العنوان:	مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة
المصدر:	مجلة البحث العلمي في التربية
الناشر:	جامعة عين شمس - كلية البنات للآداب والعلوم والتربية
المؤلف الرئيسي:	الصحفي، مصباح أحمد حامد
مؤلفين آخرين:	عسكول، سناء بنت صالح(م. مشارك)
المجلد/العدد:	ع20, ج10
محكمة:	نعم
التاريخ الميلادي:	2019
الصفحات:	493 - 534
رقم MD:	1029923
نوع المحتوى:	بحوث ومقالات
اللغة:	Arabic
قواعد المعلومات:	EduSearch
مواضيع:	الأمن السيبراني، الحاسب الآلي، جدة، المرحلة الثانوية
رابط:	http://search.mandumah.com/Record/1029923

مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة

The Level of Computer Teachers' Awareness of Cybersecurity in Secondary Schools in Jeddah

إعداد

أ/ مصباح أحمد حامد الصحفي

الماجستير في القيادة التربوية ـ قسم القيادة التربوية ـ كلية العلوم الصحية والسلوكية والتعليم ـ جامعه دار الحكمة ـ جدة

د/ سناء صالح عسكول

كلية العلوم الصحية والسلوكية والتعليم، بجامعه دار الحكمة ـ جدة

مستخلص الدراسة:

هدفت الدراسة إلى الكشف عن مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينه جدة. وتكون مجتمع الدراسة من جميع معلمات الحاسب للمرحلة الثانوية بمدينة جدة للعام الدراسي ١٤٤٠هـ -٢٠١٩م.

وعددهن (٣٥٢) معلمة حسب المعلومات الواردة من إدارة تعليم جدة.

عينة الدراسة: تم استخدام المعادلات الإحصائية لحساب حجم العينة المناسبة للبحث. تم توزيع الاستبانة على كل المجتمع، وقد تم استعادة (١٠٦) وتم استبعاد استبانتين غير قابلة للتحليل وتم اختيار العينة بالطريقة العشوائية البسيطة.

منهجية الدراسة وأدواتها: استخدمت الباحثة المنهج الكمي لمناسبته هذه الدراسة.

أهم النتائج:

- أكدت الدراسة على وجود ضعف وقصور لدى معلمات الحاسب الآلي- في الوعي بمفاهيم الأمن السيبراني.
- أكدت الدراسة على وجود ضعف لدي معلمات الحاسب الآلي- في الوعي بمستوى الأمن السيبراني.
- عدم وجود فروق ذات دلالة إحصائية بين بين متوسطات استجابات أفراد عينة الدراسة عند مستوى الدلالة (≤٠،٠٥) في درجة وعي معلمات الحاسب بالأمن السيبراني تعزى لمتغيرات الدراسة الحالية (سنوات الخبرة- المؤهل العلمي- الدورات التدريبية).

الكلمات المفتاحية:

الأمن السيبراني- الهندسة الاجتماعية – الاحتيال الالكتروني.

Abstract:

The problem of the study: The problem of the study is determined by the following main question: - The level of awareness of cyber security at computer teachers of the secondary stage in Jeddah city

The study population consists of all the computer parameters of the secondary stage in Jeddah for the academic year 1440 H-2019. The number of them (352) is according to the information received from the Jeddah Education Department.

The sample was used to calculate the appropriate sample size for the research. The questionnaire was distributed to the whole community in order to obtain the largest number of responses. 106 were retrieved and two questionnaires were excluded.

Methodology and tools: The researcher used the quantitative approach for the study

Main results:

• The study confirmed the weakness and lack of weakness and weakness of individuals - including computer teachers - in awareness of the concepts of security Sirany.

• The study confirmed the weakness and lack of weakness and weakness of individuals - including computer teachers - in awareness of the level of cybersecurity.

• There were no statistically significant differences between the average responses of the study sample members at the level of significance (00,05) in the degree of awareness of computer teachers in cybersecurity due to the current study variables (years of experience, qualification, training courses).

Key words: Cybersecurity, Social Engineering , Electronic Fraud.

المقدمة والإطار العام للدراسة:

مقدمة introduction :

احدثت التكنولوجيا في القرن العشرون والواحد والعشرون ثورة ونقله نوعيه كبيرة، حيث سيطرت على حياتنا اليومية ودخلت في تفاصيلها، سواءً الحياة العلمية أو العملية. واصبحت امور حياتنا متعلقة باستخدام الانترنت والتكنولوجيا، ورغم كل الايجابيات والراحة والتي توفرها لنا التكنولوجيا، الا أنه ظهرت مشكلات ومن أهمها سلبيات الجرائم السيبرانية التي تهدد الأمن الشخصي والدولي بكافة أنواعه. فكان لزاماً على معلمة الأجيال توعية الطالبات في جميع المراحل وخاصة المراحل الثانوية وتحذيرهم من الغزو الفضائي الضار الموجهة الذي يستهدف العقيدة والوطن ووحدته والأخلاق والقيم (المنتشري.١٤٤٠هـ) ومن التحديات انبثقت مع هذه التطور والتقدم للتكنولوجيا وهي الأمن السيبراني: وهو أنه لا بد أن نقوم بحماية سير هذه العمليات وحماية البيانات والتطبيقات وحفظ المعلومات الوطنية للأفراد والدولة، والمحافظة عليها؛ يعني منع أي دخول عليها غير مرخص أو العبث بها والتي لا بد أن يكون هناك نظام قوي يحمي هذه الخدمات والمعلومات التي توفرها وتزوّدنا بها هذه التكنولوجيا الجميلة عبر الفضاء الإلكتروني,ونعمل على وعي المعلمات وخصوصاً معلمات الحاسب الآلي .

ولقد أصبح الامن السيبراني حديث العالم بأسره، بل وأصبح جزءاً اسياسياً من أي سياسات أمنية أو اقتصادية أو سياسية اخرى، حيث أصبح صُناع القرار في مختلف الدول يضعون مسائل الامن السيبراني كأولويه في سياستهم (العتيبي.١٤٣٨).

وكلما أصبح الامن السيبراني موضوعاً للاهتمام العام والجهود البحثية بشكل متزايد، كلما ازداد عدد الدراسات التي تبحث أدوار المعلمين والمعلمات بشكل خاص كوضع قواعد في المنهج والصف على فهم الامن السيبراني بشكل واضح. وتمكين الطالبات من مهارات حل المشكلات، وتقديم مشورة الأقران، وتوعية الأهل بالأمن السيبراني من خلال اجتماعات أولياء الأمور، ومن خلال النشرات الإخبارية.

وحيث أن الأمن السيبراني من المواضيع البحثية الحديثة في العالم العربي التي لم تحظى بالقدر الكافي من الاهتمام على مستوى البحث العلمي، ولايمكن إغفال بعض الجهود القليلة، وخاصة في الجانب التعليمي ولدى المعلمات برغم أنه من أهم الكفايات لمعلمات الحاسب الآلي؛ لذا يهتم البحث الحالي بالتعرف على مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينه جدة.

مشكلة البحث Research problem :

من خلال تناول العديد من الدراسات والبحوث السابقة مثل دراسة الغدين وآخرون(٢٠١٨) والتي استهدفت الكشف عن الكشف عن صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، ودراسة صلاح الدين(٢٠١٠) والتي استهدفت تحديد طرق الحماية التكنولوجية بأنواعها وأشكالها المختلفة، ودراسة الشهري(١٤٢٩ه) والتي استهدفت تطوير التعاون بين الإدارة المدرسية والمؤسسات الأمنية في مجال التوعية الأمنية لطلاب المرحلة الثانوية ، تلاحظ الباحثة اهتمام كافة الدراسات السابقة بأهمية الأمن السيبراني وضرورة التدريب على مهاراته والوعي به لدى المواطنين بصفة عامة والمعلمين بصفة خاصة.

ومن خلال عمل الباحثة في التعليم وخبرتها في الميدان وجدت أن مستوى الوعي بالأمن السيبراني ضئيل جداً لدى العديد من المعلمات بشكل كل عام، وذلك باعتباره أحد أهم كفايات التأهيل المهني لديهن، وتم التركيز على معلمات الحاسب الآلي لأن على عاتقهن التوجيه والارشاد التقني، وتتمثل مشكلة البحث الحالي في ضرورة الوعي بأهمية الأمن السيبراني في ظل الاستخدام الدائم للشبكة العنبوتية من جانب المعلمين باعتبارها مصدر أساسي من مصادر المعلومات في العصر الحالي، ولتأكيد مشكلة الباحثة أجرت الباحثة دراسة لمعرفة مستوى وعي معلمات الحاسب الآلي بالأمن السيبراني للوقوف على نقاط الضعف في تطبيق مبادئ الامن السيبراني في المدارس. لما له اهمية لأمننا الوطني واستقرارنا الاقتصادي. وفي حدود علم الباحثة لا يوجد دراسات على مستوى الوطن العربي وكذلك الصعيد المحلي تتناول وعي معلمات الحاسب الآلي للآمن السيبراني.

ومن خلال ما سبق ينبثق عن هذه المشكلة التساؤل الرئيسي التالي: ما مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينه جدة)

تجيب الدراسة عن التساؤلات الفرعية:

١. هل توجد فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد مجتمع الدراسة عند مستوى الدلالة ($\leq$ 0,05 a) في درجة وعي معلمات الحاسب بالأمن السيبراني تعزى لاختلاف الدورات التدريبية، المؤهل العلمي، وسنوات الخبرة؟
٢. ما مدى وعي معلمات الحاسب الالي بمدينه جدة بماهيه الأمن السيبراني؟
٣. ما مدى وعي معلمات الحاسب الآلي بمدينه جدة بطرق المحافظة على نظام الأمن السيبراني؟

أهمية البحث research importance:

أولاً: الأهمية العلمية:

١- هذه الدراسة تعد من الدراسات العربية القليلة في مجال الأمن السيبراني، والتي يُمكن أن تثري الإنتاج الفكري في هذا المجال.
٢- إنها واحدة من الدراسات القليلة التطبيقية في حدود معرفة الباحثة التي تتناول موضوع قياس مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينه جدة.

الأهمية التطبيقية:

الإلمام بالأمن السيبراني ركن حيوي ليس فقط على الصعيد الشخصي للفرد والمجتمع بل مهم لأمن الدولة، مما يُمكن متخذي القرار في وزارة التعليم من استخدام منهج يُركز على الأمن السيبراني.

- حداثة الدراسة ومواكبتها للتغير المحلي والعالمي في مجال الأمن السيبراني، قد يُساعد في تطوير المعلمين والمعلمات في هذا المجال، والذين بدورهم قادرين على توعية الطلاب والطالبات أولاً ثم المجتمع.
- قد تُساعد نتائج الدراسة في إيجاد حلول عملية من خلال حماية الفرد والمجتمع في ظل تنامي المخاطر والتهديدات التي تعترض هذا المجال الحيوي.

أهداف البحثresearch goals :

تسعى الدراسة الحالية إلى تحقيق الأهداف الآتية:

- التعرف على مدى وعي معلمات الحاسب الآلي بمدينة جدة بماهية الأمن السيبراني.
- التعرف على مدى وعي معلمات الحاسب الآلي بمدينة جدة بطرق المحافظة على نظام الأمن السيبراني.

مفاهيم الدراسة ومصطلحاتهاConcepts and terminology of the study :

الأمن السيبرانية: بأنه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه (جبور،٢٠١٢).

الهندسة الاجتماعية: هي التلاعب بالبشر وخداعهم بهدف الوصول على بيانات أو معلومات، كانت ستظل خاصة وآمنة ولايمكن الوصول إليها، بهدف اختراق النظام (البوابة العربية للأخبار التقنية ،٢٠١٧).

القرصنة الإلكترونية تعرفها الباحثة بأنها اختراق لأجهزة الحاسوب عبر شبكة الإنترنت ويقوم بهذه العملية شخص أو مجموعة من الأشخاص لديهم خبرة واسعة في برامج الحاسوب، إذ يمكنهم بواسطة برامج مساعدة اختراق حاسوب أخر والتعرف على محتوياته.

الجريمة الإلكترونية: بأنها "كل فعل غير مشروع صادر عن إرادة آثمة يقرر له القانون عقوبة أو تدبيرًا احترازيًّا، وتعتمد الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، على المعلومة بشكل رئيس." (الكعبي ،٢٠٠٥، ص ٣٢)

الاحتيال الإلكتروني (التصيد الاحتيالي): هو نوع من أنواع الجرائم الإلكترونية. يستخدمه مجرمون لاستدراج مستخدم شبكة الإنترنت للكشف عن معلومات شخصية حتى يتمكن هؤلاء المجرمون من استغلالها لصالحهم. (المهندس. ٢٠١٦).

وفي ضوء ذلك تعرف الباحثة الجريمة الإلكترونية بأنها: أي شكل من أشكال الجرائم المعروفة في قانون العقوبات طالما كانت مرتبطة باستخدام وتوظيف تقنية المعلومات.

حدود البحث search limits:

تقتصر حدود الدراسة على ما يلي:

الحدود الموضوعية: وتتمثل في الكشف عن قياس مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينه جدة)

الحدود المكانية: سوف تجرى الدراسة فى المدارس الحكومية مع التركيز على معلمات الحاسب الآلي للمرحلة الثانوية التابعة لإدارة جدة.

الحدود الزمانية: تم تطبيق الدراسة خلال الفصل الثاني من العام الدراسي ٢٠١٩-٢٠٢٠ م.

الحدود البشرية: اقتصرت الدراسة على عينه من معلمات للمرحلة الثانوية تخصص (حاسب الي) من ادارة تعليم جدة.

الإطار النظري:

يتناول الفصل الحالي الإطار النظري للبحث متضمناً الأدبيات والدراسات والبحوث السابقة، حيث يشمل على مفهوم الأمن السيبراني، وأهميته، والعوامل المؤثرة فيه وطرق تنميته وأهمية الوعي بالأمن السيبراني لدى المعلمات.

المحور الأول: الأمن السيبراني:

مفهوم الأمن السيبراني:

الأمن السيبراني عبارة عن مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به و سوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني، كما أن الأمن السيبراني هو سلاح استراتيجي بيد الحكومات والإفراد لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول(جريدة المواطن، ٢٠١٧)

الفرق بين مفهوم أمن المعلومات والأمن السيبراني:

يتقاطع مجالا أمن المعلومات والأمن السيبراني من جهة الاهتمام بأمن المعلومات الإلكترونية "السايبري"ة، فالأمن السيبراني يعتني بأمن كل ما يوجد بالسايبر ومن ضمنه "أمن المعلومات" بينما يهتم مجال أمن المعلومات بأمن المعلومات وإن كانت على السايبر، وعلى الرغم من الاتفاق المذكور آنفاً بين المجالين إلا أن هنالك نقاط اختلاف جوهرية بين المجالين، وبصورة أكثر تحديداً تستطيع أن تلاحظ الفروقات التالية:

- الأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا تهتم بذلك.
- أمن المعلومات يهتم بأمن المعلومات الفيزيائية "الورقية" بينما لا يهتم الأمن السيبراني بذلك (الطيب، ٢٠١٨).
- كما يشير (المبارك، ٢٠١٦) إلى أن مفهوم Cyber Security هو مفهوم أوسع من أمن المعلومات ويتضمن تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية أو الخارجية والتي يتم تخزينها في خوادم داخل أو خارج الشركة من الاختراقات، كما أن مفهوم Information Security هو حماية المعلومات أو أنظمة المعلومات من النفاذ غير المصرح أو السرقة أو التعديل أو التشهير لحفظ سرية وخصوصية العملاء وبقاء المعلومات محفوظة وفقاً لنهج CIA.

أهمية الأمن السيبراني:

احتلت أبحاث ودراسات آمن المعلومات مساحة واسعة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة، بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات.

ومن عناصر الأمن السيبراني الواجب توافرها لضمان الحماية الكافية للمعلومات.

أولاً: السرية والآمن:Confidentiality وتعني التأكد من أن المعلومات لا تكشف ولا بتطلع عليها من قبل أشخاص غير مخولين بذلك.

ثانيًا: التكاملية Integration وسلامة المحتوى:Content integrity وهو التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله، وعلى نحو خاص لم يتم تدميره أو تغييره أو العبث به

فـي آيـة مرحلـة مـن مراحـل المعالجـة أو التبـادل، سـواء فـي مرحلـة التعامـل الـداخلي مـع المعلومات أو عن طريق تدخل غير مشروع.

ثالثًا: استمرارية توفر المعلومات أو الخدمةContinuation : إذ يجب التأكد من استمرار عمل النظـام المعلومـاتي واسـتمرار القـدرة علـى التفاعـل مـع المعلومـات وتقـديم الخدمـة لمواقـع المعلوماتية، وأن المستخدم لن يتعرض إلى منع الاستخدام أو الدخول إلى النظام.

رابعًا: عدم إنكـار التصـرف المرتبط بالمعلومـات ممن قـام بـه: ويقصد بـه ضمان إنكـار الشخص المتصل بالمعلومات أو مواقعها بقيامه بتصرف ما، بحيث تتوافر قدرة إثبات هذا التصرف وأن شخصا ما في وقت معين قد قام بـه، كذلك عدم قدرة مستلم رسـالة معينـة علـى إنكـار استلامه لهذه الرسالة.

العوامل التي تؤثر على الأمن السيبراني:

أولاً: الابتزاز الإلكتروني:

تأثرت جريمة الابتزاز الالكتروني بالتقدم العلمي والتكنولوجي المعاصر، وبرزت أساليب إجرامية بتقنيات لم تكن معروفة من قبل وطوعت التقنيات الحديثة لارتكاب الجريمة في مراحلها المختلفة من تخطيط وإعداد وتنفيذ وتضليل وتمويه للإفلات من العدالة فاستخدمت الأجهزة والأدوات والتقنيات الحديثة في ارتكاب الجرائم التي تميزت بالعنف، ويصاحب التقدم العلمي والتكنولوجي ظهور أنماط من الجريمة لم تكن معروفة من قبل، ويأتي في مقدمتها الدخول غير المشروع على شبكات الحاسب، ونظم المعلومات ونشر الفيروسات وإتلاف البرامج، وتزوير المستندات ومهاجمة المراكز المالية والبنوك، التي تؤدي إلى الحروب الإلكترونية، والإرهاب الإلكتروني ونشر الشائعات والأكاذيب، إضافة إلى نشر الرزيلة والإباحية، وغيرها من الجرائم الإلكترونية.

ويعرف الابتزاز الإلكتروني بأنه استخدام وسائل التقنية الحديثة للحصول على مكاسب مادية أو معنوية عن طريق الإكراه من شخص أو أشخاص أو حتى مؤسسات، ويكون ذلك الإكراه بالتهديد بفضح سر من أسرار المبتز بعد أن ينشب الجاني أنيابه على الضحية ويتمكن من جمع صور قد تكون فاضحة أو حتى مقاطع مصورة يكون مقابل عدم الفضيحة مبلغ مالي ضخم وإلا نشر الصور والفيديوهات (البادي، ٢٠١٧).

أسباب الأبتزاز الإلكتروني:

تُصنف بعض الأدبيات (الترتوري، ٢٠٠٦، طه، ١٩٩٠؛ اللبان، ٢٠٠٠) الدوافع المختلفة للجريمة الالكترونية بصفة عامة والابتزاز الالكتروني بصفة خاصة.

دوافع نفسية: يأتي العامل النفسي في المقام الأول بالنسبة للدوافع، فالشخص الذي يكون في صحته النفسية خللا واعتلال؛ تجده غير منضبط في التصرفات والأفعال، ولا يبالي بالنتائج المترتبة على ما يفعل لأنه لا يعتبر بمبدأ الموازنة وقياس الأمور قبل فعلها والشروع فيها، ولا يعتبر بالمحاذير الدينية أو القانونية أو العرفية، بل يعمل ما يحلو له ويراه هو المناسب ولو عارضه جميع أهل الأرض في ذلك.

دوافع جنسية: تتحول الدوافع الجنسية غير المنضبطة إلى قائد لصاحبها في غير هدى منه أو روية، بل كل همه هو إشباع رغباته التي لا تنتهي، ويزداد الأمر سوءا عندما لا يقنع بما ألفه وتعود عليه من مناظر جنسية بل يريد التوسع في ذلك والحصول على وجوه جديدة وأشخاص قريبين إليه وبالتالى يحاول قدر المستطاع في الاختراق أو التجسس على من يقع عليهم اختياره ليفوز بما يصبو إليه من المتعة المحرمة.

دوافع عقائدية: أن العقيدة من أقوى الدوافع والقوى المحركة للأشخاص، والتي بها يكون لدى الإنسان الاستعداد للتخلي عن الحياة بأسرها، فما هو الظن بما هو أيسر من ذلك.

دوافع عنصرية: ومن الدوافع أيضا الدوافع العنصرية، والتي تميز بين عنصر وآخر أو قبيلة أو عرق وبين آخرين، حيث تجد أن هناك بعض القبائل أو الأعراق لا يحبون القبيلة الأخرى أو العرق الآخر فتجد بعضهم يحاول عمل أعمال تخريبية من شأنها جر مشاكل على القبيلة أو العرق الأخر سواء باستخدام التدمير أو الابتزاز الإتلاف أو نشر الشائعات والأكاذيب أو غيره من طرق وأنواع الجرائم المعلوماتية.

والجدير بالذكر، أن المملكة العربية السعودية كانت أول دولة عربية سنت نظامًا خاصًا لمكافحة الجريمة الإلكترونية، تلتها الإمارات العربية المتحدة، وبعد ذلك سلطنة عمان، غير أن الطبيعة الوطنية لهذه الأنظمة من جانب، والثغرات القانونية الموجودة بها من جانب آخر، تجعلنا ندعو إلى سن نظام قانوني دولي يأخذ في اعتباره السمة الإفتراضية التي تتم فيها تلك الجرائم، يكون مبنياً على قاعدة معلومات موثقة شاملة، وتدعيم أجهزة الأمن بما فيها الشرطة الجنائية الدولية "الإنتربول" بكافة المعطيات اللازمة لتكوين خبراء مختصين في التقنية الإلكترونية(العباس، ٢٠١٥).

وفي هذا الصدد يشير البحث الحالي إلى ضرورة تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية؛ وخصوصا الإنتربول؛ وفي هذا المقام من الممكن أن تنضم الدول العربية إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الانترنت وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية والانترنت والعمل على دراسة ومتابعة المستجدات على الساحة العالمية.

إحصائيات الجرائم الإلكترونية في العالم:

إن دول الخليج المراتب الأولى في هذا النوع من الجرائم حيث يقدر خبراء في التكنولوجيا، أن هناك ٣٠ ألف جريمة ابتزاز إلكتروني على مستوى دول الخليج وحدها سنوياً، و٨٠% من الضحايا هن من الإناث، ووفقاً لمسؤولين خليجيين، فإن ٥٠% من المشتركين في شبكات التواصل الاجتماعي يستخدمون غرف المحادثة، ما يجعل عدداً كبيراً منهم عرضة للابتزاز وبالأخص الجنسي (قاسمي، ٢٠١٨).

رصدت الأجهزة المختصة نحو مليوني جريمة إلكترونية سجلها عام ٢٠١٥ م فيما يتعلق بقضايا الابتزاز الإلكتروني وقرابة ٣٠ ألف خليجي تعرضوا للابتزاز الإلكتروني عن طريق البرنامج المرئي سكايب، ووسائل التواصل الأخرى، فيما ركز آخرون على غياب الخصوصية وتلاعب بعض العاملين في محال الهواتف المتحركة بفيديوهات وصور هواتف زبائنهم، وسجلت القيادة العامة لشرطة دبي سابقاً ١٣ جريمة ابتزاز بمقاطع جنسية مخلة، نفذها أشخاص من خارج الدولة ومن خلال اصطياد ضحايا من كبار الموظفين عبر الإنترنت، وابتزازهم مادياً بعد الإيقاع بهم وتصويرهم في أوضاع مخلة(مرسي، ٢٠١٧).

ثانياً: التنمر الالكتروني:

مع التطور التكنولوجي ظهر ما يسمى بالتنمر الإلكتروني (bullying – Cyber) والذي يكون عادة عن طريق وسائل التواصل الاجتماعي والذي يهدف للإيذاء من خلال شبكات تكنولوجيا المعلومات بطريقة متكررة ومتعمدة، ويعرفه القانون الأمريكي بأنه قد يحدث عن طريق إرسال الشائعات عن شخص ما في الإنترنت بقصد تكريه الناس به أو ربما يصل لدرجة انتقاء ضحايا ونشر مواد لتشويه سمعتهم وإهانتهم. يمكن عمل ذلك من خلال الرسائل النصية،

الصور والرسومات، مقاطع الفيديو، المكالمات الهاتفية، البريد الإلكتروني، غرف المحادثة، المحادثة الفورية والمواقع الإلكترونية ومواقع التواصل الاجتماعي (علون، ٢٠١٦).

والتنمر هو إيقاع الأذى الجسمي أو النفسي أو العاطفي أو المضايقة أو الإحراج أو السخرية من قبل إنسان متنمرٍ على إنسان آخر أضعف منه، أو أصغر منه أو لأي سبب من الأسباب وبشكل متكرر والفرد المتنمر هو الذي يضايق، أو يخيف، أو يهدد (Jaana,2011)، او يؤذي الآخرين الذين لا يتمتعون بنفس درجة القوة التي يتمتع بها، وهو يخيف غيره من الطلاب في المدرسة، ويجبرهم على فعل ما يريد بنبرته الصوتية العالية واستخدام التهديد (الصبيحين والقضاة، ٢٠١٣، ٣٦).

ثالثًا: الجرائم الالكترونية:

يعرفها الكعبي (٢٠٠٥، ٣٢) على أنها "كل فعل غير مشروع صادر عن إرادة آثمة يقرر له القانون عقوبة أو تدبيراً احترازياً، وتعتمد الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، على المعلومة بشكل رئيسي، وهذا الذي أدى إلى إطلاق مصطلح "الجريمة المعلوماتية" على هذا النوع من الجرائم.

ويمكن القول بأن الجريمة الإلكترونية باعتبارها مظهرًا جديدًا من مظاهر السلوك الإجرامي لا يمكن تصورها إلا من خلال ثلاث مظاهر، إما أن تتجسد في شكل جريمة تقليدية يتم اقترافها بوسائل إلكترونية أو معلوماتية، أو في شكل استهداف للوسائل المعلوماتية ذاتها و على رأسها قاعدة المعطيات و البيانات أو البرامج المعلوماتية، أو أن يتم اقتراف الجرائم العادية في بيئة إلكترونية كما هو الأمر بالنسبة لجرائم الصحافة (اللمتوني، ٢٠١٤، ٤٨).

الآثار الاجتماعية والنفسية للجرائم الإلكترونية:

مجمع التكنولوجيا والإنترنت شبيه بالمجتمع الإنساني الذي يوجد فيه أطياف مختلفة من الناس أكثرهم الأسوياء ولكن يوجد منهم ذوي الأخلاق السيئة، والطفل المراهق teenager يكون متشوقًا لاكتشاف العوامل الجديدة التي يدخلها وهو ما قد يجعله عرضة للجرائم والاستغلال والتحرش ووسيلة للتجسس على أسرته لذلك يحتاج الأطفال والمراهقون إلى مراقبة الوالدين للتأكد من أن تجربتهم مع العالم التخيلي cyberspace تجربة مفيدة وبناءة ومن دون مشاكل، وبالرغم من حدوث بعض مشاكل الإساءة وسوء المعاملة abuse عبر الإنترنت فإن الحالات المبلغ عنها تعتبر قليلة وربما هناك العديد من الحالات التي لا يعلم الوالدان بحدوثها لأن الطفل لا يتحدث بها أمام والديه أو يعلم الوالدان بها ويكتفيان بتوجيه الأطفال ونصحهم أو منعهم من استخدام الشبكة لفترة معينة دون التبليغ عن الحوادث إلى الجهات المسؤولة، ونظرًا لكثرة المشاكل التي تتزايد مع المراهقين فقد تم إنشاء موقع خاص للتبليغ عن المراهقين المفقودين ويحوي نصائح للسلامة خاصة للمراهقين وكيفية تعاملهم مع التكنولوجيا(ابن عسكر، ٢٠١٢، ٣٢).

وتؤكد دراسة قام بإجرائها كل من: كراوت وآخرون (1998) Kraut الكشف عن الآثار السلبية الناتجة عن تعرض الأشخاص لجرائم الانترنت والاستخدام الكثيف للإنترنت على البناء العاطفي السوي وعلى المشاركة الاجتماعية للذين يستخدمون الإنترنت، تكونت عينة الدراسة من (١٦٩) فردا من (٧٣) عائلة أمريكية ممن لم يمض على اشتراكهم في الإنترنت أكثر من سنتين، إذ أشارت نتائج الدراسة إلى أن التعرض للجرائم المعلوماتية يقلل قنوات الحوار بين أعضاء الأسرة الواحدة، ويقلص عدد الأصدقاء، ويرفع حالة الاكتئاب والوحدة لدى المستخدمين.

كما أن الجريمة الالكترونية تتميز بعدة خصائص لعل من أبرزها ما يلي (جواد، ٢٠١٥، ٢٩):

- في الغالب لا يتم الإبلاغ عن جرائم الأنترنت، وذلك إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير، لذا نجد أن معظم جرائم الأنترنت تم اكتشافها بالمصادفة بل وبعد وقت طويل من ارتكابها بالإضافة إلى أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة، والعدد الذي تم اكتشافه هو رقم خطير وبعبارة أخرى الفجوة بين عدد هذه الجرائم الحقيقي، وما تم اكتشافه فجوة كبيرة.
- من الناحية النظرية يسهل ارتكاب الجريمة ذات الطابع التقني، كما أنه من السهل إخفاء معالم الجريمة، وصعوبة تتبع مرتكبيها.
- هذه الجرائم لا تترك أثرا لها بعد ارتكابها، علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت، فليست هناك أموال أو مجوهرات مفقودة وإنما هي أرقام تتغير في السجلات ولذا فإن معظم جرائم الأنترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابه.
- تعتمد هذه الجرائم على ذكاء مرتكبيها ويصعب على القانون والمحقق التقليدي التعامل مع هذه الأنواع من الجرائم إذ يصعب عليه متابعة جرائم الأنترنت والكشف عنها، فهي جرائم تتسم بالغموض والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية.
- الوصول للحقيقة يستوجب الاستعانة بخبرة فنية عالية المستوى في مجال تقنيات الحاسوب والشبكات الأنترنت.

طرق تنمية الأمن السيبراني:

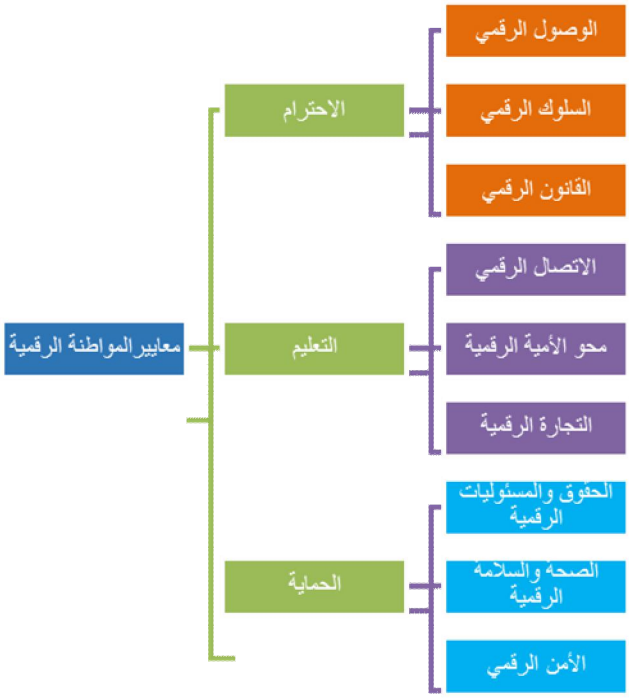
أكدت كثير من الدراسات التي تناولت الأمن السيبراني إلي ضرورة توعية المستخدمين لشبكات المعلومات، ونظمها بطرائق المحافظة علي المعلومات، و عليه فقد اهتم كثير من الباحثين في مجال دراسات الأمن الرقمي بهذا الموضوع، فتناولوا طرق تنمية الأمن السيبراني لدى المستخدمين، وضرورة إكساب مستخدمي المعلومات المهارات اللازمة للحفاظ علي معلوماتهم وضمان حمايتها، ويمكن تناول تلك الطرق بمزيد من التفصيل كما يلي:

التدريب على المواطنة الرقمية:

المواطنة الرقمية: هي مجموعة القواعد والضوابط والمعايير والأعراف والأفكار والمبادئ المتبعة في الاستخدام الأمثل والقويم للتكنولوجيا الرقمية، والتي يحتاجها المواطنون صغاراً وكباراً أثناء التعامل مع تقنياتها من أجل استخدامها بطريقة مناسبة وآمنة وزكية، وبما يؤدى إلى المساهمة في رقي الوطن، ومن خلال عمليات الإتاحة العادلة ودعم الوصول الإلكتروني، والتوجيه، والحماية، توجيه نحو منافع التقنيات الحديثة، وحماية من أخطارها (الدهشان والفويهي، ٢٠١٥، ١٠-١١).

معايير المواطنة الرقمية:

تتفق عدة دراسات ومنها (الدوسري، ٢٠١٧)؛ المسلماني، ٢٠١٤)؛ (الجزار، ٢٠١٤) على مجموعة من المعايير التي تشكل أساس الاستخدام الملائم للتقنية، وتوفر نقطة انطلاق لمساعدة جميع مستخدمي التقنية على فهم أساسيات المواطنة الرقمية، ويمكن عرض تلك المعايير كما في الشكل التالي:



شكل رقم (١) معايير المواطنة الرقمية

ثالثاً: الهندسة الاجتماعية:

مصطلح الهندسة الاجتماعية اسم يوحي في ظاهره أنه من أشكال الهندسة المحمودة التي عمرت البشرية علما ونفعا بينما هو في الحقيقة خطر محدق على المعلومات الشخصية للمواطن كفرد وأمن معلومات القطاع الحكومي والخاص (أحمد، ٢٠١٤، ٢٢-٢٣)؛ كما يمكن تعريف الهندسة الاجتماعية باختصار بأنها التلاعب بالبشر وخداعهم بهدف الحصول على بيانات أو معلومات، كانت ستظل خاصة وآمنة ولا يمكن الوصول إليها، بهدف اختراق النظام (البوابة العربية للأخبار التقنية، ٢٠١٧).

أخطار ضعف الأمن السيبراني:

يمكن تصنيف أنواع المخاطر التي تتعرض لهم الأمن السيبراني إلى:

أولا :المخاطر الداخلية:

وهي أخطار من داخل نظام المعلومات، ومن الأمثلة عليها (محمد، ٢٠١٤)؛ (صالح، ٢٠١٦):

(١)الأخطاء البشرية:

تعد التهديدات البشرية لنظم المعلومات من أخطر التهديدات وأكثرها تأثيرا في تقدمها، حيث تتنوع أساليب التهديدات البشرية وتشمل الأفعال المقصودة وغير المقصودة من قبل المستخدمين المخولين وغير المخولين باستخدام النظام، وعلى واضعي السياسات الأمنية بذل أقصى جهد لتقليل هذا النوع وتقليصه وتحديد المسؤولية في حال حدوث مثل هذا النوع من المخاطر فعلى سبيل المثال يجب أن يكون الوصول إلى المعلومات من قبل المستخدمين مبنيا لتجنب هذا النوع من الأخطاء: إيقاف حساب المستخدمين الذين يذهبون في أجازه أو إلغاؤه في حال تركهم للعمل.

ومن هذه المخاطر، ما يأتي:

- أخطاء إدارة النظام وتعني الأخطاء التي تحدث في أثناء التركيب أو الإدارة أو تشغيل نظم المعلومات والحاسوب.
- خطا مشغل الحاسوب الشخصي بشطب الملفات عن طريق الخطأ، أو عدم الاحتفاظ بنسخ احتياطية للرجوع إليها عند حدوث مشكلة ما.
- الإهمال المقصود بترك المعلومات في متناول الأيدي.
- خطأ في برمجة النظم وتصميم قواعد البيانات.
- الاستخدام غير المخول للنظم والإفصاح عن معلومات العملاء.
- الاحتياط والتلاعب وإساءة الاستخدام.
- سرقة موجودات الحاسوب مع أجهزة وبرامج وبيانات.
- التخريب المعتمد للبرامج والأجهزة.

(٢) **خلل في المعدات**: ويتضمن أعطال أجهزة الحواسيب والطرفيات ووسائط الربط ومن أهم الأسباب التي تؤدي إلى تعطل المعدات مشكلات الكهرباء، والتكييف والتهوية والرطوبة والتدفئة وتسرب السوائل. ومن ضمن مشكلات المعدات أيضا مشكلة عدم توافقها فعلى سبيل المثال تبين أن استخدام بطارية سانيو في جهاز انتل المحمول قد يؤدي إلى التسبب بخلل في دوائره: مما أدى إلى اشتعال النار.

(٣) **أخطاء في البرمجيات:** بما أنه لا توجد طريقة مؤكدة تثبت أن البرنامج يعمل بدقة متناهية تحت كل الظروف، فإن هناك أخطاء محتملة من البرمجيات تؤدي إلى النتائج غير النتائج المتوقعة أو المطلوبة، ومن الأمثلة ذلك بعض المشكلات التي قد تواجهها في أثناء استخدامك لبرنامج المايكروسوفت أوفيس، مثل مشكلة الهوامش، حيث يقوم المستخدم بتحديد هوامش معينة للصفحة والطباعة لا تكون كما تم تحديده.

(٤) أخطاء في البيانات: بما أن المعلومات التي نحصل عليها من نظم المعلومات تأتي من معالجة البيانات التي يتم إدخالها، فإن صحة المعلومة تعتمد على صحة البيانات التي يتم إدخالها.

(٥) **نقاط الضعف أو الثغرات:** وتعني عنصرا أو نقطة أو موقعا في النظام يحتمل أن ينفذ من خلاله المعتدي أو يتحقق بسببه الاختراق، فمثلا يعد الأشخاص الذين يستخدمون النظام نقطة ضعف إذا لم يكن تدريبهم كافيا لاستخدام النظام وحمايته، وقد يكون الاتصال بالإنترنت نقطة ضعف إذا لم يكن الموقع المكاني للنظام نقطة ضعف إذا لم يكن مجهزا بوسائل الوقاية والحماية عموما، فأن نقاط الضعف هي الأسباب المحركة لتحقيق التهديدات أو المخاطر، ويرتبط هذا الاصطلاح باصطلاح وسائل الوقاية، وتعني الطريقة المتبعة لحماية النظام، مثل: كلمات السر والإقفال ووسائل الرقابة وحواجز العبور وغيرها.

ثانياً: المخاطر الخارجية:

قد يتعرض النظام إلى أخطار من خارج نظام المعلومات، ومن الأمثلة عليها:

أخطار الكوارث الطبيعية:

وتتضمن الكوارث الطبيعية، ومن الأمثلة عليها: الهزات الأرضية، والزوابع، والفيضانات التي يمكن أن يقضي حدوثها على المعدات والبرمجيات ووسائط الاتصال، وقد لا تكون أساليب الحماية كافية كحالات الهزات الأرضية والبراكين، إلا أنها قد تخف من الأضرار المترتبة على ذلك.

طرق الوقاية من أخطار ضعف الأمن السيبراني:

هناك عدة طرق للوقاية من ضعف الأمن السيبراني، ومنها:

أولا :تدريب المستخدمين:

يجب تأهيل المستخدمين وتوعيتهم وتدريبهم على استخدام نظم المعلومات التي تتمتع بمزايا الأمن والسرية؛ لما لذلك من أهمية في الحفاظ على أمن المعلومات وسريتها وحماية المستخدمين أنفسهم من الوقوع في المحظور دون قصد، وعلى المؤسسة وضع التوجيهات الكافية لضمان وعي عام ودقيق بمسائل الأمن، بل أن المطلوب بناء ثقافة الأمن لدى العاملين والتي تتوزع بين وجوب مراعاة أخلاقيات استخدام التقنية بين الإجراءات المطلوبة من العاملين لدى ملاحظة أي خلل، كما أن عليها تحديد ما يتعين على المستخدمين القيام به وما يحظر عليهم القيام به في معرض استخدام للوسائل التقنية المختلفة(الدباغ، ٢٠١٢، ١٢٣):

ثانيا :تأمين وتحديد إمكانية الوصول إلى النظام:

إن الدخول إلى أنظمة الشبكة الحاسوب وقواعد البيانات ونظم المعلومات ومواقع المعلوماتية عموما، يمكن تقييده بالعديد من وسائل التعرف إلى شخصية المستخدم وتحديد نطاق لاستخدام، وهو ما يعرف بأنظمة التعريف والتحويل، والتعريف أو الهوية مسألة تتكون من خطوتين، الأولى وسيلة التعريف بشخص المستخدم، والثانية قبول وسيلة التعريف أو ما يسمى التوثيق من صحة الهوية المقدمة (جمعة، ٢٠١٤، ٢٧):

وتختلف وسائل التعريف تبعا للتقنية المستخدمة، وهي نفسها وسائل أمن الوصول إلى المعلومات أو الخدمات في قطاعات استخدام النظم أو الشبكات أو قطاعات الأعمال الإلكترونية، وعلى نحو عام، فأن هذه الوسائل تتوزع إلى ثلاث أنواع، وهي:

١- شيء ما يملكه الشخص، مثل بطاقة الصراف الآلي أو غير ذلك.

٢- شيء ما يعرفه الشخص، مثل كلمات السر أو الرقم الشخصي أو غير ذلك.

٣- شيء ما يرتبط بذات الشخص أو موجودة فيه، مثل بصمة الإصبع أو بصمة العين والصوت أو غيرها (المركز الديموقراطي العربي، ٢٠١٥).

ثالثاً: النسخ الاحتياطية:

وتتضمن عملية النسخ الاحتياطية عمل نسخ إضافية من البيانات والمعطيات الخاصة بنظم المعلومات أو الحالة التقنية للنظام ككل، من مثل حسابات المستخدمين وكلمات المرور الخاصة بهم وبريدهم الإلكتروني والبيانات المخزنة على إحدى وسائط التخزين سواء داخل النظام أو خارجه وفقا لجدول زمني معين تحدده المؤسسة، وتخضع عمليات الحفظ إلى قواعد يتعين أن تكون محددة سلفا وموثقة ومكتوبةً ويجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية.

رابعًا :أمن الوقاية من الفيروسات:

فهناك إجراءات وقائية عدة يعني تطبيقها المؤسسة في كثير من العواقب الوخيمة التي قد تترتب على الإصابة بالفيروسات (بطوش، ٢٠٠٨؛ وهدان، ٢٠١٢):

-الاحتفاظ بسجل لكل عمليات التعديل في برامج التطبيقات بحيث يتم تسجيل وقائع نقل البرامج المعدلة جميعها إلى البيئة الإنتاجية، وبخاصة تلك البرامج التي يتم الحصول عليها من خارج المؤسسة.

-تثبيت برنامج التحقق من وجود فيروسات على أنا يكون هذا البرنامج موجودا دائما في الذاكرة وتقوم هذا البرنامج بالتأكد من عدم وجود الفيروسات المعروفة لها ويجب تحديثها

باستمرار لكي يكون لها القدرة على مواجهة الفيروسات الجديدة وبعض هذه البرامج يقوم بمقارنة محتويات بعض مناطق القرص (الصلب أو اللين) أو بعض مناطق الذاكرة بمحتوياتها المتوقعة والمفترض أن توجد فيها.

-تجهيز نسخ احتياطية من البرمجيات وحفظها بحيث يمكن استرجاع نسخة نظيفة (غير ملوثة بالفيروس) من البرامج عند الحاجة.

-توعية المستخدمين بعدم تحميل أي برنامج غير موثوق المصدر في حساباتهم الشخصية، فهذا أوسع الأبواب لإدخال الفيروسات إلى النظم التي عند دخولهما ربما تصيب الأقراص والأجهزة جميعها التي في الشبكة.

-يجب أن يتم فحص البرمجيات أو اختيارها قبل السماح بنشرها في المؤسسة للاستخدام العام، على جهاز مستقل غير مرتبط بالشبكة. ويجب أن يتضمن الاختبار البحث عن أي سلوك غير مفهوم في البرنامج كأن يخرج رسائل لا داعي لها على الشاشة مثلا، ولو أن خلو البرنامج من مثل هذا السلوك غير المفهوم لا يعني بالضرورة نظافة البرنامج، فالفيروسات تظل كامنة ولا تكشف عن سلوكها إلا في اللحظة المناسبة.

خامساً :الجدار الناري:

تسريع أداء الجدران النارية وتقديم خدماتها بل وأيضًا في تضمينها قدرات متعددة تفوق ما كان متوفرا في تلك الأيام، وتتمثل هذه القدرات بما يلي (Sheikli,2014):

- التحقق من هوية المستخدمين: ذلك أن أول ما اضافة المطورون إلى الجدران النارية الأولى كانت القدرات القوية للتحقق من الهوية، وإذا كانت السياسيات الأمنية التي تتبعها المؤسسة تسمح بالنفاذ إلى الشبكة من شبكة خارجية، مثل الإنترنت، فإنه لابد من استخدام ميكانيكية ما للتحقق من هوية المستخدمين.

-الشبكات الافتراضية الخاصة: أما الإضافة الثانية إلى الجدران النارية للإنترنت فكانت التشفير البيني للجدران النارية firewall- to firewall وكان أول منتج من هذا النوع هو Ans interlock، وهذه المنتجات هي ما ندعوها اليوم بالشبكات الافتراضية الخاصة virtual private networks.

-مراقب المحتوى Content Screening وخلال الفترة الأخيرة أصبح من الشائع استخدام الجدران النارية كأدوات لمراقبة المحتوى الوارد إلى الشبكة.

-ومن بعض الإضافات التي وضعت في برمجيات الجدران النارية هي البحث عن الفيروسات، ومراقبة عناوين الإنترنت، منع برمجيات جافا، وبرمجيات فحص ومراقبة الكلمات السرية.

سادسا :التشفير:

يعد التشفير بوجه عام وتطبيقاته العديدة وفي مقدمتها التواقيع الإلكترونية، الوسيلة الوحيدة تقريبا لضمان عدم إنكار التصرفات عبر الشبكات الإلكترونية، وبذلك فأن التشفير يمثل الاستراتيجية الشمولية لتحقيق أهداف الأمن من جهة، وهو مكون رئيس لتقنيات ووسائل الأمن الأخرى، خاصة فى بيئة الأعمال الإلكترونية والتجارة الإلكترونية والرسائل الإلكترونية وعموما البيانات المتبادلة بالوسائط الإلكترونية.

وسائل حماية الوصول إلى المعلومات:

تُعد كلمة المرور من أضعف الوسائل المستخدمة لتحديد هوية المستخدم، وضمان عدم وصول غير المخولين للمعلومات، وذلك لإمكانية التعرف إليها، فغالباً ما يميل الإنسان إلى اختيار

كلمات مرور سهلة التذكر، بينما توفر السمات الحوية طرائق آمنة للتوثيق و تحديد الهوية، إذ تستخدم هذه الخصائص الفسيولوجية للإنسان من أجل توثيق هويته، و من أمثلة هذه الخصائص (فكري، ٢٠١٤، ١٨٣):

- بصمة الصوت :تقوم هذه التقنية على تسجيل صوت الشخص المتحدث وتحليل نبرته.
- بصمة العين :تستخدم هذه التقنية (كاميرا فيديو) لالتقاط الأنماط المعقدة للأنسجة في القزحية أو الأوعية الدموية في شبكية العين. ويندرج تحت هذه التقنية نوعان: بصمة قزحية العين، بصمة شبكية العين.
- بصمة الأصبع :تعمل هذه التقنية على تحليل خصائص بصمة الأصبع ومقارنتها لكونها تختلف من شخص إلى آخر، ولا يمكن أن تتكرر عند شخصين.
- بصمة الوجه :تحلل تقنية التعرف إلى الوجه سمات وجه الشخص التي لا تتغير بسهولة باستخدام (كاميرا فيديو) رقمية.
- هندسة اليد :تعتمد تقنية هندسة اليد على التقاط صورة ثلاثية الأبعاد لليد وتحليل شكلها من حيث طولها، ومواقع الأصابع و المفاصل.. وغيرها من الخصائص، ثم حفظها في قاعدة البيانات.

الوعي بأهمية الامن السيبراني وأهميته لمعلمات الحاسوب:

يرى الصوفي (٢٠١٢، ١٧) إلى أن الأهمية المتزايدة للحديث عن عصر المعلوماتية، ودور التكنولوجيا في العملية التعليمية ناتج عن الأسباب الآتية:

- لا يوجد أي نظام يمكن أن يكتفي بالوسائل التقليدية دون تغيير، فالتغيير يتطلب القدرة على التفكير، والمراجعة، والمرونة، والقدرة على الاستيعاب.
- الانفجار المعرفي الذي يواجه هذا العصر، فقد زاد نمو المعارف بشكل مضاعف وأستحدث كثير من التعريفات.
- يواجه التعليم تحدياً خطيراً من جانب وسائل الإعلام والاتصال بفضل ما حدث فيها من ثورة واسعة نتيجة التطور التكنولوجي، فهذه الوسائل سريعة الحركة، وهذا يحتم على المعلم تجديد نفسه وعلمه بهذه الوسائل واستخدامها ونقل هذا إلى طلابه.
- ينتظر المجتمع الحديث من المعلم أن يكون قادرا على التطوير والإبداع والتفكير الخلاق، إذ إن المجتمع لا يحتاج إلى المعلم التقليدي الذي تعود تكرار نفسه ومعارفه وخبراته، فقد ثبت أن الطرائق التكنولوجية المبرمجة للتعلم تنمي القدرة على التفكير الإبداعي بدرجة أكبر من الطرائق التقليدية.

وإذا كان التدريب على الأمن السيبراني ضرورة في المؤسسات التعليمية؛ فإن تدريب معلمي ومعلمات الحاسب عليه من الضروريات للحفاظ على نظام المعلومات داخل المدرسة ومما يؤكد ذلك ويدعمه دراسة المطيري(٢٠١٥) والتي هدفت إلى تقييم الأداء التدريسي لمعلمات الحاسب الآلي في المرحلة المتوسطة في ضوء معايير الجمعية العالمية للتقنية في التعليم(ISTE)، إذ قامت الباحثة بإعداد قائمة بمعايير الأداء التدريسي لمعلمات الحاسب مقننة للبيئة السعودية مكونة من ستة معايير هي: التمكن العلمي، والتخطيط الجيد للتدريس، وتوظيف بيئات تعلم وتعليم فعال، واستخدام استراتيجيات تعلم وتعليم ملائمة لأهداف وطبيعة منهج الحاسب، وتقويم تعلم وتعليم الطالبات، والتنمية المهنية، وبلغ عدد المؤشرات ٣٨مؤشراً، وقد كان أداء معلمات الحاسب الآلي المتصّلة بالمعايير الستة بشكل عام لم يحقق الحد الأدنى من الكفاية،

في حين حقق معيار التمكن العلمي الكفاية فقط، وقد أوصت الدراسة بأهمية المعايير لتقييم الأداء التدريسي للمعلمين ودعم التثقيف بها ونشرها.

وسعت دراسة (Lim et al., 2015) إلى تحديد كيفية تصميم وتنفيذ دورة إعداد المعلم قبل الخدمة في تقنية المعلومات والاتصال وأمن المعلومات، وفق الكفايات التعليمية في جامعة ميرلاند الصينية، واعتمدت على نظام التصميم التعليمي لتطوير الكفايات التعليمية لمعلمي الحاسب قبل الخدمة، وتم استخدام منصة التعلم عبر الإنترنت لتسهيل تبادل الخبرات في استخدام تكنولوجيا المعلومات والاتصالات للتعليم والتعلم، وتوصلت الدراسة إلى أن طرائق التدريس المبتكرة مع المحتوى وبدعم من المنصة عن بعد تعزز من فعالية الكفايات التقنية في التعليم.

ثانياً: الدراسات السابقة والتعقيب عليها:

اطلعت الباحثة على العديد من الدراسات العربية والأجنبية المتوفرة في مجال الامن السيبراني. بالإضافة الى عدد من الدراسات في مجال أمن المعلومات فوجدت قلة في عدد الدراسات في هذا المجال فيما يتعلق بدور المعلمين والمعلمات لتوعية الطلاب بهذا المفهوم.

مدى إفادة البحث الحالي من الإطار النظري:

- بناء استبانة البحث الرئيسية والتأكد من صدقها وثباتها؛ حيث يمكن الإفادة منها في التعرف على كيفية إعداد أدوات جمع البيانات الخاصة بالبحث الحالي، بالاطلاع على أدوات القياس وأدوات المعالجة الخاصة بالدراسات السابقة بشكل إجرائي.
- كما استفاد البحث الحالي من الدراسات السابقة في تدعيم مشكلة البحث الحالي باعتبارها مبررات لإجراء البحث الأمر الذي يجعل البحث الحالي تلبية لما نادت به الدراسات والبحوث السابقة.

وبناءً على ذلك تم تقسيم الدراسات السابقة الى محورين حسب علاقتها بموضوع الدراسة كما يلي:

أولاً: الدراسات التي تتعلق بالأمن السيبراني:

هدفت دراسة جوران (Goran, 2017) بعنوان " Cyber Security Risks in Public High Schools: أخطار الأمن السيبراني في مدارس التعليم الثانوي " إلى تحليل مشاكل الأمن السيبراني في مدرسة ثانوية عامة واقتراح حلول عملية. وتم استخدام عينة من المدارس الثانوية واستخدام منهجية دراسة الحالة وكانت النتيجة هذه الورقة دراسة حالة عن مدرسة ثانوية حضرية وتدرس نقاط ضعفها أمام مختلف الهجمات الإلكترونية وذلك من خلال توضيح أخطار الهجمات الالكترونية وكيفية الوقاية منها.

هدفت دراسة الشمري، (٢٠١٥) بعنوان " رؤية استراتيجية لحماية الفضاء الالكتروني للمملكة العربية السعودية". الى بيان مفهوم الفضاء الإلكتروني وحدوده وخصائصه وتعريف الفجوة الإلكترونية واستعراض واقع الفضاء الالكتروني في المملكة العربية السعودية، وبيان أخطار الفضاء الالكتروني، وبيان وعي المسؤولين عن أمن المعلومات، واستجلاء المعوقات التي تحد من قدرة المملكة على مواجهه أخطار الفضاء الالكتروني، وقد استخدم الباحث المنهج الوصفي التحليلي وتحليل المضمون بالإضافة الى المنهج الاستقرائي الاستنباطي. وتوصلت الدراسة الى وجود بعض المخاطر التي تهدد الفضاء الالكتروني الخاص بالمملكة العربية السعودية، ومدى وعي المسؤولين عن أمن المعلومات بالمملكة بتلك المخاطر، وتوصلت كذلك إلى وجود الكثير من المعوقات التي تحد من قدرة المملكة على مواجهه تلك المخاطر.

هدفت دراسة (Minho٢٠١٧) ، بعنوان: تدريس الامن السيبراني للمراهقين والمراهقين غير الفنيين: Design Of Cyber Security Awareness Program For The First

Year Non-It Students" إلى تدريس الأمن السيبراني لدى الطلاب غير الفنيين. تكونت عينة الدراسة من (٢٥) من طلاب الجامعة. اشتملت الدراسة على برنامج منظم يهدف إلى تعريف الطلاب كيفية حماية خصوصياته وكيفية التصدي للهجمات الإلكترونية. وتوصلت نتائج الدراسة إلى كفاءة البرنامج المعد في تحسين الأمن السيبراني لدى عينة الدراسة.

هدفت دراسة (Nakama& Paullet , 2018) بعنوان " الضرورة الملحة للتعليم في مجال الأمن السيبراني: أثر الابتكار المبكر للكلية في المجتمعات الريفية في هاواي: " The Urgency for Cybersecurit Education Impact of Early College Innovation in Hawaii Rural Communities " إلى تعليم الطلاب عبر المراحل الدراسية بالجامعة كيفية التصدي للهجمات السيبرانية. فقد أشارت الدراسة إلى أن هناك مجموعة مهمة أخرى من المهارات المهمة في ديناميكيات الدورات الدراسية على الإنترنت في الكليات الجامعية الأولى للتغلب على قيودها السياقية: (١) تعلم كيفية التنقل في نظام إدارة التعلم، و (٢) إرسال وتلقي الرسائل بفعالية بين الطلاب وأعضاء هيئة التدريس. ساهمت الدراسة في إكساب الطلاب استراتيجيات التعلم عبر الإنترنت لأن الطلاب قد يشعرون أنه يعني أنهم غير قادرين على إكمال المهام الأكاديمية دون مساعدة، والتي يمكن أن تهدد القيمة الذاتية .ونتيجة لذلك، يفشل العديد من طلاب الجامعات في طلب المساعدة المطلوبة، معتبرين أنها محرجة، وقبول الهزيمة، وشيء يمكن تجنبه كلما أمكن. من خلال نجاح البرنامج فقد ساهمت الدراسة على تنمية الأمن السيبراني لدى طلاب الجامعة عبر المراحل الدراسية بها.

هدفت دراسة كوغلينج (Coughlin, 2017) بعنوان " تصميم برنامج للوعي بالأمن السيبراني لدى طلبة السنة الاولى بالجامعة للطلاب غير متخصصي تكنولوجيا المعلومات: Cybersecurity Education For Adolescents And Non-Technical Adults" إلى أخطار الأمن السيبراني التي يتعرض لها المراهقون وغير البالغين الراشدين، وتقييم الأساليب المتاحة التي يمكن من خلالها تدريبهم على أن يكونوا أكثر إدراكًا لقضايا الأمن السيبراني وتمكينهم من الدفاع عن أنفسهم ضد الهجوم بشكل أفضل. أشارت نتائج الدراسة إلى أن الطلاب يتعرضون للعديد من الهجمات الإلكترونية التي من شأنها أن تؤثر بالسلب على الطلاب. كما أشارت نتائج الدراسة إلى وجود مجموعة من الحلول التي يمكن من خلالها التصدي للهجمات الالكترونية.

هدفت دراسة (Pye,2016) بعنوان: تدريس الامن السيبراني بالصف الثاني عشر بالمدارس: Teaching Cybersecurity In K-12 Schools" إلى فحص الحاجة إلى التثقيف الأمني السيبراني المنفذة في صفوف الأطفال في المناهج الدراسية .k-12 وتمثلت تساؤلات الدراسة فيما يلي: ما هي المناهج الدراسية أو الإستراتيجيات التي تعتمد على المدرسة والتي تم تجربتها في تعليم الأمن السيبراني والسلامة والسلوك الأخلاقي فيK-12 ؟ ما هي بعض العوائق التي تحول دون تشكيل المناهج الدراسية وتكييفها وتنفيذها والتي تتناول الأمن السيبراني؟ كيف يمكن التغلب على العوامل التي تحد من استخدام المناهج الدراسية في مكافحة الأمن السيبراني؟ أشارت نتائج الدراسة إلى ضرورة تعليم الطلاب (K-12) الأمن السيبراني في المدارس الثانوية وتزوديهم بالتوجيهات واحتياجات السلامة في استخدام التكنولوجيا ويعد مسئولية المدرسة ، كما أشارت نتائج الدراسة إلى أن تعريض الشباب لقضايا الأمن السيبراني خلال سنوات تكوينهم يجعلها جزءًا لا يتجزأ من حياتهم.

ثانياً: الدراسات المتعلقة بوعي المعلمات بالأمن السيبراني وأمن المعلومات:

هدفت دراسة الغديان وآخرون (٢٠١٨) بعنوان " صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين " إلى الكشف عن أهم صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين .وتكونت عينة الدراسة من (٥٢٣) مستجيبا على أدوات الدراسة موزعين إلى ثلاث شرائح، حيث بلغ عدد أعضاء هيئة الأمر بالمعروف والنهي عن المنكر (٤٨) عضوا، بينما بلغ عدد المستشارين النفسيين (٤٨) مستشاراً، وكذلك بلغ عدد المعلمين والمعلمات (٣٦٨) معلما ومعلمه، تم اختيارهم عشوائيا. ولتحقيق أهداف الدراسة استخدم الباحثون ثلاثة مقاييس من إعدادهم تمثلت في مقياس صور الجرائم الإلكترونية، ومقياس دوافع الجرائم الإلكترونية، ومقياس الآثار النفسية للابتزاز الإلكتروني بعد التحقق من خصائصها السيكو مترية. وقد أشارت نتائج إلى وجود فروق ذات دلالة إحصائية في الدوافع المادية، والانفعالية، ودوافع التسلية بين المستشارين النفسيين، والمعلمين لصالح المعلمين، وبين المعلمين ورجال الهيئة لصالح المعلمين. أما الفروق في الدوافع الجنسية فكانت بين المعلمين ورجال الهيئة لصالح رجال الهيئة. وأخيرا بينت نتائج الدراسة أن هناك فروقا دالة إحصائيا في درجة تقدير الآثار النفسية لجرائم الابتزاز الإلكتروني تعزى لاختلاف فئة المستجيب (المعلمين والمعلمات، والمستشارين النفسيين)، وكانت الفروق بين المستشارين النفسيين والمعلمين لصالح المستشارين النفسيين.

وهدفت دراسة عبدالمجيد (٢٠١٨) بعنوان "الأمن الإلكتروني ضرورة ملحة لأمن المجتمعات: مقترح الأسرة الآمنة الخاص بتوعية المجتمع العربي الخليجي في أمن المعلومات لكل من الطلاب والوالدين " إلى الكشف عن عن دور الآباء والأمهات في حماية أبنائهم من خطر الاختراق والابتزاز الإلكتروني. فقد أجرت هذه الدراسة مقارنة بين كثير من الأسر الآباء والأمهات والأبناء التي حظيت بفرصة التأهيل المناسب لاستخدام هذه التقنيات، وبين تلك الأسر غير المدربة. وقد كانت هذه المقارنة من أجل معرفة دور الآباء والأمهات في حماية أطفالهم من الاختراقات الإلكترونية. وقد وجدت الدراسة أن هناك دورًا مهمًّا جِّدا للوالدين في حماية أطفالهم من التهديدات الإلكترونية، بما في ذلك الحالات التي يكون فيها لدى الأبناء مستوى تعليمي كافٍ في التعامل مع هذه التكنولوجيا الجديدة. ولذا فقد قام الباحث بطرح مقترح تأهيلي خاص بحفظ الخصوصية الإلكترونية للطلاب والطالبات يشمل جميع فئات التعليم العام والخاص، إضافة إلى برنامج لتأهيل الآباء والأمهات على حد سواء. ويهدف هذا البرنامج إلى المساهمة في رفع الثقافة الأمنية لدى المجتمع وحماية الأبناء من هذا الخطر المحدق بهم.

هدفت دراسة السعيد (٢٠١٨) بعنوان " التعلم المدمج: مدخل تكنولوجي لتنمية مهارات الاستخدام الآمن للإنترنت والوعي بأخلاقيات التكنولوجيا المعاصرة " إلى قياس فعالية برنامج قائم على التعلم المدمج في تنمية مهارات الاستخدام الآمن للحاسوب والإنترنت والوعي بأخلاقيات التكنولوجيا المعاصرة لدى تلاميذ الحلقة الإعدادية. ولتحقيق هذا الهدف تم تصميم برنامج للتعليم المدمج بنظام إدارة التعلم الإلكتروني Moodle وتطبيقه على مجموعتين تجريبية وضابطة (٣٦ تلميذ بكل مجموعة) بمدرسة أحمد زويل للتعليم الأساسي بمدينة دمياط الجديدة بمحافظة دمياط. كما تم تطبيق أدوات البحث قبليا وبعديا على تلاميذ مجموعتي البحث وبعد التحليل الإحصائي تم التوصل إلى فعالية البرنامج في تنمية مهارات الاستخدام الآمن للحاسوب والإنترنت والوعي بأخلاقيات التكنولوجيا المعاصرة لدى تلاميذ الحلقة الإعدادية. كما هدفت دراسة الجثعمي (٢٠١٧) بعنوان " مستوى الوعي بقضايا أمن المعلومات لدى طالبات المرحلة الثانوية بالمدارس الحكومية بمدينة الرياض " إلى معرفة مستوى وعي طالبات المرحلة الثانوية في المدارس الحكومية بمدينة الرياض بقضايا أمن المعلومات. وقد طبقت هذه الدراسة على المدارس الثانوية الحكومية للبنات بمدينة الرياض، وبلغ عدد عينة الدراسة ٤٢٩ طالبة . ولتحقيق أهداف الدراسة استخدام المنهج الوصفي المسحي، كونه أنسب المناهج البحثية لهذه الدراسة، واستخدمت الاستبانة أداة لجمع البيانات المتعلقة بالدراسة. توصلت الدراسة لمجموعة من النتائج منها: أن العدد الأكبر من الطالبات عينة الدراسة بنسبة ٤٣,١% كان مستوى فهمهن ومعرفتهن بالقضايا المتعلقة بأمن المعلومات جيدة جداً. وأن الغالبية العظمى من طالبات المرحلة الثانوية في المدارس الحكومية بالرياض بنسبة ٩٤,٤% كان لديهن علم بأن حاسباتهن الإلكترونية يمكن أن تصاب بفيروسات. كما توصلت الدراسة أيضاً إلى ما أن نسبته ٨٥,٣% من الطالبات عينة الدراسة يعملن بضرورة استخدام كلمة سر على أجهزتهن الإلكترونية لحمايتها من الاختراق والتجسس.

هدفت دراسة ناصف (٢٠١٧) بعنوان " ممارسة برنامج مقترح من منظور خدمة الجماعة لتنمية وعى الشباب بمخاطر الجريمة الإلكترونية : مطبقة على عينة من الشباب بجمعية الأهرام للعلوم والتكنولوجيا بالمنصورة - محافظة الدقهلية " الى اختبار العلاقة بين ممارسه برنامج مقترح من منظور خدمه الجماعة و تنميه وعي الشباب بمخاطر الجريمة الالكترونية، وتكونت عينه الدراسة من ٥١ شاب من اعضاء جمعيه الاهرام للعلوم والتكنولوجيا بالمنصورة بينما يستخدم تكنولوجيا المعلومات بانتظام من المشتركين في اعلان في انشطتها بصفه منتظمة لمده لا تقل عن ستة شهور ولا التي يترتب عليها استيعابهم لبعض مخاطر الجريمة الإلكترونية م تقسيمهم إلى مجموعتين إحداهما تجريبية والأخرى ضابطة. تمثلت ادوات الدراسة على مقياس وعى الشباب بمخاطر الجريمة الالكترونية. أشارت نتائج الدراسة إلى أن عينه الدراسة من الشباب اعضاء الجماعة التجريبية لديهم وعي منخفض بمخاطر الجريمة الإلكترونية، كما اشارت نتائج الدراسة الى كفاءه البرنامج في خدمه الجماعة في تنميه وعي الشباب بمخاطر الجريمة الإلكترونية لدى أفراد المجموعة التجريبية مقارنة بأفراد المجموعة الضابط.

هدفت دراسة القصير (٢٠١٤) بعنوان " آليات مقترحة لتفعيل التوعية الأمنية لدى طلاب المرحلة المتوسطة من وجهة نظر المديرين والمعلمين بمنطقة القصيم التعليمية" إلى التعرف على واقع ومعوقات التوعية الأمنية لدي طلاب المرحلة المتوسطة من وجهه نظر المديرين والمعلمين في منطقه القصيم التعليمية وكذلك التعرف على اليات تفعيل التوعية الأمنية لديهم اعتمدت الدراسة على المنهج الوصفي المسحي و استخدم الباحث الاستبانة كاداه لجمع البيانات اللازمة للدراسة مكونات عينه الدراسة من ٢١٩ من المديرين والمعلمين للمرحلة المتوسطة في منطقه القصيم التعليمية . أشارت نتائج الدراسة الى ان تنظيم المدارس لزيارات طلابية منظمه للجهات

الأمنية الشرطة ومكافحه المخدرات والهيئات ونحوها. أن يوظف المعلم بعض المواقف التربوية والتعليمية للتوعية الأمنية. ندرة تزويد المدرسة بنتائج الابحاث التي تعالج دور المدرسة في زيادة الوعي بالتوعية الأمنية.. ضعف التنسيق بين المدرسة والجهات الأمنية. ضعف المام الطلاب في مفهوم التوعية الأمنية ومجالاتها. أن تربيه النشء على الدين والفضيلة كفيل بإبعادهم عن الشرور.

هدفت دراسة المعايطة (٢٠١٣) بعنوان " اتجاهات الطلبة الجامعيين نحو دور التوعية الأمنية في الوقاية من الجريمة " الى التعرف على اتجاهات الطلبة الجامعيين نحو دور التوعية الأمنية في الوقاية من الجريمة و من اجل تحقيق هذا الهدف تم تصميم استبانة والذات على عينه عنقوديه بلغ حجمها ٥٩٠ طالب وطالبه في الجامعات الأردنية مقطع الأردنية اليرموك والسعودية الاساليب الإحصائية المناسبة لاستخراج نتائج الدراسة وقد توصلت الدراسة الى أن هناك دور للتوعية الأمنية في الوقاية من الجريمة من وجهه نظر الطلبة الجامعيين، كما اشارت نتائج الدراسة إلى أن اتجاهات الطلبة الجامعيين نحو دور التوعية الأمنية في الوقاية من الجريمة كانت ايجابيه ، كذلك اشارت النتائج إلى عدم وجود فروق ذات دلاله إحصائية في اتجاهات الطلبة الجامعيين نحو دور التوعية الأمنية في الوقاية من الجريمة تبعا للنوع الاجتماعي، وأشارت أيضاً إلى وجود فروق ذات دلاله إحصائية في اتجاهات الطلبة الجامعيين نحو دور التوعية الأمنية في الوقاية من الجريمة تعزي لمتغير السنه الدراسية والكلية ومستوى دخل الاسرة.أسفل النموذج

وهدفت دراسة العبيد (٢٠١٢) بعنوان "التوعية الأمنية في مدارس المرحلة الثانوية بالمملكة العربية السعودية الواقع والأهمية دراسة ميدانية على الإدارة العامة للتربية والتعليم بمنطقة القصيم للبنين" إلى التعرف على واقع ممارسة أساليب التوعية الأمنية في مدارس المرحلة الثانوية بالمملكة العربية السعودية، ومعرفة أهمية ممارسة أساليب التوعية الأمنية في مدارس المرحلة الثانوية. تمت من خلال المنهج الوصفي، حيث تكون مجتمع الدراسة من معلمي ومشرفي ومديري المدارس الثانوية الحكومية (بنين) بمدينة بريدة بمنطقة القصيم التعليمية بالمملكة العربية السعودية في الفصل الدراسي الأول من العام الدراسي ١٤٣٠/١٤٣١ هـ البالغ عددهم (١٨٠٩) وتوصلت الدراسة في نتائجها إلى أن واقع ممارسة أساليب التوعية الأمنية في مدارس المرحلة الثانوية بالمملكة العربية السعودية هو واقع ضعيف، وأن أهمية ممارسة أساليب التوعية الأمنية في مدارس المرحلة الثانوية بالمملكة العربية السعودية من خلال الأساليب التي ذكرت في الدراسة هي أساليب مهمة وذات درجة عالية.

التعقيب على الدراسات السابقة:

أهم النتائج التي توصلت إليها تلك الدراسات:

١- أكدت دراسة السعيد (٢٠١٨)؛ ناصف (٢٠١٧)؛ Mahno(2012) على فعالية البرامج والوحدات المقترحة في تنمية الوعى وتحقيق أهداف الثقافة المعلوماتية والأمن السيبراني ، كما أكدت هذه الدراسات على أن هناك قصوراً في المناهج والبرامج الدراسية سواء فى مرحلة التعليم الجامعي أو قبل الجامعي.

٢- أشارت دراسة(Nakama(2018؛ Coughin(2012) إلى أن برامج إعداد المعلم الحالية لا تحقق أهداف الأمن السيبراني .

٣- أشارت دراسة الغديان وآخرون (٢٠١٨)؛ السعيد (٢٠١٨)؛ الجثعمي (٢٠١٧) القصير (٢٠١٤) إلى تدنى مستوى المبادئ والأبعاد والمفاهيم الأمنية فيما يتعلق بالإلكترونيات وطرق التعامل مع الحاسوب والانترنت وعدم توافرها بالمناهج والمقررات الدراسية.

٤- أشارت المعايطة (٢٠١٣) إلى أن المقررات البيئية عجزت عن زيادة التحصيل لدى الطلاب أو إحداث تغيير في اتجاهات الطلاب الإيجابية نحو الأمن السيبراني.

التعقيب العام على الدراسات السابقة:

١- نواحي الاتفاق والاختلاف بين الدراسات السابقة والدراسة الحالية:

باستعراض الدراسات السابقة تُعلق الباحثة على تلك الدراسات لتُبين أوجه الشبه والاختلاف بينها وبين الدراسة الحالية وما أفادته تلك الدراسات لهذه الدراسة ومكانة الدراسة الحالية بين تلك الدراسات وما يميزها عن الدراسات السابقة.

يتضح من الدراسات السابقة أن أهدافها تتفق وأهداف الدراسة الحالية حيث أشارت هذه الدراسات إلى أهمية الاهتمام بتنمية الأمن السيبراني والاتجاهات المعلوماتية لدى الأفراد بصفة عامة والمعلمين بصفة خاصة.

- أوجه الاتفاق مع الدراسات السابقة:

اتفقت الدراسة الحالية مع الدراسات السابقة فى أدوات الدراسة وهي الاستبيان مثل دراسة القصير (٢٠١٤)؛ (2014) Ye. واعتمدت التحليلي الوصفي التحليلي في تحليل البيانات والوصول للنتائج مثل دراسة كل من الشمري (٢٠١٥)؛ القصير (٢٠١٤)؛ الخثمعي(٢٠١٧) بينما اختلف الدراسة الحالية مع بعض الدراسات الأخرى التي استخدمت مناهج مثل منهج دراسة الحالية كما في دراسة Goran(2017) والمنهج شبه التجريبي كما في دراسة ناصف(٢٠١٧) .

٢-أوجه الاختلاف مع الدراسات السابقة:

كما اختلفت الدراسة الحالية مع الدراسات السابقة في جزء من العينة حيث اقتصرت الدراسات السابقة على عينة طلاب المرحلة الثانوية كما في دراسة كل من Goran (2017)؛ العبيد (٢٠١٢) وطلاب المرحلة المتوسطة كما في دراسة القصير (٢٠١٤)؛ السعيد (٢٠١٨) وطلاب المرحلة الجامعية كما في دراسات كل من Minho(2017)؛ المعايطة(٢٠١٣).وكما اختلفت في عينية الدراسة .

تتميز الدراسة الحالية عن الدراسات السابقة بأنها تتناول مدى وعي المعلمين والمعلمات في فهم ونشر مفهوم الأمن السيبراني.

فالمعلم يعتبر الأساس في تحقيق الأمن السيبراني، فهو الموجه والمرشد والمعاون للطالب ، فالبرغم من أهمية الوحدات والبرامج وبالرغم من أهمية الدروات التدريبية وغيرها من الأنشطة الهامة في تحقيق الأمن السيبراني إلا أن بعضها لم يحقق ذلك إلى حد كبير نظراً لأن هذه الأنشطة والبرامج لا تبرز المضمون بالصورة المناسبة لعدم توافر المشرفين المتخصصين ، أو أنهم لم يتلقوا تدريباً مناسباً ، مما يتطلب ضرورة البحث عن إجراءات ومداخل أخرى تسهم في تحسين مستوى الثقافة المعلوماتية لدى المجتمع المدرسي والفئة الأكثر قدرة على التعامل مع تلك المعطيات هم معلمات الحاسب الآلي .

٣- أوجه الإفادة من الدراسات السابقة:

- ساهمت الدراسات السابقة في بلورة مشكلة البحث الحالي وتحديد الإطار النظري للدراسة الحالية ومن ثم تم اختيار المنهج المناسب لإجراء البحث.

الطريقة والإجراءات:

يتناول هذا الفصل وصفًا لمجتمع الدراسة وعينتها، وأدواتها المستخدمة في جمع البيانات، وطرق التحقق من صدقها وثباتها، كما يتناول الإجراءات المتبعة في تطبيق الدراسة ومتغيرات الدراسة، وأساليب المعالجة الإحصائية المستخدمة في استخراج النتائج.

منهج البحث:

استخدمت الباحثة المنهج الكمي لمناسبته طبيعة الدراسة، والمنهج الكمي هو طريقة مُنظمة ومُنسقة لجمع وتحليل البيانات التي تم جلبها من مختلف المصادر ويتطلب استخدام الأدوات الحاسوبية والإحصائية والرياضية لاستخلاص النتائج. يسعى البحث الكمي إلى قياس المشكلة وفهم مدى تأثيرها بالبحث عن نتائج قابلة للقياس على عدد أكبر من الأفراد (ريما ماجد، ٢٠١٦، ٢٦).

وذلك من خلال أدوات البحث المتمثلة في استبانة الوعي بالأمن السيبراني.

مجتمع البحث:

تكون مجتمع الدراسة من جميع معلمات الحاسب للمرحلة الثانوية بمدينة جدة للعام الدراسي ١٤٤٠هـ -٢٠١٩م.وعددهن (٣٥٢) معلمة حسب المعلومات الواردة من إدارة تعليم جدة.

عينة البحث:

تم استخدام المعادلات الإحصائية لحساب حجم العينة المناسبة للبحث. تم توزيع الاستبانة على كل المجتمع بهدف الحصول على أكبر عدد من الردود، وقد تم استعادة (١٠٦) بدرجة ثقة ٩٥% وخطأ تقديري ٠،٠٥ وتم استبعاد استبانتين غير قابلة للتحليل وتم اختيار العينة بالطريقة العشوائية البسيطة. ثم تم توزيع الاستبانة من خلال قاعدة البيانات الموجودة عند رئيسة شعبة قسم الحاسب الآلي بإدارة تعليم جدة.

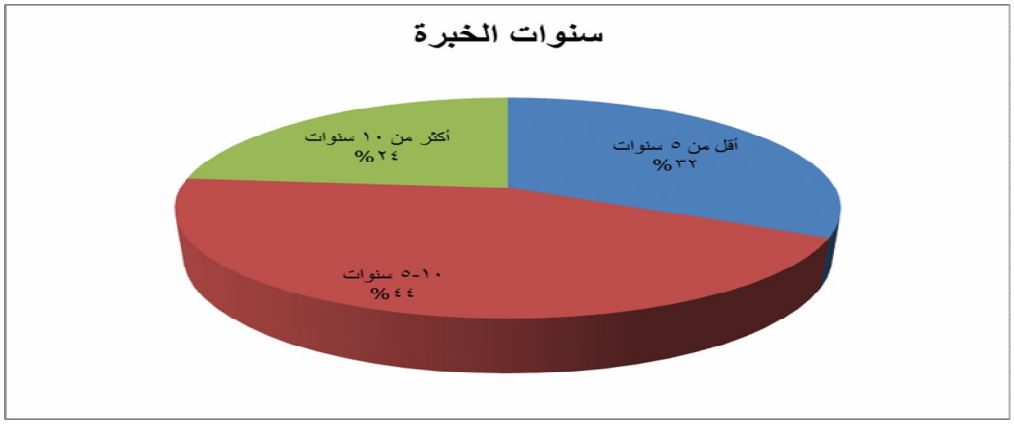
قامت الباحثة بتصميم الاستبانة على نموذج جوجل (Google form)، وتم إرسال روابط الاستبانة على المعلمات، كما تم توزيع الاستبانة على عدد من المعلمات ممن تعذر عليهن الاستجابة على الاستبيان إلكترونياً، وكان عدد الاستجابات الكاملة على فقرات الاستبيان (١٠٦) وشكلت أفراد الدراسة أي ما نسبته (٣٠,١١%) من مجتمع الدراسة الأصلي. والجدول التالي يوضح المتغيرات الديموغرافية لدى عينة البحث:

جدول (١) توزيع أفراد الدراسة حسب نوع المدرسة والخبرة والمؤهل العلمي

	المتغير	الفئات	التكرار	النسبة المئوية
المعلمات	سنوات الخبرة	أقل من ٥ سنوات	٣٤	%٣٢,٠٧
		٥-١٠ سنوات	٤٧	%٤٤,٣٣
		أكثر من ١٠ سنوات	٢٥	%٢٣,٦
	المؤهل العلمي	بكالوريوس	٧٩	%٧٤,٥٣
		ماجستير فأكثر	٢٧	%٢٥,٤٧
	الدورات التدريبية	لا يوجد	١٢	%١١,٣٢
		دورة إلى ثلاث دورات	٦٨	%٦٤,١٥
		أكثر من ثلاث دورات	٢٦	%٢٤,٥٣

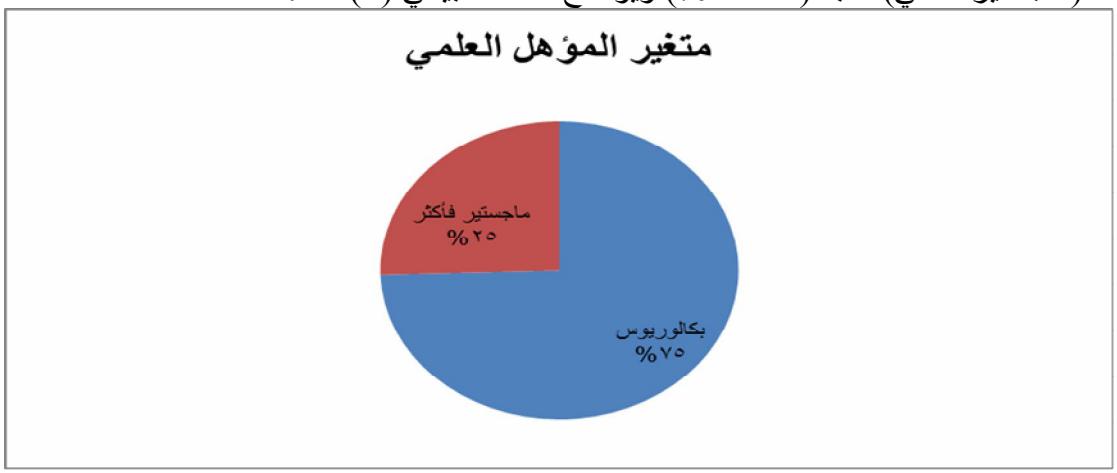
يتضح من الجدول (١) ما يأتي:

١- **سنوات الخبرة**: بلغت نسبة معلمات الحاسب اللاتي يمتلكن خبرات أقل من ٥ سنوات (٣٢,٠٧%) واللاتي يمتلكن خبرات من ٥-١٠ سنوات (٤٤,٣٣%) بينما المعلمات اللاتي يمتلكن سنوات خبرة أكثر من ١٠ سنوات بلغت نسبتهن (٢٣,٦%) ويوضح الشكل البياني (١) ذلك:



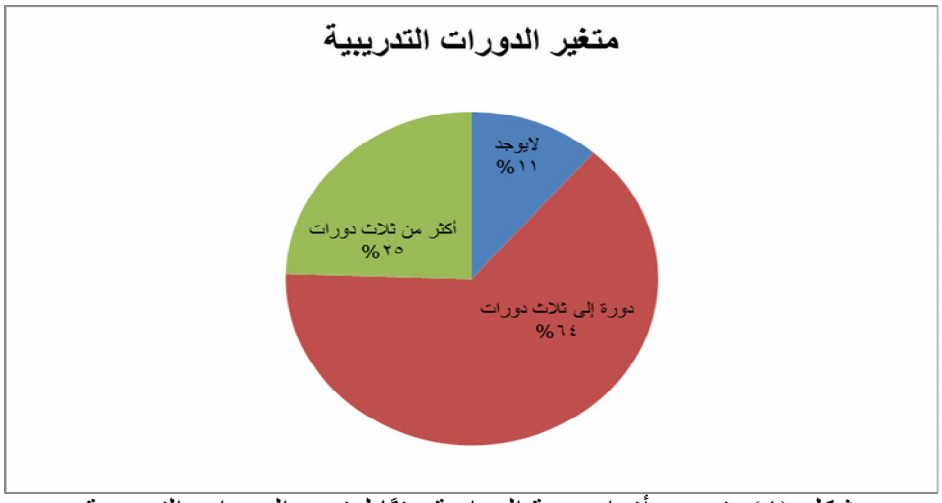
شكل (٢): توزيع أفراد عينة الدراسة وفقًا لمتغير سنوات الخبرة

٢- **المؤهل العلمي:** بلغت نسبة معلمات الحاسب الحاصلات على مؤهل البكالوريوس (٧٤,٥٣%)، وبينما بلغت نسبة المعلمات الحاصلات على مؤهلات أعلى من البكالوريوس (ماجستير فأعلي) نسبة (٢٥,٤٧%) ويوضح الشكل البياني (٢) ذلك:



شكل (٣): توزيع أفراد عينة الدراسة وفقًا لمتغير سنوات المؤهل العلمي

١- **ومن حيث الدورات التدريبية:** بلغت نسبة معلمات الحاسب اللاتي حصلن على دورات تدريبية أكثر من ثلاث دورات (٢٤,٥٣%) من إجمالي عينة الدراسة، وحصلت (٦٤,١٥%) من إجمالي العينة على دورات تدريبية من (دورة إلى ثلاث دورات) في حين لم تحصل نسبة(١١,٣٢%) من عينة معلمات الحاسب على أية دورات تدريبية في مجال الأمن السيبراني، ويوضح الشكل البياني(٣) ذلك :



شكل (٤): توزيع أفراد عينة الدراسة وفقًا لمتغير الدورات التدريبية

أدوات الدراسة:

أولًا: استبيانه عن واقع الوعي بالأمن السيبراني لدى معلمات الحاسب للمرحلة الثانوية بمدينة جدة:

استخدمت الدراسة الاستبانة كأداة لجمع المعلومات، وتكونت الاستبانة من جزئين أساسين؛ الأول منهما عبارة عن بيانات وصفية عن المشارك في الاستبانة، والجزء الثاني يتكون من مكونين يمثلان الأركان الأساسية لعملية الوعي بالأمن السيبراني، وهذه المكونات هي:

المجال الأول: الوعي بماهية الأمن السيبراني.

المجال الثاني: الوعي بطرق المحافظة على نظام الأمن السيبراني.

وقد تم بناء الاستبانة وذلك بعد الاطلاع على الأدب التربوي والدراسات السابقة المتعلقة بمشكلة الدراسة واستطلاع رأي عينة من المتخصصين عن طريق المقابلات الشخصية ذات الطابع غير الرسمي قامت الباحثة بما يلي:

- تحديد المجالات الرئيسة التي شملتها الاستبانة.
- صياغة الفقرات التي تقع تحت كل مجال.
- إعداد الاستبانة في صورتها الأولية والتي شملت (٣٠) فقرة.
- عرض الاستبانة على المشرف وتعديلها من أجل تحديد مدى ملاءمتها لجمع البيانات.
- عرض الاستبانة على (٤) محكمين من المتخصصين في البحث.
- بعد إجراء التعديلات التي أوصى بها المحكمون تم تعديل وصياغة بعض الفقرات وقد بلغ عدد فقرات الاستبانة بعد صياغتها النهائية (٢٩) فقرة موزعة على ثلاثة، معتمدة على نظام ليكرت الخماسي (موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة).
- والملحق رقم (١) يبين الاستبانة في صورتها النهائية.

صدق الاستبانة:

قامت الباحثة بتقنين فقرات الاستبانة وذلك للتأكد من صدقها كالتالي:

أولًا: صدق المحكمين:

تم حساب صدق الاستبانة الخارجي من خلال عرضها على مجموعة من المحكمين ذوي الاختصاص والخبرة في المجال محل الدراسة، وذلك للقيام بتحكيمها بعد اطلاع هؤلاء المحكمين على عنوان الدراسة، وتساؤلاتها، وأهدافها.

وبناء على آراء المحكمين وملاحظاتهم تم التعديل لبعض العبارات، وكذلك إضافة وحذف بعض العبارات بحيث أصبحت صالحة للتطبيق في الصورة النهائية، كما تم دمج عبارات أوافق بشدة مع أوافق وعبارات لا أوافق بشدة مع عبارة لا أوافق، ويتضمن الملحق (١) الاستبانة النهائية التي تم التوصل إليها بعد عملية التحكيم وتم استخدامها في عملية جمع البيانات من أعضاء هيئة التدريس بالكلية.

صدق الاتساق الداخلي:

تم التعرف على مدى اتساق أداة الدراسة من خلال حساب معاملات الارتباط بين العبارات والمحور الذي تنتمي إليه كل عبارة باستخدام معامل ارتباط بيرسون (Person Correlation)،

حيث جرى التحقق من صدق الاتساق الداخلي للاستبانة بتطبيق الاستبانة على عينة استطلاعية مكونة من (٢٠) معلمة من معلمات الحاسب من إدارة تعليم جدة، وذلك عن طريق نماذج جوجل(Google form) وتم حساب معامل ارتباط بيرسون بين درجات كل مجال من مجالات الاستبانة والدرجة الكلية للاستبانة وكذلك تم حساب معامل ارتباط بيرسون بين كل فقرة من فقرات الاستبانة والدرجة الكلية للمجال الذي تنتمي إليه وذلك باستخدام البرنامج الإحصائي (SPSS)، ويوضح الجدول (٣) نتائج حساب معاملات الارتباط بين كل عبارة والمحور الذي تنتمي إليه.

جدول (٢) معامل ارتباط كل فقرة من فقرات المجال الأول: الوعي بماهية الأمن السيبراني

م	الفقرة	معامل الارتباط	مستوى الدلالة
١	أدرك أهمية الأمن السيبراني لمدرستي.	٠,٤٤٦	دالة عند ٠,٠١
٢	لدي إلمام بمفهوم الأمن السيبراني.	٠,٦٤١	دالة عند ٠,٠١
٣	لدي معرفة بمخاطر فتح روابط ومرفقات البريد الإلكتروني.	٠,٨٢٤	دالة عند ٠,٠١
٤	لدي معرفة بمخاطر فيروسات الهواتف الذكية.	٠,٥٠١	دالة عند ٠,٠١
٥	لدي معرفة بمفهوم التصيد (الاحتيال) الإلكتروني.	٠,٥٤٧	دالة عند ٠,٠١
٦	لدي معرفة تامة بمخاطر تنزيل البرامج والملفات من الإنترنت.	٠,٨٤٧	دالة عند ٠,٠١
٧	لدي معرفة تامة بمفهوم الهندسة الاجتماعية.	٠,٧٤٥	دالة عند ٠,٠١

ر الجدولية عند درجة حرية (٣٨) وعند مستوى دلالة ٠,٠١= ٠,٣٩٣

ر الجدولية عند درجة حرية (٣٨) وعند مستوى دلالة (٠٥,٠) = ٠,٣٠٤

جدول (٣) معامل ارتباط كل فقرة من فقرات المجال الثاني: الوعي بطرق المحافظة على نظام الأمن السيبراني.

م	الفقرة	معامل الارتباط	مستوى الدلالة
١	استخدم برنامج للحماية من الفيروسات بصورة مستمرة.	٠,٣٨	دالة عند ٠,٠١
٢	أقوم بتحديث برنامج الحماية من الفيروسات بصورة مستمرة.	٠,٥٢	دالة عند ٠,٠١
٣	اتفحص جهاز الحاسب الآلي المكتبي /المحمول بصورة منتظمة.	٠,٢٧	دالة عند ٠,٠١
٤	استخدم جدار الحماية على جهاز الحاسوب الخاص بي.	٠,٥٥	دالة عند ٠,٠١
٥	أقوم بتحديث نظام التشغيل بصورة دورية.	٠,٥٢	دالة عند ٠,٠١
٦	أقوم بعمل نسخة احتياطية للملفات المهمة.	٠,٥٩	دالة عند ٠,٠١
٧	لا أفتح رسالة إلكترونية غير معروفة لدي.	٠,٥٥	دالة عند ٠,٠١
٨	أقوم بالرد عندما تصلني رسالة بريد الكتروني عن الفوز بجائزة نقدية أوعينه وشراكة في صفقة تجارية.	٠,٣٧	دالة عند ٠,٠١
٩	لا أتسوق أو أشتري سلعة معلن عنها في مواقع التواصل الاجتماعي أو من خلال الإعلانات.	٠,٥٥	دالة عند ٠,٠١
١٠	لا أتسوق أو أشتري سلعة معلن عنها في مواقع التواصل الاجتماعي أو من خلال الإعلانات.	٠,٥٨	دالة عند ٠,٠١
١١	أنا على علم بالخصائص اللازمة لإنشاء كلمة مرور جيدة عند الدخول للمواقع على الويب.	٠,٥٩	دالة عند ٠,٠١
١٢	استخدم نفس كلمة المرور لجميع مواقع التواصل الاجتماعي والبريد الإلكتروني.	٠,٥٥	دالة عند ٠,٠١
١٣	استخدم نفس كلمة المرور للمواقع التي أحتاجها لإجراء عمليات مالية مثل مواقع البنوك ومواقع التسوق الإلكترونية.	٠,٦٣	دالة عند ٠,٠١
١٤	لدي معرفة بخطورة إرسال كلمة المرور عبر البريد الإلكتروني	٠,٥٧	دالة عند ٠,٠١
١٥	أقوم بتغيير كلمة المرور بانتظام.	٠,٥٦	دالة عند ٠,٠١
١٦	أقوم بقراءة اتفاقيات المستخدم لبرنامج مجاني قبل الضغط على " أوافق"	٠,٥٨	دالة عند ٠,٠١
١٧	يوجد قانون مستقل للجريمة السيبرانية في السعودية.	٠,٥٥	دالة عند ٠,٠١
١٨	يوجد تشريعات ولوائح للأمن السيبراني في السعودية.	٠,٦٣	دالة عند ٠,٠١

ر الجدولية عند درجة حرية (٣٨) وعند مستوى دلالة ٠,٠١= ٠,٣٩٣

ر الجدولية عند درجة حرية (٣٨) وعند مستوى دلالة (٠,٠٥) = ٠,٣٠٤

يتضح من الجدول السابق أن جميع الفقرات ترتبط بالدرجة الكلية للمجال الذي تنتمي إليه ترتبط ارتباطًا ذا دلالة إحصائية عند مستوى دلالة ٠,٠١ وهذا يؤكد أن الاستبانة تتمتع بدرجة عالية من الاتساق الداخلي.

وللتحقق من صدق الاتساق الداخلي للمجالات قامت الباحثة بحساب معاملات الارتباط بين درجة كل مجال من مجالات الاستبانة والمجالات الأخرى وكذلك كل مجال بالدرجة الكلية للاستبانة والجدول (١٠) يوضح ذلك.

جدول رقم(٤) مصفوفة معاملات ارتباط كل مجال من مجالات الاستبانة والمجالات الأخرى للاستبانة وكذلك مع الدرجة الكلية

المجال	المجال الأول: الوعي بماهية الأمن السيبراني.	المجال الثالث: الوعي بطرق المحافظة على نظام الأمن السيبراني.
المجال الأول: الوعي بماهية الأمن السيبراني.	١,٠٠	
المجال الثاني: الوعي بطرق المحافظة على نظام الأمن السيبراني.	٠,٥٥	١,٠٠

ر الجدولية عند درجة حرية (٣٨) وعند مستوى دلالة ٠,٠١= ٠,٣٩٣

ر الجدولية عند درجة حرية (٣٨) وعند مستوى دلالة (٠٥,٠) = ٠,٣٠٤

يتضح من الجدول السابق أن جميع المجالات ترتبط ببعضها البعض وبالدرجة الكلية للاستبانة ارتباطًا ذا دلالة إحصائية عند مستوى دلالة ٠,٠١ وهذا يؤكد على أن الاستبانة تتمتع بدرجة عالية من الثبات والاتساق الداخلي.

ثبات الاستبانة:

أجرت الباحثة خطوات التأكد من ثبات الاستبانة وذلك بعد تطبيقها على أفراد العينة الاستطلاعية من معلمات الحاسب للمرحلة الثانوية بمدينة جدة بطريقتين وهما التجزئة النصفية ومعامل ألفا كرونباخ .

طريقة التجزئة النصفية:

تم استخدام درجات العينة الاستطلاعية لحساب ثبات الاستبانة بطريقة التجزئة النصفية حيث احتسبت درجة النصف الأول لكل مجال من مجالات الاستبانة وكذلك درجة النصف الثاني من الدرجات وذلك بحساب معامل الارتباط بين النصفين ثم جرى تعديل الطول باستخدام معادلة سيبرمان براون، والجدول التالي يوضح ذلك:

جدول (٥) يوضح معاملات الارتباط بين نصفي كل مجال من مجالات الاستبانة وكذلك الاستبانة ككل قبل التعديل ومعامل الثبات بعد التعديل

الأبعاد	عدد الفقرات	الارتباط قبل التعديل	معامل الثبات بعد التعديل
المجال الأول: الوعي بماهية الأمن السيبراني.	٧	٠,٩٠٣	٠,٩٠٦
المجال الثاني: الوعي بطرق المحافظة على نظام الأمن السيبراني.	١٨	٠,٨٦٩	٠,٨٦٣
المجموع	٢٥	٠,٩٢٥	٠,٨٩٢

يتضح من الجدول السابق أن معامل الثبات الكلي= ٠,٨٩٢ وهذا يدل على أن الاستبانة تتمتع بدرجة عالية من الثبات تطمئن الباحثة إلى تطبيقها على عينة الدراسة.

اختبار ألفا كرونباخ :

تم حساب الثبات Reliability بطريقة ألفا كرونباخ (Cronbach's alpha). ويوضح جدول (٨) معاملات الثبات التي تم الحصول عليها بحساب الثبات، وكذلك يتضمن الصدق الذاتي والذي يتم حسابه بأخذ الجذر التربيعي لمعامل الثبات.

جدول (٦) يوضح معاملات ألفا كرونباخ لكل مجال من مجالات الاستبانة وكذلك للاستبانة ككل

المجال	عدد الفقرات	معامل الفا كرونباخ
المجال الأول: الوعي بماهية الأمن السيبراني.	٧	٠,٨٠
المجال الثاني: الوعي بطرق المحافظة على نظام الأمن السيبراني.	١٨	٠,٧٨
المجموع	**٢٥**	٠,٩١

يتضح من الجدول السابق أن معامل الثبات= ٠,٩١ وهذا يدل على أن الاستبانة تتمتع بدرجة عالية من الثبات تطمئن الباحثة إلى تطبيقها على عينة الدراسة.

الأساليب والمعالجات الإحصائية:

يتطلب تحليل البيانات التي تمثل استجابات عينة الدراسة على بنود الاستبانة استخدام بعض الأساليب الإحصائية الوصفية والاستدلالية وهي:

١- التكرارات والنسب المئوية للموافقة

٢- المتوسط الحسابي

٣- الانحراف المعياري

٤- المتوسط الحسابي الموزون

٥- اختبار التاء للعينات المستقلة

٦- تحليل التباين أحادي الاتجاه(ANOVA)

٧- **تم تحليل نتائج الدراسة** باستخدام البرنامج الإحصائي (SPSS) (Statistical Package for Social Sciences) الإصدار الثامن عشر.

عرض وتحليل بيانات الدراسة ومناقشة نتائجها:

يتضمن هذا الفصل عرض نتائج الدراسة التي هدفت إلى التعرف على مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة، وتم تناول ذلك كما يلي:

السؤال الأول: ما مدى وعي معلمات الحاسب الآلي بمدينة جدة بماهية الأمن السيبراني؟

للإجابة عن هذا السؤال تم حساب المتوسطات الحسابية والانحرافات المعيارية لتقديرات أفراد العينة لدرجة وعي على مجالات الدراسة والأداة الكلية حيث كانت كما هي موضحة في الجدول:

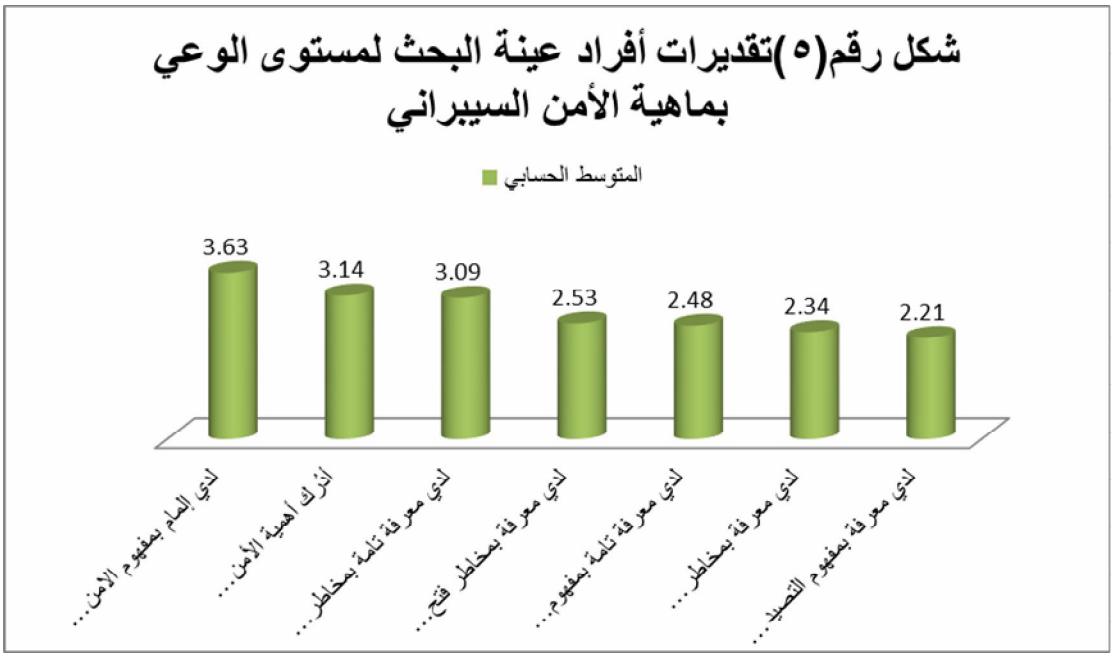
جدول رقم (٧) المتوسطات الحسابية والانحرافات المعيارية لتقديرات أفراد عينة البحث لمستوى الوعي بماهية الأمن السيبراني على المكون الأول للاستبانة: الوعي بماهية الأمن السيبراني.

رقم الفقرة	نص الفقرة	المتوسط الحسابي	الانحراف المعياري	الدرجة	الاستجابة
١	لدي إلمام بمفهوم الامن السيبراني.	٣,٦٣	١,١٣	الأولى	عالية
٢	أدُرك أهمية الأمن السيبراني لمدرستي.	٣,١٤	١,٣٧	الثانية	عالية
٣	لدي معرفة تامة بمخاطر تنزيل البرامج والملفات من الأنترنت.	٣,٠٩	١,٤١	الثالثة	عالية
٤	لدي معرفة بمخاطر فتح روابط ومرفقات البريد الالكتروني.	٢,٥٣	١,٢١	الرابعة	متوسطة
٥	لدي معرفة تامة بمفهوم الهندسة الاجتماعية.	٢,٤٨	١,٣٥	الخامسة	متوسطة
٦	لدي معرفة بمخاطر فيروسات الهواتف الذكية.	٢,٣٤	١,١٤	السادسة	متوسطة
٧	لدي معرفة بمفهوم التصيد(الإحتيال)الالكتروني.	٢,٢١	١,٠٨	السابعة	متوسطة

ويتضح من الجدول السابق أن المتوسطات الحسابية للفقرات تراوحت ما بين (٣,٦٣) كحد أعلى، و(٢,٢١) كحد أدني، وقد نالت عبارات (لدي إلمام بمفهوم الأمن السيبراني - أدُرك أهمية الأمن السيبراني لمدرستي) على أعلى درجات استجابة، ويرجع ذلك إلى عدة عوامل أهمها توجهات ومنطلقات ومرتكزات التطوير التربوي التي انطلقت من توصيات العديد من المؤتمرات التي تنادي بضرورة نشر الوعي الرقمي والثقافة الرقمية لدى المعلمين والمعلمات في مراحل التعليم المختلفة، وضرورة ربط علميات الإشراف باستخدام التكنولوجيا الحديثة واعتماد الإشراف على عمليات التوجيه والتثقيف التكنولوجي.

كما نالت عبارات أخرى مثل:(لدي معرفة تامة بمفهوم الهندسة الاجتماعية- لدي معرفة بمخاطر فيروسات الهواتف الذكية- لدي معرفة بمفهوم التصيد (الاحتيال الإلكتروني) على درجات أقل في متوسطاها ويرجع ذلك إلى عدم التطرق لتلك المفاهيم في المجتمع المدرسي ووسائل الإعلام العامة بخلاف بعض المفاهيم والمصطلحات الشائعة الأخرى التي تعرفها المعلمات وإن كانت بدون تحديد دقيق لأبعاد تلك المفاهيم.

وتتضح النتائج السابقة في الشكل التالي:



وتتفق نتائج هذا السؤال مع دراسة حنان عبد القوى (٢٠١٦)، ودراسة (Ribble, Bailey, 2006)، والتي أكدت علي ضعف وقصور لدي وضعف لدي الأفراد – ومنهم معلمات الحاسب الآلي- في الوعى بمفاهيم الأمن السيراني كأحد أبعاد المواطنة الرقمية. وترى الدراسة الحالية بأن هُناك فهم عام لمفهوم الأمن السيبراني وأهميته وليس بتفاصيل المفهوم.

السؤال الثاني: ما مدى وعي معلمات الحاسب الآلي بمدينه جدة بطرق المحافظة على نظام الأمن السيبراني؟

للإجابة عن هذا السؤال تم حساب المتوسطات الحسابية والانحرافات المعيارية لتقديرات أفراد العينة لدرجة وعي على مجالات الدراسة والأداة الكلية حيث كانت كما هي موضحة في الجدول:

جدول رقم (٨) المتوسطات الحسابية والانحرافات المعيارية لتقديرات أفراد عينة البحث لمستوى الوعي بماهية الأمن السيبراني على المكون الثالث للاستبانة: الوعي بطرق المحافظة على نظام الأمن السيبراني.

رقم الفقرة	نص الفقرة	المتوسط الحسابي	الانحراف المعياري	الدرجة	الاستجابة
١	أستخدم برنامج للحماية من الفيروسات بصورة مستمرة.	٤,٤٦	١,٨٣	الأولى	عالية جدًا
٢	أقوم بتحديث برنامج الحماية من الفيروسات بصورة مستمرة.	٤,٨١	١,٨٦	الثانية	عالية جدًا
٣	اتفحص جهاز الحاسب الآلي المكتبي /المحمول بصورة منتظمة.	٤,٢٤	١,٦١	الثالثة	عالية جدًا
٤	أستخدم جدار الحماية على جهاز الحاسوب الخاص بي.	٤,٠٤	١,٧٤	الرابعة	عالية جدًا
٥	أقوم بتحديث نظام التشغيل بصورة دورية.	٣,٧٣	١,٠١	الخامسة	عالية
٦	أقوم بعمل نسخة احتياطية للملفات المهمة.	٣,٥٨	١,٢٥	السادسة	عالية

رقم الفقرة	نص الفقرة	المتوسط الحسابي	الانحراف المعياري	الدرجة	الاستجابة
٧	لا أفتح رسالة إلكترونية غير معروفة لدي.	٣,٣٧	١,٤٤	السابعة	عالية
٨	أقوم بالرد عندما تصلني رسالة بريد الكتروني عن الفوز بجائزة نقدية أوعينه أوشراكة في صفقة تجارية.	٣,١٩	١,٧٨	الثامنة	عالية
٩	لا أتسوق أو أشتري سلعة معلن عنها في مواقع التواصل الاجتماعي أو من خلال الإعلانات.	٣,١٤	١,٨٥	التاسعة	عالية
١٠	لا أتسوق أو أشتري سلعة معلن عنها في مواقع التواصل الاجتماعي أو من خلال الإعلانات.	٣,١٠	١,٣٣	العاشرة	عالية
١١	أنا على علم بالخصائص اللازمة لإنشاء كلمة مرور جيدة عند الدخول للمواقع على الويب.	٢,٣٤	١,١٤	حادي عشر	متوسطة
١٢	أستخدم نفس كلمة المرور لجميع مواقع التواصل الاجتماعي والبريد الالكتروني.	٢,١٨	١,٤٨	ثاني عشر	متوسطة
١٣	استخدم نفس كلمة المرور للمواقع التي أحتاجها لإجراء عمليات مالية مثل مواقع البنوك ومواقع التسوق الإلكترونية.	٢,٢٠	١,٣٥	ثالث عشر	متوسطة
١٤	لدي معرفة بخطورة إرسال كلمة المرور عبر البريد الإلكتروني	٢,١١	١,٤٤	رابع عشر	متوسطة
١٥	أقوم بتغيير كلمة المرور بانتظام.	٢,٠٢	١,٣٩	خامس عشر	متوسطة
١٦	أقوم بقراءة اتفاقيات المستخدم لبرنامج مجاني قبل الضغط على " أوافق"	١,٩٥	١,١٤	سادس عشر	منخفضة
١٧	يوجد قانون مستقل للجريمة السيبرانية في السعودية.	١,٨٧	١,٤٨	سابع عشر	منخفضة
١٨	يوجد تشريعات ولوائح للأمن السيبراني في السعودية.	١,٧٤	١,٣٥	ثامن عشر	منخفضة

ويتضح من الجدول السابق أن المتوسطات الحسابية للفقرات تراوحت مابين (٤,٤٦) كحد أعلى، و(١,٧٤) كحد أدني، وقد نالت مجالات (استخدم برنامج للحماية من الفيروسات بصورة مستمرة- أقوم بتحديث برنامج الحماية من الفيروسات بصورة مستمرة- أتفحص جهاز الحاسب الآلي المكتبي/ المحمول بصورة منتظمة- استخدم جدار الحماية على جهاز الحاسوب الخاص بي) على أعلى درجات استجابة وكانت بدرجة (عالية جدًّا).

بينما جاءت عبارات (أقوم بقراءة اتفاقيات المستخدم لبرنامج مجاني قبل الضغط على " أوافق"- يوجد قانون مستقل للجريمة السيبرانية في السعودية- يوجد تشريعات ولوائح للأمن السيبراني في السعودية) بدرجة منخفضة، وقد يرجع ذلك إلى أن معلمات الحاسوب يقمن بالعديد من الإجراءات والعمليات المرتبطة بالتعامل مع البرمجيات وتطبيقات الحاسوب مما يجعل المعلمات لا يقرأن اتفاقيات وشروط كل برنامج يقمن بتنزيله وتثبيته على الأجهزة، كما وجد قصور في معرفة تصنيفات القوانين والتشريعات المتعلقة بالجرائم السيبرانية. النتيجة كانت متوقعة حيث إنها عامة في المجتمعات وليست حصرًا على معلمات الحاسب والمفروض يكنّ حريصات في فهم شروط الاتفاقيات.

السؤال الثالث: **هل** توجد فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد مجتمع الدراسة عند مستوى الدلالة (≤ 0,05 a) في درجة وعي معلمات الحاسب بالأمن السيبراني تعزى لاختلاف الدورات التدريبية، المؤهل العلمي، وسنوات الخبرة؟

وللإجابة عن هذا السؤال استخدم البحث الحالي اختبار "ت" واختبار التباين الأحادي وكانت النتائج على النحو التالي:

١- متغير الدورات التدريبية:

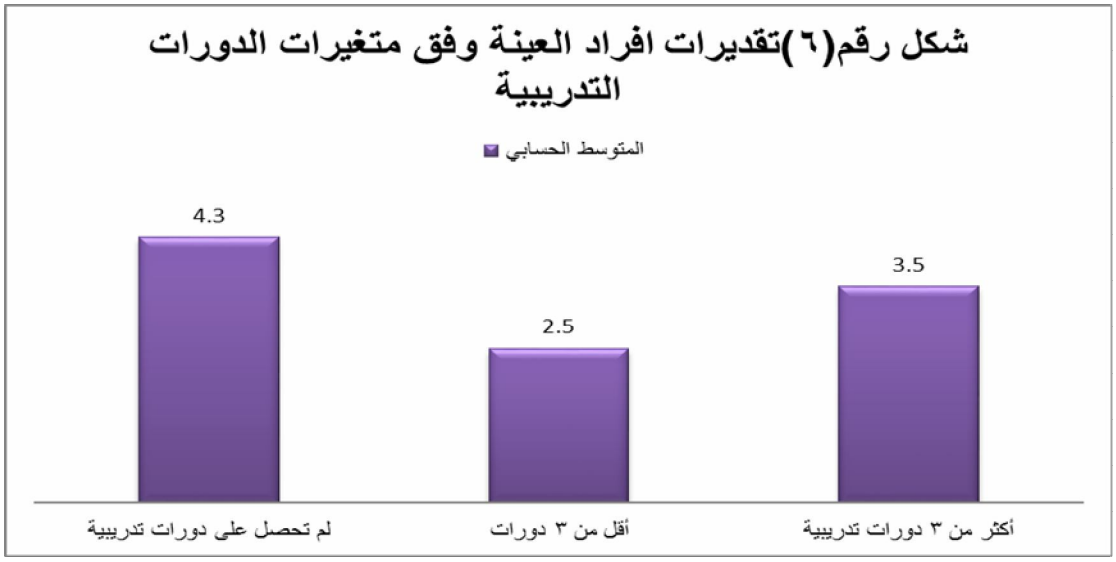
وللإجابة عن هذا السؤال استخدمت الباحثة اختبار التباين الأحادي.

جدول رقم (٩) مصدر التباين ومجموع المربعات ودرجات الحرية ومتوسط المربعات وقيمة "ف" للاستبانة تعزى لمتغير الدورات التدريبية

البعدان	المصدر	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة"ف"	مستوى الدلالة
المجال ككل	بين المجموعات	٨٧،٤٢٢	٢	٤٣،٧١١	٠،١٢٠	٠،٨٨٧ غير دالة
	داخل المجموعات	٧٦٤،١١	١٠٤	٣٦٥،٦٥١		
	المجموع الكلي	٧٦٥،٥٣	١٠٦			

يتضح من خلال الجدول السابق أن قيمة " ف" المحسوبة تساوي (١٢٠،٠) وهي أقل من قيمة (ف) الجدولية عند مستوى الدلالة(٠،٠٥) وبذلك لا يوجد فروق ذات دلالة إحصائية بين بين متوسطات استجابات أفراد مجتمع الدراسة عند مستوى الدلالة (0,05≤) في درجة وعي معلمات الحاسب للأمن السيبراني تعزى لاختلاف الدورات التدريبية، وقد يرجع ذلك إلى أن معلمات الحاسوب بغض النظر عن الدورات التدريبية فإن مستوى الوعي بالأمن السيبراني واضح لديهم إلى حد بعيد باعتبار أنه يمكن ملاحظته بسهولة، وتدربوا عليه عمليًا من واقع عملهم وتعاملهم مع الحاسب بصورة مستمرة.

ويمكن عرض النتائج السابقة كما في الشكل التالي:

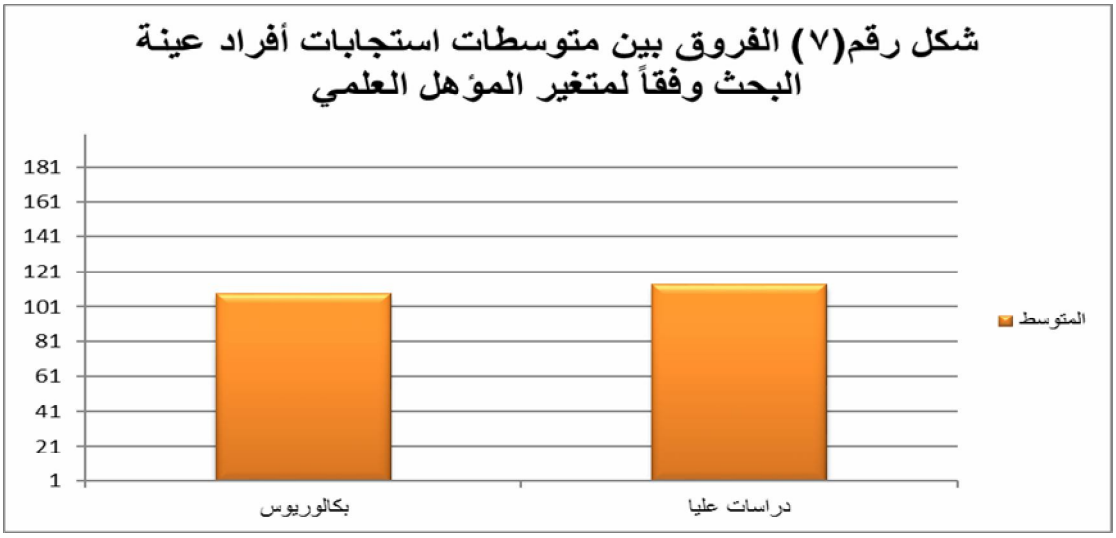


٢- متغير المؤهل العلمي:
وللإجابة عن هذا السؤال استخدم الباحث اختبار "ت".

جدول رقم (١٠) المتوسط والانحراف المعياري وقيمة "ت" للاستبانة تعزى لمتغير المؤهل العلمي

المقياس	المؤهل العلمي	العدد	المتوسط	الانحراف المعياري	قيمة ت	مستوى الدلالة
	بكالوريوس	٧٩	١٠٨,٣٣	١٩،٤٩٦	١،٨٥٠	غير دالة
	دراسات عليا	٢٧	١١٣,٣٥	١٧،٨٧٨		

يتضح من خلال الجدول السابق أن قيمة (ت) المحسوبة تساوي (١,٨٥٠) وهي أصغر من قيمة(ت) الجدولية والتي تساوي (٩٨،١) عند درجة حرية (١٩٠). وهذا يشير إلى عدم وجود فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد عينة الدراسة عند مستوى الدلالة (0,05≥) في درجة وعي معلمات الحاسب بالأمن السيبراني تعزى لمتغير المؤهل العلمي، وقد يرجع إلى متابعة المشرفات التربويات لمستجدات الأمن السيبراني، وما يرتبط بها تطورات ونشرات وأبعاد مستحدثة، مدفوعين بأهمية التنمية المهنية المستدامة واطلاعهم على الجديد فيما يخص الحاسب والتطورات والمستجدات المرتبطة بهم.



٣- متغير سنوات الخبرة:

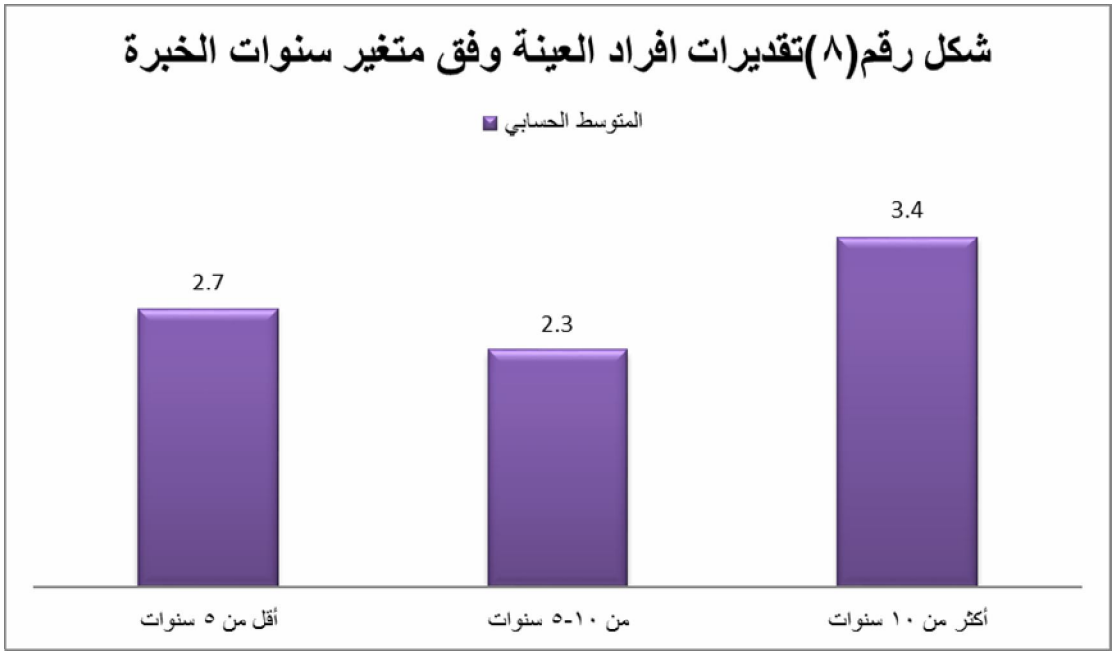
وللإجابة عن هذا السؤال استخدمت الباحثة اختبار التباين الأحادي والجدول التالي رقم () يبين ذلك:

جدول رقم (١١) مصدر التباين ومجموع المربعات ودرجات الحرية ومتوسط المربعات وقيمة "ف" للاستبانة تعزى لمتغير سنوات الخبرة

البعدان	المصدر	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة"ف"	مستوى الدلالة
المقياس ككل	بين المجموعات	٠,٩١٤	٢	٠,٤٧١	١,٢٣	٠،٢٩ غير دالة
	داخل المجموعات	١١٣,٣٦٧	١٠٤	٠,٣٨٢		
	المجموع الكلي	٧٦٥،٥٣	١٠٦			

يتضح من خلال الجدول السابق أن قيمة " ف" المحسوبة تساوي (١,٢٣) وهي أقل من قيمة (ف) الجدولية عند مستوى الدلالة (٠,٠٥) وبذلك لا يوجد فروق ذات دلالة إحصائية بين بين متوسطات استجابات أفراد عينة الدراسة عند مستوى الدلالة (≤٠,٠٥) في درجة الوعي بالأمن السيبراني تعزى لاختلاف سنوات الخبرة.

ويمكن عرض النتائج السابقة كما في الشكل التالي:



وربما ترجع هذه النتيجة إلى أن إلمام المعلمات بتلك النماذج باعتبار أن موضوعات الأمن السيبراني ومفاهيمها منتشرة في الأوساط التربوية والأوساط التقنية مما يكون لدى المعلمات معرفة كافية لديهم والتطرق إلى التفاصيل الخاصة بها بصرف النظر عن سنوات الخبرة لديهن.

نتائج الدراسة:

بعد الاطلاع على الأدبيات والدراسات السابقة يمكن عرض ملخص لأهم نتائج الدراسة الحالية كما يلي:

١. يهتم الأمن السيبراني بأمن كل ما هو موجود على السايبر من غير امن المعلومات، في حين أن أمن المعلومات لا يهتم، كما يهتم أمن المعلومات بأمان المعلومات المادية، في حين أن الأمن السيبراني لا يهتم بها.
٢. من اهم الدوافع للجريمة الالكترونية بالمملكة العربية السعودية من خلال الادبيات اتت ترتيبها على النحو التالي:
٣. الدوافع النفسية – الجنسية- العقائدية – العنصرية.
٤. أن المملكة العربية السعودية كانت أول دولة عربية سنت نظامًا خاصًا لمكافحة الجريمة الإلكترونية، تلتها الإمارات العربية المتحدة، وبعد ذلك سلطنة عمان.
٥. من الصعب اكتشاف الجريمة الإلكترونية، حيث يبدو من الواضح أن عدد الحالات التي اكتشفت فيها هذه الجرائم قليل مقارنة بالجرائم التقليدية. يمكن تفسير الأسباب الكامنة وراء صعوبة اكتشاف الجريمة السيبرانية من خلال حقيقة أن هذه الجريمة لا تترك أي تأثير خارجي مرئي يمكن للجاني أن يرتكب هذه الجريمة في دول وقارات أخرى، لأن الجريمة الإلكترونية هي جريمة عبر وطنية.

٦. اكتشاف الجريمة السيبرانية ليس بالأمر السهل، وان ذلك الأمر يتطلب الكثير من الجهد والخبرة.
٧. تتطلب طبيعة الجريمة الإلكترونية عمومًا طرقًا غير تقليدية للتحقيق. يتطلب اكتشاف الأدلة الرقمية ودعمها إجراءً سريعًا، لأن الأدلة الإلكترونية غير جوهرية ويمكن القضاء على أي أدلة أو أدلة من جانب مرتكبي الجرائم الإلكترونية. وإجراء الفحص وإجراء التحقيقات والتفتيش والاستجواب بشأنها في الجرائم التقليدية، بالنظر إلى وهج الجرائم الإلكترونية والحصانة.
٨. من اهم أسباب الابتزاز الإلكتروني في المملكة على الفرد والمجتمع: قلة ثقافة مستخدمي الإنترنت وانعدام أمنهم لوجود مثل هذه الجرائم، والتي تشكل عقبة رئيسية أمام تطوير التجارة الإلكترونية والاتصال الإلكتروني في العالم العربي، وخاصة المعاملات الإلكترونية بشكل عام ، ولكن قد يفقد الفرد المستندات والمعلومات الشخصية والصور الشخصية بسبب هذه الاختراقات الإلكترونية.
٩. تفتقر العديد من الحكومات العربية إلى الموارد البشرية والمالية، فضلاً عن إرادة واضحة وحازمة لمتابعة الأنشطة غير القانونية من أراضيها. وفي هذا الصدد، يجب التركيز على الحاجة إلى التعاون بين القطاعين العام والخاص والمجتمع المدني لتعزيز ثقافة احترام القانون في الفضاء الإلكتروني وحماية الحقوق والحريات الأساسية.
١٠. تبين من خلال الادبيات ان هناك ثغرات تشريعية في النظم القانونية العربية فيما يتعلق بالقضايا المتعلقة بتحقيق الأمن والثقة في الفضاء الإلكتروني.
١١. توضح هذه الدراسة أنه يمكن توفير التوعية وتأكيد ضمان المعلومات في شكل جذاب. تم استخدام الوعي السرياني لتلبية مجموعة محددة من متطلبات تدريب المعلمات، مما يدل على أنه مرن بما فيه الكفاية لتوضيح مجموعة من موضوعات الأمان في مجموعة متنوعة من البيئات، العامة منها والمؤسسة على حد سواء.

توصيات الدراسة Recommendations of the study:

في ضوء ما توصل إليه البحث من نتائج، كانت أهم التوصيات ما يلي:

١. توفير برامج تدريبية مجانية متعمقة في الأمن السيبراني للمعلمات الآتي على رأس العمل.
٢. إلحاق المعلمات بدبلومات بالأمن السيبراني يرفع مستوى الفهم والوعي والتطبيق لديهن.
٣. دمج الأمن السيبراني في البرامج التربوية الموجودة محليًا.
٤. إصدار تعاميم خاصة بالأنظمة والتشريعات المستحدثة للأمن السيبراني من الوزارة وتعميمها للمدارس.
٥. دمج الأنظمة والتشريعات ضمن مدونة السلوك الوظيفي.
٦. ضرورة اهتمام المؤسسات التعليمية بالندوات والورش التدريبية التي تبرز أهمية تطوير الأمن السيبراني.
٧. الاستعانة بالخبرات في وزارة التعليم لتطوير وسائل الأمن السيبراني في مختلف المؤسسات التعليمية.
٨. توفير الحوافز المادية والمعنوية للمطورين والمبرمجين.
٩. تدريب معلمات الحاسب على خطوات وإجراءات تتصدى لأي سلوك غير مقبول في المجتمعات الرقمية.

قائمة المراجع

أولاً: المراجع العربية:

إبراهيم، خالد ممدوح (٢٠٠٩). فن التحقيق الجنائي في الجرائم الإلكترونية. الإسكندرية: دار الفكر الجامعي.

ابن عسكر، منصور بن عبد الرحمن (٢٠١٢). "استطلاع آراء الشباب السعودي حول دور المؤسسات الاجتماعية في التبصير بالجرائم الإلكترونية." مجلة دراسات وأبحاث - جامعة الجلفة - الجزائر ع ٦: ٨ - ٣٥.

أحمد، شاذلى صديق محمد، وأحمد عوض حاج علي (٢٠١٥). "اكتشاف هجوم التصيد الالكتروني باستخدام خوارزمية تحسين الحد الادنى التسلسلية." مجلة الدراسات العليا: جامعة النيلين - كلية الدراسات العليا مج٣، ع١٢: ١٠٢ - ١١٩ .

أحمد، عبد الخالق محمد (٢٠١٤). "الهندسة الاجتماعية." المال والاقتصاد: بنك فيصل الاسلامي السوداني ع٧٥: ٢٢ - ٢٣.

البادي، محمد بن حمد (٢٠١٧). الابتزاز الإلكتروني، جريدة الرؤية الإلكترونية، متاح على: http://cutt.us/zuAf8

بطوش، كمال (٢٠٠٨). "الجريمة داخل البيئة الإليكترونية نتيجة تطور تكنولوجي أم بداية إجرام جديد؟ " مجلة الأكاديمية للدراسات الاجتماعية والإنسانية: جامعة حسيبة بن بوعلي بالشلف: ٤٨ - ٥٥.

البوابة العربية للأخبار التقنية (٢٠١٧). الاختراق بالهندسة الاجتماعية.. ماذا تعرف عنه؟، متاح على: http://cutt.us/tpz9w

الترتوري، محمد عوض وجويحان، أغادير عرفات(٢٠٠٦)، علم الإرهاب الأسس الفكرية والنفسية والاجتماعية والتربوية لدراسة الإرهاب، الطبعة الأولى، دار الحامد.

ثريا قاسمي (٢٠١٨). عربيات في شرك الابتزاز الجنسي، متاح على: http://cutt.us/AtBzp

جريدة الإمارات اليوم (٢٠١٥). صدمة آخر الليل: تحقيق: محمد فودة، متاح على: http://cutt.us/IsX2H .

جريدة الشعب الجديد (٢٠١٣). مقال بعنوان: ٣٠ ألف خليجي يتعرضون لابتزاز جنسي عبر الإنترنت، متاح على: http://cutt.us/CJnce .

جريدة المواطن (٢٠١٧) ماهو الأمن السيبراني؟، متاح على: https://www.almowaten.net/?p=1500515

جمعة، صفاء فتوح(٢٠١٤) مسئولية الموظف العام فى إطار تطبيق نظام الإدارة الإلكترونية، دار الفكر والقانون، المنصورة، مصر.

جواد، أشرف حسن محمد (٢٠١٥). "الجريمة المعلوماتية والإلكترونية: أنواعها وخصائصها وطرق الوقاية منها ".مجلة الدراسات المالية والمصرفية - الاكاديمية العربية للعلوم المالية والمصرفية - الأردن مج٢٣، ع١: ٢٩ - ٣٣ .

الحربي، أمينة بنت حجاب عبد الله (٢٠١٦). تصور مقترح لتنمية الوعي الوقائي لدى الفتيات للوقاية من جرائم الابتزاز، أطروحة دكتوراه-جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاجتماعية والإدارية، قسم علم الاجتماع، تخصص علم اجتماع الجريمة.

حسن، عبيد صالح (٢٠١٥). "سياسة المشروع الإماراتي لمواجهة الجرائم الإلكترونية ".الفكر الشرطي مج٢٤، ع٩٥: ٢١ - ٥٢ .

دبابنة، شيرين (٢٠١٥). "الجرائم الالكترونية القرصنة الالكترونية ".مجلة الدراسات المالية والمصرفية - الاكاديمية العربية للعلوم المالية والمصرفية - الأردن مج٢٣، ع١: ١٩ - ٢٢.

الدباغ، رائد عبدالقادر حامد، و بشرى علي زينل(٢٠١٢). "فاعلية التدريب في تحقيق نجاح أمن نظم المعلومات: دراسة استطلاعية لآراء عينة من العاملين في نظم المعلومات بجامعة الموصل ".تنمية الرافدين: جامعة الموصل - كلية الادارة والاقتصاد مج ٣٤، ع ١١٠: ١٢٣ - ١٤٠ .

الدريبي، فهد(٢٠١٧). الأمن السيبراني، ما هو؟ متاح على: https://www.fadvisor.net/blog/2017/11/what_is_cyber_security/

الدليجان، عهود عبد العزيز (٢٠١٠). عرض لأشهر وسائل السمات الحيوية. مركز التميز لأمن المعلومات. متاح في: http://coeia.edu.sa

الدهشان، جمال علي خليل، و هزاع بن عبدالكريم الفويهي(٢٠١٥). "المواطنة الرقمية مدخلا لمساعدة أبناءنا على الحياة في العصر الرقمي ".مجلة البحوث النفسية والتربوية - كلية التربية جامعة المنوفية - مصر مج٣٠، ع٤: ١ - ٤٢.

الدوسري، فؤاد فهيد شائع (٢٠١٧). "مستوى توافر معايير المواطنة الرقمية لدى معلمي الحاسب الآلي ".دراسات فى المناهج وطرق التدريس -مصر ع٢١٩: ١٠٧ - ١٤٠.

الزبيدي، فوزي حسن (٢٠١٥). "منهجية تقييم أخطار الأمن القومي: دراسة تحليلية لمنهجية تقييم أخطار الأمن القومي ".NSRA رؤى استراتيجية: مركز الإمارات للدراسات والبحوث الاستراتيجية مج٣، ع١١: ٨ - ٤٧ .

سعيد، فهد عبد العزيز (٢٠١٠). الخصوصية عبر الإنترنت، المقالات العالمية، مركز التميز لأمن المعلومات.

السكران، عبد الله بن فالح بن راشد (٢٠١٢). "دور المعلم في تقديم التوعية الأمنية: دراسة ميدانية علي معلمي المرحلة الثانوية بمدينة الرياض." مجلة البحوث الأمنية: كلية الملك فهد الأمنية - مركز البحوث والدراسات مج ٢١، ع ٥٣: ١٣٧ - ١٩٣

السلطان، فهد السلطان(١٤٢٩هـ). التربية الأمنية ودورها في تحقيق الأمن الوطني، بحث مقدم إلى الندوة العلمية "الأمن مسؤولية الجميع". الأمن العام، الرياض.

السليمان، ياسين (٢٠١٥). الابتزاز الإلكتروني.. خطر المافيات الدولية يحدق بشباب الخليج، الخليج أونلاين، متاح على: http://cutt.us/UP2tw .

السموني، خالد الشرقاوي (٢٠١٢). "مكافحة الجرائم الالكترونية على ضوء التشريعين الوطني والدولي." المجلة المغربية للإدارة المحلية والتنمية - المغرب ع ١٠٢: ١٢٧ - ١٣٧.

السويحلى، محمد أحمد (٢٠١٥). "تكاتف الجهود العربية لمكافحة الجريمة الالكترونية ".مجلة الدراسات المالية والمصرفية - الاكاديمية العربية للعلوم المالية والمصرفية - الأردن مج٢٣، ع١: ٦ .

شلتوت، محمد شوقي (٢٠١٦). "المواطنة الرقمية: ترف فكرى أم ضرورة؟ " مجلة فكر - مركز العبيكان للأبحاث والنشر - السعودية ع١٥: ١٠٤ - ١٠٥.

الشمري، فلاح(١٤٢٨ه) جريمة ابتزاز النساء ودور جهاز الحسبة في مكافحتها، رسالة ماجستير غير منشورة، جامعة مؤته، الأردن.

الشهري، فايز بن عبد الله (٢٠٠٥). التحديات الأمنية لوسائل الاتصال الجديدة – دراسة الظاهرة الإجرامية على شبكة الإنترنت. – دراسة الظاهرة الإجرامية على شبكة الإنترنت، المجلة العربية للدراسات الأمنية والتدريب، المجلد ٢٠، العدد ٣٩،

الشهري، موسى (١٤٢٩ه). تطوير التعاون بين الإدارة المدرسية والمؤسسات الأمنية في مجال التوعية الأمنية لطلاب المرحلة الثانوية، رسالة ماجستير غير منشورة، جامعة الملك خالد، أبها

صالح، سادات فيصل عبدالفتاح، و معاوية محمد الحسن عبدالله (٢٠١٦). "أثر نظام الرقابة الداخلية فى تحقيق أمن المعلومات المحاسبية: دراسة ميدانية." مجلة جامعة القرآن الكريم والعلوم الإسلامية: جامعة القرآن الكريم والعلوم الإسلامية - مركز بحوث القرآن الكريم والسنة النبوية س١٩، ملحق: ١٩١ - ٢٣٤ .

صلاح الدين، أشرف. "طرق الحماية التكنولوجية بأنواعها وأشكالها المختلفة." في أعمال ندوات: مكافحة الجريمة عبر الانترنت - وورشة عمل: أمن المعلومات والتوقيع الإلكتروني: المنظمة العربية للتنمية الإدارية القاهرة: المنظمة العربية للتنمية الإدارية، (٢٠١٠): ٢٠٣ - ٢١٥.

الصوفي، عبد الله. (٢٠١٢). التكنولوجيا الحديثة والتربية والتعليم، ط٣ عمان: مؤسسة الوراق للنشر والتوزيع.

الصيقل، يزيد بن إبراهيم (٢٠١٧). العوامل المحددة للجرائم الإلكترونية، أطروحة دكتوراه-جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاجتماعية، قسم علم الاجتماع، تخصص علم اجتماع الجريمة.

طه، محمود سري (١٩٩٠). الحاسوب في مجالات الحياة. الهيئة المصرية العامة للكتاب، القاهرة، ١٩٩٠م.

الطيب، مصطفي (٢٠١٨) الفرق بين أمن المعلومات والأمن السيبراني، مدونة علوم، متاح على: http://cutt.us/hOmY0

عابدين، محمد الفاتح (٢٠١٨) الابتزاز الإلكتروني.. جريمة العصر، متاح على: http://cutt.us/NEyQg

العادلي، محمود (٢٠٠٦). " الجرائم المعلوماتية " ورقة عمل مقدمة في مجال مكافحة الجرائم الالكترونية"، سلطنة عمان.

العباس، بومامى(٢٠١٥). "الجريمة الإلكترونية نتاج أجهزة ومواقع تواصل إجتماعى." مجلة جيل العلوم الإنسانية والاجتماعية: مركز جيل البحث العلمي ع١٢: ١٦١ - ١٨٧.

علوان، عماد عبده محمد (٢٠١٦). "أشكال التنمر في ضوء بعض المتغيرات الديموغرافية بين الطلاب المراهقين بمدينة أبها." مجلة التربية: جامعة الأزهر - كلية التربية ع١٦٨، ج١: ٤٣٩ - ٤٧٣.

علي موسي الصبحيين، محمد فرحان القضاة (٢٠١٣). سلوك التنمر عند الاطفال والمراهقين" مفهومه، أسبابه، علاجه"، مكتبة الملك فهد الوطنية، الرياض.

العيد نوال (١٤٣٢). بحوث ندوة الابتزاز: المفهوم- الأسباب- العلاج، بحث مقدم لمركز باحثات لدراسات المرأة، الرياض.

الغديان، سليمان بن عبد الرزاق، يحيى بن مبارك خطاطبة، و عز الدين عبدالله عواد النعيمي (٢٠١٨). "صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين." مجلة البحوث الأمنية: كلية الملك فهد الأمنية - مركز البحوث والدراسات مج٢٧، ع٦٩: ١٥٧ - ٢٢٧.

فتيحة، عمارة، وبدرة عمارة (٢٠١٤). "الحماية الجنائية للمعلومات الالكترونية في إطار قانون الملكية الفكرية." مجلة الحقيقة: جامعة أحمد دراية أدرار ع٣١: ٢٠٧ - ٢٤٨.

الفرجابي، صلاح الدين محمد علي (٢٠١٧). "الجرائم الإلكترونية باستخدام شبكة الانترنت والبريد الإلكتروني ".المال والاقتصاد (بنك فيصل الاسلامي السوداني) - السودان ع٨١: ٣٦ - ٣٩.

فكري، ايمن عبد الله (٢٠١٤) الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض.

قطامي، نايفة ومنى الصرايرة (٢٠٠٩) الطالب المتنمر، دار المسيرة للنشر والتوزيع والطباعة، عمان.

الكعبي، عبيد (٢٠٠٥). "الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت"، دار النهضة العربية القاهرة.

اللبان، شريف درويش (٢٠٠٠). تكنولوجيا الاتصال- المخاطر والتحيات والتأثيرات الاجتماعية، ط١، الدار المصري اللبنانية، القاهرة،

اللمتوني، عبد الرحمن (٢٠١٤). الإجرام المعلوماتي بين ثبات النص وتطور الجريمة، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع.

مازن، حسام الدين محمد (٢٠١٦). إصحاح مناهج العلوم وبرامج التربية العلمية وهندستها إلكترونيا في ضوء تحديات ما بعد الحداثة والمواطنة الرقمية. "المؤتمر العلمي الثامن عشر: مناهج العلوم بين المصرية والعالمية - الجمعية المصرية للتربية العلمية - مصر القاهرة: مركز الشيخ صالح كامل - جامعة الأزهر: ٧٧ - ٩٣.

المبارك، عبد الله (٢٠١٦) ما الفرق بين Cyber Security و Information Security ؟، متاح على: http://cutt.us/Hq8uE

محمد، محمد أحمد ثابت(٢٠١٤). "فوضى المعلومات الشبكية و تأثيرها على ضعف الإفادة من المعلومات: دراسة تحليلية على الشبكات الاجتماعية." مجلة بحوث في علم المكتبات والمعلومات: جامعة القاهرة - كلية الآداب - مركز بحوث نظم وخدمات المعلومات ع١٣: ١٢٧ - ١٨١.

محمود، رعد سعدون، و حسن جلوب كاظم (٢٠١٥). "الجرائم الالكترونية ".مجلة الدراسات المالية والمصرفية - الاكاديمية العربية للعلوم المالية والمصرفية - الأردنمج٢٣، ع٣: ٣٥ - ٤٠.

مرسي، أحمد (٢٠١٧) «الابتزاز الإلكتروني».. جريمة سلاحها الخوف من الفضيحة، جريدة الاتحاد، متاح على الرابط: http://cutt.us/Vkrz6

المركز الديمقراطى العربى(٢٠١٥). استراتيجية أمن المعلومات فى ظل حروب الجيل السادس، متاح على: https://democraticac.de/?p=19750

المسلماني، لمياء إبراهيم (٢٠١٤). التعليم والمواطنة الرقمية: رؤية مقترحة، القاهرة: عالم التربية، ١٥(٤٧)، ١٥-٤٩.

المسيري، هيثم (٢٠١١). "تقنيات البنوك الإلكترونية." في أعمال ملتقيات وندوات (المصارف الإسلامية: الواقع والتحديات) - المنظمة العربية للتنمية الإدارية - مصر القاهرة: المنظمة العربية للتنمية الإدارية،: ٢١٩ - ٢٢٨.

مصبح، عمر عبد المجيد (٢٠١٦). "دور النقود الالكترونية فى جرائم غسل الأموال ".مجلة الحقوق - كلية الحقوق - جامعة البحرين - البحرين مج١٣، ع١: ١٦٠ - ١٩٣.

مصري، عبد الصبور عبد القوي على (٢٠١٢). التنظيم القانوني للتجارة الإلكترونية، مكتبة القانون والاقتصاد، الرياض.

المطيري، سامي بن مرزوق نجاء (٢٠١٥). المسئولية الجنائية عن الابتزاز الإلكتروني في النظام السعودي، أطروحة (ماجستير)-جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الشريعة والقانون.

المطيري، نورة مشعان. (٢٠١٤). تقييم الأداء التدريسي لمعلمة الحاسب الآلي بالمرحلة المتوسطة في ضوء معايير الجمعية العالمية للتقنية في التعليم (رسالة ماجستير غير منشورة). كلية التربية، جامعة القصيم، السعودية.

المنشاوي، محمد عبد الله (٢٠٠٣): جرائم الإنترنت في المجتمع السعودي، رسالة ماجستير، كلية الدراسات العليا، جامعة الملك سعود.

المنشاوي، محمد عبد الله (٢٠٠٣): جرائم الإنترنت في المجتمع السعودي، رسالة ماجستير، كلية الدراسات العليا، جامعة الملك سعود.

موسى، مصطفى محمد (٢٠٠٩) التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة، القاهرة.

موقع الابتزاز الالكتروني: عقوبة جريمة الإبتزاز في دولة الإمارات العربية المتحدة، متاح على: http://cutt.us/8G6BI

النصر، تركي بن حمد هلال (٢٠١٧). لتحقيق في جريمتي التحرش والابتزاز عبر الشبكات الإلكترونية: دراسة تطبيقية على هيئة التحقيق والادعاء العام بالمنطقة الشرقية، رسالة ماجستير - جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الدراسات الأمنية.

نوال بنت عبد العزيز العيد(١٤٣٥هـ). الابتزاز: المفهوم، الأسباب، العلاج، متاح على: http://nawalaleid.com/cnt/lib/768

الهاجري، إياس (٢٠٠٢). بحث بعنوان (جرائم الانترنت)، متاح على: http://cutt.us/Zj4C6

هالة حسن بن سعد الجزار (٢٠١٤). "دور المؤسسة التربوية فى غرس قيم المواطنة الرقمية: تصور مقترح ".دراسات عربية في التربية وعلم النفس - السعودية ع٥٦: ٣٨٥ - ٤١٨.

هيئة الاتصالات وتقنية المعلومات السعودية: نظام مكافحة جرائم المعلوماتية، متاح على الرابط: http://cutt.us/mJSuI

وزارة الاتصالات وتكنولوجيا المعلومات المصرية (٢٠١٩). الأمن السيبراني، متاح على: http://www.mcit.gov.eg/Ar/TeleCommunications/Cyber_Security

وهدان، وهدان (٢٠١٢). "جرائم الحاسوب: أنواعها وأخطارها." المعرفة: وزارة الثقافة س ٥١، ع ٥٩٠: ١٩٢ - ١٩٩.

ثانياً: المراجع الأجنبية:

Bulach,T; Osborn, R., & Samara, M., (2012) Bullying in Secondary Schools: What it looks like aiitl How to Manage it?. New York: Sage Publishing.

Connell, N., Schell-Busey, N., Pearce, A., & Negro, P. (2013). Badgrlz? Exploring sex differences in cyberbullying behaviors. Youth Violence and Juvenile Justice, 12 (3), 209.

Debray Stéphane (2013) Internet face aux substances illicite complice de la cybercriminalité ou outil de prevention – DESS media électronique et internet – uinversité de Paris.

Jaana, J; Cornell, D; Sheras, G. (2011). Identification of School Bullies by Survery Methods. Professional School Counseling, 9 ,(4), 305 - 313.

Kotler, James. “A Survey of Sanctions Awarded for E-Discovery Violations.” Proof, Vol. 17, No. (2), American Bar Association, (Winter 2009).

Kraut, R., Patterson, M., lundmark, V., kiesler, S., Mukophadhyay, T. & scherlis, W. (1998). Internet paradox: A social technology that reduces social involvement and psychological well-being? American Psychologist, 53(9), 1017- 1031.

Lapidot-Lefler, N., & Dolev-Cohen, M. (2015). Comparing cyberbullying and school bullying among school students: prevalence, gender, and grade level differences. Social psychology of education, 18(1), 1-16.

Lim, Cher Ping, Yan, Hanbing & Xiong, Xibei. (2015). Development of pre-service teachers' information and communication technology (ICT) in education competencies in a mainland Chinese university. Educational Media International, 52(1), 15-32.

Lipson, G. (2001). Bullying in schools fighting the bully Battle. Eribaum: National School Safety Center, NJ.

Rossein, Merrick T. Nuts and Bolts of Electronic Evidence. Employment Discrimination Law and Litigation, (November 2010).

Sheikli, Mazen Haitham Razouki. "Firewall Using Genetic Algorithm as Computational Tools." Al - Ma'amoun College Journal: Al - Ma'moun College, University, p. 24 (2014): 217 - 228.

Shepherd, K. & Edelmann, M. (2005) Reasons for internet use and anxiety, Journal of Personality and Individual Differences, 39(5), 949-958.