر شبكة الانترنت بطريقة آمنة بحيث لا يمكن قراءتها لغير المرسل إليه وتختلف عن بقية طرق التشفير الأخرى في عدم طلب اتخاذ أي خطوات لتشفير المعلومات المراد حمايتها من مرسل البيانات فكل ما يفعله المستخدم هو التأكد من استخدام هذا البروتوكول ،حيث يقوم هذا البرنامج بربط المتصفح الموجود على جهاز المستخدم المشتري بجهاز خادم خاص لموقع الشراء إذا كان الخادم الموقع باستخدام بروتوكول تحكم النقل وبروتوكول الانترنت TCP/IP، ويعمل البرنامج كطبقة آمنة وسيطة بين بروتوكول تحكم النقل وبروتوكول نقل النص المتشعب http(**).

5- نظام التحويلات المالية الالكترونية EFT(***)

نظام EFT هو عملية منح الصلاحية لمعرفة ما للقيام بحركات التحويلات المالية الدائنة والمدنية الكترونيا من حساب مصرفي إلى حساب مصرفي آخر، وهذه العملية تتم عبر الهواتف والأجهزة الكمبيوتر وأجهزة المودم عوضا عن استخدام الأوراق.

(*) hyper text. Transfer protocol

(**) secure socket layer

(***) electronic funds transfer

ونظرا لسرعة العمليات التجارية الالكترونية ظهر الاحتياج إلى نظام يتيح لهم القيام بكافة العمليات المصرفية التي يحتاجونها بسرعة شديدة توافق سرعة التجارة الالكترونية ، وعليه كان نظام EFT من أهم النظم التي اشرتت وزاد الاعتماد عليها نظرا لأنها تتم بسرعة شديدة بالإضافة إلى الفوائد التالية.

- السلامة والأمن: حيث ألغت المقاصة الآلية والتحويلات المالية الالكترونية الخوف من سرقة الشيكات الورقية والحاجة إلى تناقل الأموال السائلة بالإضافة الى:
- تقليل الأعمال الورقية مثل الشيكات التقليدية وغيرها من المعاملات الورقية؛
- تحسن التدفق النقدي وسرعة تناقله؛
- توفير المصاريف وتسيير العمل ألغت المقاصة الالكترونية حاجة العميل و التاجر إلى زيادة المصرف؛ لإيداع قيمة التحويلات المالية مما يعني تسيير الأمر ورفع فعالية نظام العمل وتقليل الجهد والنفقة؛
- تنظيم الدفعات حيث يكفل الاتفاق على وقت اقتطاع وتسديد قيمة التحويلات المالية وتنظيم عمليات الدفع دون أي تخوف في إمكان عدم السداد في الوقت المحدد؛
- زيادة رضا العميل وتوطيد الثقة في التعامل مع التاجر او المنظمة.

6- نظام تحويل البيانات الكرتونيا EDI:

- نظام EDI^(*) هو مجموعة من المعايير المستخدمة في تبادل معلومات العمل من أجهزة الكمبيوتر التابعة للشركاء التجاريين وتنفيذ صفقات العمل بطريقة الكرتونية لا تعتمد على الورق ، ومن العمليات التي يقوم بها نظام EDI الاستعمالات، طلبات الشراء والتسعير ،حالة الطلبيات ،جدولة المواعيد ، الشحن، الاستقبال ،دفعات الفواتير، العقود، بيانات الإنتاج، المبيعات ومن فوائد نظام EDI:
- منع التزوير أو التحسس أو القرصنة ؛
 - تخفيض المصاريف الإدارية وتقليل الجهد المبذول في التعامل مع الوثائق وأعمال البريد؛
 - توفير الوقت بنقل المعلومات بشكل أسرع؛
 - تحسين العلاقة بين الزبائن والتاجر؛

(*) Electronic Data Interchange

- يزيد EDI من القدرة التنافسية للمنظمة التي تعتمد.

7- نظام الشراء عبر الانترنت (**): OBI

معيار OBI ترعاه شركة american expren وتدعمه شركات البرمجيات مثل شركة microsoft و oracle ويحظى المعيار بقبول ومصداقية شركات معروفة مثل شركة general electric و ford و united technologie.

وسعى معيار obi إلى أن يكون معيارا موحدا متفقا عليه لمواكبة نوع محدد من أنواع التجارة الالكترونية وهي الأعمال الموجهة للأعمال B2B، كما يسعى معيار OBI إلى تحقيق امن وسرية المعاملات (خصوصا المالية) وتسعى كذلك إلى تنميط المعاملات المالية التي تجرى عبر الانترنت من اجل تسهيلها ودفع مستوى فاعليتها الأمنية

8- معيار التبادل المالي المفتوح OFX (***)

كانت بدايات استخدام معيار OFX في عام 1997، وقد قام بتصميمها ورعايتها شركات microsoft و intuit و checkfree، وقد جرى دعمها والمصادقة عليها من جانب اغلب المؤسسات المالية العريقة bank of america و wells fargo و cite bankk حيث جرى تصميم هذا المعيار وتطويره من اجل التعامل مع نوع محدد من المنظمات (الأعمال) فهي تركز على معالجة قضايا الأمن والسرية التي تتعلق بالمعاملات المالية بين المؤسسات المالية وكذلك بين هذه الأخيرة وزبائننها والتي تتم عبر الانترنت .

9- جدار النار: fire wall

بسبب كثرة الخروقات التي تتعرض لها مواقع المتاجر الالكترونية وعمليات الاختراق والتدمير التي تتعرض إليها الملفات الخاصة في أجهزة الحاسوب وفي خوادم الويب، فقد جرى ابتكار تكنولوجيا الجدران النارية. وجدار النار هو برنامج يمكن تشغيله على نفس حاسوب خادم الويب أو حاسوب آخر مرتبط بخادم الويب، ويمارس جدار النار عمله عن طريق إجراء عملية فحص لرزم بروتوكول

(**) Open Buying on the Internet

(***) Open- Financial Exchange Specification

الانترنت IP الجواله بين خادم الانترنت والزبون ويجري التحكم في البيانات والمعلومات على أساس عنوان بروتوكول الانترنت IP ورقم المنفذ في كلا الاتجاهين ن جدار النار يمكنه إعاقه ومنع جميع محاولات الدخول إلى الشبكة المحمية بهذا الجدار الناري.

ويهدف جدار النار بدرجة أساسية إلى توفير الجانب الأمني ، كما انه يقدم خدمات أخرى مثل:

- تقسيم إحصاءات حول حركة المستخدمين والزائن من الشبكة إليها؛
 - تحديد الخدمات التي يطلبها ويرغب فيها هؤلاء المستخدمين والزائن؛
 - تحديد ورصد الأعمال والتصرفات المشبوهة التي يمارسها بعض المستخدمين؛
 - بناء تصور متجدد بالتعديلات الضرورية على سياسات وإجراءات الأمن في ضوء ما يكشفه جدار النار، وفي ضوء مستوى جموده أمام محاولات الاختراق والتخريب المتعمد.
- فعلا سبيل المثال يمكن التحكم في جميع المستويات الذين يدخلون إلى شبكة الانترنت من احد مزودات خدمة الانترنت ومنعكم من الوصول إلى حاسوب / حواسيب محددة، ويمكن إعاقه منفذ/ منافذ محددة من أي محاولة دخول إلى الشبكة المحمية بجدار ناري.
- إذن فهناك عدة بدائل أمام المنظمة في وضع جدار النار أهمها:
- السماح بكل الطلبات وكل محاولات الدخول باستثناء حالات محددة؛
 - السماح بكل الطلبات وكل محاولات الدخول في حالات استثنائية.
- هناك نوعين رئيسيان من حوائط المنع هما :

- مرشحات مجموعات البيانات: وهذه يتم استخدامها من خلال **ROUTERS**؛
 - تطبيقات تحكم في البوابات : والتي تعمل على حاسبات آمنة خاصة.
- إذا فتامين وحماية مواقع المتاجر الالكترونية يجب أن يتم على عدة مستويات هذه المستويات يتمثل في الآتي:

- مستوى حوائط النار؛
- مستوى شبكة الاتصالات؛
- مستوى التشغيل الخاص بالحاسب الموجود عليه موقع المعلومات؛
- مستوى المعلومات وقواعد البيانات الموجودة بالموقع؛

- مستوى الحاسب الموجود عليه موقع المعلومات؛
- مستوى أدوات وبرامج مواجهة الفيروسات؛
- مستوى الخطة العامة والسياسات الخاصة بتأمين وسلامة المعلومات؛
- مستوى الأفراد وتدريبهم .

المراجع:

- اكرم عبد الوهاب، التجارة الالكترونية، مكتبة لبن سينا للطباعة والنشر، القاهرة، 2004.
- نزار النعسان، مساهمة التجارة الالكترونية في زيادة القدرة التنافسية وتخفيض التكاليف، من الموقع:
- منير محمد الجنبهي، البنوك الالكترونية، دار الكتب الجامعي، الاسكندرية، 2005.
- منير محمد الجنبهي، البنوك الالكترونية، دار الكتب الجامعي، الاسكندرية 205.
- عبد القادر بن عبد الفتوح، الحكومة الالكترونية، مجلة العلوم والتقنية، العدد 65، محرم 1424، الرياض.
- رأفت رضوان، "عالم التجارة الالكترونية"، القاهرة: المنظمة العربية للتنمية الإدارية، 1999.
- طارق عبد العال حماد، "التجارة الالكترونية"، الدار الجامعية، مصر، 2002/2003.
- البنك الاهلي المصري، التجارة الالكترونية: تطويرها ومستقبلها، النشرة الاقتصادية، العدد الثاني، المجلد، 2002، 51.

[http:// www.t-koshak-com/vb/showthread-php.\(15/06/2007\)](http://www.t-koshak-com/vb/showthread-php.(15/06/2007))

- MARCEL PUCCOIN . Next l'argemen electronique . bakque ,hier . aujourd'hui ,demain ed . sefi 1996.