الجامعة الإفريقية العقيد أحمد دراية - أدرار
كلية الآداب والعلوم الإنسانية
قسم علوم التسيير
اليوم الدراسي حول:
التجارة الإلكترونية في الجزائر- الواقع والآفاق
استمارة المشاركة

الاسم : أمحمد + محمد + وهيبة
اللقب: بن الدين + شهيدي + حليمي
الوظيفة : أستاذ مساعد + أستاذ مساعد + أستاذ مساعد
المؤسسة : جامعة أدرار+ جامعة تلمسان + جامعة تلمسان
الهاتف : 063/03/60/04 - 091/21/98/92
الفاكس: .
البريد الالكتروني : mus01dine@yahoo.fr
أريد أن أشارك في اليوم الدراسي بمحاضرة ملصقة
المحور: الإطار القانوني المنظم للتجارة الإلكترونية
عنوان المداخلة: أمن الشبكات من مخاطر التهديدات الإلكترونية ودوره في تعزيز التجارة الإلكترونية

أمن الشبكات من مخاطر التهديدات الإلكترونية ودوره في تعزيز التجارة الإلكترونية

مقدمة :

لقد شهد العقد الأخير من هذا العصر نمواً هائلاً لشبكة المعلومات العالمية أو الإنترنت، سواء بعدد المستخدمين أو بعدد المواقع الإلكترونية التي تزودهم بالمعلومات. حيث تشير إحصائية انترنت وورد ستاتس (Internet World Stats, 2006) إلى أن عدد الأشخاص الذين أتيح لهم النفاذ إلى الانترنت بلغ حوالي 16 مليون شخص عام 1995، وتضاعف هذا العدد بشكل كبير ليصبح حوالي 1022 مليون شخص في عام 2006. كما أن عدد المواقع الإلكترونية شهد

نمواً هائلاً أيضا حيث بلغ حوالي 6 مليون موقع عام 1996، وتضاعف هذا العدد بشكل كبير ليصبح حوالي 65 مليون موقع في عام 2005[1].

ولا شك أن هذا التطور المتزايد لشبكة الإنترنت مكنها من لعب دور البؤرة الرئيسية لعصر المعلومات ومكنها من أن تكون القاعدة الصلبة في عالم إدارة الأعمال والتسيير. وتعد التجارة الإلكترونية من أهم معالم هذا التطور بتأثيرها الإيجابي في الكلفة والتسويق وخدمة الزبائن والكفاءة الإدارية وغيرها.

ولعل من أهم العوامل التي تعزز وتدعم بناء مجتمع المعلومات وتنمي التجارة الإلكترونية هو توفير الأمن وتعزيز الثقة لدى المتعاملين ، من خلال خلق بيئة آمنة يعمل فيها الأطراف جميعا البائعون والمشترون والفنيون وكل من لهم صلة بذلك ، وضمن هذا السياق فإن هذه الورقة المتواضعة جاءت كمحاولة لإبراز أهم التهديدات الإلكترونية والمخاطر الناجمة عن استعمال الشبكة العالمية والتي تعيق نمو حجم التجارة الإلكترونية وكذا الحلول التقنية للتقليل منها بالإضافة إلى مختلف الجهود الرامية لتذليلها والحد من انتشارها معتمدين على المحاور الرئيسية التالية:

أولا : ماهية التجارة الإلكترونية وأهميتها
ثانيا : التأثير الإستراتيجي للإنترنت في الأعمال الإلكترونية
ثالثا: متطلبات أمن التجارة الإلكترونية
رابعا: الاعتداءات المحتملة التي تتعرض لها الأنشطة التجارية عبر شبكة الاتصالات
خامسا : بعض الحلول التقنية للوقاية من خطر التهديدات الالكترونية
سادسا: الجهود الدولية والإقليمية والوطنية لأمن المعاملات التجارية الإلكترونية

أولا: ماهية التجارة الإلكترونية وأهميتها :

شهدت التجارة الدولية في السنوات الأخيرة تغيرا جذريا نجم عن تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية وقدرة شبكة الانترنت تكنولوجيا على أن تجمع دول العالم في سوق الكترونية عالمية وفي تبادل للمعلومات تتيح مزايا واسعة المدى للاقتصاديات النامية والمتقدمة على حد سواء.

ونتيجة لهذه التطورات الاقتصادية والاجتماعية والعلمية والتكنولوجية التي شهدتها المجتمعات ، ظهرت التجارة الإلكترونية كموضوع من مواضيع ما يعرف بالاقتصاد الرقمي Digital Economy حيث يقوم الاقتصاد الرقمي على حقيقتين :- التجارة الإلكترونية و تقنية المعلومات Information Technology- IT فتقنية المعلومات أو صناعة المعلومات في عصر الحوسبة والاتصال هي التي خلقت الوجود الواقعي والحقيقي للتجارة الإلكترونية باعتبارها تعتمد على الحوسبة والاتصال ومختلف الوسائل التقنية للتنفيذ وإدارة النشاط التجاري.

---

[1]. عماد أبو الرب - ليلى رشيد حسن" **إطار نموذج لتقويم جودة المواقع الإلكترونية"** موجود بموقع

http://www.arabcin.net/arabiaall/4-2006/5.html أكتوبر 2007

ويمكن تعريف التجارة الالكترونية على أنها تبادل السلع والخدمات عبر إلكترونيا [2] ،كما عرفت منظمة التعاون الاقتصادي والتنمية OCED التجارة الإلكترونية على أنها "المعاملات التجارية التي تتم من قبل الأفراد والهيئات التي تعمل على معالجة ونقل البيانات الرقمية بما فيها الصوت والصورة من خلال شبكات مفتوحة مثل الانترنت أو مغلقة مثل Minitel Aolوالتي تسمح بالدخول إلى شبكات مفتوحة "[3]وقد ظهرت هذه التجارة اعتمادا على توفر تكنولوجيتين رئيسيتين هما تكنولوجيا الاتصالات وتكنولوجيا المعلومات اللتين أفرزتا ضمن اندماجهما البنية التحتية - الانترنت، و التي أوجدت بدورها القاعدة الاقتصادية والاجتماعية لنشر التجارة الكترونيا ما بين صغار ومتوسطي الناشطين في التجارة.

ويُمكن تقسيم نشاطات التجارة الإلكترونية بشكلها الحالي إلى قسمين رئيسين هما:

تجارة إلكترونية من الشركات إلى الزبائن الأفراد (Business-to-Consumer)، ويُشار إليها اختصارا بالمصطلح B2C، وهي تمثِّل التبادل التجاري بين الشركات من جهة والزبائن الأفراد من جهة أخرى.

تجارة إلكترونية من الشركات إلى الشركات (Business-to-Business)، ويُشار إليها اختصارا بالرمز B2B؛ وهي تمثِّل التبادل التجاري الإلكتروني بين شركة وأخرى[4].

لقد بدأت التجارة الالكترونية تشكل تحديا للقواعد التحليلية والعملية للتجارة الدولية وتحدث ثورة فيها لمجموعة من الأسباب يأتي في مقدمتها : قدرتها في تخفيض تكاليف الصفقات عالميا ومن ثم فهي تقلل من العقبات الجغرافية التقليدية , فضلا عن ذلك فأنها تسمح بظهور منافسين جدد في عدد متزايد من الأسواق ويمكن لشركات (واقتصاديات) صغيرة أن تصبح منافسا ناجحا في الأسواق باستنادها إلى شبكات المعلومات الأمر الذي يجعل البائع والمشتري يعرفان على الفور الأسعار والنوعية وشروط التسليم التي يعرفها مختلف المنافسين.

ونتيجة لذلك تطورت التجارة الالكترونية بسرعة كبيرة جدا فمن (8) مليارات دولار عام 1997 إلى (150) ملياراً عام 2000 و (300) مليار عام 2002 ويتوقع أن تصل إلى أكثر من (1000) مليار دولار عام 2020 . وأمام كل ذلك يتوقع أن تؤدي التجارة الالكترونية إلى حدوث مجموعة من النتائج المهمة والتي يمكن تحديد أهمها كالآتي:-

1- الحضور العالمي ، حيث تمكن التجارة الإلكترونية من تحقيق حالة من الحضور العالمي لأداء الأعمال على نطاق عالمي.

2 - يتمتع المستهلكون بفوائد مماثلة لما تحصل عليه الشركات تقريبا فهم يستطيعون التبضع بأسعار أفضل والاختيار من مجموعة واسعة من المنتجات والتحرر في الوقت نفسه من القيود الجغرافية لحدود الحي أو المدينة ومن ثم شراء السلع والخدمات من جميع أنحاء العالم عبر الانترنت , ومع هذه القدرة على الاختيار يستطيع المستهلكون التأثير في نوعية وسعر السلع التي يشترونها.

---

[2] السيد أحمد عبد الخالق**"التجارة الإلكترونية والعولمة"** بحوث ودراسات ، المنظمة العربية للتنمية الإدارية ، مصر ، 2006، ص 34.

[3] زايري بلقاسم، طوباش علي، **"طبيعة التجارة الإلكترونية وتطبيقاتها المتعددة"** مجلة المستقبل العربي ، عدد ماي 2003، ص 70.

4 حازم سكيك **"التجارة الإلكترونية"** مجلة فيزياء بلا حدود، موجودة بموقع ، http://hazemsakeek.com/magazine/index.php?option=com_content&task=view&id=37&Itemid=53 نوفمبر 2007.

3 - وعلى المستوى الوطني تؤثر التجارة الالكترونية في القدرة التنافسية وحركية المشاريع وسلوك المستهلك في البلد وفي الوقت الراهن لا تمتلك البلدان النامية القدرة على التوسع بسبب الأسواق المحدودة . وستخلق لها التجارة الالكترونية على الفور أسواقا جديدة بتوسيع نطاق تغطيتها وبالتالي حجم أعمالها.

4 - يؤدي استعمال تكنولوجيا المعلومات والاتصالات إلى وضع اقتصادي عديم الاحتكاك (Frictionless)حيث تكون فيه كلفة العملية التجارية اقرب إلى الصفر , وتتلاشى فيه الحواجز ما بين الدول والأسواق , فضلا عن ذلك فان التعامل المباشر دون وجود وسطاء في العملية التجارية سيؤدي إلى انخفاض كلفة الإجراءات التجارية وبالنتيجة سينعكس على كلفة الإنتاج مما سيشجع المنتجين للدخول في مسالك جديدة في الإنتاج والتسويق.

5 - تنامي استخدام النقود الالكترونية , حيث تعمل بعض المؤسسات المالية على تطوير جميع وسائل الدفع المعروفة لتتناسب مع مقتضيات التجارة الالكترونية وفي هذا المجال فقد جرى تطوير استخدام الشيكات الورقية إلى نظام الشيكات الالكترونية , ويعتمد تحويل الشيكات الورقية إلى شيكات رقمية على أساس الدراسات التي تمت في الولايات المتحدة والتي أوضحت أن البنوك تستخدم سنويا أكثر من 500 مليون شيك ورقي تكلف إجراءات تشغيلها حوالي 79 سنتا لكل شيك وتتزايد أعداد الشيكات بنسبة 3% سنويا وعندما أجريت دراسة عن إمكانية استخدام الشيكات الالكترونية اتضح أن تكلفة التشغيل للشيك يمكن أن تنخفض إلى 25 سنتاً وهو ما يحقق وفرا يزيد عن 250 مليون دولار سنويا في الولايات المتحدة فقط[5] .

ثانيا: التأثير الاستراتيجي للإنترنت في الأعمال الالكترونية :

ليس هناك أدنى شك من أن الأعمال الالكترونية قبل الانترنت كانت في مرحلة تطور خطية بطيئة لكنها قفزت بفضل استخدام تقنيات الانترنت لتمثل أهم ظاهرو تكنولوجية رافقت ولادة القرن الواحد والعشرين ، وبالنتيجة وبفعل تأثير تكنولوجيا الانترنت ظهرت الأعمال الإلكترونية والتجارة الالكترونية ، وانتقل تركيز الشركات الكبيرة منذ منتصف التسعينات إلى بناء نظم المعلومات المتكاملة مع المستفيدين من الزبائن والموزعين والموردين وتجار التجزئة والجملة والمنظمات التي تعمل في مجال التسهيلات اللوجيستية .

ولقد غيرت شبكة الانترنت قواعد العمل في عالم الأعمال لأنها مكنت قبل كل شيء من استثمار الفرص المتاحة في بيئة تكنولوجيا المعلومات لتحقيق نمو مطرد ومكاسب كبيرة وقد ساعدت في هذا السياق التطورات النوعية الهائلة في مجال تكنولوجيا المعلومات والاتصالات وخاصة بعد زيادة القدرات التقنية للأقمار الصناعية ونمو قوة الحوسبة ، وبطبيعة الحال تشكل الشبكة العنكبوتية العالمية (WWW) الجزء الأهم من الإنترنت ، وتتكون الويب من مجموعة من المستندات المختزنة على مئات الآلاف من أجهزة الكومبيوتر والتي تسمى صفحات الويب ، هذه الصفحات تزود المستخدمين بالمعلومات التي يحتاجونها ومن مجموعة الويب يتكون موقع الويب الذي قد تشرف عليه جامعة، مؤسسة، حكومة، وكالة أو شركة أو فرد.[6]

ولقد مر استخدام الانترنت في التجارة الالكترونية بمراحل ارتبطت بتطور التصفح والبرمجة واستخدام الشبكة ، حيث بدأت التجارة الالكترونية على شبكة الانترنت برسائل قوائم البريد

---

[5] باسم عبد الهادي حسن " **المزايا الاقتصادية التي تقدمها التجارة الالكترونية** " جريدة الصباح ، صادرة عن مركز الإعلام العراقي ، موجودة بموقع : http://www.alsabaah.com/paper.php?source=akbar&mlf=interpage&sid=41375 نوفمبر 2007.

[6] سعد غالب ياسين، بشير عباس العملاق "**الأعمال الإلكترونية** " دار المناهج للنشر والتوزيع، عمان، الأردن 2006، ص 55.

الالكتروني من أشخاص لبيع سيارة أو منزل ، وكان المشتري يتصل بالبائع ويتفاوض معه عبر البريد على السلعة ، وظهرت أيضا تطبيقات بيع وشراء الأسهم وتذاكر السفر على الإنترنت وعلى شبكة خاصة.

بانتشار شبكة الانترنت ثم ظهور ونمو شبكة ويب خلال النصف الثاني من التسعينيات بدأت الشركة تستخدم البريد الالكتروني مع خدمات استعراض وإنشاء مواقع ويب لعرض أنشطتها ومنتجاتها ووسائل الاتصال بها وبينها .ومع زيادة إمكانية الشبكة وتطورها وتطور تقنية البرمجة والاستعراض زادت مواقع وطرق ووسائل التجارة والبيع والتسويق ، وانتقلت الأعمال من تبادل الرسائل والإعلان عن المنتجات إلى نشاط التسويق والترويج والبيع.

وبتطور تقنيات الاتصالات الشبكية والوصول إلى أدوات تأمين أمكن استخدام بطاقات الائتمان* في دفع قيمة البضائع عبر الانترنت .وتطورت الأعمال الإلكترونية بين الشركات لتنتقل إليها الصفقات التجارية بتفاصيلها وأعمالها الإدارية والوثائق وفواتير الشحن والعقود وأوامر التحويل البنكي وعروض الأسعار والاعتمادات المستندية وغيرها بمفاهيم تختلف عن الطريقة التقليدية . ثم نشأت الأسواق الرقمية كمواقع تلاق لشركات مختلفة بشبكة معلومات واحدة تحتوي على بياناتهم وتديرها شركة مستقلة تقوم بإظهار مؤشرات المعلومات والتقارير للمشتركين لتبادل المعلومات التجارية واستثمارها في عقد الصفقات بينهم .

ولإعطاء أكثر أمان لشبكات الاتصال، ظهرت بطاقة الائتمان الذكية** لتحل محل بطاقات الائتمان العادية وتتيح سرية التعاملات المالية عبر الشبكة .

ولقد أدركت المؤسسات التجارية أهمية الانترنت ويمكن إبراز مدى أهمية الإنترنت بالنسبة للشركات التجارية من أن نسبة 76% من عدد المشتركين الجدد في الإنترنيت هي من نصيب الشركات والمؤسسات التجارية والتي ساهم في تزايد نسبها العديد من العوامل من بينها :

- انخفاض أسعار أجهزة الكومبيوتر .
- تطور شبكة الإنترنت وزيادة السرعة التي تعمل عليها.
- الحاجة إلى الإنترنت كملتقى عالمي للمعلومات والاتصالات .
- وجود سوق لعدد من المستخدمين يمكن الوصول إليه.
- وجود حالات ناجحة من شركات التجارة الإلكترونية.[7]

ثالثا: متطلبات أمن التجارة الإلكترونية:

1- التكاملية Integrity: وهي القدرة على إثبات أن المعلومات المعروضة على موقع الويب أو أن المعلومات المرسلة أو المستقبلة عبر الإنترنت يُعَدِّلها أي شخص غير مخول للقيام بهذا التعديل أو التبديل.

---

* **بطاقة الائتمان** : هي بطاقة بلاستيكية تحتوي على معلومات خاصة بالمتعامل كاسمه ورقم حسابه وبموجب هذه البطاقة يستطيع المتعامل الاستفادة من خدمات العديد من المحلات التجارية المتفقة مع البنك على منح الائتمان له على أن يقوم بسداد قيمة مشترياته للبنك ، ويتقاضى البنك عمولة بيع من هذه المحلات التجارية ومحلات الخدمات ، وبالتالي فإن الركيزة الأساسية التي تقوم عليها فكرة الائتمان هي أن الجهة المصدرة للبطاقة تجعل الوفاء بالقيمة للتاجر على أن يقوم باستردادها من حامل البطاقة على دفعات مؤجلة مما يحقق معنى الائتمان.

** **البطاقة الذكية** : هي بطاقة تحتوي معالج دقيق يسمح بتخزين الأموال من خلال البرمجة الأمنية وهذه البطاقة تستطيع التعامل مع بقية الكومبيوترات ولا تتطلب تفويض أو تأكيد صلاحية البطاقة من أجل نقل الأموال، وتتميز بعدة عناصر للحماية ضد عمليات التزوير وسوء الاستخدام من الغير في حالة سرقتها أو محاولة تقليدها .

[7] عبد الحميد بسيوني" **أساسيات ومبادئ التجارة الإلكترونية** " دار الكتب العلمية للنشر والتوزيع، القاهرة ، مصر ،2003، ص 20.

2- عدم النكران No repudiation: وهي القدرة على إثبات أن المشاركين في أعمال التجارة الإلكترونية لا ينكرون الأفعال التي قاموا بها تفاعلياً online.
3- الموثوقية Authenticity: وهي القدرة على إثبات هوية الشخص أو الكيان الذي تتعامل معه على الإنترنت.
4- السُّرية Confidentiality: وهي القدرة على إثبات أن الرسائل والمعطيات ستكون متاحة فقط للأشخاص المخولين للاطلاع عليها.
5- الخصوصية privacy: وهي القدرة على التحكم في استخدام المعلومات التي يقدمها المستخدم عن نفسه للتاجر أو البائع.
6- المُتاحيَّةAvailability: وهي القدرة على إثبات أن موقع التجارة الإلكترونية سيستمر بالتصرف كما هو مخطط له، أي وَفقاً لِما هو مبني من أجله.[8]

رابعا: الاعتداءات المحتملة التي تتعرض لها الأنشطة التجارية عبر شبكة الاتصالات :

لعل من أهم العوامل التي تعزز وتدعم بناء مجتمع المعلومات وتنمي التجارة الالكترونية هو توفير الأمن والثقة لدى المتعاملين من خلال وجود بيئة آمنة يعمل فيها البائعون والمشترون والفنيون وكل من لهم صلة بذلك.

ولقد أبدى الكثيرون – دولا وأفرادا- مخاوفهم من عدم تمكنهم من الحفاظ على سرية Privacy المعلومات والبيانات التي يجري تدولها على الشبكات الالكترونية ، كما كشف عن ذلك بعض التقارير الصادرة عن الحكومة الالكترونية في 1975 بإنجلترا ، حيث أبدت تلك التقارير المخاوف من استخدام الحاسب في تيسير ونقل وتخزين المعلومات والحصول عليها من أي مكان من العالم ونقلها من نظام لآخر . كما كشفت دراسة أجرتها صحيفة Wall Street Journal.January 2000 ، أنه في الوقت الذي عبر فيه 60% من الأمريكان عن سعادتهم في التعامل مع الحكومة الالكترونية ، عبر حوالي 50 % عن مخاوفهم من انتهاك السرية الخاصة بهم .

والواقع أن توفير البيئة الآمنة يعد مطلبا حيويا ، ليس فقط لتأمين التجارة الالكترونية وتطورها بصفة عامة ، بل لما يمارسه من تأثير خطير على نقل البيانات والمعلومات إلى الدول النامية بالذات ، والتي ستكون شديدة التأثير بما تتخذه الدول الأخرى من إجراءات ضدها في هذا المجال ، إن لم تعمل على توفير حماية متكافئة Equivalent Protection .لذا فإن عدم توفير الحماية يمكن أن يشكل عقبة كأداء ضد التدفقات التجارية باستخدام هذه الوسيلة .

و يتألف موقع الويب ونظام الانترنت من وجهة نظر التهديدات المحتملة التي يمكن أن تواجهها إلى ثلاث مكونات ، كل منها يمكن أن يتعرض للتهديد وهي : الأجهزة ، والبرامج وملفات البيانات .وتختلف مصادر التهديد تبعا للقائمين بها وطرقهم المختلفة في الوصول إلى تنفيذ هذه التهديدات.[9] ومن أهم هذه التهديدات الأمنية ما يلي:

1- **البرمجيات الخبيثة Malicious code**:
ومن أشهرها **الفيروسات،** وهي برامج لها القدرة على أن تنسخ وتنشر نفسها إلى ملفات أخرى، و**الديدان** شكل آخر لهذه البرمجيات، ولها القدرة على الانتقال من جهاز إلى آخر عبر الشبكة، ومن الأنواع الخطيرة أيضاً **أحصنة طروادة** Trojan horses التي تظهر للمستخدم كأنها ملفات

---

[8] مصطفى سمارة**"أمن التجارة الإلكترونية"** مجلة المعلوماتية، مجلة فصلية تصدر عن مركز المصادر التربوية بإدارة مراكز مصادر التعلم والمكتبات المدرسية ، المملكة العربية السعودية ،العدد17، تموز ،2007.موجودة على الموقع،
http://infomag.news.sy/index.php?inc=issues/showarticle&issuenb=17&id=364

[9] عبد الحميد بسيوني **"أساسيات ومبادئ التجارة الالكترونية"** المرجع السابق، ص 54.

مفيدة (تعليمية مثلاً) لكنها تقوم بأفعال شريرة عند تشغيلها. ومن البرامج الشريرة أيضاً ما هو خاص بالأجهزة المحمولة و تكون مكتوبة بلغة البرمجة جافا وتُحمل إلى الزبون عند دخوله موقع الويب.

2- **القرصنة hacking**:

يمكن هنا أن نعرف مفهومين هامين في هذا المجال وهما **القرصان** hacker أي الشخص الذي يحاول الوصول غير المشروع إلى أنظمة الحاسوب، والمفهوم الثاني هو المخرب cracker أي الشخص الذي يستفيد من المعلومات التي يقدمها القرصان للقيام بأفعال تخريبية عدائية.ونم أكثر أدوات القرصنة المستعملة من قبل الهاكرز هي : **أحصنة طروادة**[10] أو() حيث يضع المخربون برنامجا مخبأ داخل البرامج العادية لمنشأة ما ، ويواصل الكومبيوتر عمله بصورة طبيعية في الوقت الذي يجمع فيه البرنامج المخبأ البيانات ويجري تعديلات سرية في البرنامج والملفات ويمحو أو يدمر البيانات أو حتى يسبب إغلاقا كاملا ، وأحصنة طروادة يمكن أن تبرمج لتدمير كل آثار وجودها بعد التنفيذ.

3- **تزوير أو سرقة بطاقات الاعتماد Credit card fraud/theft**:

يمكن للقراصنة الوصول إلى ملفات بطاقات الاعتماد ومعلومات الزبائن الأخرى المخزنة على مخدمات التاجر أو البائع ليجري فيما بعد استخدام هذه المعلومات المسروقة لإنشاء بطاقات اعتماد بهويات وهمية.

4- الخداع spoofing:

وذلك باستخدام عناوين بريد إلكتروني مزيفة أو انتحال شخصية شخص آخر.

5- **هجوم رفض الخدمة attack Denial of service**: يقوم المهاجمون بإغراق الموقع بالطلبات غير المفيدة، من ثَم يتوقف الموقع عن الخدمة وتصبح الشبكة في حالة اختناق.

6- **هجوم رفض الخدمة الموزع attack Distributed Denial of service**: يستخدم المهاجمون عدداً هائلاً من الحواسيب للقيام بالهجوم على شبكة معينة.

7- **التجسس sniffing**: وذلك باستخدام برنامج للتجسس يراقب المعلومات المنتقلة عبر الشبكة،ثم سرقة المعلومات الهامة من أي مكان على الشبكة.

ولقد أعلنت شركة مكافي، مؤخرا، عن أخطر عشرة تهديدات تتوقع أن تتربص بأنظمة الكمبيوتر وتكنولوجيا المعلومات في عام2007، وذلك طبقا للدراسات التي أجرتها مختبرات "مكافي أفيرت".

وبحسب هذه الدراسات، ومع الأخذ بعين الاعتبار أن هنالك أكثر من 217 ألف نوع مختلف من التهديدات إلى جانب الآلاف غيرها من التهديدات غير المعروفة، فإن كل الدلائل تشير إلى أن أعداد البرمجيات الضارة التي يطلقها المجرمون المحترفون في ارتفاع متواصل. وأخطر عشرة تهديدات أمنية لعام 2007، وفق مختبرات "مكافي أفيرت" هي، دون ترتيب:

1- ارتفاع أعداد مواقع سرقة كلمات السر، مستخدمة صفحات تسجيل مزيفة لمواقع خدمات الإنترنت الشهيرة مثل eBay.

2- تواصل أحجام البريد الإلكتروني غير المرغوب فيه ارتفاعها المطرد خصوصا الرسائل التي تحتوي على صور.

3- استخدام الهاكرز hackers ، اعتمادا على تزايد انتشار وشعبية تداول ملفات الفيديو عبر الإنترنت، ملفات MPEG لنشر برامجهم الضارة.

4- تنامي ظاهرة مهاجمة الهواتف الجوالة، خصوصا مع ارتفاع مستويات "الذكاء" في أجهزة الهاتف وانتشار تقنيات الربط بينها.

5- ستصبح برامج الإعلانات ظاهرة شرعية في أعقاب الزيادة في البرامج التجارية غير

---

[10] طارق عبد العال حماد "**التجارة الإلكترونية – المفاهيم- الأبعاد – التحديات** " الدار الجامعية ، الإسكندرية ، مصر، 2002-2003، ص 161.

المرغوب فيها PUPs.
6- ستظل سرقة الهويات الشخصية وضياع البيانات مشكلة عامة، وهي الجرائم التي تعود جذورها عادة إلى سرقة أجهزة الكمبيوتر الشخصي، وضياع ملفات الحفظ الاحتياطي.
7- تزايد استخدام برامج bots، أو برامج الكمبيوتر التي تؤدي مهام تلقائية، فهي من الأدوات المفضلة لدى الهاكرز.
8- عودة البرامج الطفيلية الضارة مرة أخرى، أو الفيروسات التي تعبث بالملفات الموجودة على القرص الصلب.
9- تزايد أعداد الأدوات الخفية في أنظمة تشغيل 32 بت، ولكن في المقابل سيتم تعزيز إمكانات الحماية والعلاج منها.
10- ستظل الثغرات غير المحمية سببا رئيسا للقلق، خصوصا مع ظهور سوق سوداء تتاجر بها.
يقول جيف جرين نائب أول رئيس لمعامل "ماكافي أفيرت" وتنمية المنتجات "إن أجهزة الكمبيوتر أصبحت خلال فترة قصيرة من الزمن جزءا حيويا ومهما من الحياة اليومية. وهناك احتمالات كبيرة ليجني كُتّاب الفيروسات أموالا طائلة من وراء ذلك. ومع ما نراه من زيادة في الأساليب الفنية المعقدة، تزداد صعوبة قدرة المستخدم العادي على التعرف على الفيروسات أو تجنُّبها".

ويرى الباحثون في معامل "مكافي" أن هناك أدلة على ارتفاع الجرائم الاحترافية والمنظمة، ويرجع ذلك إلى تأليف الفيروسات، حيث تتلقفها فرق تطوير خبيثة وتستخدمها في إنشـــاء برامج حاقدة، وتختبرها، وتشغِّلها، وتصدرها. وستنتشر الأساليب المعقدة مثل تعدد الأشكـال، وعودة الفيروسات الطفيلية، والأدوات الخفية، والنظم الآلية، والأشكال الجديدة من التشفير المعقد. علاوة على ذلك، ستظهر التهديدات في شكل حزم أو مشفرة للتمويه وجذب الأنظـار بعيدا عن غرضها الأساسي الخبيث بشكل أسرع وأكثر تعقيدا.

8- الاحتيال المالي على الإنترنت:

الاحتيال المالي على الإنترنت أو الـ:Phishing كما يسمى هو طريقة يحاول من خلالها اللصوص السطو على هوية المستخدم وكلمة المرور الخاصة به عبر صفحات تسجيل مزيفة مع التركيز على مهاجمة الخدمات الشهيرة على الإنترنت مثل eBay. وكما ثبتت توقعـات معامل "مكافي أفيرت" بزيادة هجمات الاحتيال المالي على الإنترنت عقب إعصار كاتـرينا، فإن خبراء "مكافي" يتوقعون مزيدا من الهجمات التي تستفيد من رغبة الناس في مسـاعدة غيرهم من ذوي الحاجة. وعلى النقيض من ذلك، فمن المتوقع أن يقل عدد الهجمات علـى الشركات المزوِّدة بخدمات الإنترنت ISPs مع ثبات نسبة الهجمات التي تستهدف القطـاع المالي.[11]

9- البريد المتطفّل أو البريد الإغراقي أو العشوائي (Spam emails, Junk mail, or Bulk mail)

البريد الإلكتروني سبام هو بريد يرسل إلى صندوق بريدك من جهة لا تعرفها وبدون علاقة سابقة مع المرسل، وسبامر "spammer" إذا صح التعبير هو الشخص المسؤول عن هذه الرسائل ، ويتميز البريد السبام بأنه عادةَ يتم إخفاء عنوان بريده الإلكتروني أو تزوير بريده الإلكتروني ويدعي بأنه من أحد المؤسسات المعروفة والمرموقة،

---

[11] بدون صاحب المقال" **10 تهديدات أمنية تواجه أنظمة الكمبيوتر يتصدرها سرقة كلمة السر** "مقال صحيفة الاقتصادية الالكترونية - تقنية المعلومات –الرياض ، السعودية، الجمعة, 14 ذو القعدة 1428 هـ الموافق 2007/11/23 م - العدد 5156، موجود بموقع **/ http://aleqt.com/news.php?do=show&id=59736**

يُعتبر البريد السبام من المعوّقات المهمة لانسياب المعلومات في العالم؛ لأنه يعتبر، برأي خبراء المعلومات، طاعون العصر الرقمي في العالم وفيما يلي بعض الإحصائيات والآراء في هذا الصدد.

حيث ورد في تقرير الدكتور "روبرت هورتن" في مؤتمر القمة العالمية لمجتمع المعلومات بالاشتراك مع الإتحاد الدولي للاتصالات، الذي عُقد في جنيف في شهر أيلول عام 2003م، والذي كان يدور حول "التصدي لظاهرة بريد السبام"، حيث قال : لقد أضحى البريد غير المرغوب فيه أو التجاري أو السبام في سرعة نموه طاعون العالم الرقمي بحيث تتصاعد نسبة البريد الإلكتروني المتطفل في العالم مع بداية عام 2005 إلى 80% من البريد المتداول عبر العالم، كما إن إرسال المتطفلين مئات الملايين من الرسائل الإلكترونية يومياً يكبد الاقتصاد العالمي خسائر مقدّرة بحوالي **خمسة وعشرون مليار دولار سنويا** ومع ازدياد الاعتماد على خدمة الإنترنت والبريد الإلكتروني، سواء على الصعيد الشخصي أم على الصعيد العام، يُمثّل البريد المتطفل معوّق أساسي لتنمية مجتمع المعلومات .

ولقد أصبح بريد السبام من المشاريع المربحة للغاية، وذلك لأن كلفة إنشاء المشروع هي قليلة جداً نسبةً للأرباح التي قد تجنى، بحيث تبلغ كلفة البريد الإلكتروني الواحد لـ 0.0005 دولار أميركي في بلدان العالم المتقدمة: أي أنه لكل عشرة آلاف رسالة بريد الكتروني تكلف مرسلها حوالي الخمسة دولارات فقط [12]

10- تهديد الأجهزة المتنقلة:

ستشهد تكنولوجيات الاتصالات ارتفاع معدل التهديدات الموجهة ضد الأجهزة المتنقلة mobile devicesحيث أن استخدام تكنولوجيا الهاتف الذكي smart phone قد لعب دورا دوريا في انتقال التهديدات من الكمبيوترات الشخصية شبه الثابتة متعددة الوظائف إلى الأجهزة "القابلة للارتداء" بحجم الكف. ومع زيادة الاتصال عبر تكنولوجيات مثل البلوتوث، والرسائل القصيرة، والرسائل الفورية، والبريد الإلكتروني، والواي فاي، ومنافذ USB، والأجهزة السمعية "أوديو"، والفيديو، والويب، لتزيد من احتمالات انتقال الإصابة بين الأجهزة وبعضها البعض.

11- Adwareأو برامج الإعلانات المزعجة:

ستظل سرقة الهوية وفقدان البيانات قضيتين عامتين. وتشير لجنة التجارة الفدرالية الأمريكية إلى أن نحو عشرة ملايين أمريكي يقعون ضحايا لمزوري الهويات كل عام. وغالبا ما تشهد هذه الجرائم سرقة كمبيوتر، أو فقدان بيانات احتياطية، أو سرقة نظم معلومات. وبينما يتوقع خبراء "مكافي" أن يظل عدد الضحايا مستقرا على نحو نسبي، فإن كشف الشركات عن بيانات مفقودة أو مسروقة، وزيادة حوادث السرقة على الإنترنت، والنصب على شركات البيع القطاعي وأجهزة الصراف الآلي، وتقارير الإبلاغ عن سرقة أجهزة كمبيوتر محمولة تحتوي على بيانات سرية. كل هذه الأسباب ستستمر في طرح الموضوع كقضية عامة.

12- البوتس" boots أو البرامج ذات المهام التلقائية:

وهي برامج كمبيوتر تؤدي مهاما تلقائية وهذا النوع من المهام يُؤدى في البيت، وتقدمه مواقع ويب ذات مظهر احترافي كبير، عبر إعلانات مصنّفة، بل وعبر الرسائل الفورية. وهذا جزء

---

[12] سمير يحي عمري" **معوّقات انسياب المعلومات الإلكترونية في العالم العربي** " ،بحث مقدم لفعاليات المؤتمر السادس عشر للاتحاد العربي للمكتبات والمعلومات، الجزائر، 19 - 21 مارس 2006.

مهم من السبب وراء القدرة على إمكانية تشغيل العديد من البوتس من جميع أرجاء العـالم. ولكي يقوم اللصوص بالحصول على بضاعة (غالبا من أجل إعادة بيعها)، أو الدفع ببطاقـة اعتماد مسروقة، يجب عليهم المرور بلوائح صارمة إذا كانت البضاعة في طريقها إلـى بلد آخر. وللتحايل على هذه اللوائح، فإنهم يقومون باستخدام الأشخاص المزيفين فـي بلـدان المنشأ[13]

ـ ويلاحظ أن ما سبق ذكره من جرائم وتهديدات لا يمثل كل الجرائم المحتملـة بل يوجد غيرها كثير ، وأيا كان الأمر يجب التعامل مع هذه الجرائم وغيرها بما يؤمن التجارة الإلكترونيـة ويكفل نموها وتطورها على شبكة الانترنت .

خامسا : بعض الحلول التقنية للوقاية من خطر التهديدات الالكترونية:

1. تشفير البيانات:

التشفير(Encryption) هو عملية تحويل المعلومات إلـى رمـوز. بحيث تصبح محميـة من عمليات الوصول غير المرخص بها باستخدام برنامج مفتاح تشفير قبل إرسال الرسالة ، وتكون لـدى المسـتقبل قـدرة اسـتعادة الرسـالة الأصـلية بعمليـة عكسـية لفـك التشـفير (Decryption)14. والهدف هو جعل المعطيات المخزنـة والمعطيات التـي يجـري نقلهـا علـى الإنترنـت آمنـة. ثـم إن عمليـة التشـفير تُحقـق تكامليـة الرسـالة (message integrity) وتُحقـق عـدم النكـران (no repudiation) والتوثق (authentication) والسرية (confidentiality). ومن أنواع التشفير:

التشفير المتناظر Symmetric Key Encryption:

يمكن أن نسمي هذا التشفير أيضاً "التشفير بالمفتاح السري" وفي هذا التشفير يمتلك المرسل والمستقبل نفس المفتاح لتشفير وفك تشفير الرسالة، وهذا يتطلب مجموعة مفاتيح جديدة في كل مرة.

التشفير غير المتناظر Key Encryption Public:

ويسمي أيضاً "التشفير بالمفتاح العام" ويحل هذا النوع من التشفير مشاكل التشفير السابق المتمثلة في ضرورة تبادل المفتاح السري بطريقة آمنة بين الطرفين. أما في هذا النوع من التشفير فيستخدم المرسل المفتاح العام(يكون متاحاً للجميع) للمستقبل لتشفير الرسالة وعندما تصل الرسالة للمستقبل يستخدم مفتاحه الخاص(لا يعرفه أحد سواه) ليفك تشفير الرسالة، وهذا يعني أنه لن يستطيع أحد القيام بفك التشفير سواه.

التشفير بالمفتاح العام مع استخدام التوقيع الإلكتروني وعملية تهشير الرسالة:

يقوم المرسل في البداية بتهشير الرسالة باستخدام تابع تهشير وبعد ذلك يشفر الرسالة بالمفتاح العام الخاص بالمستقبل، ثم يشفرها بالمفتاح الخاص به(توقيع إلكتروني) وعندما تصل الرسالة للمستقبل يفك تشفيرها بالمفتاح العام للمرسل وبذلك يتوثق المستقبل من المرسل، ويضمن عدم نكرانه من أنه بعث الرسالة وذلك لأنها موقعة رقمياً منه(أي لأنها مشفرة بالمفتاح الخاص بالمرسل) ثم يفك المستقبل التشفير الثاني للرسالة باستخدام مفتاحه الخاص، ثم يستخدم نفس تابع التهشير ليستعيد الرسالة الأصلية .إن عملية التهشير تفيد المستقبل في التحقق أن الرسالة لم تُعدَّل على الطريق.

2. قناة الاتصال الآمنة(SSL, S-HTTP, VPNs):

Secure Sockets Layer (SSL):

تعتمد هذه التقنية على تأسيس جلسة اتصال آمنة يجري التفاوض عليها بين المرسل والمستقبل (جلسة اتصال آمنة بين الزبون والمخدم وتكون كل الطلبات والإجابات بينهما مشفرة)

---

[13] بدون صاحب المقال" **10 تهديدات أمنية تواجه أنظمة الكمبيوتر يتصدرها سرقة كلمة السر** "مقال صحيفة الاقتصادية الالكترونية ـ تقنية المعلومات ـالرياض ، السعودية، الجمعة, 14 ذو القعدة 1428 هـ الموافق 2007/11/23 م - العدد 5156، موجود بموقع **/ http://aleqt.com/news.php?do=show&id=59736**

[14] عبد الحميد بسيوني"**أساسيات التجارة الالكترونية**" المرجع السابق، ص 55.

نظام الاتصال **S-HTTP** :وهي تقنية بديلة مصممة للعمل مع البروتوكول HTTP تتيح طريقة آمنة للاتصال وتبادل الرسائل.

Virtual Private Networks (VPNs): وهي تقنية تسمح للمستخدمين الذين يعملون عن بعد بالوصول وصولاً آمناً إلى الشبكة الداخلية للشركة، مثلاً عن طريق الإنترنت باستخدام بروتوكولات خاصة لإنشاء قناة آمنة من نوع نقطة لنقطة point-to-point كالبروتوكول PPTP(Point-to-Point Tunneling Protocol).

3- Protecting networks (firewalls): وهو تطبيق برمجي يعمل مرشحاً بين الشبكة الخاصة بالشركة وبين الإنترنت، لذا لا ينتقل من شبكة الشركة و إليها إلا ما هو مسموح له بالمرور.

4- Proxy Servers: وهو تطبيق برمجي يعالج كل الاتصالات الخارجة من الشبكة الداخلية للشركة والمرسلة إلى الإنترنت، فهو يتصرف كمتكلم عن الشبكة الداخلية غير المرئية للإنترنت.[15]

5- نظام المعاملات الإلكترونية الآمنة Secure Electronic Transaction(SET):

تم تطوير هذا النظام بالتعاون بين شركات (فيزا وماستر كارد) بغرض تأمين المعاملات المالية على شبكة الإنترنت باستخدام بطاقات الائتمان ، حيث يوفر هذا النظام درجة تشفير عالية ونتيجة استخدام النظام لطبقات متعددة من التشفير من مستوى الشبكة إلى مستوى موقع ويب يصعب فك شفرته إلا بصعوبة شديدة لأجهزة عالية التقنية ، ويحقق نظام المعاملات الإلكترونية الآمنة SET ضمانات أساسية منها :

التكاملية Integrity : بضمان أن الرسالة المرسلة هي التي يتم استقبالها بإرسال توقيع رقمي في اتجاه واحد يتم فكها للتأكد من أن الرسالة المرسلة هي المستقبلة.

السرية Confidentiality : بتشفير محتويات الرسالة والمعلومات المالية .

الموثوقية Authentication : بالتحقق من شخصية حامل بطاقة الائتمان، والتي تضمن للبائع شخصية المشتري دون أن يعرف البائع رقم ائتمان المشتري ، والتحقق من شخصية البائع وقبوله العمل بنظام المعاملات الإلكترونية الآمنة SET[16]

سادسا: الجهود الدولية والإقليمية والوطنية لأمن المعاملات التجارية الإلكترونية:

تبذل عديد الجهود على المستوى الإقليمي والدولي لحماية وأمن المعاملات الإلكترونية حيث سعى كل من مجلس أورب ومنظمة التعاون الاقتصادي والتنمية OCED لوضع بعض المبادئ الدولية لحماية البيانات في الثمانينات من القرن العشرين وتبعتها في ذلك الأمم المتحدة في عام 1990 بوضع بعض الإرشادات لتنظيم ملفات البيانات الشخصية بالحاسب الآلي والتي تعرف بمبادئ حسن السلوك أو السير الحسن فيما يتعلق بالمعلومات وتتمثل هذه المبادئ التي يمكن أن تتضمنها التشريعات والقواعد الدولية بإيجاز فيما يلي :

1- جمع البيانات الشخصية يجب أن يكون الحصول عليه قانونيا وعلى نحو يتسم بالعدالة بإعلام الشخص بذلك.
2- يجب الحصول على البيانات اللازمة لتحقيق الغرض القانوني الذي جمعت من أجله فقط وعدم جمع معلومات لا حاجة لها.
3- يجب أن تكون البيانات التي تم جمعها دقيقة ، وتتم مراجعتها بصفة دورية للتأكد من أنها ظلت دقيقة وحديثة حتى تاريخ الاستفادة منها .
4- يجب أن يقترن جمع البيانات بتوفير الشفافية من خلال إعلام الأشخاص بالأغراض التي ستستخدمها.

---

[15] مصطفى سمارة، المرجع السابق ،
[16] عبد الحميد بسيوني ، المرجع السابق ، ص 64.

5- من حق الأشخاص أن يستفسروا ويسألوا عما إذا كانت بياناتهم الشخصية قد استخدمت كما أن لهم الحق في الحصول على نسخة منها ، ولهم الحق في تصحيح البيانات غير الدقيقة أو غير الصحيحة.وكذا الاعتراض عن استخدام بياناتهم إذا لوحظ أن ثمة أغراض أخرى لاستخدامها كاستخدامها مثلا في عملية التسويق.

6- تنص المبادئ كذلك على ضرورة توفر إجراءات مناسبة في التشريعات الوطنية ضد أي مخاطر تنشأ من جمع المعلومات الشخصية سواء أكانت المخاطر تنشأ من فقدانها ، أم من تعرضها للدمار أم من الإفصاح أم من التدخل العمدي واتخاذ إجراءات لتنظيم ذلك كتدريب العمال أو فحص الأجهزة ، أو اتخاذ إجراءات تكنولوجية مثل التشفير أو وضع ضوابط للدخول إلى الشبكة.

7- يجب توافر نظام يمكن من خلاله تقديم شكوى ضد انتهاك المبادئ السابقة أثناء التعامل مع معالجة البيانات الشخصية، وكذا توفير إطار إجرائي يضمن التوافق مع مثل هذه القواعد.[17]

هذا وتسهر بعض المنظمات العالمية على مراقبة نشاطات التجارة الإلكترونية مثل المنظمة العالمية للملكية الفكرية الويبو(WIPO) القائمة على حماية الملكية الفكرية في جميع أنحاء العالم ، باحتفاظها على مكانة الصدارة في تقديمها لخدمات تسوية منازعات أسماء الحقول على الانترنت من خلال "مركز الويبو للتحكيم والوساطة " كما تسعى إلى حماية التجارة الإلكترونية عبر تأسيس تدابير من شأنها أن توفر إطار قانوني موحد ، واضح ومعروف من طرف المنتفعين بالعلامات التجارية والوصول إلى توصيات من شأنها هي الأخرى جعل كل الحقوق في الإشارات المميزة ذات طابع إقليمي وخاصة العلامات التجارية والأسماء التجارية والبيانات الجغرافية لمساعدة المحاكم الوطنية والسلطات المختصة في تطبيق القوانين الخاصة بهذا الشأن.

كما تقوم الشبكة العالمية لمراقبة العمليات التجارية ♦RICC بمراقبة العمليات التجارية من خلال تغطية نقص الحماية المفروض على البيانات الشخصية بإجرائها لحملات الكترونية هدفها القضاء على نظم البيع الالكتروني الغير مشروعة والتي تبحث على الانتعاش والربح السريع ، حيث كشفت في حملتها الصحية الالكترونية سنة 1997عن وجود 1100 موقع الكتروني تشكل خطر في منظور التمثيل والتي تلقت كلها إخطارات وإنذارات عبر رسائل الكترونية بتصحيح وضعيتها القانونية لكن بعد مرور حوالي شهر ، قامت 28 % من المواقع المستهدفة بتعديل وضعيتها ، أو انسحبت تماما.[18]

هذا وتسعى جهود لجنة الأمم المتحدة –اليونسترال (UNICITRAL)♦♦ إلى إيجاد توازن بين التجارة التقليدية والتجارة الالكترونية وتحديدا فيما يتعلق بأنشطة التحويل النقدي عبر الشبكات والتعاقد باستخدام وسائل التقنية ، ويعالج القانون موضوع العقود وإبرامها ومسائل التواقيع الالكترونية ومعايير الأمن والحماية اللازمة للبيانات الشخصية وغيرها من الموضوعات.[19]

---

[17] السيد أحمد عبد الخالق**"التجارة الإلكترونية والعولمة"** المرجع السابق ، ص 100

♦ أنشأت الشبكة سنة 1991 بمناسبة انعقاد مؤتمر اجتمع فيه ممثلي كل من : المنظومة الأوربية لحماية المستهلك ، الدول الأعضاء داخل الجمعية الأوربية للتبادل الحر بمدين كوبنهاجن ، تضم الشبكة 29 دولة من أورب وآسيا وأمريكا وأعضاء من منظمة OCED

[18] شافع بلعيد عاشور **"العولمة التجارية والقانونية للتجارة الالكترونية"** دار هومة للطباعة والنشر والتوزيع ، الجزائر 2006 ، ص 104

♦♦ **لجنة اليونسترال**: لجنة قانون التجارة الدولية التابعة للأمم المتحدة ،تضم في عضويتها غالبية دول العالم الممثلة لمختلف النظم القانونية الرئيسة ، وغرضها الرئيس تحقيق الانسجام بين القواعد القانونية الناظمة للتجارة الالكترونية وتحقيق وحدة القواعد المتبعة وطنيا في التعامل مع مسائل التجارة العالمية.

19 مركز التعليم المفتوح في تعليم الحاسوب**"التجارة الإلكترونية ، الاتجاهات الدولية والإقليمية والوطنية"** موجودة بموقع http://www.opendirectorysite.info/e-commerce/03.htm

نوفمبر 2007.

وعلى الصعيد الوطني فقد كانت الولاية الألمانية Hesse أول من أصدر قانونا موجها بشكل مباشر لحماية البيانات الشخصية في 1970، ثم تلتها بعد ذلك القوانين من السويد والولايات المتحدة ، وتوالت القوانين من معظم الدول الأوربية المتقدمة خلال عقد السبعينات . لكن المشكلة تمثلت في أن التباين بين هذه التشريعات كان يمثل تهديدا يعوق حرية تدفق البيانات بين الدول ، لذا تدخلت كل من الـ OCED والمجلس الأوربي لوضع مبادئ مشتركة تتبعها الدول المتخلفة وتمثل الأساس للتشريعات الوطنية ثم جاءت المم المتحدة- من خلال الجمعية العامة – لوضع بعض المبادئ التي تمثل الحد الأدنى الواجب مراعاته في البيانات الشخصية.

خاتمة :

يتزايد يوماً بعد يوم عدد التجار الذين يعربون عن تفاؤلهم بالفوائد المرجوة من التجارة الإلكترونية، إذ ستسمح هذه التجارة الجديدة للشركات الصغيرة بمنافسةَ الشركات الكبيرة. ولعل هذا التفاؤل سيحدث العديد من التقنيات لتذليل العقبات التي يواجها الزبائن، ولا سيما على صعيد سرية وأمن المعاملات المالية على الإنترنت، ولا يتأتى هذا إلا من خلال

- القيام بعملية تقدير للمخاطر risks وهي عملية هامة جداً ولابد من مراعاتها منذ البداية.
- وضع وتطوير سياسة أمنية وهي مجموعة من الإجراءات التي تهدف إلى الاستفادة من المعلومات المتوفرة عن المخاطر، بغية ترتيبها حسب أهميتها، ومن ثم تحديد المخاطر المقبولة كهدف وتحديد آليات لتحقيق الأهداف.
- تطوير خطة تنفيذية، من خلال مجموعة من الأفعال المطلوبة لتحقيق أهداف الخطة الأمنية.
- إنشاء منظومة أمنية مسئولة عن الأمن وتثقيف وتدريب العاملين، وإبقاء الإدارة مدركة للقضايا الأمنية وعمليات التحكم بالوصول والإجراءات المتبعة للتوثق.
- القيام بعملية مراقبة وتدقيق أمني، قَصْدَ مراجعة العمليات والإجراءات الأمنية. كما يمكن للتعاون الدولي أن يلعب دورا مهما في تهيئة البيئة الأمنية الداعمة لبناء مجتمع المعلومات في الدول النامية ، من خلال المساعدة في بناء استراتيجيات إلكترونية ، والتعاون في مجال المعاملات الإلكترونية في جميع مراحلها . وخلاصة الأمر أن التجارة الإلكترونية قد أصبحت حقيقة قائمة، وأن آفاقها وإمكاناتها لا تقف عند حد وبالرغم من أن 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.

قائمة المراجع:

01/ السيد أحمد عبد الخالق**"التجارة الإلكترونية والعولمة"** بحوث ودراسات ، المنظمة العربية للتنمية الإدارية ، مصر ، 2006،.

02/ طارق عبد العال حماد "**التجارة الإلكترونية – المفاهيم- الأبعاد – التحديات** " الدار الجامعية ، الإسكندرية ، مصر، 2002-2003،
03/ زايري بلقاسم، طوباش علي، "**طبيعة التجارة الإلكترونية وتطبيقاتها المتعددة**" مجلة المستقبل العربي ، عدد ماي 2003،.

04/ سعد غالب ياسين، بشير عباس العملاق "**الأعمال الإلكترونية** " دار المناهج للنشر والتوزيع، عمان، الأردن 2006،.
05/ عبد الحميد بسيوني" **أساسيات ومبادئ التجارة الإلكترونية** " دار الكتب العلمية للنشر والتوزيع، القاهرة ، مصر ،2003،.
06/ شافع بلعيد عاشور "**العولمة التجارية والقانونية للتجارة الالكترونية**" دار هومة للطباعة والنشر والتوزيع ، الجزائر 2006 ، .
07/ سمير يحي عمري" **معوّقات انسياب المعلومات الإلكترونية في العالم العربي** " ،بحث مقدم لفعاليات المؤتمر السادس عشر للاتحاد العربي للمكتبات والمعلومات، الجزائر، 19 - 21 مارس 2006.

08/ عماد أبو الرب - ليلى رشيد حسن" **إطار نموذج لتقويم جودة المواقع الإلكترونية**" موجود بموقع http://www.arabcin.net/arabiaall/4-2006/5.html أكتوبر 2007

09/ حازم سكيك "**التجارة الإلكترونية**" مجلة فيزياء بلا حدود، موجودة بموقع ، http://hazemsakeek.com/magazine/index.php?option=com_content&task=view&id=37&Itemid=53 نوفمبر 2007.

11/ باسم عبد الهادي حسن " **المزايا الاقتصادية التي تقدمها التجارة الالكترونية** " جريدة الصباح ، صادرة عن مركز الإعلام العراقي ، موجودة بموقع : http://www.alsabaah.com/paper.php?source=akbar&mlf=interpage&sid=41375 نوفمبر 2007.

12/ مصطفى سمارة"**أمن التجارة الإلكترونية**" مجلة المعلوماتية، مجلة فصلية تصدر عن مركز المصادر التربوية بإدارة مراكز مصادر التعلم والمكتبات المدرسية ، المملكة العربية السعودية ،العدد17، تموز ،2007.موجودة على الموقع، http://infomag.news.sy/index.php?inc=issues/showarticle&issuenb=17&id=364
13/ بدون صاحب المقال" **10 تهديدات أمنية تواجه أنظمة الكمبيوتر يتصدرها سرقة كلمة السر** "مقال صحيفة الاقتصادية الالكترونية - تقنية المعلومات –الرياض ، السعودية، الجمعة, 14 ذو القعدة 1428 هـ الموافق 2007/11/23 م - العدد 5156، موجود بموقع / http://aleqt.com/news.php?do=show&id=59736
15/ مركز التعليم المفتوح في تعليم الحاسوب"**التجارة الإلكترونية ، الاتجاهات الدولية والإقليمية والوطنية**" موجودة بموقع http://www.opendirectorysite.info/e-commerce/03.htm نوفمبر 2007