درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات

Study Title: The degree of Awareness of Middle Stage Female Teachers of Cybersecurity In Public Schools In Jeddah City From The Point of View of The Teachers

إعداد

فاطمة يوسف المنتشري

د/ رندة حريري

كلية العلوم الصحية والسلوكية والتعليم - جامعة دار الحكمة بجدة

Doi: 10.33850/ejev.2020.101830

استلام البحث: ٧ / ٥ / ٢٠٢٠ قبول النشر: ٢٥ / ٥ / ٢٠٢٠

المستخلص:

هدفت الدراسة إلى التعرف على درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. ولتحقيق أهداف الدراسة تم اتباع المنهج الكمي الوصفي التحليلي، وتم إعداد استبانة مكونة من (٢١) فقرة، وتشمل ثلاثة محاور: مفاهيم الأمن السيبراني، مخاطر الأمن السيبراني، وانتهاكات الأمن السيبراني. وتم تطبيق الاستبانة على عينة عشوائية مكونة من (٣٦٢) من معلمات المرحلة المتوسطة بمدينة جدة. وأظهرت النتائج أن معلمات المرحلة المتوسطة على درجة متوسطة من الوعي بكل من مفاهيم الأمن السيبراني، مخاطر الأمن السيبراني، وانتهاكات الأمن السيبراني، وعدم وجود فروق ذات دلالة إحصائية عند مستوى (0.05) تُعزى إلى متغيري المؤهل الدراسي، وعدد سنوات الخبرة بين استجابات المعلمات في حين أظهرت النتائج وجود فروق ذات دلالة إحصائية عند مستوى دلالة (0.05) تُعزى إلى متغير دورات تدريبية في الأمن السيبراني. وتوصلت الدراسة إلى بعض التوصيات أهمها عقد دورات تدريبية للمعلمات في مجال الأمن السيبراني، وورش عمل حول إجراءات الحماية ضد المخاطر والانتهاكات السيبرانية، التنسيق بين وزارة التعليم والجهات المشرفة على الأمن السيبراني كالهيئة الوطنية للأمن السيبراني لاتخاذ الإجراءات اللازمة ولتنمية الوعي لدى المعلمات في مجال الأمن السيبراني.

الكلمات المفتاحية: مفاهيم الأمن السيبراني – المخاطر السيبرانية – الانتهاكات السيبرانية.

Abstract:

The study aimed at identifying the degree of awareness of middle stage female teachers of cybersecurity in public schools in Jeddah city from the point of view of the teachers. To achieve the study objectives, a descriptive analytical quantitative methodology was adopted. A questionnaire prepared from (21) items divided into three fields: cybersecurity concepts, cybersecurity risks, and cybersecurity violations. The sample of the study consisted of (362) female teachers at middle schools in Jeddah city. The results of the study showed a middle degree of awareness for both of cybersecurity concepts, cybersecurity risks, and cybersecurity violations. There is no statistically significant differences at level (0.05) attributed to the variables of academic qualification and experience years between the responses of the female teachers, while there are statistically significant differences at level (0.05) attributed to the variable of cybersecurity courses. The following recommendations are based on the study findings: Organize cyber security courses. Organize workshops to discuss how to protect ourselves against cyber security risks and prevent data breaches. Coordinate between ministry of education and national cybersecurity authority to take the required procedures to increase cyber security awareness between female teachers.

Key words: cybersecurity concepts - cybersecurity risks - cybersecurity violations.

مقدمة:

أدت الثورة الرقمية المعاصرة إلى تطورات هائلة غير مسبوقة، شملت جميع مجالات النشاط الإنساني، بما في ذلك الأنشطة الحياتية اليومية وصولًا إلى المجالات العلمية والتربوية والسياسية والاقتصادية، وغير ذلك من مجالات، وترافق ذلك مع تدفق المعلومات المختلفة عبر شبكة الإنترنت، وانتشار لوسائل الوصول لمصادر المعلومات، بما في ذلك الحواسيب المكتبية، والمحمولة، والهواتف الذكية.

وكما كان لظهور شبكة الإنترنت وتدفق المعلومات أثرًا مهمًّا في كافة المجالات الحياتية، فقد شكل هذا الأمر مصدر تهديد لمستخدمي الشبكة العنكبوتية، عبر ما يُعرف بالهجمات السيبرانيةCyber Attacks أو الجرائم السيبرانية Cyber Crimes، التي يُمكن من خلالها إيقاع خسائر فادحة عبر التسبب في شلل بيئة المعلومات والاتصالات الخاصة بمستخدم ما أو بجهة معينة، مما قد يصل في بعض الأحيان إلى خسائر فادحة، قد تصل إلى التلاعب بالبيانات أو تزييفها، أو محوها من أجهزة الحواسيب (خليفة، ٢٠١٧، ص ٩).

وتزداد أهمية الأمن السيبراني باعتباره يشمل جميع الجوانب التعليمية، والاجتماعية، والاقتصادية، والإنسانية، وباعتباره ممثلًا لقدرة الدولة على حماية مصالحها وشعبها، في مختلف مجالات حياته اليومية، ومسيرته نحو التقدم بأمان، ومن كونه يرتبط ارتباطًا وثيقًا بسلامة مصادر الثروة المعلوماتية في العصر الحالي، والقدرة على الاتصال والتواصل، وهي المحور الذي يتكون حوله الإنتاج، والإبداع، والقدرة على المنافسة (جبور، ٢٠١٢، ص ٧).

ووفقًا لدراسة مسحية أجراها مكتب الأمم المتحدة عام (٢٠١٢م) شملت الدول الأعضاء في منظمة الأمم المتحدة، وعددها (١٩٣) دولة، وُجد أن (١١٤) دولة لديها برامج وطنية للأمن السيبراني، وأن (٤٧) دولة أناطت تلك المهمة لمؤسسات مدنية منها المدارس والجامعات (خليفة، ٢٠١٧، ص ١٧٣)، فعلى سبيل المثال قامت الولايات المتحدة بإنشاء معهد مهني لاستقطاب البرامج القصيرة المختصة بالأمن السيبراني بحضور أكثر من ألف ومئتان مشاركٍ عالميٍّ ما بين طلاب، ومعلمين، لدورات مدتها من يوم إلى خمسة أيام (عبد الصادق، ٢٠٠٩).

وقد اهتمت دول العالم بدور المؤسسات التربوية؛ نظرًا لدور تلك المؤسسات في إعداد المعلمين بشكل يُمكنهم من التعامل مع كافة التطورات التكنولوجية، والتي يُتوقع أن تصل إلى آفاق أبعد في عالم الغد، وما يتطلبه هذا التعامل من درجة وعي كافية بالأمن السيبراني.

وفي إطار تلك المبادرة قام مركز علوم الحاسوب والتكنولوجيا والهندسة والرياضيات STEM التابع لأكاديمية الولايات المتحدة البحرية في ولاية ميريلاند بتدريب المعلمين في مختلف المراحل الدراسية، عبر ورش عمل تربوية للتدريب على أساسيات تكنولوجيا الإنترنت والأمن السيبراني، وشمل ذلك موضوعات التشفير، الشبكات، وسائل التواصل الاجتماعي، الفيروسات، البرمجيات الخبيثة، التوثيق، القرصنة (Fees et. al., 2018)، واتخذ الاتحاد الأوربي عام (٢٠٠٩) قرارًا بإدراج المفاهيم المتعلقة بالأمن السيبراني ضمن المناهج الدراسية في (٢٤) دولة أوربية، وذلك في مختلف المراحل الدراسية (R.Solms & S.Solms, 2015)، واتخذت العديد من الدول الآسيوية

إجراءات مماثلة لتفعيل دور المؤسسات التربوية، ودور المعلم في مجال الأمن السيبراني، ومنها: اليابان، سنغافورة، ماليزيا، الهند، وبنجلاديش (Sarker et. al., 2019).

وعلى صعيد البحث العلمي، فقد أكدت العديد من الدراسات التي تناولت الأمن السيبراني أهمية دور المعلم باعتباره قائدًا وموجهًا وقدوةً للطلبة داخل الصف، ومنها دراسة (Pusey & Sadera, 2011)، والتي أشارت إلى أهمية تنمية مفاهيم الأمن السيبراني لدى المعلمين بما يمكنهم من تأهيل طلابهم للتعامل بقدر كبير من الوعي والمسؤولية، والالتزام بالنواحي الأمنية عند تعاملهم مع مصادر المعلومات الرقمية المختلفة، وأكدت الدراسة الصادرة عن التحالف الوطني للأمن السيبراني في الولايات المتحدة (Pruitt-Mentle, 2008) على أهمية تعزيز الوعي لدى المعلمين بأهمية دورهم في مجال الأمن السيبراني، وانعكاس هذا الدور على إعداد الطلبة للاستخدام الرشيد لشبكات المعلومات، ومن الدراسات الأخرى التي تناولت دور المعلم وأهميته في هذا المجال دراسة(R.Solms & S.Solms, 2015) ، ودراسة (Black Clark, 2018 &) والتي أكدت على أهمية مشاركة المعلمين لمعارفهم وخبراتهم التقنية، ونقل تلك الخبرات إلى طلابهم، وذلك خلال معمل افتراضي صُمم بهدف تنمية الأمن السيبراني، وأظهرت الدراسة الدور الفعال للمعلمين في تنمية الأمن السيبراني لدى الطلبة، وأشارت دراسة (Bicak, Liu & Murphy, 2015) إلى أهمية وعي المعلمين بكافة التطورات المتعلقة بتحديات ومفاهيم الأمن السيبراني، وحيوية هذا الدور بالنسبة لإعداد الطلبة في التعامل مع البيئات السيبرانية في عالم المستقبل.

ويتضح من العرض السابق أهمية تعزيز الأمن السيبراني في ظل الثورة الرقمية والتكنولوجية المعاصرة، وما اتخذته دول العالم من إجراءات للالتزام بقواعد ومفاهيم الأمن السيبراني، وما أولته تلك الدول من أدوار مهمة للمؤسسات التربوية، وخاصة دور المعلم وأهمية امتلاكه الوعي المناسب بالأمن السيبراني، وما أكدت عليه الدراسات السابقة في هذا المجال.

مشكلة الدراسة ومبرراتها:

بناءً على التقرير السنوي الصادر من مركز الأمن الإلكتروني (٢٠١٩) الذي أشار إلى حجم التهديدات الإلكترونية في السعودية باستخدام البرمجيات الخبيثة وأدوات وطرق جديدة بهدف الوصول إلى المعلومات الحساسة وإلحاق الضرر بالجهات الحكومية والخاصة، ويعتبر التعليم أحدها حيث بلغت نسبة الخسائر الإلكترونية ١٤%، وتعد أكبر نسبة مقارنة بالقطاعات الأخرى. http://bit.ly/32x6Dif

واستنادًا إلى ما توصَّلت إليه بعض الدراسات السابقة من نتائج، وما قدمته من توصيات؛ كدراسات (Pusey & Sadera, 2011)؛ و(Pruitt-Mentle, 2008)؛ و(R.Solms & S.Solms, 2015)؛ و (Black & Clark, 2018)؛ و (Bicak, Liu

& Murphy, 2015)، التي أكدت جميعها على أهمية الأمن السيبراني، وتعزيز مفاهيمه في التعليم، وضرورة إكساب الوعي للمعلمين بما يضمن الحماية الشخصية للبيانات والمسؤولية التكنولوجية.

واستنادًا إلى توصيات بعض المؤتمرات التي عقدت في مجال الأمن السيبراني؛ لمواجهة التغيرات المتسارعة في تقنيات الثورة الصناعية الرابعة التي تستوجب المسؤوليات الرقمية، وإعداد مصفوفة للمعايير الأخلاقية لاستخدام النظم التكنولوجية، وعولمة التعلم بما يحسن بيئة المعلم والمتعلم، ويتواكب مع عصر الاقتصاد المعرفي: كمؤتمر الأمن السيبراني ٢٠١٩م بالرياض، ومؤتمر تقنيات الأمن السيبراني ٢٠١٩م بحائل، ومؤتمر التكنولوجيا وحلول البرمجيات ٢٠١٩م بالقاهرة، والمؤتمر الدولي للثورة الصناعية الرابعة ٢٠١٨م بسلطنة عمان.

وللتأكد من مشكلة الدراسة تم إجراء دراسة استطلاعية على (٣٠) معلمة من معلمات المرحلة المتوسطة للفصل الدراسي الأول عام ١٤٤٠-١٤٤١ه، وكان الهدف من إجراء الدراسة هو الكشف عن مدى الوعي بمفاهيم الأمن السيبراني، ومدى تمكنهن من التعامل مع الأجهزة الحاسوبية والهاتف النقال، التي تتطلب الحماية الشخصية والمسؤولية الرقمية، وأعد استبيان استطلاعي؛ لاستطلاع آراء المعلمات حول مدى معرفتهن بالأمن السيبراني، ومدى احتياجهن له ملحق (٣)، وبتحليل البيانات ملحق (٤)، أسفرت نتائج الدراسة الاستطلاعية أن وعي معلمات بالأمن السيبراني منخفض ، كما أسفرت بعض النتائج أنه لا يوجد لديهن أي فكرة تمامًا عن بعض مفاهيم الأمن السيبراني.

وفي ظل اجتياح الثورة الصناعية الرابعة (الذكاء الاصطناعي، وإنترنت الأشياء)، وارتفاع نسبة المستخدمين من المعلمات للشبكة العنكبوتية، وما يرتبط بهذا الاستخدام من مفاهيم تتعلق بالأمن السيبراني، ولتفادي الوقوع كضحية للجرائم الإلكترونية التي لا تستثني أحدًا من مستخدمي الشبكة، دولًا ومنظمات وأفراد فمن الضروري معرفة درجة وعي المعلمات بالأمن السيبراني، بهدف الاستخدام الآمن للإنترنت وغيرها من مصادر المعلومات الرقمية.

وبالإضافة لندرة الدراسات العربية التي تطرقت إلى دور المعلم في مجال الأمن السيبراني، حيث لم تجد الباحثة على حد اطلاعها أي من الدراسات العربية في هذا المجال على الرغم من أهمية هذا الدور في حماية مصادر المعلومات المختلفة، وما تمثله تلك المعلومات من أهمية في عصر الثورة المعلوماتية، حيث تعبير هذه الدراسة أول دراسة عربية في المجال التربوي؛ لتعزيز الأمن السيبراني لدى معلمات المرحلة المتوسطة بمدينة جدة في حدود اطلاع الباحثة.

وفي ضوء ما سبق فقد اتجه اهتمام الباحثة إلى معرفة درجة وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بالأمن السيبراني.

أسئلة الدراسة:

تتلخص مشكلة الدراسة في السؤال الرئيس التالي:

ما درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات؟

ويتفرع من هذا السؤال الأسئلة البحثية التالية:

١. ما درجة وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بمفاهيم الأمن السيبراني؟

٢.ما درجة وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بمخاطر الأمن السيبراني؟

٣.ما درجة تعرض معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة لانتهاكات الأمن السيبراني؟

٤. هل توجد فروق ذات دلالة إحصائية عند مستوى (٠,٠٥) بين متوسطات تقديرات المعلمات لكل من (مفاهيم- مخاطر - انتهاكات) الأمن السيبراني تعزى لمتغيرات البحث (الخبرة - المؤهل الدراسي- الدورات)؟

أهداف الدراسة:

تهدف الدراسة إلى الكشف عن درجة وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بالأمن السيبراني من وجهة نظر المعلمات، ويتفرع منه الأهداف التالية:

١. الكشف عن درجة وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بمفاهيم الأمن السيبراني.

٢. الكشف عن درجة وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بمخاطر الأمن السيبراني.

٣. الكشف عن درجة تعرض معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة لانتهاكات الأمن السيبراني.

أهمية الدراسة:

يمكن تناول أهمية الدراسة من جانبين: الأهمية النظرية، والأهمية التطبيقية، على النحو التالي:

أ. الأهمية النظرية:

١.قد تكون الدراسة الحالية نواة لأبحاث مستقبلية تتبنى اتجاهات حديثة في التعلم.

٢.قد تكون الدراسة الحالية إضافة جديدة للبحث العلمي والدراسات العربية النادرة في هذا المجال.

٣- تلقي الدراسة الضوء على أهمية دور معلمات المرحلة المتوسطة في مجال الأمن السيبراني، وبحسب العديد من الدراسات، ومنها دراسة (Bicak, Liu & Murphy,

2015) فإن للمعلمين والمعلمات أدوار محورية، لا يُمكن تجاهلها، في مجال تنمية الوعي حول الأمن السيبراني.

٤. تأتي هذه الدراسة استجابة للتوجهات العالمية في تعزيز ورفع درجة الوعي بالأمن السيبراني لدى معلمات التعليم العام.

٥. تأتي الدراسة استجابة لجهود حكومة المملكة العربية السعودية في مجال نشر الوعي بالأمن السيبراني، وتدريب الطلبة والخريجين والمعلمين والموظفين على تطبيق الأمن السيبراني في كافة مجالات الحياة.

ب. الأهمية التطبيقية:

يُمكن إيجاز الأهمية التطبيقية للدراسة في النقاط التالية:

١. توجيه اهتمام القائمين على برامج إعداد المعلم في كليات المعلمين، إلى أهمية إدراج مفاهيم الأمن السيبراني ضمن تلك البرامج.

٢. جذب اهتمام المسؤولين في وزارة التعليم نحو أهمية عقد دورات تدريبية بشكل مستمر للمعلمين في مجال الأمن السيبراني.

٣. قد تقدم نتائج الدراسة بعض الخطوط الإرشادية لواضعي السياسات التعليمية، إذ تؤدي إلى إعادة النظر في طبيعة أدوار ومهام المعلم في عصر المعلوماتية، واتخاذ ما يلزم لإعداد وتأهيل المعلم لمواجهة الثورة المعلوماتية المعاصرة.

٤. العمل على توجيه اهتمام الباحثين التربويين لتناول موضوع الأمن السيبراني، والذي لم يحظ بالاهتمام الكافي من قبل التربويين، على الرغم من أهميته في عصر المعلوماتية.

٥. رفع درجة الوعي لدى العاملين في المجال التربوي بخصوص الأمن السيبراني، وأهمية الالتزام بمفاهيم الأمن السيبراني عند التعامل مع مصادر المعلومات المختلفة.

حدود الدراسة:

تكونت حدود هذه الدراسة مما يلي:

- الحدود الموضوعية: مفاهيم الأمن السيبرانية.
- الحدود البشرية: أجريت هذه الدراسة على معلمات المرحلة المتوسطة.
- الحدود المكانية: طبقت هذه الدراسة في مدينة جدة.
- الحدود الزمانية: نفذت الدراسة في الفصل الدراسي الأول من العام الدراسي (١٤٤٠هـ -١٤٤١هـ).

مصطلحات الدراسة:

الأمن السيبراني:

يعرف خليفة (٢٠١٧، ص ١٣٧) الأمن السيبراني بأنه: "جميع الأدوات والسياسات، ومفاهيم الأمن، والضمانات الأمنية، والمبادئ التوجيهية، ومداخل إدارة

المخاطر، والإجراءات والتدريب، وأفضل الممارسات والتقنيات التي يُمكن استخدامها بهدف حماية الفضاء السيبراني، وتنظيم الأصول المعلوماتية للمستخدم".

وعرفه Canongia & Mandarino (2014,P63) بأنه: "فن وجود واستمرارية مجتمع المعلومات، من خلال ضمان وحماية المعلومات وأصولها وبنيتها التحتية في الفضاء السيبراني".

ويعرف إجرائيًا بأنه يشكل جميع إجراءات حماية شبكات المعلومات، ضد كافة الأعمال والممارسات التي تستهدف التلاعب بتلك المعلومات، وإلحاق الأذى بالمستخدمين، بما يشمل الحماية ضد الاختراق، وبث البرمجيات الخبيثة والفيروسات، والوصول غير المصرح به، وغير ذلك من ممارسات سلبية.

الإطار النظري

مفهوم الأمن السيبراني:

يُعد مفهوم الأمن السيبراني من المفاهيم الحديثة نسبيًا، والتي ظهرت في إطار الثورة الرقمية والتكنولوجية المعاصرة، والتي أدت إلى تدفق المعلومات بشكل كبير وغير مسبق، مع تعدد وسائل الاتصال إلى مصادر المعلومات عبر أجهزة الحواسيب، وغيرها من الأجهزة المحمولة، وفي هذا السياق ظهر مفهوم الأمن السيبراني ليعبر عن الجانب الأمني المرتبط بحماية تلك المعلومات، وشكل هذا المفهوم محل اهتمام العديد من المؤسسات الرسمية والباحثين.

وحسب تعريف الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية (٢٠١٨، ص٢٦) فإن الأمن السيبراني هو:" حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك".

ويُعرفه "بوسي وساديرا"(Pusey & Sadera (2011, p.82 : "بأنه الإجراءات التقنية الهادفة إلى حماية البيانات، والهوية الشخصية، والمعدات التقنية من أي شكل من أشكال الوصول غير المسموح به إلى تلك المعلومات أو المعدات".

ويرى Crompton, Thompson, Reyes, Zhou and Zou (2016, p.3) أن الأمن السيبراني: "يمثل العملية أو الحالة التي تكون بموجبها المعلومات وأنظمة المعلومات محمية بشكل تام ضد أي شكل من أشكال الإتلاف أو الوصول غير المسموح به لتلك المعلومات والأنظمة، أو التلاعب بها أو إساءة استخدامها".

وفي ضوء ما سبق، يتضح الاتفاق بين الباحثين في أن الأمن السيبراني يمثل مفهوم أمني خاص بحماية المعلومات، وكل ما له صلة بتلك المعلومات من عمليات

وخدمات وأجهزة وتقنيات، ضد أي شكل من أشكال الوصول غير المسموح به، أو استخدام تلك المعلومات بشكل سلبي، أو بما يمثل خطرًا على الجهات أو الأفراد ذوي الصلة بتلك المعلومات.

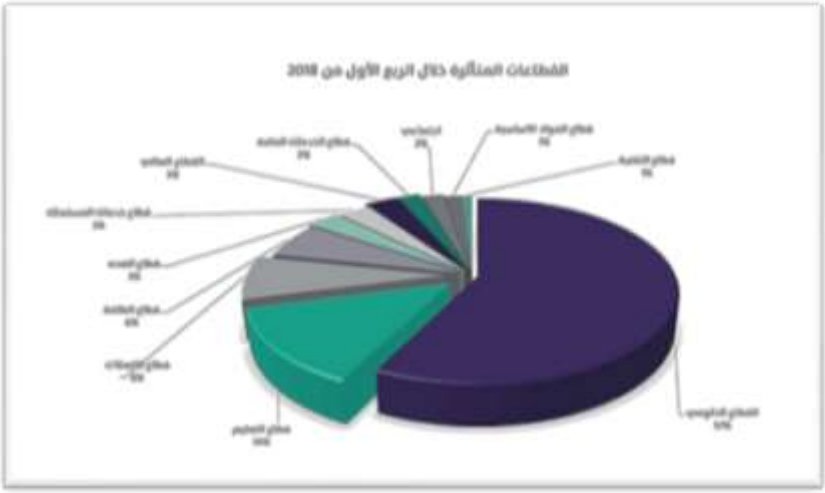
الأهمية التربوية للأمن السيبراني:

ساهم انتشار استخدام وسائل الوصول إلى شبكة الإنترنت عبر العديد من الأجهزة المحمولة بالإضافة إلى الحواسيب، واعتماد الحياة المعاصرة في معظم مجالاتها على التكنولوجيا الرقمية، على وقوع العديد من المعلمين حول العالم كضحية لأحد أشكال المخاطر والانتهاكات السيبرانية، ويترتب على تلك المخاطر والانتهاكات العديد من الأضرار المادية والنفسية والمعنوية التي تؤثر على المعلم، وعلى المؤسسة التعليمية التربوية، وهذه الأضرار تُكسب الأمر السيبراني أهمية خاصة بالنسبة لكل معلم في عالم اليوم (Wilson, 2014). ومما يزيد من الأهمية التربوية للأمن السيبراني أنه قد يتعرض المعلمون إلى الانتهاكات والمخاطر السيبرانية دون أن يكون لديهم دراية بتلك المخاطر والانتهاكات، ومدى خطورتها على التصفح الآمن للإنترنت، وهو ما يدعو إلى ضرورة رفع مستوى الوعي بأهمية الأمن السيبراني لدى هؤلاء المعلمين، وضرورة تضافر الجهود من قبل المدرسة ووزارة التعليم في هذا الشأن (R. Solms & S. Solms, 2015).

ويوجز stewart & Shilingford (2011) الأهمية التربوية للأمن السيبراني على النحو التالي:

- ضمان سرية وخصوصية الوثائق التعليمية والحفاظ على سلامتها بشكل مستمر.
- متابعة ومراقبة وتطوير وضبط نظام المعلومات والأمن في المدرسة.
- حماية المعلمات والمدرسة من الهجمات السيبرانية في الفضاء السيبراني.

ونجد أنَّ هناك العديد من التهديدات الإلكترونية التي تعرضت لها المملكة العربية السعودية، ومنها قطاع التعليم بشكل خاص، حيث بلغت نسبة الخسائر الإلكترونية في هذا المجال ١٤%، وتعد أكبر نسبة مقارنة بالقطاعات الأخرى، وهنا تبرز الأهمية التربوية للأمن السيبراني، مما يتطلب رفع مستوى وعي المعلمين والتربويين في هذا المجال http://bit.ly/32x6Dif . ويوضح شكل (١) قطاع التعليم في المملكة العربية السعودية المتأثر بالتهديدات السيبرانية، خلال الربع الأول من عام ٢٠١٨.



شكل (١) قطاع التعليم في المملكة المتأثر بالتهديدات السيبرانية، خلال الربع الأول من عام ٢٠١٨م. http://bit.ly/32x6Dif

ومن السرد السابق يتضح الأهمية التربوية للأمن السيبراني في حماية المعلومات المهمة والحساسة لدى المعلمين والمؤسسات التربوية، وكذلك تثقيف المعلمين بعدم التعرض للانتهاكات والمخاطر السيبرانية، وتوفير طرق الوقاية ضد الهجمات السيبرانية؛ للحفاظ على أمن المؤسسة التعليمية والمعلم.

أهداف الأمن السيبراني:

تسعى المؤسسات التربوية حول العالم إلى تطبيق الأمن السيبراني؛ بهدف تحقيق العديد من الأهداف، وتشير صائغ (٢٠١٨) إلى أن الأمن السيبراني يهدف إلى:

- توفير بيئة آمنة تتمتع بقدر كبير من الموثوقية في مجتمع المعلومات.
- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات.
- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف المستخدمين والمؤسسات.
- توفير المتطلبات اللازمة للحد من المخاطر والجرائم السيبرانية التي تستهدف المستخدمين.
- مقاومة البرمجيات الخبيثة وما تستهدفه من إحداث إضرار بالغة بالمستخدمين وأنظمة المعلومات.
- الحد من التجسس والتخريب الإلكتروني على مستوى الوزارة والمعلمين.

- التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة بأنواعها وسد الثغرات في أنظمة المعلومات.

مفاهيم الأمن السيبراني:

يشمل مفهوم الأمن السيبراني مجموعة من المفاهيم الخاصة بحماية المستخدمين من الوقوع كضحايا للمخاطر والانتهاكات السيبرانية، وفيما يلي عرض لبعض تلك المفاهيم حسب ما جاء في العديد من الدراسات والمراجع التي تناولت تلك المفاهيم.

التنمر الإلكتروني Bullying: يُقصد به استخدام تكنولوجيا الاتصالات لأغراض التحرش، المضايقة والإزعاج، التهديد، الابتزاز، وغير ذلك من صور الإيذاء (Hinduja & Patchin, 2010)، وانتشر التنمر الإلكتروني كأحد أشكال المخاطر السيبرانية بصورة كبيرة مع انتشار الأجهزة الكفية والهواتف الذكية، وتشير الإحصاءات في كل من الولايات المتحدة الأمريكية وبريطانيا أن نحو ٢٢% من المعلمين كانوا ضحايا لأحد أشكال التنمر الإلكتروني، وقد يقع المعلم ضحية لأكثر من شكل من أشكال التنمر الإلكتروني. (Rayan, Kariuki, and Yilmaz ,2011)

التشهير الإلكتروني Defamation: حيث يتم بث أفكار وأخبار من شأنها الإضرار الأدبي أو المعنوي بالشخص أو الجهة المقصودة، وتتنوع طرق الاعتداء بداية من الدخول على الموقع الشخصي للشخص المُراد التشهير به (الضحية) وتغيير محتوياته، أو عمل موقع آخر ينشر فيه أخبار ومعلومات غير صحيحة عن هذا الشخص، ولا يقتصر التشهير على الأفراد فقط بل قد يمتد ليشمل الأنظمة التعليمية والسياسية والدينية، من خلال بث أخبار وفضائح ملفقة، أو إنشاء مواقع مخصصة للتشهير بتلك الأنظمة أو الطعن في المعتقدات الدينية (متولي، ٢٠١٥).

التصيد الإلكتروني Phishing: والمعروف أيضًا بالخداع هو أحد أشكال الجرائم السيبرانية، ويتم من خلال استخدام الرسائل الإلكترونية التي صُممت لتبدو كأنها تابعة لجهة حقيقية أو من خلال الإعلانات المنتشرة على بعض المواقع، والتي يتم من خلالها استهداف المستخدمين للحصول على معلوماتهم الحساسة مثل تفاصيل الائتمان، والمعلومات الشخصية، وكلمات السر وما إلى ذلك من معلومات (ابو منصور، ٢٠١٧، ص٣٦).

الهندسة الاجتماعية Social Engineering: ويُطلق عليها علم أو فن اختراق العقول، وانتشر هذا المصطلح مع انتشار شبكات التواصل الاجتماعي، ويُشير إلى مجموعة من الأساليب التي يستخدمها المجرمون في الحصول على المعلومات الحساسة، أو إقناع الضحايا بتنفيذ بعض الإجراءات التي تساعد على اختراق أنظمتهم والإضرار بها (عبد الصادق، ٢٠١٤).

وتُعد الهندسة الاجتماعية من أكثر المخاطر السيبرانية انتشارًا؛ لأنها لا تقتصر على الاتصال عبر شبكة الإنترنت، بل قد تتم خلال المواقف الحياتية، ويستغل المهاجم سذاجة الضحايا للحصول على المعلومات الخاصة بهم، وازدادت حالات الهندسة الاجتماعية بشكل كبير مع انتشار مواقع التواصل الاجتماعي، حيث يستغل المهاجمون ما ينشره رواد هذه المواقع من معلومات للإيقاع بهم، وإيذائهم بشكل أو بآخر (Johnson, 2013).

الإرجاف الإلكتروني Destabilization: ويُقصد به بث الأخبار المحبطة والمسيئة ونشر الشائعات بغرض إحداث الخوف والاضطرابات وزعزعة الأمن والإيمان في نفوس الناس (المنتشري والمنتشري، ٢٠١٨)، ويُعتبر بث هذه الأخبار وغيرها مما يندرج ضمن الشائعات وسيلة خطيرة لإرباك الرأي العام، ويُستخدم الإرجاف الإلكتروني والشائعات بشكل عام كوسيلة لتحطيم مصادر الأخبار الحقيقية، وطُعم للحصول على الحقيقة، حيث تُشاع أنباء كاذبة عن موضوع معين أحيانًا بقصد الحصول على الأنباء الصحيحة عنه. (عبد الحليم، ٢٠٠٩).

التغرير والاستدراج Grooming: غالب ضحايا هذا النوع من المخاطر هم صغار السن من مستخدمي شبكة الإنترنت، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة على الإنترنت، وقد تتطور إلى التقاء مادي بين الطرفين (متولي، ٢٠١٥).

التجسس الإلكتروني Cyber-espionage: يتم التجسس الإلكتروني بواسطة برامج معينة تحصل سرًّا على معلومات عن المستخدم عن طريق الربط بالإنترنت، وخاصة بدعاوي دعائية وإعلانية، وعادة ما يتم تضمين برامج التجسس في شكل مكوّنات مجانية خفية، أو برامج مشاركة يُمكن تنزيلها من شبكة الإنترنت، وبمجرد تركيب برنامج التجسس يبدأ بمراقبة حركة المستخدم على الإنترنت، وينقل المعلومات إلى الجهة المهاجمة (القحطاني، ٢٠١٥).

الاحتيال الإلكتروني Fraud: يتخذ الاحتيال الإلكتروني طرقًا متعددة، منها إيهام الضحية (المجني عليه) بوجود مشروع كاذب، وقد يتخذ اسم أو صفة كاذبة، تمكنه من الاستيلاء على الضحية، فيتم التواصل مع الضحية من خلال اتصال الجاني بالضحية عن طريق الشبكة، أو قد يتعامل الجاني مباشرة مع بيانات الحاسب فيستعمل البيانات الكاذبة التي تساعده في الخداع والاحتيال عليه. (الربيعة، ٢٠١٨).

ويتضح مما سبق أن هناك العديد من تلك المفاهيم لها أهمية خاصة للمعلمين، ومع الأخذ في الاعتبار أن الوعي بتلك المفاهيم يُعد ضرورة حتمية ليس فقط بالنسبة لمستخدمي الحاسوب، بل كذلك لمستخدمي الهواتف الذكية التي تتصل بشبكة الإنترنت، وأن الولوج إلى شبكة الإنترنت، يتطلب الوعي بتلك المفاهيم لتجنب المخاطر، والانتهاكات الناجمة عن الجهل بها، ويوجز شكل (٢) قائمة بتلك المفاهيم.

شكل (٢) بعض مفاهيم الأمن السيبراني من إعداد الباحثة

الانتهاكات السيبرانية:

تشير الانتهاكات السيبرانية إلى كل نشاط خبيث يسعى إلى الحصول على تنازلات من جهة ما، أو يتسبب في إضعاف السرية، أو النزاهة، أو تعطيل توافر نظم الحواسيب، أو المعلومات، أو الاتصالات، أو الشبكات، أو البنية التحتية المادية، أو الافتراضية التي تتحكم فيها أجهزة الحواسيب، أو أنظمة المعلومات، أو المعلومات الموجودة فيها (بانقا، ٢٠١٩).

انتهاك الخصوصية Violation of Privacy: حيث تعتبر من الحقوق الفردية التي نصت عليها التشريعات الداخلية والاتفاقات الدولية، والحياة الخاصة، والأحاديث الخاصة، والمحادثات الهاتفية، والمراسلات، والحقوق المالية، والمعتقدات الدينية، والمسكن، والاسم، والمهنة، وللمعلم الحق الكامل في الحفاظ على خصوصية معلوماتية وبياناته وترشيد استخدامها، ومن صور انتهاكها في الفضاء السيبراني ما يلي:

- إدخال معلومات وهمية، وانتحال الشخصية بهدف حصول المعتدي على مبالغ مالية.
- التجسس الإلكتروني بتتبع العيوب واصطياد الأخطاء.
- التصنت ومحاولة الوصول إلى السجلات الخاصة والاعتداء على الحياة الخاصة. (الهزاني، ٢٠١٨).

انتهاك أمن المعلومات Information Security Violation: وتعرف المعلوماتية إجرائيًا بمجموعة البيانات التي تخضع للمعالجة والتحليل والتفسير والاستخدام المنظم لأغراض معينة؛ لتحقيق زيادة المعرفة، وتشمل الانتهاكات المعلوماتية جرائم الدخول إلى نظام المعلوماتي، وسرقة المعلومات وتزيفها وتظليلها وإعاقة العمل المعلوماتي وتغيير المعلومات السرية وتعطيل الأنظمة وحجب الخدمة. (الردفاني، ٢٠١٥).

انتهاك الملكية الفكرية Violation of Intellectual Property: وتشمل تلك الانتهاكات وضع اسم المختلس على عمل، وانتهاك تقليد ختم المؤلف، والاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة. (ابن تاج، ٢٠١٨).

انتهاك المواقع Violation of Sites: تعرف المواقع الإلكترونية إجرائيًّا بمجموعة من صفحات إلكترونية ومصادر للمعلومات يمكن التفاعل معها ومشاهدتها عبر الحواسيب، أو الأجهزة النقالة، ويمكن للمجرمين انتهاك وتدمير المواقع الإلكترونية، والتلاعب بالبيانات، والمعلومات، والاضرار بها، وتهديدها بالفيروسات والبرامج الخبيثة والاختراقات (الهزاني، ٢٠١٨).

ويتضح مما سبق أن مرتكبي تلك الانتهاكات السيبرانية يبذلون جهودًا جبارة لتدمير المواقع والاستيلاء على بيانات المعلمين، وسرقة المعلومات، والتهديدات الإلكترونية، وأن تلك الانتهاكات تكبد المؤسسة التربوية خسائر مادية ومالية فادحة. ويوجز شكل (٣) الانتهاكات السيبرانية التي تم التطرق إليها.

شكل(٣) انتهاكات الأمن السيبراني من إعداد الباحثة

المخاطر السيبرانية:

تُعرف مخاطر الأمن السيبراني باعتبارها "المخاطر التي تمس عمليات أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إدارتها أو صورتها أو سمعتها)، أو أصول الجهة أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية الوصول غير المصرح به، أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات، أو نظم المعلومات" (الهيئة الوطنية للأمن السيبراني، ٢٠١٨، ص٣٢).

وتتخذ مخاطر الأمن السيبراني العديد من الأشكال التي تستهدف إلحاق الأذى بالمعلمين والمؤسسات التربوية، وأن تلك المخاطر تطال العديد من مكونات وقيم المجتمع

وتؤثر على مستخدمي الفضاء السيبراني بصورة خطيرة جدًّا، ومن تلك المخاطر ما يتصل بالجوانب التالية:

الجانب الديني: حيث تُسهم بعض مواقع الإنترنت، وصفحات التواصل الاجتماعي في التأثير سلبيًّا على المعلمين من خلال زعزعة بعض الثوابت والمعتقدات الدينية التي يؤمن بها، وتُروج لبعض الأفكار السلبية بشكل مكثف لتحيل المعلمين إلى نوع من التناقض في العقيدة، مما يوقع بعض المعلمين في حبائل التطرف الديني، وقد تعمد بعض المواقع إلى التشكيك في المعتقدات الدينية وبث بعض الأفكار الواهية التي تبعد المعلمين عن الالتزام بتعاليم الدين الحنيف. (حسن، ٢٠١٨).

الجانب الأخلاقي: وذلك من خلال نشر قيم وثقافات ضارة بالمجتمع بواسطة دول ومؤسسات ذات أغراض تتعارض مع القيم الثقافية السائدة، ويُلاحظ ذلك من خلال مواقع الإنترنت التي تحتوي مواد تخرج عن حدود الأدب والأخلاق واللياقة، ولها تأثير سلبي على المعلمين في انتشار الكذب والأفعال الفاضحة والرذيلة، والتي تُسهم في الانحلال الأخلاقي للمجتمعات. (العريشي والدوسري، ٢٠١٥).

الجانب الوطني: أدى شيوع النقل الرقمي إلى خلق مشكلة أمنية وطنية، حيث أصبح من السهل استراق السمع والتجسس الإلكتروني، بما يشمل الكثير من المجالات التعليمية والأمنية، بالإضافة إلى مخاطر تعطيل الأعمال الحكومية، أو العبث بالمعلومات او إتلافها أو إخفائها. (الردفاني، ٢٠١٥).

ويتضح من العرض السابق أنَّ هناك العديد من المخاطر السيبرانية التي تؤثر سلبًا على المعلمين والمؤسسة التربوية، وتدمر الدين والأخلاق والوطن، والبنى التحتية، وتؤدي إلى خسائر مادية ومعنوية، وبالتالي يوجز شكل (٤) المخاطر السيبرانية التي تم التطرق إليها.

شكل (٤) مخاطر الأمن السيبرانية من إعداد الباحثة

تجارب دولية في الاهتمام التربوي بالأمن السيبراني:

يهتم الاتحاد الدولي للاتصالات (ITU,2019) بتعزيز الأمن السيبراني حول العالم، ويُصدر العديد من النشرات والتقارير حول الأمن السيبراني، مع توضيح للجهود التي ينبغي بذلها للتوعية بالأمن السيبراني وتعزيزه، وفي إطار هذا الاهتمام يُصدر الاتحاد

الدولي للاتصالات ITU تقريرًا سنويًّا يرصد واقع الأمن السيبراني في دول العالم بعنوان: مؤشر الأمن السيبراني العالمي، (Cybersecurity Global Index (GCI، ويقيس المؤشر الالتزام بالأمن السيبراني من خلال خمسة أبعاد وهي: البعد القانوني، البعد التقني، البعد التنظيمي، بناء القدرات، التعاون. ويشير التقرير الصادر عام ٢٠١٨م إلى أن ٦٠% من دول العالم تطبق حملات توعية بالأمن السيبراني للمعلمين والطلبة والتربويين، وأن ٦٣% من دول العالم تنظم برامج تدريبية في مجال الأمن السيبراني. ويوضح جدول (١) قائمة بالدول العشر الأوائل في ذلك المؤشر في عامي ٢٠١٧م، و٢٠١٨م، إلى جانب ترتيب الدول العربية في هذين العامين على المستوى الإقليمي والعالمي.

جدول (١)

ترتيب الدول العشر الأوائل في مؤشر GCI عامي ٢٠١٧م، ٢٠١٨م، وترتيب الدول العربية الأوائل في هذا المجال

نتائج عام ٢٠١٧م			نتائج عام ٢٠١٨م		
الدول العشر الأوائل	ترتيب بعض الدول العربية		الدول العشر الأوائل	ترتيب بعض الدول العربية	
	الدول العربية	الترتيب العالمي	الترتيب الإقليمي	الدول العربية	الترتيب العالمي	الترتيب الإقليمي
سنغافورة	عُمان	٤	١	المملكة المتحدة	السعودية	١٣	١
الولايات المتحدة	مصر	١٤	٢	الولايات المتحدة	عُمان	١٦	٢
ماليزيا	قطر	٢٣	٣	فرنسا	قطر	١٧	٣
عُمان	تونس	٤٠	٤	ليتوانيا	مصر	٢٣	٤
أستونيا	السعودية	٤٦	٥	أستونيا	الإمارات	٣٥	٥
موريشيوس	الإمارات	٤٧	٦	سنغافورة	الكويت	٦٧	٦
أستراليا	المغرب	٤٩	٧	إسبانيا	البحرين	٦٨	٧
جورجيا	البحرين	٦٥	٨	ماليزيا	الأردن	٧٤	٨
فرنسا	الجزائر	٦٨	٩	كندا	تونس	٧٦	٩
كندا	الأردن	٩٣	١٠	النرويج	المغرب	٩٣	١٠

ويتضح من جدول (١) أن المملكة العربية السعودية استطاعت إحراز تقدم هائل في مجال الالتزام بالأمن السيبراني، حيث تقدم ترتيب المملكة نحو ثلاث وثلاثون درجة، من المركز ست وأربعين على مستوى العالم عام ٢٠١٧م، إلى المركز ثلاثة عشر، والمركز الأول

عربيًّا، وذلك بسبب اهتمامها بالأمن السيبراني، وما قامت به من بعض الإنجازات في هذا المجال، واستحداث كلية الأمن السيبراني في عدد من الجامعات؛ كجامعة الملك سعود، وجامعة جدة. ويوجز شكل (٥) ترتيب الدول العشر الأوائل على مستوى العالم في مؤشر الأمن السيبراني، بينما يعرض شكل (٦) ترتيب بعض الدول العربية في مؤشر الأمن السيبراني إقليميًّا وعالميًّا.

شكل (٥) الدول العشر الأوائل عالميًا في مؤشر الأمن السيبراني عام ٢٠١٨م

شكل (٦) ترتيب بعض الدول العربية إقليميًّا وعالميًّا على مؤشر الأمن السيبراني عام ٢٠١٨م

وفيما يلي عرض لبعض التجارب الدولية والعربية في مجال الأمن السيبراني التربوي:

تجربة الولايات المتحدة الأمريكية:

اهتمت الولايات المتحدة بتعزيز الوعي بالأمن السيبراني من خلال المناهج الدراسية، وخاصة ضمن مدخل STEM التعليمي، بالإضافة إلى العمل على جعل مقررات علوم الحاسوب والأمن السيبراني جزءًا أساسيًّا من المناهج الدراسية في مختلف

المراحل التعليمية، ويُشرف على تلك الجهود المركز القومي لبحوث التعليم السيبراني المتكامل National Integrated Cyber Education Research (NICERC) Center، وأسس المركز عام ٢٠١٦، ويسعى إلى تعزيز قدرات جميع المعلمين في مجال الأمن السيبراني، ودمج الطلبة لاستكشاف الفضاء السيبراني بكل أبعاده، وإعداد أجيال من الخريجين المختصين في مجالات العلوم والتكنولوجيا والرياضيات والهندسة والأمن السيبراني (https://nicerc.org/).

تجربة ماليزيا:

لماليزيا تجربة رائدة في مجال الأمن السيبراني حيث بدأت بتوظيفه في التعليم، وأنشأت مركز CyberSecurity Malaysia (CSM)، وتأتي هذه المبادرة للتوعية الأمنية عبر الإنترنت، وتثقيف وتعزيز الوعي بشأن المشكلات التكنولوجية والاجتماعية التي تواجه مستخدمي الإنترنت، وخاصة المخاطر التي يواجهونها على الإنترنت، واستهدفت هذه المبادرة توعية المعلمين والطلبة والمنظمات والمواقع الاجتماعية، وخصصت لكل منهم موقعًا على الإنترنت يصف المخاطر السيبرانية وكيفية الوقاية منها مزودًا بمقاطع فيديو. https://www.cybersecurity.my/en/index.html

تجربة أستراليا في الأمن السيبراني:

تم إنشاء المعهد الأسترالي لبحوث الأمن السيبراني، وهو أول مركز أسترالي إستراتيجي منسق في مجال البحوث والتعليم بين الوكالات الحكومية والقطاع الخاص والباحثين. ويسعى إلى تركيز الحكومة على الأمن السيبراني من خلال الجمع بين شبكة تعاونية للتصدي للتهديدات السيبرانية وتحسين فرص تطوير مهنيين متخصصين في مجال الأمن السيبراني. ويقدم المعهد تعليمًا أمنيًّا في المرحلة الجامعية والدراسات العليا من خلال منهج دراسي متسق وتعليم متميز وستعمل الحكومة مع القطاع الخاص، ومؤسسات خدمة الولايات والأقاليم والمهارات لدعم التوسع في التدريب على الأمن السيبراني في منظمات التدريب؛ ليشمل ذلك تطوير التدريب المهني على الأمن السيبراني، والتركيز على طلاب الجامعات إلى برنامج أوسع من المسابقات، وفرص تطوير المهارات لمجموعة أوسع من المشاركين. https://www.cyber.gov.au/.

تجربة المملكة العربية السعودية:

وتأتي تجربة المملكة العربية السعودية كأحد التجارب العربية الرائدة في هذا المجال، ويُشرف على تلك الجهود الهيئة الوطنية للأمن السيبراني، والتي تأسست بموجب أمر ملكي كريم برقم (٦٨٠١) صدر بتاريخ ١٤٣٨/١٢/١١هـ، وترتبط بمقام خادم الحرمين الشريفين – أيده الله – وهي الجهة المختصة في المملكة بالأمن السيبراني والمرجع الوطني في شؤونه (الربيعة،٢٠١٨).

وعلى صعيد الجهود التربوية، قررت إنشاء كلية الأمن السيبراني والبرمجة والذكاء الاصطناعي، وتسعى الكلية إلى بناء وتأهيل قدرات وطنية شابة محترفة بأحدث الوسائل التقنية التي يُمكن من خلالها المساعدة في تحقيق أهداف رؤية المملكة ٢٠٣٠م، والتي تهدف إلى التحول إلى مجتمع معرفي وتقني ينافس الدول العالمية المتقدمة في الإبداع التقني المعلوماتي والرياضيات الذهنية، وبالأخص في المجال السيبراني والبرمجة. وفي إطار هذا الاهتمام فقد عُقدت مسابقة "الهاكاثون" Cyber Space بمشاركة ستة وأربعون طالبًا وثمانون طالبة جميعهم من طلبة الجامعات السعودية، وتتضمن المسابقة تطبيق عملي لهجمات سيبرانية، وإجراءات الأمن السيبراني التي يتم اتخاذها لصد تلك الهجمات.https://nca.gov.sa/pages/ncsa.html

وفي ضوء الاطلاع على تلك التجارب السابقة، يتضح الاهتمام الدولي والمحلي بالأمن السيبراني في مجال التربية، وما تقدمه تلك الدول من جهود ومراكز ومشروعات وجامعات لتطوير الأمن السيبراني ورفع مستوى الوعي لدى المعلمين والطلبة.

دور وزارة التعليم في تنمية الوعي بالأمن السيبراني:

تؤدي وزارة التعليم دورًا مهمًّا في إعداد العلمين للقيام بأدوارهم المستقبلية، ومواكبة التطورات العلمية والتقنية المتسارعة، مع الأخذ في الاعتبار أن المدارس تُعتبر من أكثر المؤسسات عُرضة لخطر الانتهاكات السيبرانية، حيث ينتشر استخدام تكنولوجيا المعلومات والاتصالات في المدارس لأغراض تعليمية وإدارية وتدريبية بشكل كبير، دون أن يترافق هذا الانتشار باتخاذ إجراءات الأمن السيبراني اللازمة أو توعية العاملين في المدارس من إداريين ومعلمين بواقع الأمن السيبراني وأهميته، ونُظر إلى هذا الموضوع بعين الاعتبار بعد وقوع العديد من حالات الانتهاك السيبراني في بعض الدول وعلى رأسها الولايات المتحدة الأمريكية، حيث شهدت العديد من المدارس الأمريكية حالات قرصنة واستيلاء على المعلومات الشخصية للآلاف من الطلبة والمعلمين والمعلمات والإداريين العاملين في تلك المدارس (Goran, 2017).

وعلى هذا أبدت وزارة التعليم الاهتمام بالأمن السيبراني للمدرسة والعاملين بها، بالإضافة إلى الدور الذي يُمكن أن تؤديه في التوعية في مجال الأمن السيبراني، ويشير "كريتزنجلر وآخرون" (Kritizingler et. al,2017) إلى بعض تلك الأدوار على النحو التالي:

١. وضع خطط على مستوى المدارس بشكل عام للتوعية بالأمن السيبراني، والتحذير من المخاطر والانتهاكات السيبرانية، بما يشمل الطلبة والمعلمين.
٢. التأكد من تطبيق جميع المدارس لسياسات واضحة بالنسبة للتعامل مع التكنولوجيا الرقمية، بما يشمل الأمن السيبراني، ويجب تعميم تلك السياسات على جميع المدارس، والإشراف على تطبيقها من قبل بعض الجهات المختصة في وزارة التعليم.

٣. أن يكون لدى وزارة التعليم خطة عمل واضحة للتعامل مع المخاطر والانتهاكات السيبرانية، وأن تتضمن تلك الخطة الجهات والمؤسسات التي يُمكن التواصل معها لمواجهة تلك المخاطر والانتهاكات.
٤. عقد دورات تدريبية لجميع المعلمين في المجالات التالية: الوعي بالأمن السيبراني لدى المعلمين، الإجراءات التي يُمكن للمعلمين اتباعها في حال وقوعهم ضحية للمخاطر والانتهاكات السيبرانية.
٥. التعاون مع بعض المؤسسات الأكاديمية كالجامعات، أو المؤسسات الاقتصادية ومؤسسات المجتمع المدني في وضع خطط التوعية بالأمن السيبراني، وتوفير المصادر والدعم اللازم للتدريب ونشر الوعي بالأمن السيبراني.
٦. إشراك الآباء في خطط وبرامج عمل المدرسة ذات الصلة بالأمن السيبراني.
٧. العمل على نشر الاهتمام بموضوع الأمن السيبراني على نطاق واسع، وذلك من خلال عقد ورشات عمل، ندوات، أيام مفتوحة مخصصة للأمن السيبراني، وضع ملصقات أو توزيع كتيبات أو نشرات للتوعية، أو عبر مواقع التواصل الاجتماعي.
٨. إدراج موضوع الأمن السيبراني ضمن أدلة المعلمين.
٩. اعتبار الوعي بالأمن السيبراني من المهارات الحياتية اللازمة للطلبة، وإدراجه ضمن القضايا المثارة أثناء التدريس والأنشطة المدرسية.

ويُمكن كذلك أن تتبنى وزارة التعليم تنظيم دورات ومخيمات صيفية متخصصة للتوعية بالأمن السيبراني، ويُقترح أن تتضمن البرامج المنفذة في تلك المخيمات تعريف المعلمات بالموضوعات التالية: تاريخ الإنترنت والأمن السيبراني، مفاهيم التشفير، المخاطر السيبرانية، التصيد والهجمات السيبرانية، أخلاقيات الإنترنت، وأخيرًا المهارات الاجتماعية لاستخدام الإنترنت، وتشمل تلك الدورات والمخيمات العديد من الأنشطة التي يُمكن تنفيذها عبر الحواسيب، أو المطبوعات والملصقات، بالإضافة إلى الأعمال اليدوية (Stewart & Shilingford, 2011).

توعية المعلمات بالأمن السيبراني

تلعب المعلمات دورًا مهمًّا داخل المدرسة في مجال التوعية بالأمن السيبراني، ويتطلب قيامهن بهذا الدور أن يمتلكن القدر الكافي من الوعي بالأمن السيبراني، وهناك العديد من الإجراءات التي يجب أن تكون المعلمة على وعي بها، خاصة فيما يتعلق بالوقاية من المخاطر والانتهاكات السيبرانية، وإجراءات الأمن السيبراني التي يُمكن تطبيقها على المستوى الفردي. وهناك العديد من الأخطاء الأكثر شيوعًا لدى مستخدمي الإنترنت، عبر الحاسوب أو بواسطة الهواتف الذكية، ويجب أن تحرص المعلمات على تجنب تلك الأخطاء، بالإضافة إلى نقل تلك الخبرات إلى الطالبات، وتتلخص فيما يلي (المبارك ، حران وإسحاق، ٢٠١٤):

١. اختيار كلمة مرور ضعيفة وعدم تجديدها.
٢. استخدام نفس كلمة المرور لجميع الحسابات.
٣. ترك جهاز الحاسوب مفتوحًا دون رقابة.
٤. فتح رسائل البريد الإلكتروني ومرفقاتها المرسلة من جهات أو اشخاص مجهولة.
٥. إدخال أو تخزين البيانات بصورة غير صحيحة.
٦. الإفصاح عن معلومات شخصية عبر مواقع التواصل الاجتماعي.
٧. عدم تحديث كل برامج مضادات الفيروسات، ونظام التشغيل ومتصفح الإنترنت.

ويتضح مما سبق أن هناك مسؤولية مزدوجة تقع على عاتق المعلمات في عصر الثورة المعلوماتية، ويتعلق الجانب الأول من هذه المسؤولية بضرورة الوعي بالأمن السيبراني، باعتباره من الأمور اللازمة لكل مستخدم للإنترنت بشكل عام، فضلًا عن أهميته بالنسبة للمعلمة بشكل خاص، نظرًا لدورها المهم في إعداد الطالبات وتوعيتهن بمخاطر وانتهاكات الأمن السيبراني. وفي ضوء العرض السابق، فإن الأمن السيبراني يُمثل مفهومًا جديدًا للأمن في عصر الثورة المعلوماتية، وذلك لمواجهة الأخطار والانتهاكات القادمة عبر الفضاء المعلوماتي أو السيبراني، وتأسست لأجله مؤسسات خاصة، وخُصصت ميزانيات ضخمة لترسيخ مبادئ هذا الأمن، كما سُنت القوانين حول العالم لتطبيق مفاهيم الأمن السيبراني ومعاقبة مرتكبي المخاطر والانتهاكات السيبرانية، كما أشار العرض السابق إلى الطرق المثلى التي ينبغي للمعلمات تطبيقها من أجل حماية أنفسهن من مخاطر وانتهاكات السيبرانية والدور الذي يُمكن أن تقدمه وزارة التعليم مع المؤسسات الحكومية والخاصة في هذا المجال من أجل رفع مستوى الوعي لدى المعلمات.

الدراسات السابقة

أولًا: دور المؤسسات الاجتماعية والتربوية في تنمية الوعي بالأمن السيبراني:

يتناول هذا المحور الدراسات التي تطرقت إلى دور المؤسسات الاجتماعية والتربوية في تنمية الوعي بالأمن السيبراني، ويشمل ذلك دور الأسرة والمدرسة والجامعات، ومن الدراسات التي اهتمت بدور المؤسسات الاجتماعية والتربوية المختلفة في تنمية الوعي بالأمن السيبراني، كانت **دراسة صائغ (٢٠١٨)** التي هدفت إلى الكشف عن العلاقة بين وعي أفراد الأسرة بمفهوم الأمن السيبراني وبين الاحتياطات الأمنية التي يتخذونها للوقاية من الجرائم الإلكترونية، وأظهرت نتائج الدراسة وجود علاقة ارتباطية دالة بين وعي الأسرة بمفهوم الأمن السيبراني، وبين الاحتياطات الأمنية التي يتخذونها للوقاية من الجرائم الإلكترونية، ووجود فروق ذات دلالة إحصائية في درجة وعي أفراد الأسرة بمفهوم الأمن السيبراني، وذلك بالنسبة لمتغيري العمل والمؤهل التعليمي. لذلك أوصت الدراسة بتعاون الجهات المعنية على تثقيف وتوعية أفراد الأسرة لمفاهيم الأمن السيبراني، وتضمين تلك المفاهيم في المناهج الدراسية. ومن جهة أخرى تناولت **دراسة**

عسكر (٢٠١٢) دور المؤسسات الاجتماعية في التبصير بجرائم تقنية المعلومات في المجتمع السعودي، وتم إعداد استبانة، وتوصلت الدراسة إلى وضع إستراتيجية مقترحة لتفعيل دور المؤسسات الاجتماعية في التعريف بالجرائم الإلكترونية.

وفي نفس السياق، هدفت **دراسة "سبيرينج" (Spiering, 2013)** إلى معرفة دور المدرسة والناشرين التربويين في التوعية بالأمن السيبراني، للوصول إلى حلول مقترحة لتنمية الوعي بالأمن السيبراني، وتم إجراء مقابلات مع المعلمين والمعلمات، وأظهرت النتائج وجود أكثر من (٢٠) مشكلة ناتجة عن نقص الوعي بالأمن السيبراني، ومنها التعرض لحالات الاستمالة، التحرش الجنسي، والتنمر الإلكتروني، سرقة الصور والملفات، بث محتوى غير أخلاقي، وانتهاكات السيبرانية، والتهديدات المختلفة، والإيذاء الجسدي، وقد تصل تلك المشكلات إلى حد وقوع حالات انتحار، وأرجع أفراد العينة من المعلمين، ومدراء المدراس، والناشرين، والمختصين في هذا المجال تلك المشكلات إلى عاملين رئيسين وهما: غياب رؤية واضحة للتوعية بالأمن السيبراني، وندرة عدد المعلمين المختصين في مجال الأمن السيبراني، وكما توصلت الدراسة إلى حاجة المعلمين إلى تقديم خطة مقترحة للتوعية بالأمن السيبراني تشمل تدريب المعلمين وتأهيلهم وتزويدهم بالمعارف والمهارات ذات الصلة بالأمن السيبراني، وتطوير معارف واتجاهات مدراء المدارس نحو الأمن السيبراني، وتأهيل البنية التحتية الرقمية في المدارس، وإشراك المختصين الرقميين في وضع برامج التدريب التربوية في الأمن السيبراني، وتقييم نتائج تطبيقها، وتطوير مستوى الإصدارات التربوية التي تتناول موضوع الأمن السيبراني.

ويتضح من هذه الدراسات الاتفاق على أهمية دور المؤسسات التربوية والاجتماعية المختلفة في تفعيل الوعي بالأمن السيبراني، والمشكلات المترتبة على عدم الالتزام بالأمن السيبراني، وما يترتب على ذلك من وقوع مخاطر وانتهاكات سيبرانية، مع التأكيد على أهمية دور المعلم في هذا المجال، وهو ما أشارت إليه نتائج دراستي عسكر (٢٠١٢) ؛ ودراسة(Spiering,2013) كما اتفقت نتائج دراسة ابن شلفوت (٢٠١٨)؛ ودراسة العمران (٢٠١١) على أهمية الدور الذي تلعبه الجامعة في رفع مستوى الوعي بالجرائم المعلوماتية والمخاطر الأمنية، واتفقت في هذا الشأن آراء الطلبة الجامعيين، وأعضاء هيئة التدريس.

ثانيًا: برامج أو طرق تدريس الأمن السيبراني:

تتطرق الدراسات في هذا المحور إلى استعراض التجارب المقترحة لتطبيق برامج أو طرق لتدريس الأمن السيبراني، ومن الدراسات التي تناولت تطوير برامج أو طرق تدريس الأمن السيبراني **دراسة "كاي" (Cai ,2018)** والتي هدفت إلى تقديم نموذج مقترح لتدريس الأمن السيبراني والانتهاكات السيبرانية، وتم إعداد إستبانة لتقييم أداء المحاضر والممارسات التدريسية، وتمت مقارنة نتائج التحصيل الدراسي للطلبة في

عامي ٢٠١٥م، ٢٠١٦م مقارنة بعام ٢٠١٤م، وأظهرت نتائج الدراسة تحسنًا واضحًا في التحصيل الدراسي للطلبة في مقرر الأمن السيبراني مقارنة بعام ٢٠١٤م، وازدياد دافعية الطلبة نحو تعلم الأمن السيبراني والانتهاكات السيبرانية، وتحسنًا في نتائج تطبيق مقياس الكفاءة الذاتية، وأوصت الدراسة بتبني نماذج تدريسية غير تقليدية لتدريس موضوعات الأمن السيبراني والانتهاكات السيبرانية. كما هدفت **دراسة "باستارد" Bustard (2018,)** إلى إعداد وحدة دراسية تناولت الأخلاقيات والانتهاكات الخاصة بالأمن السيبراني، وتحديد أثر تلك الوحدة على اندماج الطلبة في تعلم أخلاقيات الأمن السيبراني، وشملت عينة الدراسة مجموعة من طلبة مرحلة الماجستير، وتم إعداد استبانة لقياس مدى رضا الطلبة عن تلك الوحدة واندماجهم في تعلم الأخلاقيات، وكيفية التصدي للانتهاكات الأمن السيبراني، وتم تدريس تلك الوحدة على مدار ثلاث سنوات متتالية منذ عام ٢٠١٤م – ٢٠١٧م، وأظهرت نتائج الدراسة رضا الطلاب بدرجة كبيرة عن تلك الوحدة، وأن عدم التوعية بكيفية التصدي للانتهاكات والهجمات السيبرانية قد يكون له أثر سلبي على أمن المؤسسات، وأهمية معالجة القضايا الأخلاقية المتعلقة بالأمن السيبراني. وهدفت أيضًا **دراسة (Taylor, Baskett, Allen, Francis & Kifayat,2018)** إلى المقارنة بين أثر استخدام العروض التقديمية وعروض الانفوجرافيك وغيرها من عروض رسومية، واستخدام المواد التعليمية التقليدية في تدريس مفاهيم الأمن السيبراني، وتكونت عينة الدراسة من مجموعة من طلبة علوم الحاسوب في إحدى الجامعات البريطانية، وتم تقسيمهم إلى مجموعتين، حيث درست المجموعة الأولى مفاهيم الأمن السيبراني بالاستعانة بمواد تعليمية أعدها الباحثون، باستخدام العروض التقديمية وعروض الانفوجرافيك ورسوم حاسوبية متحركة لتدريس مفاهيم الأمن السيبراني، أما المجموعة الثانية فقد درست وفق الطريقة التقليدية، وتم إعداد اختبار لمفاهيم الأمن السيبراني، وأظهرت نتائج الدراسة تفوق المجموعة الأولى في تعلم مفاهيم الأمن السيبراني، ووجود فروق دالة إحصائيًّا بين متوسط درجات طلبة المجموعتين، لصالح طلبة المجموعة الأولى. وكما هدفت **دراسة (Cai, 2018)** إلى تقديم نموذج مقترح لتدريس الأمن السيبراني، فقد هدفت **دراسة "موسكال" (Moskal ,2015)** إلى وضع تصور لإنشاء مركز للتميز في الأمن السيبراني في الجامعات الأمريكية، بهدف تهيئة الخريجين للعمل في هذا المجال وأجرى الباحث دراسة مسحية شملت (١٠٠) جامعة أمريكية وذلك بمراجعة الوثائق الرسمية لمعرفة مدى الاهتمام بتدريس علوم الأمن السيبراني، وأوصت الدراسة بضرورة الاهتمام بالأمن السيبراني باعتباره من أهم الدعائم للاقتصاد الأمريكي في المستقبل المنظور.

ويُلاحظ اتفاق دراسات (Moskal , 2015)؛ ودراسة (Taylor et. al , 2018)؛ ودراسة (Bustard ,2018) ؛ ودراسة (Cai ,2018) على أهمية تطوير عملية تدريس الأمن السيبراني، وأكدت على خطر الانتهاكات والمخاطر السيبرانية، واتفقت دراستي

(Bustard,2018)؛ ودراسة (Cai ,2018) على الاهتمام بتتبع نتائج تطبيق النموذج أو الوحدة المقترحة على مدى عامين أو ثلاثة.

ثالثًا: الوعي بالأمن السيبراني لدى الطلبة الجامعيين:

يتطرق هذا المحور إلى استعراض بعض الدراسات التي استهدفت مدى وعي الطلبة الجامعيين بالأمن السيبراني، والجرائم المعلوماتية والإطار القانوني لهذه الجرائم. تناولت بعض الدراسات مدى إدراك الطلبة الجامعيين لأهمية الأمن السيبراني، ومنها **دراسة "نينكيو وآخرين" .(Nyinkeu et. Al,2018)** التي هدفت إلى تحديد مفاهيم الأمن السيبراني التي ينبغي تعزيزها لدى طلاب تكنولوجيا المعلومات، وأجرى الباحثون مقابلات حرة مع أفراد العينة، وأظهرت استجابات أفراد العينة عن أهمية تعزيز مفاهيم الاستخدام الآمن للإنترنت، والتمييز بين الأمن السيبراني وأمن الشبكات، وأوصت الدراسة بضرورة التركيز على المفاهيم الأخلاقية المتعلقة باستخدام شبكة الإنترنت والاهتمام بالتربية السيبرانية وإدراجها في المقررات الدراسية.

وهدفت دراسة (**Pusey & sadera,2011**) إلى تحديد درجة وعي المعلمين، وطلبة كلية إعداد المعلمين بمفاهيم الأمن السيبراني، الانتهاكات السيبرانية، والسلامة السيبرانية، ودرجة معرفتهم بتدريس هذه المفاهيم، وأظهرت نتائج الدراسة أن درجة معرفة المعلمين بمفاهيم الأمن السيبراني، الانتهاكات السيبرانية، والسلامة السيبرانية، درجة منخفضة جدًّا، وأن ٢٠% منهم فقط لديه وعي بدرجة متوسطة بتلك المفاهيم، وأظهرت النتائج بأهمية توعية المعلمين والطلبة بمفاهيم والانتهاكات السيبرانية، كما أظهرت النتائج أنه لا يوجد لدى المعلمين تصور واضح لكيفية تدريس تلك المفاهيم، أو كيفية إدراجها أثناء ممارساتهم التدريسية.

وفي إطار التطرق إلى الجانب القانوني للأمن السيبراني، فقد هدفت **دراسة غريب والأمير (٢٠١٧)** إلى معرفة مستوى وعي الفئة العمرية الشابة حول مفهوم الجرائم المعلوماتية في المملكة العربية السعودية، ومعرفتهم بنظام العقوبات الصادر بخصوص ذلك الموضوع، وتم إعداد استبانة، وأظهرت نتائج الدراسة أن نحو نصف أفراد العينة لديهم وعيٌ بالممارسات غير الشرعية عند استخدام الأجهزة الإلكترونية، وأن معرفة الأنظمة والعقوبات الخاصة بمكافحة الجرائم المعلوماتية كان لها دور كبير في الحد من الممارسات السلبية في تقنيات المعلومات، وأوصت الدراسة بإدراج مقرر دراسي خاص بالجرائم المعلوماتية وتوعية مستخدمي تقنية المعلومات بخطرها وعواقبها الوخيمة.

ومن خلال العرض السابق يُمكن ملاحظة اتفاق دراسة (Nyinkeu et. al. ,2018)؛ ودراسة (Pusey & Sadera ,2011) على أهمية توعية الطلبة الجامعيين والمعلمين بمفاهيم الأمن السيبراني، وإدارج مقررات دراسية خاصه بالجرائم الإلكترونية؛ لتوعيتهم بكيفية التعامل الأمثل مع التقنية.

رابعًا: الوعي بالأمن السيبراني في مرحلة التعليم ما قبل الجامعي:

يستعرض هذا المحور الدراسات التي تناولت الوعي بالأمن السيبراني في مرحلة التعليم ما قبل الجامعي، أي في مراحل التعليم العام، بما يشمل الطلبة والمعلمين والمعلمات العاملين في تلك المراحل. ولقد اهتمت العديد من الدراسات بتناول موضوع الأمن السيبراني في مرحلة التعليم ما قبل الجامعي، بما يشمل دور المعلم في هذا المجال والوعي بالأمن السيبراني، والمخاطر والانتهاكات السيبرانية في هذه المرحلة، ومنها دراسة **الرفاعي (٢٠١٨)** التي هدفت إلى معرفة درجة ممارسة طلبة المرحلة المتوسطة للتنمر الإلكتروني، ودرجة تعرضهم للتنمر الإلكتروني، أظهرت نتائج الدراسة ارتفاع درجة ممارسة التنمر من قبل طلبة المرحلة المتوسطة في مدارس مدينة الكويت، وارتفاع درجة تعرضهم للتنمر الإلكتروني، وأوصت الدراسة بضرورة إشراك الطلبة في كافة المراحل الدراسية وخاصة المرحلة المتوسطة بأنشطة وبرامج تثقيفية اجتماعية تهدف لتعريفهم بحقوقهم، وكيفية التصدي لظاهرة التنمر الإلكتروني، وتطوير المناهج المدرسية، وتضمينها برامج تساعد على مواجهة مشكلات التنمر الإلكتروني. وبصورة مماثلة هدفت **دراسة "سافاريا" (Safaria, 2016)** إلى دراسة مدى انتشار ظاهرة التنمر السيبراني كأحد أشكال الانتهاكات السيبرانية لدى طلاب المرحلة الثانوية، وعلاقته بالأسى النفسي لديهم، وتم إعداد استبانة لقياس عدد مرات التعرض لظاهرة التنمر السيبراني وأشكال التنمر، وعلاقة التعرض للتنمر السيبراني بشعور الطلاب بالأسى النفسي، وأظهرت نتائج الدراسة تعرض الطلاب للكثير من حالات التنمر السيبراني بصور متعددة، كما أظهرت النتائج وجود علاقة ارتباطية دالة موجبة بين تعرضهم للتنمر السيبراني وشعورهم بالأسى النفسي. كذلك هدفت **دراسة "جوران" (Goran, 2017)** إلى تحديد المخاطر السيبرانية التي يتعرض لها طلبة المرحلة الثانوية، وتحديد متطلبات الأمن السيبراني الخاصة بطلبة المرحلة الثانوية، وأجرى الباحث مقابلات مع المعلمين والمعلمات، وأظهرت نتائج الدراسة وجود عدد من المخاطر السيبرانية، ومنها: التصيد الإلكتروني، البرمجيات الخبيثة، التلاعب بنتائج الاختبارات الإلكترونية، عدم كفاءة قواعد البيانات، وأوصت الدراسة بأهمية رفع مستوى وعي الطلبة بخصوص الأمن السيبراني، مع معرفة كيفية تجنب المخاطر السيبرانية والانتهاكات التي قد يتعرضون لها أثناء استخدام الإنترنت.

ويتضح من خلال ماسبق اتفاق دراسات (Bele et. al, 2014)؛ ودراسة (Safaria ,2016)؛ ودراسة (Goran , 2017)؛ ودراسة الرفاعي (٢٠١٨) على أن المخاطر السيبرانية تشمل كافة مستخدمي الإنترنت حول العالم، فهذه المخاطر كغيرها من الجرائم السيبرانية لا تعرف حدودًا جغرافية، ولا تقتصر على فئة عمرية دون غيرها، فقد تستهدف الطلبة في المراحل الدراسية المختلفة، واتفقت تلك الدراسات على أهمية تنمية الوعي بالأمن السيبراني لتجنب تلك المخاطر.

وكما اهتمت دراسة (Bele et. al. ,2014) بأساليب الوقاية من الجرائم السيبرانية، فقد اهتمت بعض الدراسات بأهمية الوعي بالأمن السيبراني لدى الطلبة، أوما يتعلق بالتعامل مع شبكات المعلومات **كدراسة الخثعمي (٢٠١٨)** والتي هدفت إلى معرفة وعي طالبات المرحلة الثانوية في المدارس الحكومية بمدينة الرياض بقضايا أمن المعلومات، وتم إعداد استبانة، وأظهرت نتائج الدراسة أن (٤٣,١%) من الطالبات لديهن وعي ومعرفة بقضايا أمن المعلومات، وأن (٩٤,٤%) منهن لديهن علم بأن حواسيبهن يُمكن أن تُصاب بفيروسات، وأن (٨٥,٣%) منهن يعلمن بضرورة استخدام كلمة سر على أجهزتهن الإلكترونية من الاختراق والتجسس، وأوصت الدراسة بأهمية إدخال بعض المقررات الدراسية التي لها علاقة بقضايا أمن المعلومات لإكساب الطلاب والطالبات مهارات الحماية من مخاطر التهديدات الإلكترونية وقضايا أمن المعلومات.

ونظرًا لأهمية هذا الوعي فقد اهتمت بعض الدراسات باستعراض بعض المبادرات في هذا المجال، حيث هدفت **دراسة "كريتزنجلر وآخرين"** (Kritizingler et. al,2017) إلى استعراض المبادرات الخاصة برفع مستوى الوعي بالأمن السيبراني لدى الطلبة في مدارس جنوب أفريقيا والمدارس البريطانية، وتم ذلك من خلال استعراض الوثائق والدراسات التي تناولت تجارب هاتين الدولتين في هذا المجال، وأظهرت نتائج الدراسة وجود عدد من المبادرات شملت دمج مفاهيم الأمن السيبراني ضمن المناهج الدراسية، وتدريب المعلمين، ووضع سياسات خاصة بالأمن السيبراني، وسن قوانين وتشريعات لمكافحة الانتهاكات السيبرانية، ودمج الآباء في برامج للتوعية بالأمن السيبراني، وعقد ورش عمل وأيام مفتوحة وندوات لهذا المجال، والتوعية عبر وسائل الإعلام. وأكدت النتائج أن تدريب المعلمين في هذا المجال وعقد دورات تدريبية وورش عمل وسن القوانين تساعد على رفع مستوى الوعي لديهم .

ويتضح مما سبق تأكيد نتائج دراسة (Kritizingler et. al, 2017)على دور المعلم في تنمية الوعي بالأمن السيبراني، واتفقت نتائج دراسة (Alhejaili ,2013)؛ ودراسة الهاجري (٢٠١٧) مع تلك النتائج، مع التأكيد على حاجة المعلمين لزيادة وعيهم بالأمن السيبراني.

أوجه استفادة الدراسة الحالية من الدراسة السابقة:

- التعرف على العديد من المراجع العربية والأجنبية التي يُمكن الاستعانة بها لمزيد من الاطلاع على موضوع الدراسة الحالية.
- الاستفادة منها في صياغة مشكلة الدراسة وأسئلتها.
- إعداد الإطار النظري.
- إعداد أداة الدراسة، ومعرفة الإجراءات والأساليب الإحصائية التي يتم اتباعها للتحقق من الخصائص السيكومترية للأداة (صدق وثبات أداة الدراسة).

- معرفة الأساليب الإحصائية الواجب اتباعها لتحليل نتائج الدراسة الحالية.
- المقارنة بين نتائج الدراسة الحالية وما أظهرته نتائج الدراسات السابقة.

منهج الدراسة وإجراءاتها

منهج الدراسة:

اتبعت الدراسة المنهج الكمي الوصفي التحليلي، الذي يُعرف "باعتباره مجموعة الإجراءات البحثية التي يقوم بها الباحث بشكل متكامل لوصف الظاهرة المبحوثة معتمدًا على جمع الحقائق والبيانات وتصنيفها.

مجتمع الدراسة وعينتها:

يتكون مجتمع الدراسة من جميع معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة، خلال الفصل الأول من العام الدراسي ١٤٤١هـ، ويبلغ عددهن (٤٥٢٥) معلمة (ملحق ٧)، وبالنسبة لاختيار عينة الدراسة فقد تم مراعاة العوامل التالية (عطية، ٢٠٠٩):

- منهج البحث: العينة في المنهج الوصفي التحليلي، قد تكون أكبر من العينة في المنهج التجريبي.
- حجم المجتمع الأصلي: إذا كان حجم المجتمع الأصلي كبيرًا، وكانت الدراسة تتبع المنهج الوصفي يكون حجم العينة المسحوبة أكبر.
- مستوى الدقة والتعمق المُراد الوصول إليه: اختيار حجم عينة مناسب يُعطي نتائج أكثر مصداقية.

وتم اختيار عينة عشوائية بسيطة من معلمات المرحلة المتوسطة، والعشوائية هنا تعني أن الفرصة متساوية ودرجة الاحتمال واحدة لأي فرد من أفراد مجتمع الدراسة؛ ليتم اختياره كأحد أفراد العينة، دونما أي تأثر أو تأثير (العساف، ٢٠٠٦)، وعلى هذا الأساس تم توجيه أداة الدراسة إلى عينة من معلمات الدراسة عبر موقع "جوجل درايف" Google Drive؛ لتجيب عنها عينة من المعلمات بلغ عددهن (٣٦٢) معلمة، وهو عدد مناسب حسب ما أشار به (أبو علام، ٢٠١١)، والموضح في شكل (٧)، والذي يرى أن في حال بلغ عدد أفراد المجتمع (٥٠٠٠) فرد، فإن حجم العينة لابد ألا يقل عن (٣٥٠) فردًا، أي أن حجم العينة الحالية (٣٦٢) معلمة يُعتبر حجمًا مناسبًا بالنسبة لمجتمع الدراسة البالغ عدده (٤٥٢٥) معلمة. وبالنسبة لتوزيع أفراد العينة حسب المتغيرات التالية: المؤهل الدراسي، عدد سنوات الخبرة، عدد الدورات في مجال الأمن السيبراني، فقد جاء على النحو الموضح في جدول (٢)

جدول (٢)
توزيع أفراد العينة حسب متغيرات المؤهل وعدد سنوات الخبرة والدورات في مجال الأمن السيبراني

المتغيرات	المستويات	العدد	النسبة المئوية
المؤهل الدراسي	بكالوريوس	١٩١	٥٣%
	بكالوريوس + دبلوم تربوي	١٣٢	٣٦%
	ماجستير	٣٩	١١%
عدد سنوات الخبرة	أقل من ٥ سنوات	١٠١	٢٨%
	من ٥ سنوات إلى ١٠ سنوات	١٧٢	٤٧%
	أكثر من ١٠ سنوات	٨٩	٢٥%
عدد دورات الأمن السيبراني	لم أحصل على دورات في الأمن السيبراني	٣٥٢	٩٧%
	حصلت على دورات في الأمن السيبراني	١٠	٣%

ويتضح من جدول (٢) أن المعلمات الحاصلات على درجة البكالوريوس يمثلن ٥٣% من أفراد العينة، أما باقي أفراد العينة من المعلمات الحاصلات على درجة البكالوريوس والدبلوم التربوي فيمثلن ٣٦%، أما الحاصلات على الماجستير فنسبتهن ١١%.

وبالنسبة لتوزيع أفراد العينة حسب عدد سنوات الخبرة، يتضح أن نحو ٤٧% من المعلمات الممثلات لعينة الدراسة لديهن خبرة تتراوح من ٥ إلى ١٠ سنوات، و٢٨% لم تتجاوز سنوات الخبرة لديهن الخمس سنوات، أما المعلمات ذوات الخبرة الأكثر من ١٠ سنوات فيمثلن نحو ٢٥% من عينة الدراسة.

أما فيما يتعلق بتوزيع أفراد العينة حسب عدد الدورات في مجال الأمن السيبراني، فيتضح أن نحو ٩٧% من المعلمات لم يحصلن على أي دورة في مجال الأمن السيبراني، بينما حصل نحو ٣% من أفراد العينة على دورات في هذا المجال.

ويتضح مما سبق توزيع أفراد العينة من معلمات المرحلة المتوسطة بمدارس التعليم العام في مدينة جدة وفقًا لعدد من المتغيرات، وأن عدد العينة (٣٦٢) معلمة من مجتمع الدراسة الأصلي والبالغ عدده (٤٥٢٥) معلمة، أي أن نسبة العينة إلى المجتمع نحو ٨%، وهي نسبة مقبولة في حال المجتمعات الكبيرة العدد، وذلك على النحو الذي سبق عرضه.

أداة الدراسة:

بالنسبة للدراسة الحالية أُتخذت الاستبانة كأداة للدراسة باعتبار أن حجم العينة كبير، ويتوزع بين عدد كبير من المدارس في مدينة جدة، كذلك تضمن الاستبانة الحصول

على البيانات الخاصة بالمتغيرات التالية (المؤهل الدراسي، عدد سنوات الخبرة، الدورات في مجال الأمن السيبراني).

أ. التحقق من صدق الاتساق الداخلي للاستبانة: يُقصد بالاتساق الداخلي الاتساق في أداء الفرد من فقرة إلى أخرى، وعندما يكون الأداة متجانسة فإن كل فقرة تقيس نفس العوامل العامة التي تقيسها الأداة (عيد، ٢٠١٢)، ولحساب صدق الاتساق الداخلي للاستبانة تم تطبيقها على عينة استطلاعية مكونة من (٢٠) معلمة، ممن لا ينتمين إلى عينة الدراسة، ومن ثم تم حساب معامل ارتباط بيرسون بين درجة كل فقرة مع الدرجة الكلية للمحور الذي تنتمي إليه، وجاءت النتائج على النحو الموضح في جدول (٣).

جدول (٣)

معاملات الارتباط بين درجة كل فقرة والدرجة الكلية للمحور الذي تنتمي إليه

المحور الأول				المحور الثاني		المحور الثالث	
رقم الفقرة	معامل الارتباط	رقم الفقرة	معامل الارتباط	رقم الفقرة	معامل الارتباط	رقم الفقرة	معامل الارتباط
١	0.867**	٧	0.861**	١١	0.716**	١٧	0.662**
٢	0.883**	٨	0.781**	١٢	0.868**	١٨	0.610**
٣	0.805**	٩	0.810**	١٣	0.788**	١٩	0.884**
٤	0.773**	١٠	0.646**	١٤	0.704**	٢٠	0.868**
٥	0.702**			١٥	0.743**	٢١	0.742**
٦	0.873**			١٦	0.576**		

**معامل ارتباط دال عند مستوى دلالة ٠,٠١

يتضح من جدول (٤) أن جميع فقرات الاستبانة ترتبط بمعاملات ارتباط دالة، عند مستوى دلالة ٠,٠١ مع المحور الذي تنتمي إليه، وتم كذلك حساب معاملات الارتباط بين درجة كل محور والدرجة الكلية للاستبانة وجاءت على النحو الموضح في جدول (٤).

جدول (٤)

معاملات الارتباط بين درجة كل محور والدرجة الكلية للاستبانة

محاور الاستبانة	معامل الارتباط بين درجة المحور والدرجة الكلية للاستبانة
مفاهيم الأمن السيبراني	0.934**
مخاطر الأمن السيبراني	0.821**
انتهاكات الأمن السيبراني	0.805**
الاستبانة ككل	0.954**

**معامل ارتباط دال عند مستوى دلالة ٠,٠١

وتشير النتائج الواردة في جدول (٤) إلى أن درجة كل محور ترتبط بمعامل ارتباط دال عند مستوى دلالة ٠,٠١ مع الدرجة الكلية للاستبانة، وتؤكد النتائج السابقة أن الاستبانة تتمتع بقدر كبير من صدق الاتساق الداخلي.

ب. التحقق من ثبات الاستبانة: يُقصد بثبات الاختبار مدى استقرار الدرجات التي يحصل عليها نفس الأفراد في مرات الإجراء، سواء أُعيد الإجراء بنفس الصورة أو بصورة مكافئة لنفس الاختبار، ويشير ثبات الأداة إلى عدم وجود خطأ في القياس وإلى دقة الأداة في القياس وعدم تناقضها مع نفسها (عيد،٢٠١٢)، ولحساب ثبات الاستبانة تم تطبيقها على العينة الاستطلاعية للدراسة، ومن ثم تم حساب معامل الفا كرونباخ كمعامل ثبات لكل محور من محاور الاستبانة، وللاستبانة ككل، وجاءت النتائج على النحو الموضح في جدول (٥)

جدول (٥)
معاملات ثبات الاستبانة

محاور الاستبانة	عدد الفقرات	معامل الثبات
مفاهيم الأمن السيبراني	١٠	٠,٩٣٤
مخاطر الأمن السيبراني	٦	٠,٨٢١
انتهاكات الأمن السيبراني	٥	٠,٨٠٥
الاستبانة ككل	٢١	٠,٩٥٤

ومن خلال تلك النتائج يتضح أن جميع محاور الاستبانة ذات معامل ثبات عالٍ يتراوح بين (٠,٨٠٥ – ٠,٩٣٤)، وأن معامل الثبات للاستبانة ككل بلغ ٠,٩٥٤ وتؤكد تلك النتائج أن الاستبانة تتمتع بدرجة كبيرة من الثبات، وهو ما يعني صلاحيتها لتحقيق أهداف الدراسة الحالية.

نتائج الدراسة ومناقشتها وتفسيرها

نتائج الإجابة عن السؤال الأول:

نص السؤال الأول من أسئلة الدراسة على: «ما درجة وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بمفاهيم الأمن السيبراني؟»

تمت الإجابة عن السؤال الأول من خلال حساب المتوسطات الحسابية لاستجابات أفراد العينة على المحور الأول (محور مفاهيم الأمن السيبراني) من محاور الاستبانة، وحساب الانحرافات المعيارية لتلك الاستجابات؛ لمعرفة مدى تشتتها، ومن ثم حساب درجة وعي المعلمات بكل فقرة من فقرات المحور الأول، وفق المدى الذي تم توضيحه في الفصل الثالث، وترتيب تلك الفقرات ترتيبًا تنازليًّا حسب قيم المتوسطات الحسابية مع مراعاة قيم الانحرافات المعيارية في حال تساوي تلك المتوسطات الحسابية، وأخيرًا حساب درجة

وعي المعلمات بمفاهيم الأمن السيبراني بشكل عام وجاءت النتائج على النحو الموضح في جدول (٦).

جدول (٦)

نتائج استجابات أفراد العينة على محور مفاهيم الأمن السيبراني

م	مفاهيم الأمن السيبراني	المتوسط الحسابي	الانحراف المعياري	درجة الوعي	الترتيب
١	أؤيد طلب المدرسة من منسوباتها تغيير كلمة المرور الخاصة بالنظم الإدارية والتعليمية بشكل دوري.	**4.83**	**0.57**	كبيرة جدا	٣
٢	أقوم بنسخ ملفاتي احتياطيًا في ذاكرة خارجية.	**1.97**	**1.04**	منخفضة	٥
٣	أستخدم برمجيات خاصة لحماية الحاسب من الاختراق.	**1.82**	**1.16**	منخفضة	٨
٤	أستخدم برامج للحماية من ملفات التجسس.	**1.78**	**1.12**	منخفضة جدًا	٩
٥	أحتفظ بملفاتي وصوري في أكثر من مكان لتفادي السرقة أو التلف.	**1.77**	**1.11**	منخفضة جدًا	١٠
٦	أحذر من مشاركة معلوماتي الشخصية للغرباء عبر الشبكة العنكبوتية.	**1.9**	**1.23**	منخفضة	٦
٧	أتحقق من مصدر المعلومة المتداولة في مواقع التواصل الاجتماعي قبل إرسالها للآخرين.	**1.88**	**1.19**	منخفضة	٧
٨	أحترم آراء الآخرين ومشاعرهم عند مناقشة موضوع في التخصص عبر شبكة الإنترنت.	**2**	**1.13**	منخفضة	٤
٩	أؤيد توعية المعلمات في المدرسة بمفاهيم الامن السيبراني.	**4.9**	**0.36**	كبيرة جدًّا	١
١٠	أحتاج إلى دورات تدريبية في مجال الأمن السيبراني.	**4.89**	**0.36**	كبيرة جدًا	٢
الإجمالي		٢,٧٧	٠,٩٢	متوسطة	

وتشير النتائج الواردة في جدول (٦) إلى درجة وعي متوسطة لدى معلمات المرحلة المتوسطة بمفاهيم الأمن السيبراني بشكل عام، وتراوحت استجابات أفراد العينة على فقرات المحور الأول بين درجة وعي منخفضة جدًّا إلى منخفضة وكبيرة جدًّا، وذلك على النحو التالي:

أ. جاءت استجابات أفراد العينة على ثلاث فقرات بدرجة كبيرة جدًّا وبالترتيب التالي:

١. أؤيد توعية المعلمات في المدرسة بمفاهيم الأمن السيبراني.

٢. أحتاج إلى دورات تدريبية في مجال الأمن السيبراني.

٣. أؤيد طلب المدرسة من منسوباتها تغيير كلمة المرور الخاصة بالنظم الإدارية والتعليمية بشكل دوري.

ب. جاءت الاستجابة على ٥ فقرات بدرجة وعي منخفضة، وفق الترتيب التالي:

١. أحترم آراء الآخرين ومشاعرهم عند مناقشة موضوع في التخصص عبر شبكة الإنترنت.
٢. أقوم بنسخ ملفاتي احتياطيًا في ذاكرة خارجية.
٣. أحذر من مشاركة معلوماتي الشخصية للغرباء عبر الشبكة العنكبوتية.
٤. أتحقق من مصدر المعلومة المتداولة في مواقع التواصل الاجتماعي قبل إرسالها للآخرين.
٥. أستخدم برمجيات خاصة لحماية الحاسب من الاختراق.

ج. جاءت الاستجابة على فقرتين بدرجة وعي منخفضة جدًّا، وفق الترتيب التالي:

١. أستخدم برامج للحماية من ملفات التجسس.
٢. أحتفظ بملفاتي وصوري في أكثر من مكان لتفادي السرقة أو التلف.

نتائج الإجابة عن السؤال الثاني:

نص السؤال الثاني من أسئلة الدراسة على «ما درجة وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بمخاطر الأمن السيبراني؟»، تمت الإجابة عن السؤال الثاني من خلال حساب المتوسطات الحسابية لاستجابات أفراد العينة على المحور الثاني (محور مخاطر الأمن السيبراني) من محاور الاستبانة، وحساب الانحرافات المعيارية لتلك الاستجابات لمعرفة مدى تشتتها، ومن ثم حساب درجة وعي المعلمات بكل فقرة من فقرات المحور الثاني وفق المدى الذي تم توضيحه في الفصل الثالث، وترتيب تلك الفقرات ترتيبًا تنازليًّا حسب قيم المتوسطات الحسابية مع مراعاة قيم الانحرافات المعيارية في حال تساوي تلك المتوسطات الحسابية، وأخيرًا حساب درجة وعي المعلمات بمخاطر الأمن السيبراني بشكل عام، وجاءت النتائج على النحو الموضح في جدول (٧):

جدول (٧)

نتائج استجابات أفراد العينة على محور مخاطر الأمن السيبراني

م	مخاطر الأمن السيبراني	المتوسط الحسابي	الانحراف المعياري	درجة الوعي	الترتيب
١١	أحرص على تجنب المعلومات المخالفة للعقيدة والدين	**3.44**	**1.08**	كبيرة	١
١٢	أحترم أنظمة المملكة العربية السعودية في التعامل مع الشبكة العنكبوتية	**3.33**	**1.14**	متوسطة	٢
١٣	أحترم سياسات المواقع الإلكترونية التي أستخدمها.	**3.01**	**1.14**	متوسطة	٣
١٤	أنشر الوعي الرقمي عند التعرض للمواقف السلبية في شبكة إنترنت.	**2.54**	**1.11**	منخفضة	٦

١٥	أتجنب تجاوز القوانين التي تفرضها الدولة في استخدام الإنترنت.	2.81	1.2	متوسطة	٤
١٦	أستخدم المحتوى المرخص من قبل الناشر أو المؤلف.	2.56	1.15	منخفضة	٥
الإجمالي		٢,٩٤	١,١٣	متوسطة	

وتشير النتائج الواردة في جدول (٧) إلى درجة وعي متوسطة بمخاطر الأمن السيبراني بشكل عام لدى معلمات المرحلة المتوسطة، وتراوحت استجابات المعلمات على فقرات المحور بين درجة وعي منخفضة إلى متوسطة وكبيرة، وذلك على النحو التالي:

أ. فقرة واحدة بدرجة وعي كبيرة وهي: أحرص على تجنب المعلومات المخالفة للعقيدة والدين

ب. ثلاث فقرات بدرجة وعي متوسطة بالترتيب التالي:
١. أحترم أنظمة المملكة العربية السعودية في التعامل مع الشبكة العنكبوتية.
٢. أحترم سياسات المواقع الإلكترونية التي أستخدمها.
٣. أتجنب تجاوز القوانين التي تفرضها الدولة في استخدام الإنترنت.

ج. فقرتان بدرجة وعي منخفضة وهما:
١. أستخدم المحتوى المرخص من قبل الناشر أو المؤلف.
٢. أنشر الوعي الرقمي عند التعرض للمواقف السلبية في شبكة إنترنت.

نتائج الإجابة عن السؤال الثالث:

نص السؤال الثالث من أسئلة الدراسة على «ما درجة تعرض معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة لانتهاكات الأمن السيبراني؟»

تمت الإجابة عن السؤال الثالث من خلال حساب المتوسطات الحسابية لاستجابات أفراد العينة على المحور الثالث (محور انتهاكات الأمن السيبراني) من محاور الاستبانة، وحساب الانحرافات المعيارية لتلك الاستجابات لمعرفة مدى تشتتها، ومن ثم حساب درجة وعي المعلمات بكل فقرة من فقرات المحور الثالث وفق المدى الذي تم توضيحه في الفصل الثالث، وترتيب تلك الفقرات ترتيبًا تنازليًّا حسب قيم المتوسطات الحسابية مع مراعاة قيم الانحرافات المعيارية في حال تساوي تلك المتوسطات الحسابية، وأخيرًا حساب درجة وعي المعلمات بانتهاكات الأمن السيبراني بشكل عام، وجاءت النتائج على النحو الموضح في جدول (٨):

جدول (٨)

نتائج استجابات أفراد العينة على محور انتهاكات الأمن السيبراني

م	انتهاكات الأمن السيبراني	المتوسط الحسابي	الانحراف المعياري	درجة الوعي	الترتيب
١٧	أؤيد وضع المدرسة لنظام يمنع الوصول إلى مواقع إلكترونية التي من الممكن أن تضر بحاسبك.	4.89	0.37	كبيرة جدًا	١

١٨	أحدث برنامج الحماية الموجودة على حاسبي بشكل دوري.	**2.12**	**1.14**	منخفضة	٤
١٩	أؤيد وضع إجراءات وسياسات لحفظ الأمن السيبراني في المدرسة.	**4.8**	**0.66**	كبيرة جدًا	٢
٢٠	أستخدم التشفير لملفاتي المهمة التي أقوم بإرسالها من خلال شبكة الإنترنت.	**2.02**	**1.15**	منخفضة	٥
٢١	أراعي النزاهة في هويتي الرقمية حين استخدم مواقع التواصل الاجتماعي.	**2.56**	**1.26**	منخفضة	٣
الإجمالي		**٣,٢٧**	**٠,٩١**	**متوسطة**	

ويتضح من تلك الاستجابات أن درجة وعي المعلمات بانتهاكات الأمن السيبراني درجة متوسطة بشكل عام، وهو ما يعني احتمال تعرضهن لقدر كبير من انتهاكات الأمن السيبراني، حيث جاءت الاستجابات على فقرتين بدرجة كبيرة جدًّا، وتتعلق هاتين الفقرتين بالإجراءات التي يُمكن أن تتخذها إدارة المدرسة، وهما:

١. أؤيد وضع المدرسة لنظام يمنع الوصول إلى مواقع إلكترونية التي من الممكن أن تضر بحاسبك.
٢. أؤيد وضع إجراءات وسياسات لحفظ الأمن السيبراني في المدرسة.

أما فيما يتعلق بالإجراءات التي يجب أن تتخذها كل معلمة بشكل فردي للحماية من انتهاكات الأمن السيبراني، وعدم التعرض لتلك الانتهاكات، فقد جاءت استجابات المعلمات على تلك الفقرات بدرجة منخفضة، وذلك على النحو التالي:

١. أراعي النزاهة في هويتي الرقمية حين استخدم مواقع التواصل الاجتماعي.
٢. أحدث برنامج الحماية الموجودة على حاسبي بشكل دوري.
٣. أستخدم التشفير لملفاتي المهمة التي أقوم بإرسالها من خلال شبكة الإنترنت.

ويُمكن إيجاز النتائج المتعلقة بالإجابة عن الأسئلة الثلاثة الأولى من أسئلة الدراسة، وذلك كما أظهرته نتائج تطبيق أداة الدراسة على النحو الموضح في جدول (٩):

جدول (٩)

نتائج استجابات أفراد العينة على أداة الدراسة بشكل عام

م	درجة الوعي	المتوسط الحسابي	الانحراف المعياري	درجة الوعي	الترتيب
١	مفاهيم الأمن السيبراني	٢,٧٧	٠,٩٢	متوسطة	٣
٢	مخاطر الأمن السيبراني	٢,٩٤	١,١٣	متوسطة	٢
٣	انتهاكات الأمن السيبراني	٣,٢٧	٠,٩١	متوسطة	١
الإجمالي		**٢,٩٤**	**٠,٩٨**	**متوسطة**	

نتائج الإجابة عن السؤال الرابع:

نص السؤال الرابع من أسئلة الدراسة على «هل توجد فروق ذات دلالة إحصائية عند مستوى (٠,٠٥) بين متوسطات تقديرات المعلمات لكل من (مفاهيم_ مخاطر _ انتهاكات) الأمن السيبراني تعزى لمتغيرات البحث (الخبرة _ المؤهل الدراسي_ الدورات)؟» وللإجابة على هذا السؤال تم استخدام تحليل التباين الأحادي للتعرف على دلالة الفروق بين معلمات المرحلة المتوسطة لكل من (مفاهيم – مخاطر – انتهاكات) الأمن السيبراني تعزى إلى متغير المؤهل الدراسي والخبرة، وجاءت النتائج على النحو الموضح في جدول (١٠)، وجدول (١١):

جدول (١٠)

نتائج تحليل التباين الأحادي للفروق بين المعلمات في (مخاطر – انتهاكات – مفاهيم) الأمن السيبراني تعزى لمتغير المؤهل الدراسي

المتغير	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة F	قيمة الدلالة	مستوى الدلالة
المؤهل الدراسي	بين المجموعات	٩٢٨,٦١	٢	٤٦٤,٦٠	١,٤٩٣	٠,٢٢٦	غير دالة
	داخل المجموعات	١١١٦١٩,٣٥	٣٥٩	٣١٠,٩١			
	المجموع الكلي	١١٢٥٤٧,٩٦	٣٦١				

جدول (١١)

نتائج تحليل التباين الأحادي للفروق بين المعلمات في (مخاطر – انتهاكات – مفاهيم) الأمن السيبراني تعزى لمتغير الخبرة

المتغير	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة F	قيمة الدلالة	مستوى الدلالة
الخبرة	بين المجموعات	٥٦٦,٢٨	٢	٢٥٣,١٤	٠,٨١١	٠,٤٤٥	غير دالة
	داخل المجموعات	١١٢٠٤١,٦٨	٣٥٩	٣١٢,٠٩٤			
	المجموع الكلي	١١٢٥٤٧,٩٦	٣٦١				

وتشير النتائج الواردة في جدول (١٠) وجدول (١١) إلى عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة (0.05) بين معلمات المرحلة المتوسطة لكل من (مفاهيم – مخاطر – انتهاكات) الأمن السيبراني تعزى إلى متغير المؤهل الدراسي والخبرة.

وأيضاً تم استخدام اختبار «ت» للتعرف على دلالة الفروق بين معلمات المرحلة المتوسطة لكل من (مفاهيم – مخاطر – انتهاكات) الأمن السيبراني حسب متغير دورات الأمن السيبراني، وجاءت النتائج على النحو الموضح في جدول (١٢):

جدول (١٢)
نتائج اختبار «ت» لدلالة الفروق بين معلمات المرحلة المتوسطة لكل من (مفاهيم – مخاطر – انتهاكات) الأمن السيبراني حسب متغير دورات الأمن السيبراني

توزيع المعلمات حسب دورات الأمن السيبراني	العدد	المتوسط	الانحراف المعياري	درجة الحرية	قيمة «ت»	قيمة الدلالة	مستوى الدلالة
حصلن على دورات أمن سيبراني	١٠	٩٠,٣٠	٢٣,٦٧	٣٦٠	٥,٣٧	٠,٠٠	دالة
لم يحصلن على دورات أمن سيبراني	٣٥٢	٦١	١٦,٨٠				

يتضح من تلك النتائج وجود فروق ذات دلالة إحصائية بين معلمات المرحلة المتوسطة لكل من (مفاهيم – مخاطر – انتهاكات) الأمن السيبراني تبعًا لمتغير دورات الأمن السيبراني.

مناقشة وتفسير النتائج:

تبين من خلال الإجابة عن **السؤال الأول** «ما درجة وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بمفاهيم الأمن السيبراني؟» أن درجة الوعي متوسطة لدى معلمات المرحلة المتوسطة بمفاهيم الأمن السيبراني بشكل عام حيث جاءت استجابات أفراد العينة على ثلاث فقرات بدرجة كبيرة جدًّا، وهي حاجة معلمات المرحلة المتوسطة إلى تعزيز الوعي لديهن بمفاهيم الأمن السيبراني، والحاجة إلى تدخل المدرسة ممثلة بإدارتها في هذا المجال، واتخاذ ما يلزم من إجراءات من قبل الإدارة المدرسية. ووفقاً لتلك النتائج تُعزو الباحثة ذلك لتوفير إدارة تقنية تتمتع بقدر كبير من الموثوقية لتحقيق الأمن السيبراني في المدارس، وتعزيز حماية وسرية وخصوصية المعلومات الشخصية، والتعامل الآمن على شبكة الإنترنت، ومواجهة التهديدات والمخاطر السيبرانية المحتملة في تلك المدراس، وحماية البيانات من أي اختراق أو تعطيل أو تعديل أو استغلال غير مشروع. وجاءت هذه النتيجة متفقة مع ما ذكرته دراسة Spiering (2013) والتي أشارت إلى حاجة المعلمين للتوعية بالموضوعات ذات الصلة بالأمن السيبراني، وتأهيلهم وتطوير معارفهم في هذا المجال، ووضع خطط مقترحة للتوعية. واتفقت أيضًا مع نتيجة دراسة Nyinkeu et. al. (2018) حيث ظهرت نتيجتها إلى أهمية تعزيز مفاهيم الأمن السيبراني ورفع مستوى التوعية بالأمن السيبراني.

وكما تدل الاستجابات على درجة وعي منخفضة جدًّا لدى المعلمات في الكثير من مفاهيم الأمن السيبراني، وعدم اتخاذ التدابير والإجراءات اللازمة لحماية جهاز الحاسب أو الملفات الشخصية أو الصور، بل وما يتعلق بمشاركة المعلومات بشكل آمن، وغياب المفاهيم الخاصة بإمكانية التجسس والاختراق والسطو على البيانات. ووفقًا لتلك النتائج تُعزو الباحثة ذلك إلى ندرة الدورات التدريبية التي تختص بتعزيز مفاهيم الأمن السيبراني

لدى المعلمات، وعدم وجود منظومة أمن معلومات في المدارس تقدم التوعية والحماية بالأمن السيبراني، وندرة المتخصصين في هذا المجال مما أدى إلى وجود فجوة في التعامل مع البيانات داخل المدرسة وخارجها. وجاءت نتيجة هذه الدراسة متفقة مع نتائج الدراسات السابقة كدراسة Spiering (2013) التي أشارت إلى وجود عدد من المشكلات ناتجة عن نقص الوعي بالأمن السيبراني، ومنها: سرقة الصور والملفات، ويرجع ذلك إلى ندرة المعلمين المتخصصين في هذا المجال وعدم توعيتهم، وكما اتفقت مع نتيجة دراسة Pusey &Sadera (2011) التي أظهرت نتائجها إلى أن درجة معرفة المعلمين بمفاهيم الأمن السيبراني منخفضة جدًّا، وأن ٢٠% منهم فقط لديه وعي بدرجة متوسطة بتلك المفاهيم، كما أظهرت النتائج أنه لا يوجد لدى المعلمين صور واضحة لكيفية تدريس تلك المفاهيم، أو كيفية إدراجها أثناء ممارساتهم التدريسية. وتختلف تلك النتائج مع ما أظهرته نتائج الدراسات السابقة والتي أشارت إلى وعيٍ أكبر لدى أعضاء هيئة التدريس، كدراسة العمران (٢٠١١) والتي أظهرت وعي أعضاء هيئة التدريس في الجامعات بمفاهيم الأمن السيبراني بدرجة كبيرة، واهتمام الجامعات بتوعيتهم وتأهيلهم وتقديم الدورات في مجال الأمن السيبراني.

كما تبين من خلال الإجابة عن **السؤال الثاني** «ما درجة وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بمخاطر الأمن السيبراني؟» إلى وجود عدد من المخاطر السيبرانية؛ فباستثناء درجة الوعي الكبيرة لدى المعلمات بتجنب المعلومات التي تخالف العقيدة والدين، وهو أمر طبيعي في ظل مجتمعنا الإسلامي الذي يحرص فيه الجميع على البعد عن كل ما يخالف أو يحمل شبهة المخالفة للعقيدة والدين، والتي جاءت نتيجتها متفقة مع نتيجة دراسة العمران(٢٠١١) والتي أشارت إلى أن هناك وعيًا كبيرًا لدى أعضاء هيئة التدريس بتجنب الأمور المخالفة للعقيدة والقيم وأنظمة الدولة التي تحكم عمليات استخدام الشبكة العنكبوتية. أما فيما يتعلق بالنواحي القانونية والأنظمة السيبرانية، وسياسات المواقع الإلكترونية، وحقوق النشر والوعي الرقمي، فقد أظهرت النتائج أن المعلمات لم يَكُنَّ على نفس درجة الوعي اللاتي تَحَلَّيْنَ بها في الجوانب الدينية، حيث جاءت استجاباتهن بدرجة متوسطة أو منخفضة على هذه الجوانب، ووفقًا لتلك النتائج تُعزو الباحثة ذلك إلى عدم إثراء المعرفة، وعدم وضوح مصطلح الأمن السيبراني، وما يتعلق به من مخاطر لدى المعلمات، وعدم محاولة متابعة مستجدات الأمن الرقمي، ومعرفة الأنظمة السيبرانية، وعدم توفير الدورات وورش العمل، واستقطاب كفاءات بشرية في مجال الأمن السيبراني؛ لتأهيل المعلمات، وتبادل الخبرات والاستفادة من التجارب التي قد تتعرض لها المعلمات في الفضاء السيبراني، ونشر الوعي حول تلك التجارب. وتتفق هذه النتيجة مع ما أظهرته نتائج عدد من الدراسات التي وضحت ظهور العديد من المخاطر السيبرانية في

المدارس، مما يتطلب الحماية من تلك المخاطر والتوعية اللازمة ومنها دراسة (الرفاعي ،٢٠١٨)؛ ودراسة (Goran , 2018)؛ ودراسة(Safaria, 2018) .

وتبين أيضًا من خلال الإجابة عن **السؤال الثالث** «ما درجة تعرض معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة لانتهاكات الأمن السيبراني؟» أن درجة وعي المعلمات بانتهاكات الأمن السيبراني درجة متوسطة بشكل عام، وهو ما يعني احتمال تعرضهن لقدر كبير من انتهاكات الأمن السيبراني، حيث جاءت الإجابات على فقرتين بدرجة كبيرة جدًّا، وتتعلق هاتين الفقرتين بالإجراءات التي يُمكن أن تتخذها إدارة المدرسة. ووفقًا لتلك النتائج تعزو الباحثة ذلك إلى تخوف المعلمات من التعرض للانتهاكات السيبرانية أو قد يكون تعرضن للعديد من الانتهاكات والتهديدات السيبرانية، وسرقة معلوماتهن، وبياناتهن السرية، واختراق حساباتهم المدرسية، وجاءت هذه النتيجة متفقة مع نتيجة دراسة (Spiering (2013 والتي أشارت إلى وجود العديد من المشكلات التي يتعرض لها المعلمين نتيجة نقص الوعي بالأمن السيبراني، ومنها الانتهاكات السيبرانية والتهديدات المختلفة.

وكما تدل الاجابات إلى أن درجة الوعي منخفضة لدى المعلمات فيما يتعلق ببرامج الحماية وتحديثها بشكل دوري، وما يتعلق بإجراءات التشفير للملفات، ووفقًا لتلك النتائج تعزو الباحثة ذلك إلى عدم وجود تدريب وتأهيل للمعلمات فيما يتعلق بالحوادث الأمنية التي تهدد الأمن السيبراني، وعدم توافر سياسات لحماية البيانات الشخصية وتحديثها وتشفيرها، وعدم توافر سياسات للتعامل الأمثل مع التقنية ووسائل التواصل الاجتماعي، وعدم الإلزام باستخدام برامج الحماية، والنسخ الأصلية في المدارس؛ لحماية معلوماتهن من الانتهاكات السيبرانية، حيث تزداد أهمية هذا الإجراءات في ظل شيوع استخدام مواقع التواصل الاجتماعي، ونشر وتبادل المشاركات عبر تلك المواقع، وتبادل الملفات عبر أجهزة الحواسيب وعبر الهواتف الذكية، ويؤدي إهمال تلك الإجراءات وعدم الوعي بها إلى وقوع المعلمات وغيرهن ممن يستخدمن شبكة الإنترنت كضحايا للانتهاكات السيبرانية. وتتفق تلك النتائج مع نتيجة دراسة (Pusey & Sadera (2011 التي أظهرت نتائجها إلى أن درجة معرفة المعلمين بالانتهاكات السيبرانية منخفضة جدًّا لذلك لا بد من توعيتهم في هذا المجال. وأيضا مع دراسة (Bustard (2018 والتي أشارت إلى عدم التوعية بالانتهاكات السيبرانية قد يكون له أثر سلبي على أمن المؤسسات. ومع نتيجة دراسة Kritizingler et. al (2017) والتي أشارت إلى ضرورة سن قوانين وتشريعات لمكافحة الانتهاكات السيبرانية.

ويُمكن إيجاز النتائج المتعلقة بالإجابة عن الأسئلة الثلاثة إلى أن درجة الوعي لدى معلمات المرحلة المتوسطة بكل من مفاهيم ومخاطر وانتهاكات الأمن السيبراني هي درجة متوسطة، وهذا يدل أنهن بحاجة للتوعية والتثقيف في هذا المجال. ووفقًا لتلك النتائج تُعزو

الباحثة ذلك إلى عدم وجود منظومة متكاملة تختص بالأمن المعلوماتي تشترك فيها المدارس مع إدارات التعليم تعزز الحماية والتثقيف، وتوفير البرمجيات والبرامج والتطبيقات التي تستطيع المعلمات التعامل معها باحترافية، وعدم وضع برامج لتوعية المعلمات حول مخاطر وتهديدات الأمن السيبراني، وعدم نشر تعليمات للحفاظ على الأمن السيبراني في المدارس. وتتفق تلك النتائج مع ما أظهرته نتائج دراسة Alhejail (2013) والتي أشارت إلى حاجة معلمات المرحلة المتوسطة لرفع مستوى الوعي لديهن بالأمن السيبراني، ودراسة Kritizingler et. al (2017) والتي أظهرت نتائجها بضرورة تدريب المعلمين وتوعيتهم بكل ما يتعلق بمجال الأمن السيبراني.

وتبين أيضًا من خلال الإجابة عن **السؤال الرابع** إلى عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة (0.05) بين معلمات المرحلة المتوسطة لكل من (مفاهيم – مخاطر – انتهاكات) الأمن السيبراني حسب متغير المؤهل الدراسي، ويُمكن تفسير ذلك باعتبار أن الأمن السيبراني من المفاهيم الحديثة نسبيًّا، والتي بدأ الاهتمام به مؤخرًا بدرجة كبيرة، ولم يتم إدراجه ضمن المقررات الدراسية الخاصة بتأهيل المعلمات، أو ضمن برامج إعداد المعلمين والمعلمات، أو برامج الدراسات العليا في كليات التربية قبل الخدمة أو أثناء الخدمة. واختلفت نتيجة الدراسة الحالية مع ما أظهرته نتيجة دراسة صائغ (٢٠١٨) والتي أشارت إلى وجود فروق ذات دلالة إحصائية عند مستوى دلالة (0.05) بين إجابات أفراد الأسرة حسب متغير المؤهل التعليمي. وتشير النتائج أيضاً إلى عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة (0.05) بين معلمات المرحلة المتوسطة لكل من (مفاهيم – مخاطر – انتهاكات) الأمن السيبراني حسب متغير الخبرة، وبصورة مماثلة يُمكن تفسير ذلك في ضوء حداثة مفهوم الأمن السيبراني، وعدم إدراجه ضمن المقررات الدراسية المختلفة، مما يجعل الوعي بذلك المفهوم أمرًا لا يمثل محل اهتمام المعلمات، على اختلاف سنوات خبرتهن وعملهن في الميدان التربوي، وعدم وجود حوافز للمعلمات اللاتي لديهن خبرة في التعامل الأمثل مع التقنية وحماية البيانات المدرسية. وتختلف هذه نتيجة مع دراسة Bele et .al (2014) والتي أشارت إلى أن إعداد مقررات دراسية في مجال الأمن السيبراني قائمة على نظام التعلم المدمج وموجهة للمعلمين تعمل على إكسابهم الخبرة وتوعيتهم في مجال الأمن السيبراني. بينما تشير النتائج إلى وجود فروق ذات دلالة إحصائية عند مستوى دلالة (0.05) بين معلمات المرحلة المتوسطة لكل من (مفاهيم – مخاطر – انتهاكات) الأمن السيبراني تبعًا لمتغير دورات الأمن السيبراني، وتوضح هذه النتيجة أهمية تنظيم دورات متخصصة في مجال الأمن السيبراني بالنسبة للمعلمات من مختلف التخصصات، والأثر الفعّال لتلك الدورات في رفع مستوى الوعي لدى المعلمات اللواتي التحقن بتلك الدورات، وجاءت نتيجة هذه الدراسة متفقة مع دراسة Spiering (2013) والتي توصلت إلى تقديم خطة مقترحة للتوعية

بالأمن السيبراني تشمل تدريب المعلمين وتأهيلهم وتزويدهم بالمعارف والمهارات ذات الصلة بالأمن السيبراني، وتأهيل البنية التحتية الرقمية في المدارس، وإشراك المختصين الرقميين في وضع برامج التدريب التربوية في الأمن السيبراني، وتقييم نتائج تطبيقها لزيادة الوعي لديهم. ومع نتيجة دراسة Kritizingler et. al (2017) حيث أظهرت نتائج الدراسة إلى تدريب المعلمين، وعقد ورش عمل وأيام مفتوحة وندوات لهذا المجال لرفع مستوى الوعي لديهم.

توصيات الدراسة:

في ضوء النتائج السابقة يُمكن التقدم ببعض التوصيات على النحو التالي:

١. عقد دورات تدريبية للمعلمات في مجال الأمن السيبراني، بحيث تتناول تلك الدورات مفاهيم ومخاطر وانتهاكات الأمن السيبراني.
٢. عقد ورش عمل حول إجراءات الحماية ضد مخاطر وانتهاكات الأمن السيبراني، بإشراف مدربين مختصين في الأمن السيبراني.
٣. التنسيق بين وزارة التعليم والجهات المشرفة على الأمن السيبراني كالهيئة الوطنية للأمن السيبراني؛ لاتخاذ الإجراءات اللازمة لتنمية الوعي لدى المعلمات في مجال الأمن السيبراني.
٤. استقطاب كفاءات بشرية في مجال الأمن السيبراني ، وإدراج مقررات دراسية خاصة بمفاهيم الأمن السيبراني ضمن برامج إعداد المعلمين والمعلمات في كليات التربية وغيرها من المؤسسات الأكاديمية.
٥. إصدار نشرات دورية من قبل وزارة التعليم خاصة بمفاهيم ومخاطر وانتهاكات الأمن السيبراني، على أن تتناول تلك النشرات كل ما هو جديد في هذا المجال.

المراجع العربية:

ابن تاج، لحمر. عباس. (٢٠١٨). أخلاقيات الأعمال لإلكترونية وتحديات الأمن المعلوماتي في ظل الاقتصاد الرقمي. *المجلة المصرية للدراسات القانونية والاقتصادية – مصر*، ع ١٠ ،٢٩٩ -٣٢٩.

ابن شلفوت، جعفر. (٢٠١٨). دور الجامعات السعودية في مكافحة الجرائم الإلكترونية من وجهة نظر طلبة الجامعات: دراسة حالة جامعة نايف العربية للعلوم الأمنية. *مجلة كلية الآداب*. جامعة بورسعيد" كلية الآداب. ١٢، ٩٥٥-٩٩٥.

أبو دوح، خالد. كاظم. (٢٠١٨). الأمن السيبراني للدول والأفراد: الأمر الذي لا بد منه. *المجلة العربية*، ٣٩٨، ٣٠-٣٣.

أبو علام، رجاء. (٢٠١١). *مناهج البحث في العلوم النفسية والتربوية*. ط٧، القاهرة: دار النشر للجامعات.

أبو منصور، حسين يوسف. (٢٠١٧). توظيف تقنية التصنيف الربطي للكشف عن مواقع التصيد الإلكتروني. *المجلة العربية الدولية للمعلوماتية*. جامعة نايف العربية للعلوم الأمنية. ٥(٩)، ٣٢-٤٠.

بانقا، علم الدين. (٢٠١٩). *مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي*. الكويت: المعهد العربي للتخطيط، سلسلة دراسات تنموية، ع٣٦.

بن شلهوب، هيفاء بنت عبد الرحمن. (٢٠١٥). *طرق البحث في الخدمة الاجتماعية*. الرياض: مكتبة الشقري للنشر والتوزيع.

الجبور، منى. (٢٠١٢). الأمن السيبراني: التحديات ومستلزمات المواجهة. *اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني*. جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية. بيروت: ٢٧-٢٨ أغسطس.

حسن، حسن محمد. (٢٠١٨). مخاطر استخدام الفضاء السيبراني في الحياة الاجتماعية والثقافية والأسرية دون حماية وآثارها. *المؤتمر السابع لأمن وسلامة الفضاء السيبراني (الإنترنت) في الدول العربية*. بيروت: يوليو ٢٣-٢٥.

الخثعمي، مها بنت دخيل الله. (٢٠١٨). مستوى الوعي بقضايا أمن المعلومات لدى طالبات المرحلة الثانوية بالمدارس الحكومية بمدينة الرياض. *مجلة العلوم الإنسانية والاجتماعية*. جامعة الإمام محمد بن سعود الإسلامية، ٤٧، ٣٥٥-٤٠٠.

خليفة، إيهاب. (٢٠١٧). *القوى الإلكترونية كيف يُمكن أن تدير الدول شؤونها في عصر الانترنت*. القاهرة: العربي للنشر والتوزيع.

الربيعة، صالح بن علي. (٢٠١٨). *الأمن الرقمي وحماية المستخدم من مخاطر الانترنت*. الملتقى الأول بالإدارة العامة لتعليم بمحافظة جدة. جدة: ٢٧ أبريل ٢٠١٨.

الردفاني، محمد قاسم أسعد. (٢٠١٥). تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية. *المجلة العربية للدراسات الأمنية والتدريب*. ٣٠(٦١). ١٥٧-١٩٢.

الرفاعي، تغريد حمد. (٢٠١٨). درجة ممارسة وتعرض طلبة المرحلة المتوسطة في مدارس دولة الكويت للتنمر الإلكتروني وأثر متغير الجنس. *مجلة العلوم التربوية*. جامعة الكويت. ٤ (٣)، ١١١-١٤٥.

صائغ، وفاء بنت حسن عبد الوهاب. (٢٠١٨). وعي أفراد الاسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية. *المجلة العربية للعلوم الاجتماعية*. المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية. ١٤(٣)، ١٨-٧٠.

صفا الله، سحر محمد. (٢٠١٩). المنطقة العربية في مؤتمر دافوس للأمن السيبراني خلال السنوات الخمس الأخيرة (٢٠١٤-٢٠١٨). *مجلة قضايا ونظرات*. مركز الحضارة للدراسات والبحوث. ١٤، ٩٧-١٠٣.

عبد الحليم، محيي الدين. (٢٠٠٩). *الرأي العام مفهومه وأنواعه وعوامل تشكيله*. القاهرة: مكتبة الأنجلو المصرية.

عبد الصادق، عادل. (٢٠٠٩). *الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة*. القاهرة: مركز الدراسات السياسية والاستراتيجية بالأهرام.

عبد الصادق، عادل. (٢٠١٤). *الفضاء الإلكتروني والثورة في شؤون أجهزة الاستخبارات الدولية*. القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية.

العريشي، جبريل بن حسن؛ الدوسري، سلمى بنت عبد الرحمن. (٢٠١٥). أثر استخدام وسائل التواصل الاجتماعي على القيم والأمن الفكري لديهم: دراسة ميدانية وصفية مطبقة على طلاب وطالبات الجامعات السعودية. *مجلة دراسات في الخدمة الاجتماعية والعلوم الإنسانية*. ٣٨(١٧)، ٣٢٧٣-٣٣٤٦.

العساف، صالح. (٢٠٠٦). *المدخل إلى البحث في العلوم السلوكية*. ط٤. الرياض: العبيكان.

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

عطية، محسن. (٢٠٠٩). *البحث العلمي في التربية: مناهجه، أدواته، وسائله الإحصائية*. عمّان: دار الشروق.

العمران، حمد بن إبراهيم. (٢٠١١). الوعي بأمن المعلومات لدى أعضاء هيئة التدريس في الجامعات: دراسة حالة لجامعة المجمعة. *مجلة الاتحاد العربي للمكتبات والمعلومات*. ٨، ١٠-٤٤.

العودة، دلال. (٢٠١٥). الصراعات الدولية الحديثة. القاهرة: دار الطلائع للنشر والطباعة.
عيد، غادة. (٢٠١٢). *القياس والتقويم التربوي مع تطبيقات برنامج SPSS*، الكويت: مكتبة الفلاح للنشر والتوزيع.
غريب، ماجدة؛ الأمير، حسن. (٢٠١٧). مدى الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي. *المجلة العربية الدولية للمعلوماتية*. جمعية كليات الحاسبات والمعلومات في اتحاد الجامعات العربي، ٥(٩)، ١٧-٣٢.
القحطاني، ذيب بن عايض. (٢٠١٥). *أمن المعلومات*. الرياض: مكتبة الملك فهد للنشر.
المبارك، محمد؛ حران، منى؛ إسحاق، معتز. (٢٠١٤). *أمن المعلومات*. الخرطوم: المركز السوداني لأمن المعلومات.
متولي، أحمد حسني. (٢٠١٥). الجرائم المعلوماتية: رؤية مقترحة من منظور تربوي لدور أعضاء هيئة التدريس بكليات التربية لزيادة الوعي بمكافحة الجرائم المعلوماتية. *المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية*. جامعة الإمام محمد بن سعود الإسلامية – كلية علوم الحاسوب والمعلومات، ١٨٤-١٩٤.
المنتشري، حليمة؛ المنتشري، محمد. (٢٠١٨). *الأمن السيبراني*. جدة: معرض الكتاب الدولي الثاني.
الهاجري، محمد سعد. (٢٠١٧). دور معلمي المرحلة المتوسطة في مواجهة مخاطر شبكات التواصل الاجتماعي على الأمن الفكري للطلاب. *مجلة العلوم التربوية*. جامعة الكويت: ٣(٣)، ٣١٤-٣٣٦.
الهزاني، محمد ناصر. (٢٠١٨). المسؤولية الجنائية عن انتهاك قواعد الفضاء السيبراني: دراسة تأصيلية مقارنة بالقانون الإماراتي. *رسالة ماجستير غير منشورة*. جامعة نايف العربية للعلوم الأمنية: كلية العدالة الجنائية، قسم الشريعة والقانون.
الهيئة الوطنية للأمن السيبراني (٢٠١٨). تقرير *الضوابط الأساسية للأمن السيبراني*. الرياض: الهيئة الوطنية للأمن السيبراني

المراجع الأجنبية:

Alhejaili, H. (2013). Usefulness of teaching security awareness for middle school students. *Unpublished master thesis*. New York: Rochester institute of technology.

Bele, J., Dimc, M., Rozman, D & Jemec, A, (2014). Raising awareness of the cybercrime the use of education as a means of prevention and protection. *10th international conference mobile learning.* Spain: Madrid, 28th feb – 2nd march.

Bicak, A, Liu, M. & Murphy, D. (2015). Cybersecurity curriculum development: introducing specialties in a graduate program. *Information systems education journal (ISEDJ), 13(3), 99-110* .

Black. M., Chapman, D. & Clark, A. (2018). The enhanced virtual laboratory: extending cyber security awareness through a web-based laboratory. *Information systems education journal (ISED), 16 (6), 4-12*.

Bustard, J. (2018). Improving student engagement in the study of professional ethics: concepts and an example in cyber security. *Scientific engineer ethics. 24, 683-698.*

Cai, Yu (2018). Using case studies to teach cybersecurity courses. *Journal of cybersecurity education, research and practice. 2, 1-24.*

Canongia, C., & Mandarino, R. (2014). *Cyber security the new challenge of the information society*. In Crisis Management: Concepts, Methodologies, tools and applications: 60-80.

Crompton, B., Thompson, D., Reyes, M., Zhou, X., and Zou., X. (2016). *Cybersecurity awareness Shrewsbury public schools*. School of professional studies. Paper 3.

Fees, R., Rosa, J., Durkin, S., Murray, M., & Moran, A. (2018). Unplugged CyberSecurity: An approach for bringing computer science into the classroom. *International Journal of computer science education in schools. 2(1), 1-11.*

Johnson, M. (2013). Cybercrime, security and digital intelligence. New York: Routledge.Goran, I. (2017). Cyber security risks in public high school. *Unpublished master thesis*. City university of New York: John Jay college of criminal justice.

Hinduja, S., Patchin, J. (2010). Bullying, cyberbullying and suicide. *Archives of suicide research*. 14(3), 9-18.

International Telecommunication Union (ITU) (2019). *Global Cybersecurity Index*. Geneva .

Kritizinger, E., Bada, M., & Nurse, J. (2017). A study into the cybersecurity awareness initiatives for school learners in south africa and the uk. *10th world conference on information security education*. Rome: May 29-31.

Moskal, E. (2015). A model for establishing a cybersecurity center of excellence. *Information systems education journal*. *13(6), 97-108*.

Nyinkeu, N., Anye, D., Kwededu, L. & Buttler, W. (2018). Cyber education outside the cyber space: the case of catholic university institute of Buea. *International journal of technology in teaching and learning*. *14(2), 90-101*.

Pruitt-Mentle, D. (2008). 2008 *National cybersaftey, cybersecurity, cyberethics baseline study,* Washington: national cybersecurity alliance .

Pusey, P. & Sadera, W. (2011). Cyberethics, Cybersaftey, and Cybersecutity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. J*ournal of digital learning in teacher education. 28(2), p.82-88 .*

Rayan, T., Kariuki, M. & Yilmaz, M. (2011). A comparative analysis of cyberbullying perceptions of perspective educators: Canada and Turkey. *The Turkish online journal for educational technology*. *10(3), 1-12.*

Safaria, T. (2016). Prevalence and Impact of Cyberbullying in a Sample of Indonesian Junior High School Students. *The Turkish Online Journal of Educational Technology*. *15(1), 82-91*.

Sarker, K., Rahman, H., Rahman, K., Arman, S., Biswas, S. & Bhuiyan, T. (2019). A comparative analysis of the cyber security strategy of Bangladesh. *International journal of cybernetics & informatics (IJCI). 8(2), 1-21*.

Solms. R. & Solms, S.(2015). Cyber safety education in developing countries. *Journal of systemics, cybernetics and informatics*. *13(2), 14-19.*

Spiering, A. (2013). Improving cyber saftey awareness education at duch elementary school. *Unpublished master thesis*. Leiden: Leidein university.

Stephenson, C. (2005). Creating a national K-12 Computer Science Community. *Communication of the ACM, 48(1), 29-31*.

Stewart, K., and Shilingford, N. (2011). Cyber girls Sumer camp: Exposing middle school females to Internet security. *Unpublished master thesis*. University of Minnesota.

Taylor, M., Baskett, M., Allen, M., Francis, H., & Kifayat. K. (2018). Animations as an aid to support the teaching of cyber security concepts. *Innovations in education and teaching international*. *55(5), 532-542*.

Wilson, C. (2014). Cybersecurity education the emergence of an accredited academic discipline. *Journal of the colloquium information system security education*. *2(1), 2-13.*

مواقع الإنترنت

مركز الأمن السيبراني الاسترالي.(٢٠١٩). (https://www.cyber.gov.au/)

مركز الأمن الالكتروني السعودي.(٢٠١٩). https://nca.gov.sa/pages/ncsa.html

مركز الأمن السيبراني الماليزي.(٢٠١٩). https://www.cybersecurity.my/en/index.html

المركز العربي للبحوث القانونية.(٢٠١٩) . https://carjjorg/node/5561

المركز القومي لبحوث التعليم المتكامل (الولايات المتحدة الأمريكية). (٢٠١٩). https://nicerc.org