 https://doi.org/10.12816/0061668

The Degree of Cyber Security Awareness among Teachers in the Directorate of Karak Education

Abeer Ahmed Al-Habashneh
Ministry of Education−Jordan
abeer_759@yahoo.com

Received : 08/06/2022 Accepted :06/09/2022

Abstract:

This research aims to find out how much teachers in Karak Education Directorate know about cyber security and ways to improve their knowledge. It also tries to see if there were differences in how much they knew about cyber security. The different things that can help teachers become more aware include their gender, education level, the subjects they teach, and how long they have been teaching. The research used a method called descriptive survey to study (271) male and female teachers. The survey is distributed to these people to reach the study goal, and the validity and reliability of the survey are verified.

The study reached a number of results, the most important of which are that: the degree of cybersecurity among teachers appeared high, and that the approaches of raising cybersecurity are as follows: using the websites that deepen the moral and religious values, using safe applications and educational programs, reporting cybersecurity crimes, indulge in social life and not virtual life, raising awareness of harmful links when surfing the internet, raising awareness among teachers of the reliable sources of information, safe surfing, promoting the concepts of cybersecurity, training teacher to use strong passwords and continuously updating them, informing teachers on how to protect data and information on their personal devices, and raising their awareness of the dangers of prolonged use of the internet, introducing them to the proper manner of handling email attachments, and positive use of the internet, training them to use protection programs and firewalls and update them periodically.

The research also found that teachers' awareness of cyber security varies depending on their gender, with males being more aware than females. The study did not find any differences in awareness based on the teacher's qualifications, the subjects they teach, or their teaching experience. The results also found that there were no big differences in how teachers learn about cyber security, based on their gender, education level, subjects taught, or teaching experience. The study recommends that teachers should be trained to use protection programs and firewalls because they are proved through the results to have mediocre knowledge of these technologies.

Keywords: Degree Of Awareness, Cyber Security, Methods Of Developing Cybersecurity**.**

درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية " والتعليم قصبة الكرك"

عبير احمد عبد الرحمن الحباشنة
وزارة التربية و التعليم
abeer_759@yahoo.com

الاستلام : 2022/06/08 القبول : 2022/09/06

الملخص:

هدفت هذه الدراسة إلى الكشف عن درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية تربية وتعليم قصبة الكرك، وطرق تنمية الوعي لديهم، وهدفت كذلك إلى الكشف عن الفروق في درجة الوعي بالأمن السيبراني، وطرق تنميته لدى المعلمين تعزى للمتغيرات الآتية: (النوع الاجتماعي، والمؤهل العلمي، والمواد التي يدرّسها المعلم، وسنوات الخبرة في التدريس). وقد استخدمت الدراسة المنهج الوصفي المسحي، وتكونت عينة الدراسة من (271) معلمًا ومعلمة، ولتحقيق هدف الدراسة تم بناء استبانة، وتم التحقق من صدقها وثباتها. ومن أهم النتائج التي توصلت إليها الدراسة: أن درجة الوعي بالأمن السيبراني لدى المعلمين جاءت بدرجة مرتفعة، وأن طرق تنمية الوعي بالأمن السيبراني جاءت على النحو الآتي: استخدام المواقع الإلكترونية التي تعمق القيم الدينية والأخلاقية، واستخدام التطبيقات الآمنة والبرامج التعليمية، والإفصاح عند التعرض لأي من الجرائم السيبرانية، والاندماج بالحياة الاجتماعية، وعدم الانشغال بالحياة الافتراضية، وتعزيز الوعي بمخاطر الروابط الضارة عند تصفح الإنترنت، واستخدام الإنترنت والتطبيقات الإلكترونية كوسيلة للتعلم والبحث عن المعرفة، وتوعية المعلمين بالمصادر الموثوقة للمعلومات، والتصفح الآمن للإنترنت، والتوعية بمفاهيم الأمن السيبراني، وتدريب المعلمين بكيفية إعداد كلمة سر قوية وتحديثها باستمرار، وتثقيف المعلمين بوسائل حماية بياناتهم ومعلوماتهم على أجهزتهم الخاصة، وتوعيتهم بمشكلات استخدام الإنترنت لفترات طويلة، والتعامل مع مرفقات البريد الإلكتروني بشكل صحيح، والاستخدام الإيجابي للإنترنت، والتدريب على استخدام برامج الحماية والجدار الناري وتحديثها بشكل مستمر. كما توصلت الدراسة إلى وجود فروق دالة إحصائيًّا في درجة الوعي في الأمن السيبراني لدى المعلمين تعزى للنوع الاجتماعي ولصالح الذكور، وعدم وجود فروق تعزى للمؤهل العلمي، والمواد التي يدرّسها المعلم، وسنوات الخبرة في التدريس، كما أظهرت النتائج عدم وجود فروق دالة إحصائيًّا في طرق تنمية الوعي بالأمن السيبراني لدى المعلمين تعزى للنوع الاجتماعي، وللمؤهل العلمي، والمواد التي يدرسها المعلم، وسنوات الخبرة في التدريس، وأوصت الدراسة بضرورة تدريب المعلمين على استخدام برامج الحماية والجدار الناري، حيث إنّ النتائج كشفت عن مستوى وعي متوسط لديهم بهذه التقنية.

الكلمات المفتاحية: درجة الوعي، الأمن السيبراني، طرق تنمية الأمن السيبراني.

المقدمة:

شهدت العقود الثلاثة الماضية انتشارًا واسعًا لأعداد مستخدمي شبكة الإنترنت، والهواتف الذكية، واستخدامها في مجالات الأعمال، والتجارة، والتعليم، والترفية، والخدمات الحكومية، وغيرها من الأنشطة الاقتصادية، والاجتماعية، والثقافية. ولكن مع الانتشار المتزايد لأعداد مستخدمي شبكات الاتصالات والإنترنت فإنّ تكنولوجيا المعلومات والاتصالات تُعدّ محايدة، حيث يمكن أن تُستخدم بما هو مفيد، ويمكن أن يُساء استخدامها؛ لذلك برزت أهمية مواجهة الأخطار والتحديات، ومن أهمها الجرائم الإلكترونية التي تواجه البنى التحتية للمعلومات والاتصالات التي أصبحت تهدد الأمن الشخصي والدولي، وتؤدي إلى إيقاع خسائر فادحة للمستخدمين أو لأيّ جهات أخرى (Sadowsky, et. al., 2003).

تسعى دول العالم للتحول نحو العالم الرقمي، وتنمية البنية التحتية الرقمية؛ لمواكبة التقدم العالميّ المتسارع في الخدمات الرقمية وقدرات المعالجة الحاسوبية، وقدرات التخزين الهائلة للبيانات، والتعامل مع الذكاء الاصطناعي والإنترنت. ويعتمد التعليم اليوم بشكل كبير على شبكة الإنترنت، لذا يجب توعية المعلمين بمخاطر استخدام شبكات الإنترنت، واتخاذ إجراءات وقائية لحماية البيانات والمعلومات من الفيروسات، أو اختراقها، أو استغلالها في الإساءة إلى الآخرين. ويؤثر سوء الاستغلال المتنامي للشبكات الإلكترونية سلبًا على سلامة البنى التحتية للمعلومات الشخصية والوطنية، وعلى أمن الطلبة، ولتفادي الوقوع كضحية للجرائم الإلكترونية، فمن الضروري وجود نظام قوي يحمي هذه المعلومات والخدمات التي يوفرها الفضاء الإلكتروني، ومن هنا ظهر ما يعرف بالأمن السيبراني (الصانع وآخرون، 2020).

أصبح الأمن السيبراني حديث العالم بأسره، ويعد جزءًا أساسيًّا من السياسات الأمنية للدولة، والتي يلجأ إليها صناع القرار كأولوية في سياساتهم لحماية المعلومات والتطبيقات الوطنية للأفراد والدولة، في

جميع مجالات الحياة التعليمية، والاجتماعية، والاقتصادية، ويرتبط ارتباطًا وثيقًا بسلامة مصادر الثورة المعلوماتية، والقدرة على الاتصال والتواصل (الصحفي وعسكول، 2019). ويُعدّ الأمن السيبراني الحل الأمثل لمتابعة الاستخدام الواسع للإنترنت وتطبيقاته المختلفة؛ للتقليل من المخاطر التي تنشأ من سوء الاستخدام، حيث توجد محتويات غير مشروعة وغير مرغوبة ولها تأثير سلبي على أخلاقيات المجتمع وقيمه، فلا بد من بناء مجتمع واعٍ ومدرك لهذه المخاطر؛ ليستطيع التعامل معها وفقًا لقواعد السلامة، ومدرك للعواقب القانونية للتصرفات اللامسؤولة (جبور، 2016).

وقد اهتمت دول العالم بالمؤسسات التربوية لإعداد المعلمين للتعامل مع التطورات التكنولوجية، وما يتطلبه هذا التعامل من درجة الوعي بالأمن السيبراني (المنتشري وحريري، 2020)، وفي إطار تلك المبادرة قام مركز علوم الحاسوب والتكنولوجيا والهندسة والرياضيات (STEM) في ولاية ميريلاند بتدريب المعلمين على أساسيات تكنولوجيا الإنترنت والأمن السيبراني (Fees et.al.,2018)، واتخذ الاتحاد الأوروبي (2009) قرارًا بإدراج المفاهيم المتعلقة بالأمن السيبراني ضمن المناهج الدراسية في (24) دولة أوروبية (R. Solms& S. Solms,2015)، واتخذت دول آسيوية عديدة إجراءات مماثلة لتفعيل دور المؤسسات التربوية، وتفعيل دور المعلم في مجال الأمن السيبراني ومنها اليابان، وماليزيا (Sarker, et.al., 2019).

ويعد الأمن السيبراني من المواضيع البحثية الحديثة، وارتبطت نشأته باعتماد الأفراد على الإنترنت في كافة أعمالهم؛ مما جعل معلوماتهم عرضة للخطر والاختراقات المختلفة، لذلك لا يمكن إغفال أهميتها في الجانب التعليمي في ظل الثورة الرقمية والتكنولوجية المعاصرة؛ بسبب الاستخدام المتزايد لشبكات الإنترنت في المؤسسات التربوية. وعلى ذلك فإنّ أهمية امتلاك المعلم للوعي المناسب بالأمن السيبراني، يساعده على حماية نفسه وطلبته من هذه المخاطر التي تؤثر بشكل كبير على قيم المجتمع وأخلاقه وثقافته. لذا جاءت فكرة البحث لمعرفة مستوى وعي المعلمين بالأمن السيبراني في قصبة الكرك وتنميته لديهم.

مشكلة الدراسة:

أصبحت تكنولوجيا المعلومات جزءًا أساسيًّا من حياة البشر، ولا سيّما في مجال التعليم الذي يعتمد عليه بشكل كبير للحصول على المعرفة والمعلومات. وقد تتعرض أنظمة التكنولوجيا كغيرها من الأنظمة لمخاطر تؤثر على كفاءتها وفاعليتها، وأصبح من الضروري على المؤسسات والمنظمات والشركات وضع إجراءات لمواجهة التحديات والمخاطر والعمل على الحدّ منها.

ومن خلال عمل الباحثة في مجال التعليم، وخبرتها في الميدان كمعلمة لمبحث الحاسوب، واعتماد التعليم على المصادر الإلكترونية خاصة الشبكة العنكبوتية كمصدر أساسي من مصادر المعرفة والحصول على المعلومات، واستخدام مواقع شبكات التواصل الاجتماعي والمواقع التعليمية والألعاب الإلكترونية بكثرة من قبل الكبار والصغار، فإنّه يترتب على ذلك تعرض بعض مستخدميها للجرائم الإلكترونية كالاحتيال، والروابط الوهمية، وتعطل بعض التطبيقات، وحالات التنمر، والاختراقات، وغيرها. لذا هدفت الدراسة قياس درجة وعي المعلمين بالأمن السيبراني، وطرق تنميته؛ لما له من أهمية لحماية مجتمعنا من الانحراف والجرائم السيبرانية.

أسئلة الدراسة:

يسعى البحث للإجابة عن الأسئلة الآتية:

1. ما درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك؟

2. ما درجة تطبيق طرق تنمية الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك؟

3. هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$)، في درجة الوعي بالأمن السيبراني لدى معلمي مديرية التربية والتعليم في قصبة الكرك يعزى لمتغيرات: (النوع الاجتماعي، والمؤهل العلمي، التخصص، وسنوات الخبرة في التدريس)؟

4. هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$)، في طرق تطبيق تنمية الوعي بالأمن السيبراني لدى المعلمين مديرية التربية والتعليم قصبة الكرك يعزى لمتغيرات: (النوع الاجتماعي، والمؤهل العلمي، التخصص، وسنوات الخبرة في التدريس)؟

أهداف الدراسة:

يهدف هذا البحث إلى الآتي:

1. التعرف إلى درجة الوعي بالأمن السيبراني لدى المعلمين في قصبة الكرك.

2. التعرف إلى درجة تطبيق طرق تنمية الوعي بالأمن السيبراني لدى المعلمين في قصبة الكرك.

3. التعرف إلى دلالة الفروق –إن وجدت– في درجة الوعي بالأمن السيبراني لدى معلمي مديرية التربية والتعليم قصبة الكرك، تعزى لمتغيرات: (النوع الاجتماعي، والمؤهل العلمي، والمواد التي يدرسها المعلم، وسنوات الخبرة في التدريس).

4. التعرف إلى دلالة الفروق –إن وجدت– في طرق تطبيق تنمية الوعي بالأمن السيبراني لدى معلمي مديرية التربية والتعليم قصبة الكرك تعزى لمتغيرات: (النوع الاجتماعي، والمؤهل العلمي، المواد التي يدرسها المعلم، وسنوات الخبرة في التدريس).

أهمية الدراسة:

تكتسب الدراسة الحالية أهميتها في أنها تأتي استجابة للتوجهات

العالمية في تعزيز درجة الوعي بالأمن السيبراني ورفعه لدى مستخدمي الشبكة العنكبوتية، كمستحدث تقني ازداد استخدامه في جميع أنحاء العالم في ظل الثورة المعلوماتية، وعليه يمكن توضيح أهمية الدراسة في الآتي:

– الأهمية النظرية: يمكن للأدب النظري الوارد في الدراسة الحالية أن يضيف معرفة جديدة للباحثين، ويرفد المكتبة العربية بإطار نظري جديد حول التعرف إلى ماهية الأمن السيبراني، وتلقي الدراسة أهميتها على دور المعلمين في تطبيق طرق تنمية الوعي بالأمن السيبراني لديهم؛ مما يساهم ذلك في رفع مستوى الوعي بالأمن السيبراني لدى الطلبة.

– الأهمية العملية: يمكن أن تفيد نتائج هذه الدراسة المسؤولين في وزارة التربية والتعليم في التعرف إلى درجة وعي المعلمين في قصبة الكرك بالأمن السيبراني، وتطوير برامج إعداد المعلمين لمواجهة الثورة المعلوماتية المعاصرة، والعمل على رفع درجة الوعي بالأمن السيبراني لدى العاملين في المجال التربوي عند التعامل مع مصادر المعرفة الإلكترونية.

المصطلحات والتعريفات الإجرائية.

الوعي:

يعرف الوعي اصطلاحًا بأنه إدراك الفرد لنفسه والبيئة المحيطة به (حنفي، 2000).

يعرف إجرائيًّا بأنه المحصلة المعرفية للفرد نتيجة تعرضه لخبرات وتجارب خاضها تجاه أمر معين.

الأمن السيبراني:

يعرف الأمن السيبراني اصطلاحًا بأنه الإجراءات التقنية الهادفة إلى حماية البيانات والمعلومات، والهوية الشخصية، والمعدات التقنية من أي شكل من أشكال الوصول غير المسموح به إلى تلك المعلومات أو المعدات (Pusey & Sadera, 2011).

ويعرف إجرائيًّا في هذه الدراسة بأنه جميع الإجراءات التي تهدف إلى حماية البيانات والمعلومات والمعدات من الوصولِ غير المصرح به، وإلحاقِ الأذى بها، وتشملُ الحمايةَ من الاختراق، والبرمجيات الخبيثة كالفيروسات، وغير ذلك من ممارسات سلبية.

الوعي بالأمن السيبراني إجرائيًّا:

وتعرفه الباحثة بأنه جميع الإجراءات التي تهدف إلى حماية الفضاء المعلوماتي الخاص بالأفراد أو المؤسسات من الممارسات السلبية، بحيث تشكل درعًا مهمًّا في هذا العصر.

حدود الدراسة:

- الحدود البشرية: معلمي المدارس الحكومية في قصبة الكرك.
- الحدود المكانية: المدارس الحكومية في قصبة الكرك.
- الحدود الزمانية: الفصل الدراسي الأول للعام الدراسي (2022/2021م).
- الحدود الموضوعية: تحديد درجة الوعي بالأمن السيبراني لدى المعلمين؛ من خلال التعامل الآمن لمتصفحات الإنترنت، وحماية أجهزتهم من البرامج الخبيثة.

الإطار النظري والدراسات السابقة:

يتناول هذا الفصل الإطار النظري والدراسات السابقة ذات الصلة بالبحث.

الإطار النظري:

تمثل تكنولوجيا المعلومات جميع التقنيات المتاحة من الأجهزة، والبرامج، والتطبيقات، وشبكات الاتصال. ومع زيادة انتشار أجهزة التكنولوجية، والاعتماد الكبير على شبكة الإنترنت، زادت المخاطر التي تتعرض لها تكنولوجيا المعلومات، ويمكن تصنيف المخاطر إلى ثلاثة أنواع رئيسة، هي: المخاطر التشغيلية، والمخاطر الأمنية، والمخاطر التي تتعرض لها المؤسسة والأفراد العاملين فيها. وتحتاج أنظمة تكنولوجيا المعلومات وشبكات الاتصال إلى معاملة خاصة لتجنب هذه المخاطر والآثار المرتبطة بها، أو على الأقل تقليل آثار هذه المخاطر، وفي هذا السياق ظهر ما يعرف بالأمن السيبراني الذي أصبح جزءًا مهمًّا في أي نظام معلومات؛ ليعبر عن الجانب الأمني المرتبط بحماية المعلومات (Aljohani & Elfadil, 2020).

تاريخ الأمن السيبراني:

تعود بدايات الأمن السيبراني إلى أواخر الأربعينات من القرن الماضي وبالتحديد عام (1949)، عندما قام العالم الأمريكي المَجري جون فون نيومان بالتنبؤ بإمكانية تناسخ برمجيات الحاسوب أو إعادة إنتاج نفسها. وبعد (18) عامًا جرت أول عملية اختراق حيث كان مسموحًا للطلبة الوصول إلى جزء محدود من النظام، حيث قام مجموعة من طلاب الثانوية باستخدام حواسيبهم بتعلم لغة الحاسوب، واستطاعوا الوصول إلى النظام بالكامل. وفي السبعينات من القرن الماضي قام بوب توماس باختراع أول فيروس وكان يسمى الزاحف أو (Creeper)، ثم جاء بعده المبرمج الشهير راي توملينسون مخترع البريد الإلكتروني، ليخترع أول برنامج مضاد للفيروسات للقضاء على فيروس الزاحف (Creeper)، وفي أواخر السبعينات من القرن الماضي أيضًا، قام كيفين ميتنيك أحد مخترقي الأنظمة في العالم وهو في سن (16) عامًا باختراق حاسوب شركة برمجيات، وفي النهاية ألقي القبض عليه وسجنه كمنفذ أول الهجمات الإلكترونية، أما في عام (1986) قام الهاكر الألماني ماركوس هس باختراق حواسيب عسكرية تابعة لوزارة الدفاع الأمريكية، وكان على وشك بيع البيانات والمعلومات السرية

للمخابرات السوفيتية، لولا أن تم القبض عليه، أما في عام (1988) فكان أول دودة موريس تصيب الأجهزة المتصلة بالإنترنت حول العالم، وهكذا استمر تطور الهجمات والجرائم الإلكترونية، وتطور معها الأمن السيبراني حتى وصل إلى التقدم والتطور الذي نعيشه اليوم (Fovino, 2020).

جاء مصطلح الأمن السيبراني من لفظ السيبر (Cyber) اللاتينية، ومعناها (الفضاء المعلوماتي) وهو تعبير يصف جميع الأمور المتعلقة بحماية البيانات والمعلومات والأجهزة باستخدام آليات وتجهيزات وتطبيقات وبرمجيات من خلال شبكات الحواسيب والاتصالات والإنترنت (ماشوش، 2018)، ويعرف الأمن السيبراني (Cyber security) بأنه تنظيم وتجميع الموارد والعمليات والهياكل المستخدمة لحماية الفضاء الإلكتروني من الاختراق بصورها المختلفة التي لا تتماشى مع أحكام القانون (Craigen, et al, 2014). ويعرفها إدوارد أموروسو (Amoroso, 2007) بأنها الوسائل والأدوات المستخدمة للحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، ومواجهة القرصنة وكشف الفيروسات وتوفير الاتصالات المشفرة.

وفي ضوء ما سبق، يتضح الاتفاق بين الباحثين، في أن مفهوم الأمن السيبراني يقوم على حماية المعلومات والبيانات والتطبيقات والأجهزة، ضد أي شكل من أشكال الوصول غير المصرح به، أو استخدامها بشكل سلبي بحيث يشكل خطرًا على الأفراد أو الجهة ذات الصلة بتلك المعلومات.

يعد الأمن السيبراني في الأردن حديث العهد، وأُقرّ في عام (2019) لحماية المملكة من تهديدات، من أجل بناء قدرات أمن سيبراني وطني يضمن مواجهة التهديدات التي تعترض أنظمة المعلومات، والبنى التحتية، ومراقبة الفضاء السيبراني الوطني، وإيجاد جهة مرجعية تتولى تطبيق السياسات العامة التي تنبثق عن الإستراتيجية الوطنية للأمن السيبراني وتنفيذها، وصدر في شهر كانون الثاني من عام (2020) الموافقة على نظام المركز الوطني للأمن السيبراني، والذي أسس بموجبه المركز الوطني للأمن السيبراني. وكشف التقرير العالمي للأمن السيبراني (Global Cybersecurity Index) الصادر عن الاتحاد الدولي للاتصالات خلال الشهر تموز من العام (2021)، أن الاردن احتل المرتبة (71) عالميًّا والمرتبة العاشرة عربيًّا في مؤشر الأمن السيبراني العالمي لعام (2020) (أبو حسين،2021). وعلى الرغم من الاهتمام المتزايد في الآونة الأخيرة، وزيادة مستويات الاستثمارات الأمنية في مجال الأمن السيبراني، إلا أن عدد الحوادث الإلكترونية والتكاليف المرتبطة بها وتأثيرها على حياة الناس مستمر في الارتفاع؛ نظرًا لارتفاع استخدام الحوسبة، والاتصالات، وإنترنت الأشياء. ويشير الباحثون إلى أن ما يصل إلى (95%) من جميع الحوادث السيبرانية هي من صنع الإنسان، فالأمن السيبراني هو حالة من التعاون بين الإنسان والأتمتة، لذلك يكون الجهاز والبشر عرضة للخطر، وتظهر نتائج الأبحاث أن أكبر نقطة ضعف أمنية هي قلة وعي المستخدم، فالأدوات التكنولوجية مهمة، ولكن يعد المستخدم أهم عنصر في الأمن السيبراني (Richardson, et al., 2020).

الهجمات السيبرانية:

تعدّ الهجمات السيبرانية هجمات خليطة، بمعنى استخدام خليط بين أكثر من تقنية وأكثر من طريقة للهجوم على النظام، فقد ظهرت مؤخرًا أنماط جديدة خطيرة من الهجمات والجرائم السيبرانية التي تعتمد على تقنيات متقدمة كالحوسبة السحابية، والذكاء الاصطناعي، وإنترنت الأشياء، وأجهزة تنصت على شبكات الاتصال السلكية واللاسلكية، وبرمجيات لفك الشفيرة والاختراق لأنظمة الشبكات وقواعد البيانات وأنظمة أمن الشبكات والحواسيب؛ لاستخدامها في عمليات إجرامية وتعاملات مشبوهة دون علم أصحابها، وكذلك نشر البرمجيات الخبيثة وتطوير الفيروسات المعقدة والشرسة؛ لتخريب أو تعطيل البنى التحتية لتكنولوجيا المعلومات والاتصالات. وقد ثبت عمليًّا أنها ليست بمنأى عن التعرض للهجمات السيبرانية حتى لو كانت غير متصلة بالإنترنت (الإستراتيجية الوطنية للأمن السيبراني، 2021).

الأمن السيبراني مسؤول عن التعامل مع التهديدات المختلفة، منها: الهجمات الإلكترونية أو الجرائم الإلكترونية التي هي استغلال لثغرة في النظام أو الشبكة من أجل الوصول غير مسموح به. وتقسم الهجمات الإلكترونية إلى نوعين أساسيين وهما (Godbole, et al, 2021):

- **هجمات الأنظمة** (Systems-based attacks).
- **هجمات الويب** (Web-based attacks).

أولاً: هجمات الأنظمة (Systems-based attacks):

هي الهجمات التي تتم من خلال برمجيات خبيثة تدمر أنظمة المستخدمين، أو تقوم بالوصول غير المصرح إليها، ومن أشهر البرمجيات الخبيثة والأكثر استخدامًا (Dhulapally, 2021):

1- الفيروسات (Viruses): هي من أشهر البرمجيات الخبيثة المستخدمة، وهي عبارة عن كود من برمجيات قادرة على تكرار ونسخ نفسها، والهدف من ذلك سرقة البيانات أو الإضرار بالأجهزة، أو إصابة الملفات والأجهزة المتصلة بالإنترنت دون علم المستخدم.

2- الديدان (Worms): وهي نوع من أنواع البرمجيات الخبيثة، وهي تعمل مثل الفيروسات وسببها الملفات المرفقة بالبريد الإلكتروني.

3- برامج الفدية (Ransomwares): وهي فيروسات الفدية حيث تصاب بها ملايين الأجهزة سنويًّا، وتقوم بتشفير ملفات المستخدم وبياناته على جهازه، وعادة تطلب فدية مالية من أجل فك هذا التشفير.

4- برامج الإعلانات (Adwares): وهي برمجيات خبيثة مزعجة تقوم بنشر الإعلانات على جهاز المستخدم؛ بهدف جمع الأموال من رؤيتك لهذا الإعلان.

5- برامج التجسس (Spywares): وهي نوع من البرمجيات التي تقوم بتسجيل بيانات المستخدم وأنشطته المختلفة على الجهاز أو النظام، ومن أشهر ما تقوم به تسجيل بيانات البطاقة الإئتمانية واستخدامها فيما بعد بسحب الأموال.

6- البوت نتس (Botnets): هي مجموعة من البرمجيات الخبيثة المرتبطة بالإنترنت التي تسمح للمجرمين الإلكترونيين بالتحكم بجهاز المستخدم والوصول لجميع بياناته (Aljohani&Elfadil, 2020).

الوقاية من البرامج الخبيثة:

- عدم فتح المرفقات والروابط مجهولة المصدر.
- تجنب استخدام البرامج غير المرخصة، والبرامج غير معروفة المصدر، أو غير المحدثة، والعمل على تحديث برامج مكافحة الفيروسات باستمرار.
- التأكد من برامج أنظمة التشغيل الكمبيوتر، مثل: ويندوز، والماك، واللينوكس، واستخدام آخر تحديثات الأمان.
- النسخ الاحتياطي للبيانات بشكل دوري.
- استخدام الجدر النارية والعمل على تحديثها، والتي تمنع الملفات والبيانات التي تحتوي على برامج ضارة (Zwilling, et al, 2020).

ثانيًا: هجمات الويب (Web-based attacks):

من أنواع هجمات الويب (حسام الدين، 2017):

1- هجمات الحقن (Injection Attacks): هي نوع من الهجمات الإلكترونية يتم فيها حقن بعض البيانات بداخل تطبيق من تطبيقات الويب؛ بهدف استخراج المعلومات المطلوبة أو تغييرها أو حذفها، ولها عدة أنواع منها: حقن (SQL)، وحقن الكود، وحقن (LOG)، وحقن (XML).

2- التصيّد أو الخداع (Phishing): هي نوع من الهجمات الإلكترونية المعروفة، حيث يقوم المخترق بالادعاء بأنه شخص أو جهة معروفة كالبنك أو صديق في العمل، ويتم التصيّد سواء أكان من خلال مكالمة الهاتفية، أم من خلال رسائل البريد الإلكتروني أم الرسائل النصية، حيث يقوم المخترق بهذا بهدف إقناعك بفعل معين أو استخراج معلومة حساسة، مثل: الأرقام السرية، أو بيانات البطاقات الإئتمانية وغيرها (Tiwari, et. al, 2016).

3- هجوم القوة العمياء (Brute Force Attacks): هي واحدة من الهجمات التقليدية التي تعتمد على المحاولة والخطأ، يعتمد هذا الهجوم على تجربة المخترق لكل الاحتمالات من أجل إدخال باسوورد أو رقم (PIN) بهدف الوصول إلى البيانات السرية لشخص ما.

4- حجب الخدمة (Denial of Service): هي هجمة إلكترونية يستطيع المخترق فيها جعل الشبكة أو السيرفر غير متاحين للمستخدمين، ومن أشهر أنواع هجمات حجب الخدمة: هجمات الحجم، هجمات البروتوكول، والهجمات على مستوى التطبيق.

5- هجمات انتحال الشخصية (DNS Spoofing): هي هجمات يتم فيها التلاعب بنظام (DNS) وهو نظام أسماء النطاقات الذي يحول أسماء النطاق إلى عناوين (IP)، بحيث يقوم بتحويل الترافيك إلى حاسوب المخترق أو إلى حاسوب آخر.

6- هجمات الرجل في منتصف (Man- in –the middle Attack): هي نوع من أنواع الهجمات التي يعترض فيها المخترق محادثة أو عملية تناقل البيانات بين طرفين، ويمكنه الحصول فيها على المعلومات حساسة، والتلاعب بالردود بين الطرفين.

7- التنمر السيبراني: يعد التنمر إحدى مظاهر الجرائم الإلكترونية، والأكثر انتشارًا بين طلبة المدارس في جميع مراحل التعليم بعد وصول خدمات الإنترنت إلى عدد هائل من المستخدمين عبر العالم، ويتضمن التنمر استخدام تقنيات المعلومات والاتصالات من أجل القيام بسلوكات عدوانية ومتعمدة، بواسطة شخص أو مجموعة من الأشخاص بقصد إلحاق الأذى بالآخرين عبر البريد الإلكتروني، أو الرسائل النصية، أو غرف المحادثة، أو المواقع الإلكترونية، أو مواقع التواصل الاجتماعي، أو الألعاب التفاعلية، وغير ذلك من الوسائل التقنية. ويتضمن التنمر أشكالًا مختلفة مثل: الذم، والقدح، والتحقير، والانتحال، وإرسال الصور والفيديوهات اللأخلاقية، وسرقة الحسابات الشخصية، والمطاردة الإلكترونية وغير ذلك؛ مما يسبب ذلك بالأذى النفسي والجسدي، والمشكلات الأكاديمية والأسرية، وفقدان الثقة بالنفس وبالآخرين (الشريف وأحمد، 2020).

8- الهندسة الاجتماعية: هي الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني؛ لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية، أو يقوم بعمل ما يسهل الوصول إلى أجهزة الحواسيب أو المعلومات المخزنة فيها (الصحفي وعسكول,2019). وتعد هجمات الهندسة البشرية من أقوى الهجمات؛ لأنها تهدد جميع الأنظمة والشبكات من خلال الأنشطة الخبيثة التي يتم إجراءها من خلال التفاعلات البشرية التي تدفع بالشخص إلى إفشاء المعلومات السرية، أو كسر الإجراءات الأمنية (Salahdine& Kaabouch, 2019).

التقليل من مخاطر الهجمات السيبرانية وحمايتها:

الوقاية خير من قنطار العلاج، لذلك يجب اتخاذ تدابير وقائية للحيلولة دون الوقوع ضحية لأي نوع من الهجمات:

- أمن الشبكات (Network Security): يقوم بحماية حركة مرور البيانات على الشبكة من خلال التحكم في الاتصالات الصادرة والواردة، وكذلك منع التهديدات من داخل الشبكة أو خارجها.
- أنظمة منع فقد البيانات (DLP): يقوم بحماية البيانات على وسائط التخزين، وبرامج قواعد البيانات، وأماكن تخزين البيانات، وأثناء انتقالها على الشبكة.
- أمن الأنظمة السحابية (Cloud Security): يوفر الحماية للبيانات والملفات المستخدمة في الخدمات والتطبيقات المستندة لأنظمة السحابية.
- أنظمة كشف التسلل (IDS)، أو أنظمة منع التسلل (IPS): تعمل على كشف الهجمات السيبرانية أو منعها، واتخاذ تدابير لإيقافها.
- إدارة الهوية والوصول (IAM): تستخدم خدمات المصادقة للحد من صلاحيات وصول المستخدمين وتتبعهم، ومراقبة عمليات الوصول لحماية الأنظمة الداخلية من هجمات الوصول غير المصرح به.
- التشفير: هو عملية تغيير في البيانات لجعلها غير مفهومة، وتستخدم أثناء إرسال البيانات لمنع سرقتها.
- برامج مكافحة الفيروسات (Antivirus): تفحص أجهزة الكمبيوتر بحثًا عن التهديدات المعروفة، وتقوم كذلك باكتشاف التهديدات غير المعروفة سابقًا بناءً على سلوكهم (Sadowsky, et al.,2003).

الأهمية التربوية للأمن السيبراني:

أدت الثورة الرقمية والتطور الهائل في وسائل الاتصال وشبكاته، متبوعًا بالنمو السريع في الحواسيب الشخصية والهواتف الذكية، إلى تحسين سبل الأحوال المعيشيّة في جميع ميادين، وأصبحت متطلبًا أساسيًا ولا سيما طلبة المدارس، أي جيل الإنترنت الذي بدأ باستخدام تقنيات الاتصال منذ سنوات عمره المبكرة, وتزداد أعداد الطلبة مستخدمي الإنترنت سنويًا بشكل كبير لأغراض متعددة، منها: التعليم، الترفيه، شبكات التواصل الاجتماعي، وعلى الرغم من مزايا الإنترنت، إلا أنها أصبحت فرصًا لوقوع المعلمين والطلبة كضحايا للجرائم السيبرانية؛ لعدم امتلاكهم الوعي الكافي بتلك الجرائم وكيفية تجنبها؛ مما يترتب على ذلك أضرار مادية ونفسية ومعنوية قد تؤثر على المعلم والطالب والمؤسسة التربوية، الأمر الذي يزيد من أهمية الأمن السيبراني في مجال التعليم والتعلم (المنتشري، 2020). وتفتقر مؤسسات تربوية عديدة للبنية التحتية القوية للأمن السيبراني، والتي يجعلها غير قادرة على مواجهة التهديدات. ولتحقيق الأمن السيبراني الناجح في المؤسسة التربوية، يتطلب التعاون بين تكنولوجيا المعلومات، وقادة الإدارات في المؤسسة ليكونوا أكثر فاعلية لمنع الهجمات التي تُعرّض أنظمة تكنولوجيا المعلومات للضعف (Davis, 2018)، حيث إنّ تهديدات المؤسسة التربوية يمكن أن تضر بسمعتها، وتسبب مسؤولية قانونية وخسارة مالية (Schuesster, 2013).

تنمية الوعي بالأمن السيبراني:

أدى الاستخدام المتزايد لتقنيات الفضاء الإلكتروني ظهور مخاطر جديدة، ولا سيما مخاطر العوامل البشرية، لذلك فقد اهتم كثير من الباحثين في مجال الأمن السيبراني بضرورة توعية المستخدمين بشبكات الإنترنت، وأن يكونوا على دراية بالمخاطر المحتملة التي يواجهونها كالتنمر عبر الإنترنت، أو مواقع التواصل الاجتماعي، أو الألعاب عبر الإنترنت، وغيرها من الممارسات السلبية؛ من أجل العمل على اتخاذ الاحتياطات السلامة، وإكسابهم المهارات اللازمة للحفاظ على معلوماتهم وضمان حمايتها، وهنا يطلب من المؤسسة التعليمية تنفيذ برنامج توعية لجميع العاملين والطلبة، وهذا يساهم في تعزيز ثقافة أمنية إيجابية، وبالتالي زيادة حماية المعلومات والبيانات، وكذلك من خلال التدرب على المواطنة الرقمية (الصحفي وعسكول، 2019). ويقصد بالمواطنة الرقمية بأنها مجموعة من القواعد والمعايير والأفكار والمبادئ المتبعة في الاستخدام الأمثل الصحيح، والتي يحتاجها المستخدمون بغض النظر عن أعمارهم، أو مستوياتهم التعليمية، أو طبيعة عملهم؛ من أجل الاستخدام الأمثل لتكنولوجيا المعلومات والاتصال، وهذا يؤدي إلى الحفاظ على أمن الوطن من خلال التوجيه، والحماية، وإتاحة الوصول الإلكتروني وحمايتها من الأخطار (الدهشان والفويهي، 2015).

وتوجد طرق عديدة يجب على مستخدم الإنترنت اتباعها لتقليل مخاطر التهديد الإلكتروني أو الحدّ منها (المنتشري، 2020):

- إعداد كلمات السر القوية وتحديثها باستمرار، وعمليات التحقق الأمنية لمواقع التواصل الاجتماعي، والبريد الإلكتروني على الحاسوب أو الأجهزة الذكية.
- التحديث المستمر للجدار الناري (Firewall)، والتي تمثل أنظمة الدفاع عن البنية التحتية المعلوماتية.
- عدم فتح أي رسائل إلكترونية مجهولة المصدر عبر البريد الإلكتروني.
- التأكد من إعدادات الحاسوب وشبكة الإنترنت.
- استخدام برامج الحماية من الفيروسات وبرامج التجسس وتحديثها باستمرار.
- عمل نسخ احتياطية من البيانات والمعلومات والاحتفاظ بها خارج المؤسسة.
- عدم إرسال المعلومات الشخصية عبر البريد الإلكتروني، أو المواقع التواصل الاجتماعي.

- تبليغ الجهات الأمنية في حال تكرار الرسائل المشبوهة.
- تحميل البرامج والملفات من مواقع موثوقة.
- استخدام أجهزة مودم موثوقة مع تعطيل خاصية التحكم والتشغيل عن بُعد لأجهزة المودم.
- عقد دورات تدريبية للمعلمين حول الوعي بالأمن السيبراني، وكيفية توعية الطلبة في حال وقوعهم ضحية للمخاطر والتهديدات السيبرانية.

مع تزايد الهجمات السيبرانية على المؤسسات والأفراد وتطورها، يجب أن نكون على استعداد للاستجابة للهجمات السيبرانية، وقادرين على التصدي لها بأفضل الممارسات، ويتم ذلك من خلال الجمع بين الوعي بالأمن السيبراني، وطرق تطبيق تنمية الوعي للتقليل أو التصدي للهجمات؛ من خلال إجراء تقييمات المخاطر السيبرانية من ثلاثة مجالات رئيسة: تحديد البيانات الأكثر أهمية والتي تتطلب الحماية، وتحديد التهديدات والمخاطر التي تواجه البيانات، وتحديد الضرر الذي يتعرض له الفرد أو المؤسسة في حالة التعرض لهجمة سيبرانية، والقيام بوضع خطط، وتنفيذ إجراءات وقائية للتخفيف من مخاطر الإنترنت، مثل: برامج مكافحة الفيروسات، والجدران النارية، وأنظمة كشف الاختراقات وغيرها، ويتم ذلك من خلال المسؤولية التي تقع على عاتق المعلمين بضرورة توعيتهم بالأمن السيبراني باعتباره من الأمور المهمّة لأي مستخدم إنترنت، علاوة على أهميته بالنسبة للمعلمين بشكل خاص؛ نظرًا لدورهم المهم في إعداد الطلبة وتوعيتهم بمخاطر الأمن السيبراني وانتهاكاته، ومن هنا فإنّ الأمن السيبراني يمثل مفهومًا جديدًا في عصر الثورة المعلوماتية لمواجهة الأخطار والانتهاكات عبر الفضاء المعلوماتي، كما أشارت الدراسة إلى الطرق المثلى التي ينبغي للمعلمين تطبيقها من أجل حماية أنفسهم من مخاطر السيبرانية وانتهاكاتها، وتوعية الطلبة (هيئة الإعلام، 2021).

الدراسات السابقة باللغة العربية:

من خلال الاطلاع على الدراسات السابقة ذات العلاقة بموضوع البحث، وجدت الباحثة عددًا من الدراسات باللغتين العربية والإنجليزية التي لها علاقة بالأمن السيبراني، ولكنها قليلة لحداثة الموضوع، ومن هذه الدراسات:

– دراسة (الصحفي وعسكول، 2019)، وقد هدفت إلى الكشف عن مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة، وذلك باستخدام المنهج الوصفي، وتكونت عينة الدراسة من (352) معلمة، وتم جمع البيانات اللازمة باستخدام الاستبيان. وأكدت نتائج الدراسة وجود ضعف وقصور لدى معلمات الحاسب الآلي في الوعي بمفاهيم الأمن السيبراني، كما أكدت وجود ضعف لدى معلمات الحاسب الآلي في الوعي بمستوى الأمن السيبراني، وعدم وجود فروق ذات دلالة إحصائية في درجة الوعي لدى معلمات الحاسب الآلي بالأمن السيبراني تعزى للمتغيرات: (سنوات الخبرة، المؤهل العلمي، الدورات التدريبية).

– دراسة (المنتشري، 2020)، وهدفت إلى معرفة دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات في جدة من وجهة نظر المعلمات. وقد استخدم المنهج الوصفي التحليلي، وتكونت عينة الدراسة من (420) معلمة في عدد من المدارس الحكومية في مدينة جدة، وتم جمع البيانات اللازمة باستخدام الاستبيان. وكشفت نتائج الدراسة أن دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات ولدى طالبات المدرسة جاءت بدرجة قليلة.

دراسة (الصانع، السواط، أبو عيشة، سليمان، عسران، 2020)، وقد هدفت الدراسة إلى معرفة درجة وعي المعلمين بالأمن السيبراني، وعلاقته بتطبيق أساليب حديثة لحماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية لديهم، وتم تطبيق الدراسة على عينة تكونت من (104) معلمين ومعلمات في مدارس الطائف الحكومية والخاصة. وتم جمع البيانات باستخدام الاستبانة، وتم استخدام المنهج الوصفي الارتباطي. وأظهرت نتائج الدراسة ارتفاع وعي المعلمين بالأمن السيبراني، ووجدت علاقة ارتباطية موجبة ومتوسطة بين وعي المعلمين بالأمن السيبراني، واستخدامهم لأساليب حماية الطلبة من مخاطر الإنترنت وأساليب تعزيز القيم والهوية الوطنية، ولم تجد فروقًا ذات دلالة إحصائية بين استجابات المعلمين حول الوعي بالأمن السيبراني، وأساليب حماية الطلبة من مخاطر الإنترنت وأساليب تعزيز القيم والهوية الوطنية تبعًا لمتغيرات: (الجنس، والتخصص، والمؤهل العلمي، وسنوات الخبرة).

– دراسة (المنتشري وحريري، 2020)، وهدفت التعرف إلى درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، وقد اعتمدت الدراسة على المنهج الوصفي، واستخدمت الاستبانة لجمع البيانات، وتكونت عينة الدراسة من (362) معلمة من معلمات المرحلة المتوسطة بمدينة جدة. وأظهرت نتائج الدراسة أن درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني جاءت بدرجة متوسطة، وعدم وجود فروق ذات دلالة إحصائية تعزى للمتغيرين: (المؤهل العلمي، وسنوات الخبرة).

– دراسة (الصانع وآخرون, 2020) وهدفت إلى معرفة درجة الوعي بالأمن السيبراني، وعلاقته بتوفر القيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف. وقد تكونت عينة الدراسة من (346) تلميذًا وتلميذة من المرحلتين الابتدائية والمتوسطة، وتم توزيع الاستبانة إلكترونيًّا على عينة الدراسة، واستخدم فيها المنهج الوصفي الارتباطي، وأظهرت نتائج الدراسة أن درجة الوعي بالأمن السيبراني لدى التلاميذ جاءت (مرتفعة بدرجة كبيرة).

الدراسات السابقة باللغة الإنجليزية:

– دراسة ماهنو (Mahno, 2017) بعنوان تدريس الأمن السيبراني لطلبة الجامعة، واشتملت الدراسة على برنامج يهدف إلى تعريف الطلبة بكيفية حماية خصوصية معلوماته، وكيفية التصدي للهجمات السيبرانية. وقد جمعت البيانات باستخدام استبيان ودراسة حالة، وتكونت عينة الدراسة من (25) طالبًا من طلبة الجامعة، واستخدم فيها المنهج الوصفي التحليلي. وقد أظهرت نتائج الدراسة وجود نقص في المعرفة المتعلقة بالأمن السيبراني، وعدم إدراك الطلبة للمخاطر التكنولوجيا المستخدمة لديهم، وأثبتت نتائج الدراسة الحاجة الماسة لبرامج من أجل توعية الطلبة بالأمن السيبراني.

– دراسة الجهني والفاضل (Aljohani & Elfadil, 2020) وهدفت قياس مستوى الوعي بالأمن السيبراني لدى طلاب جامعة فهد بن سلطان، وتكونت عينة الدراسة من (212) طالبًا، وتم توزيع الاستبانة على عينة الدراسة، واستخدم فيها المنهج الوصفي الارتباطي، وأظهرت نتائج الدراسة أن درجة الوعي بالأمن السيبراني لدى الطلاب جاءت بدرجة (متوسطة).

– دراسة كريتزنجلر، بادا، ونيرز (Kritizingler, Bada, & Nurse 2020) وهدفت تحديد المبادرات الخاصة برفع مستوى الوعي بالأمن السيبراني لدى طلبة مدارس جنوب إفريقيا والمدارس البريطانية. وتم استعراض الوثائق والدراسات التي تناولت هاتين الدولتين في هذا المجال، وأظهرت النتائج وجود عدد من المبادرات شملت دمج مفاهيم الأمن السيبراني ضمن المناهج الدراسية، وتدريب المعلمين، ووضع سياسات خاصة بالأمن السيبراني، ودمج الآباء في برامج التوعية بالأمن السيبراني.

– دراسة رحمان، ساري، زيزي، وخالد (Rahman, Sairi, Zizi, & Khalid. 2020) وهدفت التعرف إلى الإستراتيجيات التي تكشف كيفية تنفيذ تعليم الأمن السيبراني في المدارس. ومن خلال استعراض الدراسات السابقة ذات العلاقة بموضوع الدراسة، والمنشورة بين عامي (2011–2019)، تم العثور على (240)، ودراسة واختيار (25) دراسة فقط ذات علاقة بموضوع البحث الحالي. وأظهرت النتائج أهمية إعداد المعلمين قبل الخدمة لتدريبهم على الممارسات الصحيحة في تطبيق الأمن السيبراني والحوسبة الآمنة؛ حتى ينعكس ذلك على طلبة المدارس، كذلك ركزت الدراسة على أهمية المدرسة أن تكون قادرة على توعية الطلبة بتطبيق الأمن السيبراني من خلال البرامج أو الأنشطة المدرسية؛ لحمايتهم من المخاطر أو التهديدات التي يواجهونها عند استخدام شبكة الإنترنت، أو مواقع التواصل الاجتماعي، أو الألعاب عبر الإنترنت.

– دراسة الزبيدي (Alzubaidi, 2021) وهدفت التعرف إلى مستوى الوعي بالأمن السيبراني في السعودية، واستخدم فيها المنهج الوصفي التحليلي، وتم جمع البيانات باستخدام الاستبانة، وطبقت الدراسة على عينة تتكون من (1230) طالبًا من الطلبة الجامعيين وطلبة الدراسات العليا، وأظهرت نتائج الدراسة أن مستخدمي الإنترنت لا يمتلكون وعيًا كافيًا بالتهديدات السيبرانية.

التعقيب على الدراسات السابقة:

لوحظ من خلال استعراض الدراسات السابقة ما يأتي:

–اتفقت الدراسة الحالية من حيث الهدف وهو الكشف عن درجة الوعي بالأمن السيبراني لدى المعلمين مع دراسة كل من (الصحفي وعسكول، 2019، الصانع وآخرون، 2020، المنتشري وحريري، 2020)، واختلفت مع دراسة كل من (السواط وآخرون، 2020، Aljohani & Elfadil, 2020، Alzubaidi, 2021) حيث طبقت على الطلبة.

–اتفقت الدراسة الحالية مع دراسة كل من (المنتشري، 2020، الصانع وآخرون، 2020، Kritizingler, et al., 2020؛ Mahno. 2017؛ Rahman, et. al 2020.) في طرق تنمية الوعي بالأمن السيبراني.

–واتفقت الدراسة الحالية مع كل من دراسات (الصحفي وعسكول، 2019، المنتشري، 2020، المنتشري وحريري، 2020، Alzubaidi, 2021؛ Mahno, 2017؛ Aljohani & Elfadil, 2020) في استخدام المنهج الوصفي التحليلي، واختلفت مع دراسة (الصانع وآخرون، 2020، السواط وآخرون، 2020) فقد استخدمت المنهج الوصفي الارتباطي.

–اتفقت الدراسة الحالية مع كل من دراسات (السواط وآخرون، 2020، المنتشري وحريري، 2020، الصانع وآخرون، 2020، المنتشري، 2020، الصحفي وعسكول، 2019 ؛Alzubaidi, 2021؛ Mahno. 2017؛ Aljohani & Elfadil, 2020) في جمع البيانات باستخدام الاستبيان، واختلفت مع دراسة (Rahman, et. al.,2020؛ Mahno. 2017) التي استخدمت المقابلات واستعراض الدراسات السابقة.

–تميزت الدراسة الحالية بأنها طبقت على معلمين ومعلمات عاملين في المدارس الحكومية في قصبة الكرك، وتعد هذه الدراسة من الدراسات الحديثة التي تناولت درجة الوعي بالأمن السيبراني، وطرق تنميته لدى المعلمين.

منهجية الدراسة وإجراءاتها:

يتضمن هذا الجزء وصفًا لمجتمع الدراسة، وعينتها، ومنهجيتها، وأداتها، وطرق التحقق من صدقها وثباتها، والأساليب الإحصائية المستخدمة في استخراج النتائج.

منهج الدراسة:

لتحقيق أهداف الدراسة، فقد استخدمت الباحثة المنهج الوصفي المسحي.

مجتمع الدراسة:

تكون مجتمع الدراسة من جميع المعلمين في مديرية تربية وتعليم قصبة الكرك، للعام الدراسي (2022–2021) والبالغ عددهم (2704) معلمين ومعلمات، منهم (885) معلمًا، و(1819) معلمة.

عينة الدراسة:

تم اختيار عينة طبقية بسيطة وبنسبة (10%) من مجتمع الدراسة، بلغ حجمها (271) معلمًا ومعلمة، (89) معلمًا، و(182) معلمة، وتم توزيع الاستبانة على العينة إلكترونيًّا باستخدام تطبيق جوجل درايف (Google Drive)، والجدول (1) يبين توزيع عينة الدراسة على متغيراتها الشخصية والوظيفية:

الجدول (1) توزيع خصائص عينة الدراسة وفقًا لمتغيراتها الشخصية والوظيفية

المتغير	مستويات المتغير	العدد	النسبة المئوية (%)
النوع الاجتماعي	ذكر	89	32.8
	انثى	182	67.2
	المجموع	271	100.0
المؤهل العلمي	دبلوم	35	12.9
	بكالوريوس	166	61.3
	دراسات عليا	70	25.8
	المجموع	271	100.0
المواد التي يدرسها المعلم	مواد علمية	102	37.6
	مواد إنسانية	125	46.1
	إداري	44	16.2
	المجموع	271	100.0
سنوات الخبرة بالتدريس	5 سنوات فأقل	28	10.3
	6–9 سنوات	95	35.1
	10 سنوات فأكثر	148	54.6
	المجموع	271	100.0

أداة الدراسة:

قامت الباحثة ببناء استبانة لتحقيق أهداف الدراسة، اعتمادًا على الأدب النظري، والدراسات السابقة كدراسة الزبيدي (2021)، ودراسة الجهني والفاضل (2020)، ودراسة الصانع وآخرون (2020)، وقد تألفت من الأقسام الآتية:

1. القسم الأول: ويتضمن المتغيرات الشخصية والوظيفية الآتية: (النوع الاجتماعي، المؤهل العلمي، المواد التي يدرسها المعلم، وسنوات الخبرة في التدريس).
2. القسم الثاني: ويتضمن الفقرات التي تقيس درجة الوعي بالأمن السيبراني وتم تمثيله بالفقرات (1–16).
3. القسم الثالث: ويتضمن الفقرات التي تقيس طرق تنمية الوعي بالأمن السيبراني، وتم تمثيلها بالفقرات (1–15).

صدق المقياس:

تم التحقق من صدق الأداة باستخدام الطريقتين الآتيتين:

صدق المحكمين: تم عرض الأداة على (5) محكمين من أعضاء هيئة التدريس في جامعتَي: مؤتة، والأردنية؛ لبيان مدى دقة العبارات وانتمائها للمجال الذي تقيسه، ومناسبتها لقياس ما بنيت لقياسه، وسلامة الصياغة اللغوية، وتم إجراء التعديلات المقترحة من قبل المحكمين، وبنسبة اتفاق (80%).

صدق البناء الداخلي:

تم التأكد من صدق البناء الداخلي للأداة من خلال تطبيقها على عينة استطلاعية من مجتمع الدراسة وخارج عينتها، بلغ حجمها (30)

معلمًا ومعلمة، ومن ثم حساب معاملات ارتباط الفقرات مع الدرجة الكلية، والجدول (2) يعرض النتائج:

الجدول (2) نتائج معاملات ارتباط بيرسون (Pearson Coefficients) بين الفقرة والدرجة الكلية لمجالها

رقم الفقرة	ارتباط الفقرة مع الدرجة الكلية لمجالها	
	معامل الارتباط	الدلالة الاحصائية
أولًا: درجة الوعي بالأمن السيبراني		
1	*0.445	0.014
2	*0.455	0.012
3	*0.442	0.014
4	**0.686	0.000
5	**0.636	0.000
6	**0.665	0.000
7	**0.665	0.000
8	**0.681	0.000
9	**0.562	0.001
10	**0.622	0.000
11	**0.640	0.000
12	**0.557	0.001
13	**0.862	0.000
14	**0.523	0.003
15	**0.632	0.000
16	**0.466	0.009
ثانيًا: طرق تنمية الوعي بالأمن السيبراني		
1	**0.727	0.000
2	**0.597	0.000
3	**0.611	0.000
4	**0.810	0.000
5	**0.843	0.000
6	**0.808	0.000
7	**0.832	0.000
8	**0.805	0.000
9	**0.819	0.000
10	**0.871	0.000
11	**0.783	0.000
12	**0.847	0.000
13	**0.753	0.000
14	**0.689	0.000
15	**0.771	0.000

***دالة إحصائيًا عند مستوى الدلالة ($\alpha \leq 0.05$).**

****دالة إحصائيًا عند مستوى الدلالة ($\alpha \leq 0.01$).**

يتضح من البيانات الواردة في الجدول (2)، أن معاملات ارتباط الفقرة مع المجال الذي تنتمي له قد تراوحت ما بين (0.442 –0.862)، أما بين المجالات والدرجة الكلية لمجال طرق تنمية الوعي السيبراني فقد تراوحت ما بين (0.597–0.871)؛ وجميعها دالة إحصائيًا عند مستوى

الدلالة ($\alpha \leq 0.05$)، وهذا يشير إلى صدق الأداة ومناسبتها لإجراء الدراسة.

ثبات المقياس: تم التأكد من ثبات المقياس بمفهوم الاتساق الداخلي، باستخدام معامل كرونباخ ألفا، وذلك من خلال تطبيق الأداة (الاستبيان) على عينة استطلاعية بلغ حجمها (30) معلمًا ومعلمة، ويبين الجدول (3) معاملات الثبات.

الجدول (3) نتائج قيم معاملات الثبات بمفهوم الاتساق الداخلي

الرقم	المجالات	عدد الفقرات	معامل كرونباخ ألفا
1	درجة الوعي بالأمن السيبراني	16	0.872
2	طرق تنمية الوعي بالأمن السيبراني	15	0.950

يتضح من البيانات الواردة في الجدول (3) بأن قيم معاملات الثبات لمجال درجة الوعي بالأمن السيبراني قد بلغ (0.872)، ولطرق تنمية الوعي بالأمن السيبراني (0.952)، وهي قيم مرتفعة وتدل على ثبات أداة الدراسة.

الوزن النسبي: تم توزيع استجابة أفراد العينة على أداة الدراسة، وفقًا لتدريج ليكرت الخماسي، حيث أعطيت الاستجابة أوافق بدرجة كبيرة (5) درجات، وأوافق بدرجة متوسطة (4) درجات، وأوافق بدرجة قليلة (3) درجات، وأوافق بدرجة قليلة جدًّا (2) درجتان، ولا أوافق أبدًا (1) درجة واحدة، وتم استخدام المتوسطات الحسابية لتفسير تقديرات أفراد العينة على الدرجة الكلية والفقرات، والجدول (4) يوضح ذلك:

الجدول (4) الوزن النسبي لتفسير تقديرات أفراد عينة الدراسة على كل من الدرجة الكلية والفقرات

المتوسط الحسابي	المستوى
1– 2.33	منخفض
2.34– 3.67	متوسط
3.68– 5	مرتفع

الأساليب الإحصائية المستخدمة في استخراج النتائج: استُخدم برنامج الحزمة الإحصائية للعلوم الاجتماعية لتحليل بيانات الدراسة، حيث تم استخدام معامل ارتباط بيرسون (pearson coefficient)، وكرونباخ ألفا (Alpha Cronbach)؛ للتحقق من صدق أداة الدراسة وثباتها، والمتوسطات الحسابية والانحرافات المعيارية للإجابة عن سؤالَي الدراسة الأول والثاني، وتحليل التباين الأحادي متعدد الاتجاهات (4Way- ANOVA) للإجابة عن سؤالَي الدراسة الثالث والرابع.

عرض نتائج الدراسة ومناقشتها:

النتائج المتعلقة بسؤال الدراسة الأول: ونصه: ما درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك؟

للإجابة عن هذا السؤال تم استخراج المتوسطات الحسابية، والانحرافات المعيارية، والرتبة، والمستوى، للفقرات والدرجة الكلية، والجدول (5) يعرض النتائج:

الجدول (5) المتوسطات الحسابية والانحرافات المعيارية، والرتبة، والمستوى لدرجة الوعي بالأمن السيبراني

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	المستوى
1	أعرف مفهوم الأمن السيبراني.	3.06	1.166	14	متوسط
2	أعرف مخاطر الروابط ومرفقات البريد الإلكتروني مجهولة المصدر.	3.73	1.097	10	مرتفع
3	أستخدم متصفح آمن للإنترنت.	3.93	1.023	8	مرتفع
4	أتجنب إرسال معلوماتي الشخصية عبر الرسائل النصية والبريد الإلكتروني.	4.27	0.966	4	مرتفع
5	أحمل برامج مضادات الفيروسات، وأحدّثها باستمرار.	3.75	1.028	9	مرتفع
6	أغيّر كلمة السر بشكل دوري.	3.39	1.136	13	متوسط
7	أختار كلمة سر قوية.	4.05	1.001	7	مرتفع
8	أحتفظ بنسخة احتياطية باستخدام تقنيات الحوسبة السحابية.	3.53	1.179	12	متوسط
9	أفعّل الجدار الناري (Firewall) على جهازي.	3.02	1.222	15	متوسط
10	أتعامل مع حالات التنمر بطرق صحيحة.	3.75	1.045	9	مرتفع
11	أتجنب نشر المعلومات المخالفة للأعراف والتقاليد.	4.31	0.958	3	مرتفع
12	أتجنب نشر المعلومات المخالفة للدين.	4.49	0.829	1	مرتفع
13	ألتزم بقوانين استخدام شبكة الإنترنت.	4.42	0.861	2	مرتفع
14	أستخدم البرامج التعليمية المرخصة.	4.18	0.900	6	مرتفع
15	أتجنب فتح الرسائل الإلكترونية مجهولة المصدر.	4.24	0.952	5	مرتفع
16	أبلغ عن المواقع المشكوك فيها للجهات المختصة.	3.63	1.179	11	متوسط
–	**الدرجة الكلية لدرجة الوعي بالأمن السيبراني**	**3.86**	**0.692**	–	**مرتفع**

تظهر النتائج الظاهرة في الجدول (5) أن المتوسط الحسابي لدرجة الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك، بلغ (3.86) بانحراف معياري مقداره (0.692)، وهذا يمثل درجة تقدير مرتفعة، ويشير إلى أن درجة الوعي مرتفعة، واحتلت الفقرة (12) المرتبة الأولى بمتوسط حسابي مقداره (4.49) وانحراف معياري بلغ (0.829)، تلتها في المرتبة الثانية الفقرة (13) بمتوسط حسابي مقداره (4.42)، وانحراف معياري بلغ (0.861)، وفي المرتبة الثالثة جاءت الفقرة (11) بمتوسط حسابي بلغ (4.31) وانحراف معياري مقداره (0.958)، أما في المرتبة الأخيرة فقد جاءت الفقرة (9) بمتوسط حسابي بلغ (3.02)، وانحراف معياري مقداره (1.222).

ويمكن أن يعزى ارتفاع درجة الوعي بالأمن السيبراني لدى المعلمين لاستخدامهم تطبيقات الهواتف الذكية: كالواتس آب، والمسنجر، والفيس بوك، وأجهزة الحاسوب على نطاق واسع، كما كان لجائحة كورونا دور كبير في رفع درجة الوعي بالأمن السيبراني لدى المعلمين؛ لاعتماد التعلم عن بُعد على تطبيقات (Ms Teams, Zoom) خلال فترات الحظر، وما رافقه من اكتساب الخبرة في التعامل مع التطبيقات المختلفة، وتوعيتهم بكيفية اتخاذ إجراءات وقائية لحماية بياناتهم من الاختراق، وتجنب الوقوع ضحية للجرائم الإكترونية، وتقليل المخاطر المترتبة من سوء استخدام شبكة الإنترنت، كما يمكن أن تعزى هذه النتيجة إلى عقد دورات رخصة قيادة الحاسوب الدولية (ICDL)، من قبل وزارة التربية والتعليم، وتشجيع المعلمين في الحصول عليها، حيث طورت من مهارات المعلمين باستخدام أجهزة الحواسيب، ومما قد يساهم في زيادة درجة وعي المعلمين في الأمن السبيراني وجود مختبرات للحاسوب في المدارس، وإدارتها من قبل متخصصين في علم الحاسوب والشبكات، واتفقت هذه النتيجة مع نتائج دراسة الصانع، والسواط، وأبو عيشة، وسليمان، وعسران (2020)، واختلفت هذه النتيجة مع نتائج دراسة الزبيدي (2021)، ودراسة الجهني والفاضل (2020)، ودراسة المنتشري (2020)، ودراسة الصحفي وعسكول (2019). أما بخصوص الفقرات: (أعرف مفهوم الأمن السيبراني، أغير كلمة السر بشكل دوري، أحتفظ بنسخة احتياطية باستخدام تقنيات الحوسبة السحابية، أفعّل الجدار الناري (Firewall) على جهازي، أُبلّغ عن المواقع المشكوك فيها للجهات المختصة)، وحصولهم على درجة متوسطة، فيمكن أن يعزى لقلة خبرة المعلمين ومحدوديّة درايتهم بأهمية مفهوم الأمن السيبراني، وعلاقته بالتعليم، وحمايتهم من الانتهاكات السيبرانية ومخاطرها، وكذلك إلى ندرة الدورات التدريبية التي تختص بمهارات متقدمة في مجال الحاسوب، مثل: (تعزيز مفهوم الأمن السيبراني كمصطلح تقني جديد، واستخدام تقنيات الحوسبة السحابية، وكيفية تفعيل الجدار الناري على أنظمة التشغيل)، أما بخصوص تغيير كلمة السر والإبلاغ عن المواقع المشكوكة، فلم يدرك المعلم أهميتها وعلاقتها بالأمن السيبراني وحمايتهم من الاختراقات. وجاءت هذه النتيجة متفقة مع ما ذكرته دراسة المنتشري (2020)، في حاجة المعلمين للتوعية بالموضوعات ذات علاقة بالأمن السيبراني، وتطوير معارفهم ومهاراتهم في هذا المجال، وكيفية استخدامها أثناء ممارساتهم التدريسية.

النتائج المتعلقة بسؤال الدراسة الثاني: ونصه: ما درجة تطبيق طرق تنمية الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك؟ للإجابة عن هذا السؤال تم استخراج المتوسطات الحسابية والانحرافات المعيارية والرتبة والمستوى، للفقرات والدرجة الكلية، والجدول (6) يعرض النتائج:

الجدول (6) المتوسطات لحسابية والانحرافات المعيارية، والرتبة والمستوى لطرق تنمية الوعي بالأمن السيبراني

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	المستوى
1	التوعوية بمفاهيم الأمن السيبراني.	4.03	1.055	9	مرتفع
2	تدريب المعلمين بكيفية إعداد كلمة سر قوية، وتحديثها باستمرار.	4.00	1.042	10	مرتفع
3	التدريب على استخدام برامج الحماية والجدار الناري وتحديثها بشكل مستمر.	3.67	1.092	13	متوسط
4	التعامل مع مرفقات البريد الإلكتروني بشكل صحيح.	3.99	1.029	11	مرتفع
5	استخدام الإنترنت والتطبيقات الإلكترونية كوسيلة للتعلم والبحث عن المعرفة.	4.11	0.938	6	مرتفع
6	توعية المعلمين بالمصادر الموثوقة للمعلومات.	4.10	0.955	7	مرتفع
7	تثقيف المعلمين بوسائل حماية بياناتهم ومعلوماتهم على أجهزتهم الخاصة.	3.97	0.967	12	مرتفع
8	الاستخدام الإيجابي للإنترنت.	4.12	0.939	5	مرتفع
9	تعزيز الوعي بمخاطر الروابط الضارة عند تصفح الإنترنت.	4.14	0.961	4	مرتفع
10	استخدام التطبيقات الآمنة والبرامج التعليمية.	4.27	0.892	2	مرتفع
11	التصفح الآمن للإنترنت.	4.08	0.959	8	مرتفع
12	توعيتهم بمشكلات استخدام الإنترنت لفترات طويلة.	3.99	1.000	11	مرتفع
13	الاندماج بالحياة الاجتماعية وعدم الانشغال بالحياة الافتراضية.	4.21	0.889	3	مرتفع
14	استخدام المواقع الإلكترونية التي تعمق القيم الدينية والأخلاقية.	4.31	0.885	1	مرتفع

15	الإفصاح عند التعرض لأي من الجرائم السيبرانية.	4.27	0.902	2	مرتفع
–	الدرجة الكلية لطرق تنمية الوعي بالأمن السيبراني	4.08	0.763	–	مرتفع

تظهر النتائج الظاهرة في الجدول (6) أن المتوسط الحسابي لدرجة الوعي بطرق تنمية الأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك، قد بلغ (4.08) بانحراف معياري مقداره (0.763)، وجاءت بدرجة تقدير مرتفعة، وتشير إلى أن درجة تطبيق طرق تنمية الوعي الأمن السيبراني جاءت بدرجة مرتفعة، وقد احتلت الفقرة (14) التي تنص على: "استخدام المواقع الإلكترونية التي تعمق القيم الدينية والأخلاقية"، على المرتبة الأولى بمتوسط حسابي بلغ (4.31)، وانحراف معياري مقداره (0.885)، تلتها في المرتبة الثانية كل من الطريقتين: "استخدام التطبيقات الآمنة والبرامج التعليمية" المُضمنة في الفقرة (10): "الإفصاح عند التعرض لأي من جرائم السيبراني" والمضمنة في الفقرة (15) بمتوسط حسابي قد بلغ (4.27) لكل منهما، وانحراف معياري مقداره (0.892) و(0.902)، وفي المرتبة الثالثة جاءت طريقة: "الاندماج بالحياة الاجتماعية وعدم الانشغال بالحياة الافتراضية". المضمنة في الفقرة (13)، بمتوسط حسابي بلغ (4.21)، وانحراف معياري مقداره (0.889)، أما في المرتبة الأخيرة فقد جاءت طريقة: "التدريب على استخدام برامج الحماية والجدار الناري وتحديثها بشكل مستمر"، المضمنة في الفقرة (3)، بمتوسط حسابي بلغ (3.67)، وانحراف معياري مقداره (1.092).

ويمكن أن تعزى هذه النتيجة إلى انتشار استخدام تكنولوجيا التعليم والاتصال، واستخدام الأجهزة الرقمية الحديثة والحواسيب، التي زادت من وعي المعلمين بطرق التعامل مع البيانات وحمايتها، فالمعلمون يرون أن استخدام المواقع الآمنة وعدم الدخول إلى المواقع المشبوهة يحتل أولوية لحماية بياناتهم الشخصية والتعليمية، فهم يستخدمون المواقع التي تعمق القيم الدينية والأخلاقية، ويستخدمون التطبيقات الآمنة، ويتجنبون استخدام التطبيقات المشبوهة ومجهولة المصدر، فهم يندمجون في حياتهم الاجتماعية، ويستخدمون العالم الافتراضي بحدود ضيقة، كما أنهم يعرفون الروابط الضارة على شبكة الحاسوب، كما أن الاستخدام الإيجابي للإنترنت من أهم وسائل حماية المعلومات، فهم على وعي بالمصادر الموثوقة، إما من خلال تجاربهم الشخصية، أو من خلال الدورات، ولديهم وعي بطرق حماية بياناتهم، وتتفق هذه النتيجة مع نتائج دراسة الصانع، السواط، أبو عيشة، سليمان، عسران، (2020) ودراسة رحمان، ساري، زيزي، وخالد (Rahman, 2020 .Sairi, Zizi, & Khalid). وأما بخصوص الفقرة: "التدريب على استخدام برامج الحماية والجدار الناري وتحديثها بشكل مستمر"، فإنها جاءت بدرجة متوسطة، ويمكن أن تعزى هذه النتيجة إلى عدم وجود تدريبات دورية، ومتابعة لمستجدات الثورة المعلوماتية، خاصة المتعلقة في كيفية تفعيل برامج الحماية والجدر النارية وعلاقتها بالمخاطر السيبرانية وتهديداتها، أو وضع خطط وبرامج لتوعية المعلمين وتثقيفهم للتعامل الأمثل مع التقنيات الافتراضية، ووسائل التواصل الاجتماعي؛ لحمايتهم من الانتهاكات السيبرانية، وجاءت هذه النتيجة متفقة مع ما ذكرته دراسة المنتشري (2020).

النتائج المتعلقة بسؤال الدراسة الثالث: والذي نصه: هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك تعزى لمتغيرات: (النوع الاجتماعي، والمؤهل العلمي، المواد التي يدرسها المعلم، وسنوات الخبرة في التدريس)؟

للإجابة عن هذا السؤال تم استخدام التباين الأحادي متعدد الاتجاهات (4 Way- ANOVA) والجدولان (7) و(8) يبيّنان النتائج:

الجدول (7) المتوسطات الحسابية والانحرافات المعيارية لدرجة الوعي بالأمن السيبراني لدى المعلمين تعزى لمتغيرات: النوع الاجتماعي، والمؤهل العلمي، المواد التي يدرسها المعلم، وسنوات الخبرة في التدريس

المتغير	مستويات المتغير	العدد	المتوسط الحسابي	الانحراف المعياري
النوع الاجتماعي	ذكر	89	3.99	0.677
	انثى	182	3.79	0.692
المؤهل العلمي	دبلوم	35	4.01	0.617
	بكالوريوس	166	3.83	0.699
	دراسات عليا	70	3.84	0.711
المواد التي يدرسها المعلم	مواد علمية	102	3.87	0.633
	مواد انسانية	125	3.79	0.738
	اداري	44	4.02	0.679
سنوات الخبرة بالتدريس	5 سنوات فأقل	28	3.81	0.710
	6–9 سنوات	95	3.88	0.733
	10 سنوات فأكثر	148	3.86	0.692

تظهر نتائج الجدول (7) وجود فروق ظاهره بين المتوسطات الحسابية لدرجة الوعي بالأمن السيبراني لدى المعلمين تعزى للنوع الاجتماعي، والمؤهل العلمي، والمواد التي يدرسها المعلم، وسنوات الخبرة في التدريس، وللتأكد فيما إذا كانت الفروق دالة إحصائيًا وحقيقية، فقد تم تطبيق اختبار تحليل التباين الأحادي التباين الأحادي متعدد الاتجاهات (4 way- ANOVA)، والجدول (8) يعرض النتائج:

الجدول (8) نتائج تحليل التباين الأحادي متعدد الاتجاهات (4 WAY- ANOVA) لبيان دلالة الفروق في درجة الوعي بالأمن السيبراني تعزى لمتغيرات: النوع الاجتماعي, والمؤهل العلمي, والمواد التي يدرسها المعلم، وسنوات الخبرة في التدريس

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة (F)	الدلالة الإحصائية
النوع الاجتماعي	2.316	1	2.316	**4.880***	**0.028**
المؤهل العلمي	0.552	2	0.276	0.582	0.560
المواد التي يدرسها المعلم	1.318	2	0.659	1.388	0.251
سنوات الخبرة بالتدريس	0.089	2	0.044	0.094	0.911
الخطأ	124.833	263	0.475		
الكلي	4165.836	271			
الكلي المصحح	129.472	270			

***دالة إحصائيًا عند مستوى الدلالة (α≤0.05).**

****دالة إحصائيًا عند مستوى الدلالة (α≤0.01).**

تظهر نتائج الجدول (8) الآتي:

1. وجود فروق دالة إحصائيًا في درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك، تعزى لمتغير النوع الاجتماعي، اعتمادًا على قيم (ف) المحسوبة الظاهرة في الجدول السابق، والبالغة (4.880) عند مستوى الدلالة (α=0.028)، وهي دالة إحصائيًا عند مستوى الدلالة (α≤0.05)، وكانت الفروق لصالح الذكور، حيث بلغ المتوسط الحسابي (3.99)، وهو أكبر من المتوسط لحسابي للإناث والبالغ (3.79).

تعزى هذه النتيجة بأن الذكور أكثر اهتمامًا واستخدامًا لأدوات التكنولوجية، والاطلاع على كل ما هو جديد في عالم الفضاء الإلكتروني، وتطبيق المهارات التي تساعدهم على حماية معلوماتهم وبياناتهم.

2. عدم وجود فروق دالة إحصائيًا في درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك تعزى لمتغيرات: المؤهل العلمي، والمواد التي يدرسها المعلم، وسنوات الخبرة بالتدريس، اعتمادًا على قيم (ف) المحسوبة الظاهرة في الجدول السابق والبالغة (F=0.582, 1.388, 0.094)، عند مستوى الدلالة (α=0.560, 0.251, 0.911)، وهي غير دالة إحصائيًا عند مستوى الدلالة (α≤0.05).

ويمكن أن تعزى هذه النتيجة إلى أن المعلم يستخدم الشبكة العنكبوتية، ولديه معرفة باستخدام الهواتف الذكية وأجهزة الحاسوب وتطبيقاتها في العملية التعليمية، بغض النظر عن مؤهله والمواد التي يدرسها وسنوات خبرته، وتتفق هذه النتيجة مع نتائج دراسة المنتشري وحريري (2020)، ودراسة الصانع، السواط، أبو عيشة، سليمان، عسران، (2020)، ودراسة الصحفي وعسكول (2019).

النتائج المتعلقة بسؤال الدراسة الرابع: والذي نصه: هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (α≤0.05)، في طرق تنمية الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك تعزى لمتغيرات: (النوع الاجتماعي، والمؤهل العلمي، المواد التي يدرسها المعلم، وسنوات الخبرة في التدريس)؟

للإجابة عن هذا السؤال تم استخدام التباين الأحادي متعدد الاتجاهات (4 Way- ANOVA) والجدولان (9) و(10) يبيّنان النتائج:

الجدول (9) المتوسطات الحسابية والانحرافات المعيارية في طرق تنمية الوعي بالأمن السيبراني لدى المعلمين تعزى لمتغيرات: النوع الاجتماعي، والمؤهل العلمي، المواد التي يدرسها المعلم، وسنوات الخبرة في التدريس

المتغير	مستويات المتغير	العدد	المتوسط الحسابي	الانحراف المعياري
النوع الاجتماعي	ذكر	89	4.18	0.734
	انثى	182	4.04	0.755
المؤهل العلمي	دبلوم	35	4.31	0.668
	بكالوريوس	166	4.05	0.778

	دراسات عليا	70	4.05	0.762
المواد التي يدرسها المعلم	مواد علمية	102	4.07	0.786
	مواد انسانية	125	4.07	0.773
	إداري	44	4.16	0.688
سنوات الخبرة بالتدريس	5 سنوات فأقل	28	3.98	0.871
	6–9 سنوات	95	4.18	0.732
	10 سنوات فأكثر	148	4.05	0.760

تظهر نتائج الجدول (9) وجود فروق ظاهره بين المتوسطات الحسابية **في طرق تنمية الوعي الأمن السيبراني** لدى المعلمين تعزى للنوع الاجتماعي، والمؤهل العلمي، والمواد التي يدرسها المعلم، وسنوات الخبرة في التدريس، وللتأكد فيما إذا كانت الفروق دالة إحصائيًا وحقيقية، فقد تم تطبيق اختبار تحليل التباين الأحادي متعدد الاتجاهات (4 way- ANOVA)، والجدول (10) يعرض النتائج:

الجدول (10) نتائج تحليل التباين الأحادي متعدد الاتجاهات (4 WAY- ANOVA) لبيان دلالة الفروق في طرق تنمية الوعي بالأمن السيبراني تعزى لمتغيرات: النوع الاجتماعي، والمؤهل العلمي، المواد التي يدرسها المعلم، وسنوات الخبرة في التدريس

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة (F)	الدلالة الإحصائية
النوع الاجتماعي	1.168	1	1.168	2.012	0.157
المؤهل العلمي	1.653	2	0.826	1.423	0.243
المواد التي يدرسها المعلم	0.083	2	0.041	0.071	0.931
سنوات الخبرة بالتدريس	1.255	2	0.628	1.081	0.341
الخطأ	152.696	263	0.581		
الكلي	4679.133	271			
الكلي المصحح	157.181	270			

***دالة إحصائيًا عند مستوى الدلالة ($\alpha \leq 0.05$).**

**** دالة إحصائيًا عند مستوى الدلالة ($\alpha \leq 0.01$).**

تظهر نتائج الجدول (10) الآتي:

عدم وجود فروق دالة إحصائيًا في **طرق تنمية الوعي بالأمن السيبراني** لدى المعلمين في مديرية التربية والتعليم قصبة الكرك تعزى لمتغيرات: النوع الاجتماعي، والمؤهل العلمي، والمواد التي يدرسها المعلم، وسنوات الخبرة بالتدريس، اعتمادا على قيم (ف) المحسوبة الظاهرة في الجدول السابق والبالغة (F=2.012, 1.423, 0.071, 1.081)، عند مستوى الدلالة (α=0.157,0.243, 0.931, 0.34) ، وهي غير دالة احصائيًا عند مستوى الدلالة ($\alpha \leq 0.05$) تعزى هذه النتيجة إلى خضوع المعلمين للدورات نفسها، واستخدامهم تطبيقات مختلفة أثناء جائحة كورونا، بحيث أصبحت لديهم دراية ووعي بطرق حماية معلوماتهم، والقدرة على التعامل مع تكنولوجيا الاتصال الحديثة، سواء أكانت أجهزة ذكية أم حواسيب.

التوصيات والمقترحات:

في ضوء النتائج التي توصلت لها الدراسة، فإن الباحثة توصي بالآتي:

1. ضرورة عقد دورات مستمرة ومحاضرات توعوية من قبل المتخصصين بعلم الحاسوب و الأمن السيبراني للمعلمين في مديرية تربية وتعليم قصبة الكرك، لتزويدهم بكل جديد عن الأمن السيبراني.
2. ضرورة تدريب المعلمين على استخدام برامج الحماية والجدر النارية، حيث إن النتائج كشفت عن مستوى وعي متوسط لديهم بهذه التقنية.
3. إجراء مزيد من الدراسات والأبحاث على المتغيرات التي تناولتها الدراسة على عينات أخرى؛ للاستفادة من نتائج الدراسة الحالية وتعميماتها.

الخاتمة:

ساهمت الثورة التكنولوجية والاعتماد على التقنيات المتطورة، بتغيير العلاقات وأساليب الحياة في جميع مجالاتها نحو الأفضل، ولكن جعلت من بياناتهم ومعلوماتهم وأجهزتهم عرضة للخطر والاختراقات المختلفة، فالجرائم الإلكترونية إذا لم يسيطر عليها سوف تصبح في غاية الخطورة، فالقضاء عليها تمامًا غير ممكن، شأنها شأن بقية الجرائم الأخرى، ولكن يمكن تنفيذ السياسات والآليات اللازمة لتقليل مخاطرها؛ لأنه بقدر تطور أساليب الجريمة تتطور أساليب مكافحتها، فالحد منها يتطلب تعاونًا مشتركًا من كافة الجهات المعنية،

وأخذ الحيطة والحذر عند استخدام البيانات والمعلومات في المجال الافتراضي؛ لتجنب الوقوع في مخاطر التصيد الشبكي والهاكرز، والحفاظ على الأمن القومي.

References:

- Abu Hussein, H. (2021). "The Legal framework for cyber security services". Master's thesis in private law. Middle East University.
- Al-Dahshan, J. Al-Fuwaihi, H (2015). "Digital citizenship is an introduction to help our children live in the digital age". Journal of Psychological and Educational Research - Faculty of Education, Menoufia University - Egypt. 30 (4). 1- 42.
- Aljohani, W., & Elfadil, N.(2020). "Measuring Cyber Security Awareness of Students: A Case Study at Fahad Bin Sultan University". International Journal of Computer Science and Mobile Computing. 9(6). 141- 155.
- Al-Montashari, F. Hariri, R. (2020). "The Degree of awareness of middle school teachers about cyber security in public schools in Jeddah from the female teachers' point of view". The Arab Journal of Specific Education. Dar Al-Hekma University, Jeddah. 4(13) 95-138.
- Al-Saanie, N. Al-Suwat, H. Abu Aisha, Z. Soleman, E. Asran, A. (2020). "Teachers' awareness of cyber security and methods of protecting students from the dangers of the Internet and promoting their national values and identity". Scientific Journal. Taif University, Saudi Arabia. 36 (6).
- Al-Sahafi, M. & Askol, S. (2019). "The level of cyber security awareness among secondary school computer teachers in Jeddah". Journal of Scientific Research in Education .10 (20). 493 – 534.
- Al-Sharif, B. & Ahmed, A. (2020). "A Guide to curbing the phenomenon of cyber bullying". Arab Studies in Education and Psychology (ASEP). (127). 23-92.
- Alzubaidi, A., (2021). "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia". Heliyon Journal. 7(2021).
- Amoroso, E., (2007). "Cyber Security, Silicon Press, Summit, NJ 07901, USA". First Edition. Library of Congress Cataloging-in-Publication Data.
- Craigen, D., Thibault, N., & Purse, R. (2014). Technology Innovation Management Review.
- Davis, D. (2018, March). "Best practices for balancing technology use and safety in a modern school". In Society for Information Technology & Teacher Education International Conference (pp.1026-1030). Washington, DC: Association for the Advancement of Computing in Education (AACE).
- Dhulapally, M. (2021). "Digital Notes on Cyber Security" (R18A0521). Department of information technology Malla Reddy College of Engineering & Technology. Autonomous Institution – UGC, Govt. of India.
- 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.
- Fovino, I. (2020). "Cybersecurity our Digital Anchor A European Perspective". European Commission, Joint Research Centre, Ispra – Italy.
- Godbole, N., Belpure, S., Gupta, B., & Wang, D. (2021). "DIGITAL NOTES ON CYBER SECURITY". Department of Information Technology. Malla Reddy College of Engineering & Technology. India.
- Hanafi, H (2000). Blogging, History, Reading, Plagiarism. From Transport to Creativity. 1 (1). Cairo: Kabba House for Printing, Publishing and Distribution. p 83.
- Hossam El Din, A. (2017). Introduction to Cyber Security. Member of Cisco Academy Yanbu. The book is translated.
- Jabbour, M (2016). "Cyber obsession of the times. Lebanon: League of Arab States". Arab Centre for Legal and Judicial Research.
- Kritizinger, E., Bada, M., & Nurse, J. (2017). "A study in to the cybersecurity awareness initiatives for school learners in south Africa and the UK 10th". World conference on information security education. Rome: May 29-31.
- Mahno, D., (2017). "Design of Cyber Security Awareness program for the First Year NON-IT Students". Tallinn University of Technology Faculty of Information Technology. Master's Thesis.
- Mashush, M. (2018). "International efforts to combat cybercrime". Hassan 1 University - Faculty of Legal, Economic and Social Sciences - Business Law Research Laboratory.
- Media Authority. (2021). Cyber Security. Department of Studies, Communication and Public Relations. Available on the site:http://www.mc.gov.jo/EchoBusV3.0/SystemAssets/PDF/f766148f-d691-4bd3-a6b5-1d023062f523_%D8%AF%D8%B1%D8%A7%D8%B3%D8%A9% 20%D8%A7%D8%B3%D8%A7%D8%A7%D8%B1%D8% A7%Dog and6%DrabeA.pdf.
- National Cyber Security Strategy. (2021). The Egyptian Arabic Republic. The Supreme Council for Cyber Security. Available on the

site.
https://mcit.gov.eg/ar/Publication/Publication_Summary/6132.

- Pusey, P. & Sadera, W. (2011). "Cyber ethics, Cyber safety, and Cybersecurity: Pre-service teacher knowledge, preparedness and the need for teacher education to make a difference". Journal of Digital Learning in Teacher Education. 28(2), 89- 88.
- Rahman. A., Sairi. I., Zizi. A., & Khalid, F. (2020). "The Importance of Cybersecurity Education in School- Malaysia". International Journal of Information and Education Technology. 10(5).378- 383.
- Richardson, M., Lemoine, P., Stephens, W., & Waller, R., (2020). "Planning for Cyber Security in Schools: The Human Factor". Educational Planning. 27(2).
- Sadowsky. G, Dempsey. J, Greenberg. A, Mack. B; Schwartz. A. (2003). "Information Technology Security Handbook(IT - SECURITY)". The International Bank for Reconstruction and Development / The World Bank Washington.
- Salahdine, F., & Kaabouch, N. (2019). "Social Engineering Attacks: A Survey". Future Internet, 11(4), 89-106.
- 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 & information (IJCI). 8(2). 1 -21.
- Schuesster, J. H. (2013). Contemporary threats and countermeasures. Journal of Information Privacy & Security, 9(2), 3-20.
- Solms. R & Solms. S. (2015). "Cyber safety education in developing countries". Journal of systemic, cybernetics and informatics. 13(2), 14 – 19.
- Tiwari, S., Bhalla, A., & Rawat, R. (2016). "Cyber-crime and security". International journal of advanced research in computer science and software engineering. 6(4), 46-52
- Zwilling. M., Klien. G., Lesjak. D., Wiechetek. L., Cetin. F. & Basim. H. (2020). "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study". Journal of Computer Information Systems. ISSN: 0887-4417 (Print) 2380-2057.