

المستهلك الإلكتروني بين الأخطار الأمنية ومتطلبات الحماية

The electronic consumer between security risks and protection requirements

طويطو محمد¹، حفصي هدى²¹ جامعة الجزائر 3، الجزائر، touitoutou@yahoo.fr² جامعة الجزائر 3، الجزائر، mkg.hafsi@yahoo.fr

تاريخ النشر: 2019-12-23

تاريخ القبول: 2019-09-29

تاريخ الاستلام: 2019-01-11

ملخص:

يقوم المستهلكون في الوقت الحاضر باستخدام التكنولوجيا بشكل كبير في حياتهم اليومية، لأنها تساعدهم على جعل الحياة سهلة وتساعد أيضاً لهم توفير الوقت والجهد وحتى المال.

فالتسوق عبر الإنترنت أصبحت واحدة من أهم الأنشطة التي يقوم فيها المستهلكون يومياً للاطلاع على السلع أو الخدمات المتاحة التي تقدمها المؤسسات المحلية والعالمية، ولكن هناك مخاطر كثيرة مرتبطة بالتسوق الإلكتروني، خاصة من جهة المستهلك أهمها على الإطلاق انتهاك الخصوصية والاطلاع على المعلومات الشخصية.

لذلك سوف نحاول من خلال هذه الورقة البحثية استعراض مفهوم التسوق الإلكتروني ومزاياه بالنسبة والمستهلك، كذلك مصادر وأبعاد الأخطار التي يتعرض لها المستهلك الإلكتروني، مفهوم الجريمة المعلوماتية وأمن المعلومات، وأخيراً الإجراءات الأمنية لحماية التعاملات التسويقية الإلكترونية.

كلمات مفتاحية: التسوق الإلكتروني، المستهلك الإلكتروني، أمن المعلومات، الحماية.

تصنيف M31، L86، L81، D18:JEL

Abstract:

Consumers are currently using technology significantly in their daily lives, because it helps them make life easy and also help them save time, effort and even money.

Online shopping has become one of the most important activities in which consumers daily to see the available goods or services provided by local and international institutions, but there are many risks associated with electronic shopping, especially from the consumer, including the most important violation of privacy and access to personal information.

So we will try through this paper to review the concept of electronic shopping and benefits for the consumer, as well as sources and dimensions of the risks to consumer electronic, the concept of cyber-crime and information security, and finally security measures to protect the marketing of electronic transactions.

Keywords: Online Shopping, Consumer Electronics, Information Security, Protection.

JEL Classification: D18, L81, L86, M31

1. مقدمة :

لقد أضحت الشبكات الإلكترونية من الضرورىات الحاصلة في عصرنا الحديث، بحيث أصبح لا غنى عنها في المؤسسات الحكومية والبلديات والبيوت، فحيثما أنتج منتج من حولك أنواع عديدة من شبكات الحواسيب التي تنقل كمهاً ثلاً من المعلومات والبيانات بيننا لأنشء خاصو المؤسسات على مستوى العالم، وتنوع هذا المعلومات والبيانات أهمية ودرجة سريتها من المعلومات العامة والعلمية العادية إلى المعلومات الحساسة وميزانها بالدول المعلومات لا استخباراتية بالغة الخطورة والسرية، وكل هذا لا نواعنا المعلومات والبيانات إنما تتمتع اقلها وحفظها في الغالب إلا حيان عبر شبكات الحاسوب على اختلاف أنواعها وأماكنها.

ومن

هنا تأتي أهمية هذا الشبكات في العالم المعاصر والتعاملات اليومية بين البشر بشكل عام، ومن هذا الأهمية تنبع خطورة ما يمثلها من هذا الشبكات وأمن المعلومات التي تتمتع ولها عبر خطوطها، فعلاً الرغم من أن تكنولوجيا الاتصال بالمعلومات تقدم الكثير من الفرص لمؤسسات الأعمال وللمستهلكين، مثل التجارة والتسويق الإلكترونيين، وكذا التسوق أو الشراء الإلكتروني، حيث أصبح هذا الأخير من أنجح استخدامات الشبكة للمؤسسات والمستهلكين على سواء، وذلك كما يفرهنا الوقت والجهد، فبدلاً من السفر لشراء احتياجات معينة من أحد البلاد، أصبح في مقدور مستخدم شبكة الإنترنت اختيار ما يشاء من هذه البضائع والأشياء التي يبحث عنها في دقائق معدودة وطلبها للتصلياً إليها فلو قوتو بأسهل طريقة، حيث أصبحت أعداد الشراء المنتجات المختلفة عبر الإنترنت من أكثر عادات مستخدمي الشبكة.

إلأن هذه الشبكة بالمقابل تعرض المعلومات الخاصة بهذه المؤسسات وهؤلاء المستهلكين لخطر كبير. ومعاًن هذه التكنولوجيا قو فربوبة عبور المجال الواسع جداً من المعلومات، إلا أنها أيضاً توفر بوابة لبرامج العبث التي تمت تطويرها من قبل أفراد مخربين بهدف سرقة وتخريب هذه المعلومات وإفسادها، وسوف تتفاقم هذا الأضرار مع تسارع التقدم في مجال الاتصال بالحواسبات، وما ينتج عن ذلك من زيادة حجم المعلومات المنقولة على شبكة الاتصال بالمعلومات المخزونة في الحاسبات، وما هذا إلا أحد الأضرار التي تعانيها العالم بأسره عند استحداث تقنيات جديدة، وكما هو في كثير من التقنيات الجديدة تولد معها محاسنها ومساوئها، ويتركز في أناسا تغليب جانب على ولذلك تطور الوسائل والتقنيات التي تتماشى مع تطور المخاطر، والتي تحفظ وتحمي أمن وسلامة المعلومات. وعليهذا، يمكن طرح الإشكالية التالية:

" فيما تتمثل التحديات والمخاطر الأمنية للتسوق الإلكتروني؟ وما هي آليات معالجتها؟ "

وفيسبباً لجلاء الغموض عن عناصر هذا الموضوع وإبراز أهم مسائله، تم تقسيم هذا العمل إلى المحاور التالية:

➤ ماهية التسوق الإلكتروني؛

➤ مصادر مخاطر التسوق الإلكتروني من وجهة نظر المستهلك؛

➤ الإنترنت والجريمة المعلوماتية؛

➤ الإجراءات الأمنية لحماية التعاملات التسويقية الإلكترونية.

2 - ماهية التسوق الإلكتروني:

يعتبر التسوق الإلكتروني نقلة حضارية مفاجئة للكثيرين حيث أصبح أكثر الدول تقدماً في التكنولوجيا، فلا شك أن التسوق الإلكتروني أصبح من أبرز المنافع التي تقدمها شبكة الإنترنت للمستخدمين، ويزداد الأفراد إقبالاً على التسوق عبر الإنترنت في جميع أرجاء العالم، ولا عجب في ذلك، فالتسوق عبر الإنترنت يجمع بين سهولة العثور على المستهلكين والعديد من المنتجات، إضافة إلى المعلومات التفصيلية عن تلك المنتجات وتعدد الخيارات، ناهيك عن الراحة في شراء ما يحتاجه من أي مكان وفي أي زمان.

2-1 تعريف التسوق الإلكتروني:

أجمع العديد من الباحثين على أن التسوق الإلكتروني يستخدم مجازاً للإشارة إلى العمليات التجارية الإلكترونية التي تتم بين مؤسسات الأعمال والمستهلكين، حيث تُوفّر للمستهلك المعلومات والخدمات التي تتيح له القدرة المناسبة للمعرفة، والتي تمكنه من اتخاذ قرار الشراء الصحيح، وبذلك يمكن تعريف التسوق عبر الإنترنت بأنه: "شكل من أشكال التبادل التجاري الذي يتم بين المؤسسات والمستهلكين، وذلك من خلال وسائل إلكترونية" (النونو، 2007، ص 42).

كما يعرف التسوق الإلكتروني بأنه: "تسوق في شكل افتراضي، حيث يتم عرض السلعة افتراضياً على المستهلك، أي أن شكل السوق هو شكل شبكي" (فقيه، 2013، ص 51).

من خلال السابق، يمكننا القول أن التسوق عبر الإنترنت أو التسوق الإلكتروني هو مجموعة الجهود التي يبذلها المستهلك عبر الإنترنت للبحث عن منتجات محددة، والمفاضلة بينها وبين المنتجات المعروضة للبيع في المتاجر الإلكترونية المختلفة المنتشرة في فضاء الإنترنت.

2-2 أساليب تطبيق التسوق الإلكتروني:

تتم عملية التسوق الإلكتروني من خلال أسلوبين أساسيين، وهما (فقيه، 2013، ص 52):

① التسوق الإلكتروني المتزامن: ويكون هذا عن طريق جمع المعلومات عن السلعة والخدمة التي يتم القيام بالشراء والدفع عن طريق الإنترنت؛

② التسوق الإلكتروني غير المتزامن: ويكون عن طريق جمع معلومات مختلفة عن السلعة عبر الإنترنت ثم القيام بعملية الشراء من أياً كان آخر للتسوق التقليدي، مثلاً المحلات التجارية أو السوبر ماركت وغيرها.

2-3 مزايا خادما التسوق الإلكتروني:

يوفر التسوق الإلكتروني العديد من المزايا للعملاء والمستهلكين، ويمكن إبراز أهمها فيما يلي (إبراهيم، 2008، صص 324-326؛ أحمد، 2009، صص 132-133؛ أبو قحف وآخرون، 2006، ص 427؛ عبد المجيد، 1998، ص 236؛ مرزق لال، 2010، ص ص 34-35):

■ معرفة كافة التفاصيل حول المنتجات، هي من المزايا الرئيسية للتسوق عبر الإنترنت، إذ من الممكن مشاهدة المعلومات التفصيلية والكاملة عن المنتجات المعروضة للبيع في المواقع الإلكترونية، ويساهم ذلك في مساعدة المستهلك على اختيار المنتج المناسب له؛

- التعرف علماء آراء الآخرين، من الفوائد المهمة للتسوق عبر الإنترنت؛ إذ يساهم في مساعدة الزبائن في اختيار المنتجات التي يفكرون بشراؤها، من خلال التعرف على آراء غيرهم حولها، وتقييم أهميتها، ويساعد ذلك الزبائن في معرفة تفاصيل أكثر حول طبيعة المنتجات؛
- التحرر من قيود الوقت والمكان، فالإنترنت تعمل 24 ساعة / 24 ساعة، وعلمدار الأسبوع، والمستهلك يمكنها التسوق واختيار بين منتجات المنظمة العالمية المختلفة وهو جالس في بيته أو مكتبه، وينتج عند ذلك تقليل في الجهد المبذول لقبول المستهلكين أثناء عملية الشراء؛
- رخص أسعار المنتجات التي تتم تسويقها عبر شبكة الإنترنت مقارنة بالمنتجات الأخرى المباعة بالطرق التقليدية. فجارة التجزئة علم لا نترت عملت تخفيضات التكاليف الثابتة، والتكاليف الإدارية بنسبة تزيد عن 50% من خلال تقديم المنتجات على شبكة الإنترنت، مما ينعكس في النهاية في شكل تخفيضات لأسعار وتحقيق مزايا تنافسية؛
- يمنح الفرصة لإجراء مقارنات لأسعار المنتجات قبل شرائها بشكل أفضل وأسرع، حيث لا يذلل المستهلكون جهداً أو وقتاً كبيراً مقارنة بما كانوا يجدون عند التجار ولعبر المحلات التجارية لمقارنة الأسعار؛
- إمكانية أكبر للاستفادة من مساعدة ونصيحة الخبراء والمتخصصين؛
- يساعد التسوق عبر الإنترنت على التغلب على الحواجز الجغرافية، حيث يمكن للمستهلكين معرفة المتاح في الأسواق منسلع وخدمات تحت خارج حدود المدينة السكنية التي يقطنون بها، حيث يمكنهم معرفة ما هو متاح لهم مستواً بالسوق القومياً والسوق العالمية؛
- عدم وجود اتصال مباشر مع البائع، حيث يجد البعض أنفسهم مرتبكون ولا يملكون الحرية الكافية بسبب وجود البائع الذي يقدد وللبيع علماً هرقب غيرهم علم شراء أشياء ليسوا بحاجة إليها، أو أتحرية الاختيار تصبح مقيدة بسبب اقتراحات البائع وتشتويشها أفكار المشتري، لكن في التسوق الإلكتروني يصبح المستهلك أكثر حرية في الاختيار والتفكير كما يجب بين مختلف المتاجر والرفوف، وأخذ الوقت الكافي للمقارنة والاختيار، وبالتالي اتخاذ قرار الشراء دون أية ضغوط؛
- الاستمتاع وتقدير الذات، إذ يوجد من المستهلكين من أن التسوق الإلكتروني دلالة علم مستوى حضارياً واجتماعياً معين، مما يجعله لجاً إلى مثل هذه التعاملات متجانب ر جسيير يفهموعا منالا اختلافاً التميز علماً أفراد المجتمع آلاً آريناً والانتماء إلى فئة معينة، كما أن البعض آلاً آر يجب آلا ستمتعاً باستخدام التكنولوجيا الحديثة للاتصال في حياتهم اليومية لخلق جزء من آلا فتخارو الثقة في النفس تجاه قدراتهم استخدام مثل هذه التكنولوجيا؛
- التنوع، حيث يجد المستهلك الإلكتروني عدد أكبر من المنتجات التي يريد علم الشبكة العالمية، إذ تفتقر أكبر المساحات التجارية إلى مثل هذه الكم الهائل من التنوع؛

■ القدرة على المقايضة، فتحتمل إمكانية شراء مباشر للعديد من المواقف وخدمة تبادل المنتجات والتحفيز والرواد موقعها، كما توجد مواقع أخرى لتعبير المزاد العلني، حيث يزايد الأفراد على السلع المعروضة، مما يسهل على المستهلك الإلكتروني عملية إيجاد الصفقات المرغوبة.

3- مصادر المخاطر المدركة في التسوق الإلكتروني من وجهة نظر المستهلك:

تفيد العديد من الدراسات الميدانية بأن أهم العوائق التي يصادفها المستهلك عند التسوق الإلكتروني عبر الإنترنت هي تلك المتعلقة بمشاكل اللوجستية، مثل عدم الالتزام بمواعيد التسليم، عدم مطابقة المنتجات وإمكانية الإرجاع، وعدم توفره المنتجات وعدم احترام آجال التسليم... إلخ، تمثل هذه العوائق جزءاً من مخاطر الشراء عبر الإنترنت، وبالإضافة إلى الصعوبات المتعلقة بالبعد الجغرافي، مخاطر الدفع الإلكتروني، عدم احترام الحياة الشخصية للمستهلك وعدم توفر السرية (قيو، 2008، ص 48-49). لكن عموماً، تم تصنيف أربعة مخاطر أساسية مرتبطة بعملية التسوق والشراء الإلكتروني، هي*: الخطر المرتبط بالمنتج، المخاطر المرتبطة بالموقع، الخطر المرتبط بتنفيذ الصفقة عن بعد، خطر استخدام الإنترنت (قيو، 2008، ص 49).

ويكمن توضيح أبعاد هذه المخاطر من خلال الجدول التالي:

الجدول رقم (01): مصادر المخاطر المدركة في التسوق الإلكتروني من وجهة نظر المستهلك

مصدر الخطر	بعد الخطر	الوصف
المنتج	الخطر الوظيفي	عدم تطابق مواصفات المنتج مع توقعات المستهلك.
الشراء عن بعد	خطر الوقت	إحتمالية استغراق البحث للتسوق عبر الإنترنت وقتاً طويلاً يمثل خسارة من وجهة نظر المستهلك.
	خطر التسليم	عدم استلام المنتج في المواعيد المحددة.
	الخطر المالي	فقدان المال ودفع تكاليف إضافية خاصة بالتسليم.
استخدام الإنترنت	الخطر الاجتماعي	التخوف من عدم مقبول الآراء من الخدمة أو الانتقاد الموجه لهم من نتائج الحصول عليها.
	الحياة	عدم الكتمان عن هوية المشتري والتدخل في حياته الشخصية واستعمال معلوماته

*مع العلم أن هذه الدراسة سوف تركز بشكل خاص على الخطر الناجم عن استخدام الإنترنت أساساً.

	الشخصية	للتداول الثلاثى ولأغراض مغايرة.
	الدفع	الخطر الناجم عن الدفع الالكترونى من خلال الإداء بمعلومات خاصة ببطاقة الائتمان عبر الانترنت.
الموقع	المصدر	التخوف من عدم مصداقية وحقيقة صاحب المتجر الالكترونى

المصدر: قيو، 2008، ص 49.

4. الإنترنت والجريمة المعلوماتية؛

كان من نتائج التطور التكنولوجى، وجود ثمة علاقة ارتباط قوية بين استخدامات الحاسب الآلى وارتكاب بعض الجرائم المستحدثة. أيا استخدام الحاسب الآلى كأداة لارتكاب بعض الأفعال غير المشروعة، يطلق عليها اسم "الجريمة المعلوماتية". وتعرف هذه الأفعال الأخيرة علمياً بأنها: "كل فعل إجرامى يعتمد أياً كان اتصاله بالمعلوماتية، ينشأ عنه خسارة تلحق بالجنب عليه وكسب يحققه الفاعل" (العلبان، 2004، ص 44). كما تعرف بأنها: "أيعمل غير قانونى يستخدم فيها الحاسب كأداة، أو موضوع للجريمة" (مراد، د. ت، ص 40).

فالمعلومات الإلكترونية تتعرض لمجموعة من المخاطر والتهديدات تعلم مراحل مختلفة ومستويات متعددة، وهي تتمثل في:

☞ المخاطر التي تتعرض لها المعلومات في مرحلة خلقها واسترجاعها وتعديلها وإلغاء المعلومات، وجامعتها وجود المعلومات داخل النظام؛

☞ المخاطر التي تتعرض لها المعلومات في مرحلة النقل، أي التبادل بين أنظمة الحاسوب؛

☞ المخاطر التي تتعرض لها المعلومات في مرحلة التخزين على وسائط خارج النظام.

وقد يكون التعقيد وكثرة المتطلبات في عملية التسويق الإلكتروني أدباً بالبرمجة الموقعية طريقة معقدة قد يحدد بزمن معين، وبسبب الانتقال السريع إلى عالم التسويق الإلكتروني وإلزام المبرمجين بها هبوط قصير قد يغفل المبرمج عن ثغرات أمنية كثيرة، منها ما يلي (الرجبية، 2012، ص 4-5؛ الغنير، القحطاني، 2009، ص 23؛ الراشد، 2012، ص 3):

4-1 مهاجمة خادم التسوق الإلكتروني:

وذلك عن طريق:

① مزود الحقن (SQL Injection): قد يتمكن المهاجم الدخول إلى النظام بدون الحاجة لعملية تسجيل الدخول،

ويتمكن من إطلاع قاعدة البيانات بما فيها من معلومات سرية أو التلاعب فيها؛

② التلاعب بالأسعار: تظهر هذه الثغرة الأمنية في التسوق الإلكتروني فقط، وهي أن يقوم المهاجم بإظهار

سعر مختلف للمنتج، وذلك عن طريق استخدام هيلبر نامج

"Achilles"، حيث يقوم بتعديل السعر من منتصف المستخدم إلى الحد الأدنى لنفسه؛

③ سهولة تغيير أسماء التجار وعناوينهم على شبكة الانترنت: فرغم أنّ المسوّق الإلكتروني يمكن من خلال المعلومات التي يقدمها المستهلك أن يتأكد من هوية المتعاملين معه وشخصياتهم، أما المستهلك فليس له فرصة للتحقق من ذلك التاجر الذي يتعامل معه؛

④ تعدي حجم الذاكرة المخصصة (Buffer Overflow): قد يتمكن المهاجم من الدخول للنظام باستخدام ثغرات أمنية في تخصيص التخزين في الذاكرة، يعمل على مجتبتها بنفسه. كما قد يستخدم المهاجم بعض البرامج الخبيثة كالفيرسات، برامج التجسس أو شباهها.

4-2 مهاجمة المتسوق الإلكتروني:

وذلك:

① خداع المتسوق أو الهندسة الاجتماعية (Social Engineering): وتعتمد هذه الطريقة على خداع أو استغلال الآخرين، ولا تحتاج إلى امتلاك المهاجم خبرات تقنية عالية. المهاجم بالبحث عن وراقت تحتوي على كل ما تروى، وأسماء مواقع إلكترونية، وأسماء معلومات هامة قام صاحبها بربطها في سلسلة المهمة لتأقوا موضعها بالقرم بمجهزها الخاص، من أجل ذلك المواقع الإلكترونية والحصول على ما تحتاج، أن يقوم المهاجم باستغلال الطيبة الآخرين عن طريق الحوار معهم ومعرفة معلومات كإسماء أو موعداً لأفراد الأسرة، واسم المدرسة الثانوية أو غيرها، ثم استغلال هذه المعلومات في استرجاع كل ما تروى من المواقع التي توفر خدمة استرجاع كل ما تروى من معرفة الإجابة على هذه الأسئلة. وبالرغم من أن هذه الطريقة منسوبة بالغة، إلا أنها تعتبر من أكثر الطرق نجاحاً وفعالية في عملية الاختراق؛

② استخدام تقنيات الاصطياد الإلكتروني و خداع المتسوق (Phishing): فقد يقوم المهاجم بإرسال رسائل بريد إلكترونية خادعة إلى المستخدمين، هذه الرسائل تتضمن روابط لمواقع إلكترونية مزيفة تدعى أنها تقدم سلع وخدمات، أو تكون للمواقع الإلكترونية مزيفة تدعى أنها بنوك أو تقدم خدمات بنكية، أو قد يرسل المهاجم (Script) ينقل المتسوق من صفحة التسوق الإلكترونية إلى صفحة أخرى يرسل بها المهاجم، ويطلب من المتسوق إدخال اسم المستخدم والرمز السري ليحفظها عند هويته باستخدامها للدخول إلى النظام التسوق الإلكتروني و يسمي المتسوق. إن هذه المواقع الإلكترونية المزيفة تكون مصممة بطريقة تشبه فيها المواقع الإلكترونية الحقيقية. فليس بيل المثال، تكون واجهة الموقع المزيفة متماثلة مع واجهة الموقع الحقيقية من ناحية الألوان وأشكال الخانات وتعبئة المعلومات، وكذلك يمكن أن يكون عنوان صفحة الموقع المزيف مختلفاً عن الموقع الحقيقي، ونتيجة لدرجة التشابه العالية فإن المستخدم قد لا يستطيع التفرقة بين الموقع المزيف والحقيقي؛

③ الثغرات الأمنية في حاسوب المتسوق: قد يستهدف حاسوب المتسوق بواسطة الثغرات الأمنية التي يجهلها المتسوق، ومن أعظم الأخطاء التي تقع فيها المتسوق من بعض خصائص اتصاله في حاسوبه، وذلك لتسهيله لسرعة عملية الشراء، مما يسهل للمخترق التجسس في الحاسوب، وسرقة الرمز السري أو رقم بطاقة الائتمان.

4-3 مهاجمة الشبكة التيبينا المتسوقوا لخد مالزود للتسوقا لالكترونى:

قد يتمكّن المهاجم من مراقبة الشبكة وسرقة المعلومات أثناء تبادل المعلومات بين المتسوق والموقع، مثل رقمية الائتمان أو الرمز السري، وغالباً ما تكون شبكة الانترنت غير مشفرة.

5. الإجراء اتالأمينية لحماية التعاملات التسويقية الإلكترونية:

من أجل حماية التعاملات التسويقية الإلكترونية يجب تطبيق مجموعة من الإجراءات اتالاحتياط اتاللازمة والتزام بها وتطويرها باستمرار، من أجل لوقاية من الأخطار والتهديدات، وهو ما سنحاول مناقشته من خلال هذا المحور.

5-1 ماهية أمن المعلومات الإلكترونية:

يعرّف أمن المعلومات الإلكترونية بأنه: "كافة الإجراءات المتخذة لمنع فقدان المعلومات بأشكال من الأشكال. أي عنى بقاء المعلومات تحت السيطرة الكاملة والمباشرة لتحقيق الإدراك الجماعى والإحساس الفعلى والتخليع عدم وجود تأثير التهديدات الفيزيائية والتخليع لبنى مجتمع المعلومات الإلكترونية، أيّا كان مصدرها، ويستدعى التأهب لها أو الفعل الرسمي لمواجهةها" (الأسطى، 2009، ص 61). كما يعرف بأنه: "المحافظة على إتاحة المعلومات وسلامتها وسريتها وملكيّتها والاستفادة منها". أو هو: "حماية جميع أنواع المعلومات ومصادر الأدوات التي تتعامل معها وتعالجها، من منظمة وغرفة تشغيل أجهزة، والأجهزة والأفراد من السرقة والتزوير والتلف والضياع والاختراق، وذلك كإتباع إجراءات وقائية وضوابط واضحة" (الحميد، نينو، 2007، صص 96-97).

وعليه، فإنّ من أهم أسباب الحاجة إلى أنظمة أمنية في التعاملات الإلكترونية، ما يلي (الحمامي، العاني، 2007، ص 20):

- منع فقدان البيانات بواسطة جهة مخترقة بأى أسلوب؛
- منع تدوير البيانات المتبادلة والمخزنة؛
- منع الحصول على بيانات خاصة؛
- منع سرقة البيانات المتناقلة بينو إقتماص شخصياً تأخر أو كينونة ما؛
- منع الإلها بوالإجرام المعلومات الإلكترونية ومنع المنافسة غير المشروعة والانتقام.

ويعتمد نظام أمن المعلومات الإلكترونية على ثلاثة أبعاد رئيسية، هي (الجنبيهي، الجنبيهي، 2005، ص 13):

① ضمان سرية معلومات المتسوق والمعلومات الحساسة (Confidentiality): وهذا

الجانبيشمل كالتدابير اللازمة لمنع إطلاع الغير المصرح لهم على المعلومات الحساسة والسرية؛

② ضمان سلامة المعلومات المتناقلة عليها من قبل الغير مصرح لهم (Integrity): فبالإضافة إلى وجوب

المحافظة على سرية المعلومات، يجب كذلك اتخاذ كافة التدابير اللازمة لحماية البيانات من التغيير؛

③ توفير المعلومات للمتسوقين حسب احتياجاتهم، بحيث لا يتضرر نظام الأمن في التسويق الإلكتروني (*Availability*): إذ أن الحفاظ على سلامة المعلومات وسريتها أمر مهم ولا ريب، لكن هذه المعلومات تصبح ذات قيمة إذا كان من غير حقلها لإطلاع عليها لا يمكنها الوصول إليها، أو أن الوصول إليها يحتاج وقتاً طويلاً.

5-2 أساليب الحماية الفنية والتقنية من الاختراقات والاعتداءات الإلكترونية:

ومع تطور أساليب الاختراقات الإلكترونية، قامت المنظمات الناشطة في مجال التسويق الإلكتروني بتوفير العديد من وسائل الحماية ضد الاختراقات والاعتداءات الإلكترونية، ومن أهمها، ما يلي (النمر، 2012، ص 4-5؛ الراشد، 2012، ص 4-7؛ قنديلجي، الجنابي، 2005، ص 357؛ أبو فارة، 2007، ص 370):

أ- تثقيف وتوعية المستخدمين بأحدث أساليب المخترقين، وكيفية تجنبها والتصدي لها؛

ب- توفير الأجهزة الصغيرة التي تولد رقم تعريف شخصي للاستخدام الفوري. وهي عبارة عن أجهزة صغيرة تعرف باسم أجهزة التعريف (Authentication token)، وهي سهلة الحمل، وتعمل على توليد رقم يسمى رقم التعريف الشخصي (PIN)، وهذا الرقم يتغير كل دقيقة تقريباً، وبشكل مستمر. وغالباً ما تقدم البنوك هذه الأجهزة للعملاء الذين يملكون محفظة بنكية تحتوي على أسهم تجارية، لأن المحافظ البنكية تحتاج إلى حماية عالية، وهي أكثر عرضة لمحاولات الاختراق وسرقة الأموال، فهذه الأجهزة تمكن العميل من بيع وشراء الأسهم وإدارة محفظته البنكية بكل سهولة وأمان وهو في منزله، فعندما يريد المستخدم الدخول للنظام لإدارة محفظته التجارية فإن عليه إدخال الرقم الظاهر في شاشة الجهاز، بالإضافة إلى الكلمة مرورة التقليدية. إن هذه الطريقة تسمى (RSA SecurID)، وهي تعتمد على توليد كلمات مرور فورية تستخدم لمرة واحدة (OTP)، وبالرغم مما تمتاز به هذه الأجهزة من قدرة على توفير حماية للمستخدم من عمليات الاختطاف الإلكتروني والهجمات على بروتوكولات التوثيق، إلا أنها تسبب بعض الإزعاج للمستخدمين، حيث يتوجب على المستخدم حملها، وكذلك قد تتعرض هذه الأجهزة للسرقة، بالإضافة إلى تكلفة صناعتها؛

ج- تطوير وسائل الدفع المالي: إذ توفر المواقع الإلكترونية العديد من وسائل الدفع، مثل: البطاقة الائتمانية التي تعتبر أكثر وسائل الدفع أماناً، وذلك لأن المنظمات المصدرة لها تتحمل كافة المسؤولية عند حدوث أخطاء، وكذلك تصدر كشوف دورية للحسابات يستطيع من خلالها المستخدم مراجعة مصروفاته. وحتى يتسنى للمستخدم الشراء بأمان، فقد وفرت البنوك البطاقة الائتمانية التي تكون مخصصة للتسوق الإلكتروني، ويقوم المستخدم بشحنها بقيمة مشترياته، وهذه هي أفضل طريقة حتى لا يتعرض رصيد المستخدم للسرقة؛

د- خدمة الرسائل القصيرة المتضمنة لكلمات مرور فورية: فعندما يريد المستخدم الدخول مثلاً إلى حسابه البنكي، فإنه يدخل اسم المستخدم الخاص به، وكلمة مرورة التقليدية، ثم بعد ذلك تصله رسالة قصيرة من البنك على جهازه المحمول، تحتوي هذه الرسالة على كلمة مرور فورية تستخدم لمرة واحدة، يقوم المستخدم بإدخالها لإكمال إجراءات التحقق من هويته، ثم بعد ذلك يتمكن المستخدم من إدارة حسابه البنكي. ولكن المشكلة التي تواجهها هذه الطريقة هي إمكانية تعرض شبكات اتصال الهواتف المحمولة للتجسس من قبل المهاجمين؛

هـ- استخدام برامج مضادة للفيروسات وتحديثها باستمرار؛

و- يجب أن يكون النظام شاملاً، أي يتطرق إلى جميع المراحل التي تمر بها البيانات، وكذلك جميع الأحوال التي تكون عليها لبيانات. كما يجب أن يكون كاملاً، بمعنى ألا تكون به ثغرات يمكن الاختراق من خلالها؛

ز- إنشاء نسخ احتياطية من المعلومات العامة والخاصة بالمستهلكين في المنظمة أو المتجر، بحيث يمكن استرجاعها لو تم فقدها؛

ح- التحكم بدخول المستخدمين باستخدام الجدار الناري أو جدار الحماية (Firewall)، وهذا لمقاومة أخطار المتطفلين والحد منها وتوفير الحماية للمنظمات. فالجدار الناري عبارة عن مكونات مادية (معدات وأجهزة) وبرمجيات خاصة توضع بين الشبكة الداخلية للمنظمة من جهة، وبين الشبكات الخارجية، ويعمل على منع أي من المستخدمين الخارجيين من التوغل في الشبكات الخاصة، والدخول غير المرخص إليها. فهو إذن نظام للحماية مزود ببرمجية خاصة تمنع الغرباء من اختراق الشبكات الخاصة، وقد صمم بطريقة تؤمن له اعتراض كل حزمة رسائل تمر بين شبكتين، وتفحص صفتها، ومن ثم رفض أي رسالة منها غير مخولة من محاولة الدخول والاختراق؛

ط- تشفير الملفات والاتصالات الشبكية؛ وهو عملية قديمة يقصد بها تحويل محتويات الرسائل بشكل يصعب على الغير معرفة المحتوى لأساس، أو إعادة تموضعها الأصلي، ولا يقوم بذلك إلا من يعرف كيفية تحويله؛

ي- تحويل العناوين الرقمية "NAT" (Network Address Translation): تتجسد هذه الفكرة في حالة الشبكات الكبيرة الداخلية للمنظمة، إذ أن هناك منشأة تسمى "IANA"، تتولى إعطاء العناوين الرقمية لمستخدميها، فتعطي عنواناً واحداً للشبكة ككل معترف به على الشبكة الخارجية، أما الحواسيب الداخلية فيعطى لها عناويناً تصلح للاستعمال الخارجي، إنما صالحة داخلياً فقط، ففي حالة ما إذا أراد الحاسوب الداخلي الاتصال بالشبكة الخارجية فإنه يمر عبر الموجه الذي يحمل عنوان الشبكة ككل، وإذا حاول المستخدم من الخارج الاتصال بأحد الحواسيب الداخلية فإنه سيتصل بالموجه الذي سيعمل عمل الجدار الناري في الغرلة والتوجيه، وبهذا لا يستطيع المتطفلين المرور إلى حواسيب الشبكة الداخلية للمنظمة؛

ك- التحديث: إن بناء البرمجيات، ومنها أنظمة التشغيل (مثل: نظام Windows)، عملية معقدة ولا تخلو من الأخطاء، كما أنها بحاجة إلى تحسينات مستمرة تبعاً لتغير لظروف استخدامها وطلبات المستخدمين، وتزايد قدرات الأجهزة، ومن ناحية أخرى فإن الحاجة إلى التحسين المستمر يفرضها وجود الثغرات الأمنية التي تكتشف بشكل مستمر في هذه البرمجيات، مما يحتم إغلاق تلك الثغرات قبل أن تستغل، وإغلاقها يتطلب تحديث البرمجيات، واكتشاف الثغرات قد يكون من قبل المنظمة المصنعة للبرنامج، وعندما تقوم المنظمة بخطوة مسبقة تصدر فيها تحديثاً لسد الثغرات الأمنية التي اكتشفتها للتو، وفي أحيان كثيرة يسبق المتطفلون إلى اكتشاف الثغرات، فيطورون برامج خبيثة تستغل هذه الثغرات؛

ل- التوقيع الإلكتروني: ويقصد به استخدام وسيلة للتحقق من أنّ صاحب المعاملة هو نفس الشخص الذي قام بإرسالها أو تنفيذها، ويطلق على هذا النوع أيضاً البصمة الإلكترونية. يتم تشفير التوقيع الإلكتروني باستخدام نظام التشفير عن طريق المفتاح العام المزدوج، حيث يضع المرسل علامة خاصة به (بصمة) ويقوم بتشفيرها بالمفتاح الخاص به، وتشفيرها أيضاً بالمفتاح العام للمرسل إليه، بعد ذلك يقوم (المرسل إليه) من خلال استخدام المفتاح الخاص به بحل الشفرة؛

م- طمس البيانات: يظن المبتدئون في تعلم الحاسوب أنهم مجرد حذف ملف ما فإنه يكون قد فقد نهائياً، ولا يعلمون أنّ الملف قد تم نقله إلى سلة المهملات، ويمكن استرجاعه، ويظن كثير من المستخدمين أنّ حذف الملف من سلة المحذوفات هو الإتلاف النهائي لذلك الملف، وهذا غير صحيح، فحذف ملف ما من وحدة التخزين يتم بحذف المؤشر الذي يدل عليه، وليس الملف نفسه، أي أنّ محتويات الملف تظل في وحدة التخزين، ولكن على هيئة مساحة فارغة يمكن الكتابة عليها، ولما كان كذلك فإنه يمكن بواسطة برامج استرجاع متخصصة استرجاع ذلك الملف. وهناك معايير معروفة لطمس البيانات، فمثلاً معايير وزارة الدفاع الأمريكية تتطلب طمس البيانات بالكتابة عليها 7 مرات، ومعياري "Peter Gutmann" يتطلب الكتابة 35 مرة، وأيضاً هناك برامج خاصة بطمس البيانات بشكل نهائي من الحاسوب، خاصة إذا كانت هذه البيانات سرية، ومن هذه البرامج كمثال: "Fine Crypt / Best Crypt"؛

ن- الاختيار الأمثل لكلمة المرور: يجب أن تكون كلمة مرور قوية لا تكون صيداً سهلاً لبرامج الاختراق. ولتكون كلمة مرور قوية يجب إتباع الخطوات التالية:

- لا تكون كلمة المرور مكونة من كلمة واحدة، مثل: monir/khald/rabah/mohamed؛
- لا تتضمن كلمة المرور معلومات شخصية، مثل: تاريخ الميلاد، اسم البلد، أو لون تحبه... إلخ؛
- لا ينبغي أن تقل كلمة المرور عن 10 خانات، لأنّ السرعة الفائقة للحواسيب الحديثة تجعل من كلمة المرور واكتشافها أمراً يسيراً؛
- تكوين كلمة المرور من خليط من الحروف الصغيرة والكبيرة، والأرقام والرموز، فكلّما كان الخليط أكثر كان اختراق كلمة المرور أصعب؛
- على المستخدم أن يخزن كلمة المرور في مكان آمن، وإن استطاع أن يخزنها في ذاكرته فهو الأفضل؛
- ونظراً للتطور الحاصل في الوسائل التكنولوجية فيمكن استعمال العناصر الحيوية في بناء كلمة المرور كال بصمات العين والصوت.

س- الحيطة والحذر: ما فائدة كل الأساليب المذكورة إذا كان الشخص غير مبال ولا يتعامل مع نظم المعلومات الإلكترونية بالحيطة والحذر، تجده أين ما جلس ترك آثاراً عن معلوماته السرية، فعلى المستخدم أو المنظمة أن تراعي ما يلي:

- وضع قوانين إدارية أمنية لاستخدام الحواسيب المحمولة وكلمات المرور؛
- تجنب أي شيء ليس له علاقة بما يبحث عنه؛

- المراقبة التقنية الدورية للتركيبية الحاسوبية؛
- المراقبة الفنية الدورية للبرامج الحاسوبية.

5-3 نصائح وإرشادات لتسوق إلكتروني آمن:

إنَّهذه النصائح هي نصائح عالمية قد اتفق عليها كبرى منظمات أمن المعلومات وخبراء واستشاريون في التسويق الإلكتروني (القحطاني، 2012، ص3؛ الحربي، 2012، ص ص5-11؛ العبودي، 2012، ص ص5-8؛ الغثير، القحطاني، 2012، ص ص3-4):

- ☞ عدم التسوق إلاّ عن طريق الجهاز الخاص بالتسوق، وبشكل عام عدم تصفح أي مواقع تتطلب معلومات سرية إلاّ عن طريق الجهاز الخاص؛
- ☞ قبل البدء في التسوق، يجب التعرف على أكثر المواقع شهرةً وأماناً في مجال التسويق الإلكتروني، مع محاولة البقاء في نطاقها وعدم الخروج عنه؛
- ☞ قراءة سياسة الموقع المتبعة أثناء إجراء معاملاتهما الإلكترونية، حيث يمكن من خلالها تحديد مستوى الأمان والخصوصية التي يقدمها الموقع، بالإضافة إلى معرفة الهيئات التي قامت بتصديق الموقع، وبالتالي يتفادى المستخدم التعامل مع المواقع غير الموثوقة؛
- ☞ التأكد من استخدام مستعرض آمن، وعدم استخدام متصفح تم إنشائه على أيدي هواة أو منظمات غير مرخص لها وغير معروفة عالمياً؛
- ☞ استخدام بطاقة الائتمان كوسيلة الدفع الأكثر أماناً، حيث تتحمل الجهة المصدرة لبطاقة الائتمان الأخطاء الصادرة من الأنظمة؛



- ☞ التأكد قبل إدخالك معلومات البطاقة الائتمانية أن عنوان الصفحة التي تطلب المعلومات يبدأ

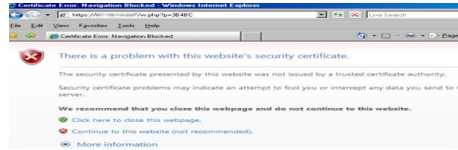
ب <https://>، وليس <http://> (حيث أنّ (s) تُعبر عن أنّ الموقع مشفر، والتواصل فيه آمن). ويجب التأكد من وجود صورة القفل أسفل المتصفح (قفل الحماية)؛

- ☞ إنَّ بعض منتحلي المواقع يقومون بتزوير العنوان ليصبح كأنه العنوان الحقيقي للموقع، ولمزيد من التأكد



بأنّ هذا العنوان هو العنوان الحقيقي للموقع وليس عنوان مزور، يجب تحديد العنوان الموجود في أعلى المتصفح

للتأكد أنه ليس بصورة أو أي شيء آخر، إنّما هو العنوان الحقيقي؛



في حالة ظهور هذه الصورة أثناء القيام بتصفح موقع يتطلب معلومات سرية يجب إغلاقه فوراً لأنّ هذا تحذير بأن الموقع غير آمن؛

عدم فتح أي رابط يأتي على البريد الشخصي يدعى فيه إلى سرعة تحديث بيانات البطاقة الائتمانية أو يقدم عرض مغري لبضاعة معينة. بل يجب فقط الذهاب للموقع عبر كتابة عنوانه باليد من خلال شريط العناوين أو بالذهاب إليه عبر المفضلة إذا كان قد حفظ من قبل للتأكد من صحة الخبر؛

في حالة شعور المتسوّق أنّ الموقع يبدو غريباً بعض الشيء، أو كانت لديه تساؤلات عن تفاصيل للمنتجات يجب أن تتوفر في الموقع ولم يجدها، أو أنّ الأسعار تبدو منخفضة بشكل مبالغ فيه، أو أنّ الموقع يشتمل على العديد من الأخطاء النحوية والإملائية، أو أنّه غير مرتب كما هو في الأصل، فيجب مغادرة الموقع مباشرة ثم محاولة الاتصال بالدعم الفني للموقع عبر البريد الإلكتروني أو الهاتف للتأكد من حالة الموقع؛

تحديث برنامج المتصفح ونظام التشغيل (الويندوز مثلاً) بشكل دوري لتفادي أي ثغرات أمنية قد تؤدي إلى اختراق المتصفح؛

استخدام مكافح الفيروسات، والقيام بتحديثه بشكل دوري، كما هناك بعض الأدوات لزيادة الأمن، مثل الجدار الناري ومكافح ملفات التجسس ومضاد مواقع الاصطياد الإلكتروني؛

عدم إخبار أي أحد بمعلومات البطاقة الائتمانية، وعدم مشاركتها مع أي أحد، وعدم وضع المعلومات السرية عنها في الأماكن العامة أو أماكن يمكن لأي أحد الوصول إليها؛

استخدام كلمة مرور قوية يصعب تخمينها، بحيث تكون مكونة من 8 خانات على الأقل، تشمل حروف وأرقام ورموز، ولا تحتوي على معلومات معروفة عن الشخص، وبالتالي يمكن توقعها بسهولة، وكذلك يجب أن

تكون كلمة المرور مختلفة عن تلك الخاصة بالدخول للنظام أو البريد الإلكتروني أو أي موقع آخر؛ لأنه في حالة اختراق أحدها، لا يتم اختراق بقية الحسابات. كما يقول المثل: "لا تضع جميع بيضك في سلة واحدة"؛

❖ القيام بتغيير الرقم السري للبطاقة بشكل دوري، مع الحرص أن تكون مختلفة عن أي رقم سري آخر حتى لا يتم اكتشافها عن طريق اكتشاف هذا الرقم السري؛

❖ التأكد من رصيد وحالة البطاقة الائتمانية بشكل دوري من البنك، للتمكن من السيطرة على الوضع في حالة وجود عملية سرقة لا قدر الله؛

❖ عدم الاحتفاظ برصيد إضافي في البطاقة الائتمانية، والاكتفاء بوضع مبلغ البضاعة المراد شرائها، وعدم الإبقاء على أي رصيد في البطاقة بعد الشراء؛

❖ الاحتفاظ بمعلومات الشراء من أي موقع، والقيام بطباعتها للرجوع لها عند الحاجة؛

❖ تجنب الشراء في الأماكن العامة حتى وإن كان باستخدام الحاسب الشخصي، فمن الممكن أن يختلس أحدهم النظر إلى المعلومات الشخصية للمتسوق محاولاً سرقتها؛

❖ استخدام بطاقة ائتمانية واحدة للتسوق الإلكتروني؛

❖ محاولة قدر المستطاع تجنب الاحتفاظ بمعلومات البطاقة الائتمانية داخل مواقع التسوق الإلكتروني، بحيث لا يتم سرقة هذه المعلومات إذا تم اختراق الموقع؛

❖ توخي الحذر عند كتابة اسم الموقع، فهناك مواقع تستغل خطأ الزائر في أحد حروف اسم الموقع المطلوب لشده والحصول على معلومات سرية عنه. فمثلاً، بدل أن تكتب:

<http://www.hotmail.com> كتبت: <http://www.hutmail.com>.

وما تجدر الإشارة إليه في الأخير، أن مجرد إتباع المستهلك للإرشادات أعلاه، يجعله يخرج من دائرة الأخطاء الشائعة. فهذه الإرشادات لم تأتي عبثاً بل أنت من واقع خبرة، ولهذا يجب أن يتذكر أنه مازال داخل دائرة الخطر، فوجب أن يكون حذراً دائماً، ويحاول أن يستعين بحدسه، وفكره وهل أن ما يفعله صحيح أم لا.

6- الخاتمة:

نظراً للانعكاسات الهامة للإنترنت على فضاءات التسويق والتسوق، وإعطائها فرصاً مدهشة لجمع وتخزين واستخدام المعلومات حول المستهلكين، فإن مسألة الحصول على البيانات بطريقة أخلاقية والمحافظة عليها يعتبر من المسائل المهمة جداً، فكثيراً ما يتم عدم احترام حقوق عدم التعرض للمعلومات الخاصة، والتدخل في الحياة الخاصة واستخدام المعلومات الشخصية لأغراض مضرّة بالمستهلك.

إنَّ التسوّق عن طريق الانترنت محفوف بالمخاطر الأمنية وأكثر عرضة لانتهاك الخصوصية، وعلى من يريد التسوّق تذكر أن هناك من يترصص به، لذا لا بد من توخي الحذر أثناء التسوّق الإلكتروني وإتباع توصيات الأمان التي عرضنا طرفاً منها. كما نؤكد أنه عند إتباع وسائل الأمان ستصبح عملية التسوّق الإلكتروني سهلة وممتعة وخالية من المخاطر.

7- قائمة المراجع:

- 1- إبراهيم، خالد ممدوح، لوجيستيات التجارة الإلكترونية، الإسكندرية: دار الفكر الجامعي، (2008).
- 2- أبوفارة، يوسف أحمد، التسويق الإلكتروني: عناصر المزيج التسويقي عبر الانترنت (ط.2). عمان: دار وائل للنشر والتوزيع، (2007).
- 3- أبوقحف، عبد السلام وآخرون، التسويق. الإسكندرية: المكتب الجامعي الحديث، (2006).
- 4- أحمد، محمد، محمد سمير، التسويق الإلكتروني. عمان: دار المسيرة للنشر والتوزيع، (2009).
- 5- الأسطل، رند عمران مصطفى. واقع استخدام التسويق الإلكتروني لدبالبنوك العاملة في قطاع غزة. رسالة ماجستير غير منشورة، الجامعة الإسلامية، غزة، (2009).
- 6- الجنيبي، منير محمد والجنيبي، ممدوح محمد. أمن المعلومات الإلكترونية. الإسكندرية: دار الفكر الجامعي (2005).
- 7- الحري، رانده بنت عبد الله بن زايد. التسوّق الإلكتروني الآمن. المقالات العلمية لمركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، (2012). تم استرجاعها في تاريخ: 2016/02/08، من الموقع الإلكتروني: [http://coeia.edu.sa].
- 8- الحمادي، علاء حسين والعاني، سعد عبد العزيز. تكنولوجيا أمنية المعلومات وأنظمة الحماية. عمان: دار وائل للنشر والتوزيع، (2007).
- 9- الحميد، محمد دباس ونيو، ماركو إبراهيم. حماية أنظمة المعلومات. عمان: دار الحامد للنشر والتوزيع، (2007).
- 10- الراشد، نورة محمد عبد الرحمن. قضايا أمن المعلومات في التجارة الإلكترونية. المقالات العلمية لمركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، (2012). تم استرجاعها في تاريخ: 2016/02/08، من الموقع الإلكتروني: [http://coeia.edu.sa].
- 11- الرجبية، دلال بنت محمد. التسوّق الإلكتروني الآمن. المقالات العلمية لمركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، (2012). تم استرجاعها في تاريخ: 2016/02/08، من الموقع الإلكتروني: [http://coeia.edu.sa].
- 12- عبد المجيد، طلعت أسعد. التسويق الفعال: الأساسيات والتطبيق. الإسكندرية: منشأة العارف، (1998).
- 13- العبودي، عبد العزيز سعد. التسوّق الإلكتروني الآمن. المقالات العلمية لمركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، (2012). تم استرجاعها في تاريخ: 2016/02/08، من الموقع الإلكتروني: [http://coeia.edu.sa].
- 14- العليان، محمد علي. الجرائم المعلوماتية. الإسكندرية: دار الجامعة الجديدة، (2004).
- 15- الغثير، خالد بن سليمان والقحطاني ومحمد بن عبد الله. أمن المعلومات بلغة ميسرة. الرياض: مركز التميز لأمن المعلومات - جامعة الملك سعود، (2009).
- 16- الغثير، خالد بن سليمان والقحطاني، محمد بن عبد الله. التسوّق الآمن. المقالات العلمية لمركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، (2012). تم استرجاعها في تاريخ: 2016/02/08، من الموقع الإلكتروني: [http://coeia.edu.sa].

- 17- فقيه، تهايم محمد عبد الرحمن. التسوق الإلكتروني وأثره على اتجاهات الأسرة الاستهلاكية في عصر المعلوماتية. رسالة ماجستير غير منشورة، جامعة أم القرى، المملكة العربية السعودية، (2013).
- 18- القحطاني، فاطمة بنت تركي بن فهد. التوقيع الإلكتروني. المقالات العلمية لمركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، (2012). تم استرجاعها في تاريخ: 2016/02/08، من الموقع الإلكتروني: [http://coeia.edu.sa].
- 19- قنديلجي، عامر إبراهيم والجناي، علاء عبد القادر. نظم المعلومات الإدارية وتكنولوجيا المعلومات. عمان: دار المسيرة للنشر والتوزيع، (2005).
- 20- قيو، كاثرين. التسويق الإلكتروني. ترجمة: واشد، وردية. لبنان: المؤسسة الجامعية للدراسات والنشر والتوزيع، (2008).
- 21- مراد، عبد الفتاح. (د.ت). شرح جرائم الكمبيوتر والإنترنت. الإسكندرية: شركة البهاء للبرمجيات والكمبيوتر والنشر الإلكتروني.
- 22- مرزق لال، إبراهيم. إستراتيجية التسويق الإلكتروني للكتاب في الجزائر: دراسة تقييمية للمواقع الإلكترونية للنشرين. رسالة ماجستير غير منشورة، جامعة منتوري - قسنطينة، الجزائر، (2010).
- 23- النمر، هبة منصور. قضايا أمن المعلومات في التجارة الإلكترونية. المقالات العلمية لمركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، (2012). تم استرجاعها في تاريخ: 2016/02/08، من الموقع الإلكتروني: [http://coeia.edu.sa].
- 24- النونو، عماد إسماعيل. التسوق عبر الإنترنت: دوافع التبني أو الرفض - دراسة ميدانية. أطروحة دكتوراه في إدارة الأعمال والتخطيط الاقتصادي، جامعة العالم الأمريكية، غزة. (2007).