

الفصل الرابع عشر

أمن التعاملات المالية والتجارية عبر الإنترنت

Financial Transactions Security

مفهوم أمن الأعمال الإلكترونية Security Concept:

يعدّ أمن وسرية المعلومات التي يجري تبادلها بين البائع والمشتري (عند إبرام صفقة ما من صفقات الأعمال الإلكترونية) من القضايا المهمة جداً والضرورية لنجاح هذه التجارة، خصوصاً عندما تتعلق المسألة بأسرار العمل (خصوصاً في مجال B2B) أو بقضايا مالية (مثل أرقام حسابات المشتريين أو البائعين وأرقام بطاقات الائتمان) إذ بإمكان استغلال البيانات المالية للبائع أو المشتري للقيام بعمليات نصب وسرقة واحتيال ولذلك فإن مسألة أمن وسرية البيانات (وخصوصاً المالية) هي من المسائل التي تستحوذ على اهتمام المختصين في مجال الأعمال الإلكترونية عبر الإنترنت، وتلجأ إلى أساليب متعددة لتحقيق الأمن والسرية مثل التشفير Encryption.

إن الأمن SECURITY هو أحد العناصر الأساسية للمزيج التسويقي الإلكتروني.

وقد برزت أهمية الأمن والسرية في تعاملات وتبادلات الأعمال والتجارة الإلكترونية بسبب عمليات الاختراق والتخريب التي يمارسها لصووس الإنترنت Internet Hackers ، وهذه العمليات أدت إلى خسائر كبيرة لمنظمات الأعمال الإلكترونية وقد أدت في أكثر من مرة إلى توقف هذه المواقع عن الأعمال بسبب الفيروسات أو عمليات التخريب التي يتسبب فيها هؤلاء اللصوص (لصوص

الإنترنت).

إن ضمان بناء خبرات حسنة عن التعاملات التجارية والمالية عبر الإنترنت يعتمد على:

أ. معدلات تواجد الزبائن إلى ممارسة الأعمال والتجارة الإلكترونية.

ب. مستوى توجه وتحول المنظمات إلى ميدان الأعمال الإلكترونية

أمن التعاملات المالية Financial Transactions Security

لقد أصبحت الأنترنت أداة أساسية للتعاملات المالية التي تجري بين الزبون ومنظمات الأعمال ومتاجرها الإلكترونية.

وهناك مجموعة من المتطلبات التي ينبغي مراعاتها في التعاملات المالية عبر الإنترنت، أهمها:

١. ضرورة توفير ضمانات كافية وأدلة وافية وعلى نطاق واسع بأن التعاملات المالية عبر الإنترنت هي تعاملات آمنة، ولن تتعرض إلى انتهاكات إجرامية.

٢. توافر الإمكانيات التكنولوجية التي تكفل إنشاء البنى التحتية الآمنة
Secure Infrastructure.

٣. ضرورة استخدام ميكانيكية سهلة في تقديم الأعمال الإلكترونية، وبحيث يجري إدراك هذه السهولة من جانب الزبون على أنها في مستوى سهولة الميكانيكيات الأخرى المستخدمة، على الأقل، أو أكثر سهولة.

٤. وجوب تحقيق الثقة بين كل الأطراف المشاركة في التعاملات المالية عبر الإنترنت، وضرورة أن تنتهي بنجاح ضمن المدى الزمني المتوقع.

٥. القدرة على التعامل مع حجم المتوقع من الزبائن والتعاملات المالية عبر الإنترنت، إذ أن زيادة هذا الحجم وعدم قيام المتجر الإلكتروني بتوفير الإجراءات والوسائل والأدوات اللازمة لمواجهة هذه الزيادة يؤدي إلى

حدوث إرباك ومشكلات تكنولوجية، ويؤدي إلى رفع مستوى التكاليف اللازمة.

مواصفة التعاملات الإلكترونية الآمنة

Secure Electronic Transactions Specification- SET-

لقد اعتمدت شركات بطاقات الائتمان معيار التعاملات الإلكترونية الآمنة لتحقيق التبادل المالي باستخدام بطاقات الائتمان عبر الإنترنت، من جانب آخر، فإن معيار التعاملات المالية الآمنة SET جرى قبوله واعتماده من جانب مزودي الكيانات البرمجية Software Suppliers (مثل شركة IBM وشركة Microsoft وشركة Netscape).

وقد جرى استخدام معيار التعاملات المالية الآمنة في أول عملية تبادل مالي عام ١٩٩٧ في الولايات المتحدة الأمريكية.

ويسعى معيار SET إلى تحقيق مجموعة من الأهداف أهمها:

١. تحقيق مستوى عال من الثقة والأمن في البيانات والمعلومات.
٢. التأكد من سلامة عملية الدفع.
٣. إضفاء الشرعية والموثوقية على أصحاب المتاجر الإلكترونية وحملة البطاقات الائتمانية.

إن المتطلبات والاحتياجات الأساسية التي جرى التركيز عليها والتعبير عنها ضمن مواصفة SET قد جرى تقسيمها إلى ما يأتي:

١. أية بيانات ومعلومات تنقل وترسل عبر الإنترنت يجب أن تظل سرية.
٢. يجب أن يظل محتوى أية عملية تبادل غير قابل للتغيير أثناء عملية نقل البيانات والمعلومات، وباستخدام مواصفة SET فإنه يمكن تصميم التوقيع الإلكتروني Digital Signature، ويمكن إدراج هذا التوقيع ضمن بيانات ومعلومات عملية التبادل يساعد على اكتشاف فيما إذا طرأ تغير عليها أثناء النقل والإرسال.

٣. يحتاج المتجر الإلكتروني إلى أن يتأكد من أن حامل بطاقة الدفع **Card Holder** هو المالك الشرعي لرقم حساب بطاقة الدفع، ومن جانب آخر، فإنه يجب أن يكون حامل البطاقة قادراً على التحقق من هوية مالك المتجر الإلكتروني، وأن يكون واثقاً من أن هذا المتجر قادر على تعاملات مالية آمنة.

٤. إن معيار **SET** يجب أن يكون قابلاً للتطبيق والتنفيذ على مدى واسع من الأدوات الإلكترونية، وأن لا يجري تفضيل كيان برمجي **Software** أو كيان مادي محدد **Hardware** على غيره بحيث يكون أكثر قدرة على تطبيق وتنفيذ المواصفة.

معيار الشراء المفتوح عبر الإنترنت:

Open Buying on the Internet- OBI-

إن معيار الشراء المفتوح عبر الإنترنت **OBI** يسعى إلى أن يكون معياراً موحداً متفقاً عليه لمواكبة نوع محدد من الأعمال الإلكترونية وهي الأعمال الموجهة للأعمال **(Business- to-Business B2B)**.

وهذا المعيار ترعاه شركة **American Express** وتدعمه شركات البرمجيات مثل شركة **Microsoft** وشركة **Oracle**، ويحظى المعيار بقبول ومصادقة شركات معروفة مثل شركة **General Electric** وشركة **Ford** وشركة **BASF** وشركة **United Technologies**.

مواصفة التبادل المالي المفتوح

Open Financial Exchange Specification- OFX-

هذه المواصفة جرى تصميمها وتطويرها من أجل التعامل مع نوع محدد من المؤسسات، فهي تركز على معالجة قضايا الأمن والسرية التي تتعلق بالتعاملات المالية بين المؤسسات المالية، وكذلك فيما بين هذه المؤسسات وبين زبائنهم والتي

تتم عبر الإنترنت.

وقد كانت بدايات استخدام مواصفة OFX في العام ١٩٩٧ ، وقد قام بتصميمها ورعايتها شركات Microsoft و Intuit و CheckFree ، وقد جرى دعمها والمصادقة عليها من جانب أغلب المؤسسات المالية العريقة (مثل Citibank و American...الخ).

معيّار تبادل البيانات آلياً

eLECTRONIC Data Interchange-EDI-Standards

وقد وجدت بالأساس من أجل العمل على تسهيل التعاملات التجارية النمطية وتسهيل عمليات التبادل. حيث أصبح حالياً بإمكان الشركات والمؤسسات الصغيرة استخدام EDI بسبب انخفاض تكاليفها بصورة حادة بسبب إمكانية استخدام الإنترنت كشبكة تخدم ال EDI.

بروتوكولات SSL و S-HTTP: SSL and S-HTTP Protocols

وهي بروتوكولات تعمل ضمن مستعرضات (متصفحات) الويب Web Browsers من أجل منع اعتراض البيانات والمعلومات التي يجري إرسالها عبر الإنترنت في أية نقطة أثناء انتقال هذه البيانات والمعلومات. كما جرى إدراج هذه البروتوكولات أيضاً ضمن نظم مزودات شبكة الويب، ولذلك فإن بروتوكول SSL يعمل على تشفير Encryptio هذه الصفحات بعد أن يملأها الزبون بالبيانات والمعلومات المطلوبة، ويجري إرسالها باستخدام المتصفح (المستعرض) بصورة مشفرة آمنة، ويجري فك وتحليل التشفير والترميز بعد أن تصل البيانات والمعلومات إلى الجهة المطلوبة بعيداً عن عبث الآخرين.

جدار النار Fire Wall

جدار النار يهدف بدرجة أساسية إلى توفير الجانب الأمني، غير أنه يقدم خدمات أخرى مثل:

تقديم إحصاءات حول حركة المستخدمين والزائين من الشبكة وإليها.

تحديد الخدمات التي يطلبها ويرغب فيها هؤلاء المستخدمون والزبائن.
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 صموده أمام محاولات الاختراق والتخريب
المتعمد.

وعندما تتخذ الإدارة قرارها بإنشاء جدار ناري فإنه ينبغي وضع سياسة واضحة
بخصوص مستوى الأمن الذي ينبغي تحقيقه، ويكون أمامها عدة بدائل أهمها:

- السماح بكل الطلبات وكل محاولات الدخول باستثناء حالات محددة.
- السماح بكل الطلبات وكل محاولات الدخول في حالات استثنائية .
- وهناك مجموعة من القضايا التي ينبغي مراعاتها عند بناء تكنولوجيا الجدار
الحاجز الناري، وأهمها:
- ضرورة تسجيل جميع فعاليات جدار النار ومراجعة وتدقيق هذه الفعاليات بصورة
مستمرة.
- وضع خطة فاعلة لمواجهة أية أعطال قد تطرأ ويتسبب بها لصوص الإنترنت
والمخربون والسعي إلى معرفة هوياتهم وملاحقتهم.
- ضرورة امتلاك منظمة الأعمال الإلكترونية لاستراتيجية أمنية فاعلة، وأن يكون
بناء جدار النار قادراً على أن يصب في تحقيق أهداف هذه الاستراتيجية.
- ضرورة تحديد المستخدمين/ الزبائن الذين يملكون حق الوصول إلى ما يقدمه
المتجر الإلكتروني.
- ضرورة تحديد البروتوكولات والخدمات المطلوبة من المستخدم/ الزبون سواء
على المستوى الداخلي أو المستوى الخارجي.