الفصل السادس عشر

سرية البيانات والتجارة الإلكترونية

يتزايد يوماً بعد يوم عدد التجار الذين يعربون عن تفاؤلهم بالفوائد المرجوة من التجارة الإلكترونية، إذ تسمح هذه التجارة الجديدة للشركات الصغيرة بمنافسةَ الشركات الكبيرة. وتُستحدَث العديد من التقنيات لتذليل العقبات التي يواجها الزبائن، ولا سيما على صعيد سرية وأمن المعاملات المالية على الإنترنت[1]، وأهم هذه التقنيات بروتوكول الطبقات الأمنية **(Secure Socket Layers- SSL)** وبروتوكول الحركات المالية الآمنة **(Secure Electronic Transactions- SET)**، ويؤدي ظهور مثل هذه التقنيات والحلول إلى إزالة الكثير من المخاوف التي كانت لدى البعض، وتبشر هذه المؤشرات بمستقبل مشرق للتجارة الإلكترونية، وخلاصة الأمر أن التجارة الإلكترونية قد أصبحت حقيقة قائمة، وأن آفاقها وإمكاناتها لا تقف عند حد .

برغم كل هذه المؤشرات التي تُبشِّر بمستقبل مشرق للتجارة الإلكترونية، إلا أنه من الصعب التنبؤ بما ستحمله إلينا هذه التجارة، ولكن الشيء الوحيد المؤكَّد بأن التجارة الإلكترونية وجِدَت لتبقى.

1 **http://www.asir1.com/as/showthread.php?t=36898**

يتصدر موضوع الأمن على شبكة الإنترنت قائمة الاهتمامات لدى معظم المستخدمين خاصة ممن يرغبون في الشراء عبر الإنترنت ولذلك نجد الأغلبية الساحقة من المستخدمين خاصة الجدد منهم يمتنعون عن الشراء عبر الإنترنت ويؤجلون الخوض في مثل هذه التجربة حتى تكتمل الصورة لديهم ويتعرفون على المزيد من درجة الأمان في استخدام بطاقات الائتمان فتعالوا معنا نتعرف على فارس التجارة الإلكترونية والسبب الرئيسي في زيادة الثقة بالتعاملات التجارية عبر الشبكة.

تقنية طبقة الفتحات الآمنة SSL[1]:

هو برنامج به بروتوكول تشفير متخصص لنقل البيانات والمعلومات المشفرة بين جهازين عبر شبكة الإنترنت بطريقة آمنة بحيث لا يمكن لأحد من الناس قراءتها غير المرسل والمستقبل وفي نفس الوقت تكون قوة التشفير فيه قوية ويصعب فكهها.

وهي تختلف عن بقية طرق التشفير في شيء واحد ألا وهو عدم الطلب من مرسل البيانات اتخاذ أي خطوات لتشفير المعلومات المراد حمايتها وكل الذي يفعله المستخدم هو التأكد من استخدام هذا البروتوكول بالقوة المطلوبة ولقد ساعدت هذه التقنية التي طورتها شركة نت سكيب على زيادة الثقة بالتجارة الإلكترونية ومستوى الأمان فيها مما جعلها أساس التجارة الإلكترونية الناجحة على مستوى العالم ولقد قامت جميع الشركات المنتجة لمتصفحات الإنترنت بالأخذ بها وتزويد متصفحاتها بهذه التقنية.

كيفية عمل هذه التقنية:

يقوم هذا البرنامج بربط المتصفح الموجود على جهاز المستخدم (المشتري) بجهاز الخادم الخاص بالموقع المراد الشراء منه وهذا طبعاً إذا كان الخادم مزوداً

1 http://www.3rbsc.com/vb/newreply.php? Do=newreply &p=1121.

بهذه التقنية أساساً ويقوم هذا البرنامج بتشفير أي معلومة صادرة من ذلك المتصفح وصولاً إلى جهاز الخادم الخاص بالموقع باستخدام بروتوكول التحكم بالإرسال وبروتوكول الإنترنت وهو ما يعرف بـ**TCP/IP** ولقد سميت بالطبقة الآمنة لأن هذا البرنامج يعمل كطبقة وسيطة تربط بين بروتوكول التحكم بالنقل وبروتوكول **(HTTP://(Hyper Text Transfer Protocol** .

وتتلخص خطوات استخدام هذه التكنولوجيا في ثلاث خطوات وهي:

يقوم الموقع بالتقدم إلى إحدى الهيئات المستقلة والتي تصدر شهادة رقمية تثبت صحة هوية الموقع، وبعد التأكد من نشاط وحسن سيرة تلك المواقع المتقدمة بالإضافة لاستكمال بعض المتطلبات الأخرى ذات العلاقة تقوم تلك الهيئة بإصدار الشهادة الرقمية الخاصة بالموقع بحيث يدون فيها كل المعلومات الهامة مثل اسم الشركة وتاريخ إصدار الشهادة وتاريخ الانتهاء، وكذلك يتم إصدار المفتاح العام والمفتاح الخاص للموقع ويقوم الموقع أيضاً بتأمين جهاز خادم مزود ببرنامج التشفير إس إس إل ليتم تخزين المفتاح العام للموقع به.

عند دخول المشتري (زائر الموقع) للصفحة الآمنة التي يدخل بها البيانات والمعلومات المطلوبة للشراء يقوم المتصفح المزود بهذا البرنامج بالارتباط بالجهاز الخادم الآمن للموقع ويطلب منه التالي: الشهادة الرقمية، مصدرها، تاريخ انتهائها وكذلك تتم المقارنة بين اسم الموقع على الشهادة مع اسم الموقع في جهاز الخادم والمقارنة بين الرقم العام المرسل من الجهاز الخادم إلى المتصفح مع التوقيع الإلكتروني للشركة وكل هذه الخطوات تتم للتأكد من مصداقية الموقع وحمايتك من الشركات الوهمية علماً بأن جميع هذه الخطوات تتم بواسطة المتصفح لديك دون علمك أو تدخلك وبعد أن يتم

التأكد من كل ذلك يقوم المتصفح بإعلامك بالنتيجة في حال عدم المطابقة أو إذا كانت هناك ملاحظات.

بعد خطوة التأكد من مصداقية الموقع والارتباط بجهاز الخادم الآمن يتم تشفير المعلومات على أساس المفتاح العام لذلك الموقع ليتم نقل المعلومات بطريقة آمنة دون أي تدخل منك ولا يستطيع أحد سرقة المعلومات أو الإطلاع عليها سوى الموقع المعتمد في الطرف الآخر والذي يملك المفتاح الخاص لفتح وإعادة المعلومات إلى وضعها الطبيعي.

كيف تحمي المواقع المعلومات الخاصة بالزبائن:

طبقاص لأهمية موضوع الأمن بالنسبة لمواقع البيع الإلكترونية فهي تتخذ الكثير من الإجراءات الاهترازية بخلاف ما تتخذه من ترتيبات متعلقة بتكنولوجيا الحماية لأن معظم العملاء يودون معرفة المزيد عن سرية تناول وتداول هذه المعلومات بعد وصولها إلى الموقع بسلام ومإذا يحدث بعد فتح التشفير ولذلك فإن معظم المواقع تقوم بعدة خطوات أخرى لحماية العملاء لأن أي اهتزاز للثقة يعني فقدان الكثير للموقع ولذلك فهي تتعامل بكل جدية في هذا الموضوع. وإليكم ملخصاً لما تتخذه كل المواقع العالمية من إجراءات لحماية البيانات الخاصة بالعملاء.

حصر فتح المعلومات المشفرة على عدد قليل من الموظفين الموثوق بهم.

يتم توزيع المعلومات بعد فتحها وفرزها إلى الأقسام المتخصصة إلكترونياً بحيث لا يتم إعطاء أي قسم سوى المعلومات التي يحتاجها فعلياً فمثلاً لا يتم إعطاء رقم بطاقة الائتمان إلا لقسم المحاسبة لخصم المبلغ ويتم تشفيرها مرة أخرى ولا يمكن لأي شخص أن يطلع عليها.

يقوم الموقع بإضافة جميع البيانات الخاصة بك في بنك المعلومات الخاصة بالموقع وهي محمية بجدران اللهب وكلمات العبور ولا يمكن لأي شخص غير

مخول له بالوصول إليها.

تقوم المواقع بعمل عدة طبقات من الصلاحيات للموظفين بحيث لا يمكن لأي موظف الوصول إلى معلومات غير مصرح له بالوصول إليها فمثلاً في قسم الشحن والتخليص ليس له من صلاحيات إلا الوصول إلى معلومات عن رقم الطلبية وتاريخها والعنوان المرسل إليه.

التحكم بالحركة في بعض أقسام الشركة فمثلاً. لا يسمح بالدخول إلى قسم بنك المعلومات إلا للموظفين المصرح لهم والذين يملكون أرقاماً سرية للدخول.

يتم الاحتفاظ بأرقام بطاقات الائتمان مشفرة في أجهزة مستقلة داخل قسم بنك المعلومات وهي غير مرتبطة بالإنترنت.

أي تداول للمعلومات بين الأقسام المختلفة بالشركة لا تحمل رقم بطاقة الائتمان وإن حصل فإنها لا تظهر سوى نوع البطاقة وآخر أربعة أرقام.

obeikan.com