دور معلمي المرحلة الثانوية العامة في تعزيز مستوى الوعي بالأمن السيبراني لدى طلابهم وسبل تعميقه.

إعداد

إيهاب إبراهيم حسن الصفتى

مدرس بقسم أصول التربية بكلية التربية جامعة الأزهر بالقاهرة

دور معلمي المرحلة الثانوية العامة في تعزيز مستوى الوعي بالأمن السيبراني لدى طلابهم وسبل تعميقه.

إيهاب إبراهيم حسن الصفتى

قسم أصول التربية بكلية التربية جامعة الأزهر بالقاهرة.

البريد الإلكتروني: EhabElsafty388.el@azhar.edu.eg

مستخلص البحث:

هدفت الدراسة الكشف عن واقع دور معلمي المرحلة الثانوية العامة في تعزيز مستوى الوعي بالأمن السيبراني لدى طلابهم وتحديد السبل المقترحة لتعميقه، ولتحقيق هذا الهدف تم استخدام المنهج الوصفي، واعتمدت الدراسة على الاستبانة في جمع البيانات، وطبقت على عينة بلغت (٤١٧) من معلمي ومعلمات المرحلة الثانوية موزعين وفق متغيرات النوع (ذكور/ إناث) والتخصص (تكنولوجيا معلومات/ لغوي/ ثقافي) والمؤهل (تربوي/ غير تربوي)، وأشارت النتائج إلى أن واقع دور معلمي المرحلة الثانوية العامة في تعزيز مستوى الوعي بالأمن السيبراني لدى طلابهم جاء متوسطاً، وأن الموافقة على السبل المقترحة لتعميق واقع دور معلمي المرحلة الثانوية العامة في تعزيز مستوى الوعي بالأمن السيبراني لدى طلابهم جاءت مرتفعة، كما أشارت النتائج إلى أنه لا توجد فروق دالة إحصائياً في استجابات أفراد عينة الدراسة تعزى لمتغير النوع، بينما وجدت فروق دالة إحصائياً في استجاباتهم تعزى لمتغير المؤهل لصالح ذوي المؤهل التربوي، كما وجدت فروق دالة إحصائياً في استجاباتهم تعزى لمتغير التخصص لصالح ذوي تخصص تكنولوجيا معلومات.

الكلمات المفتاحية: الأمن السيبراني - أمن المعلومات – الوعي – المخاطر السيبرانية.

The role of secondary school teachers in raising their students' cybersecurity awareness and ways to deepen it.

Abstract:

The study aimed to reveal the reality of the role of general secondary school teachers in enhancing the level of awareness of cybersecurity among their students and to identify proposed ways to deepen it. To achieve this goal, a descriptive approach was used, and the study relied on a questionnaire to collect data, and it was applied to a sample of (417) male and female stage teachers.

Secondary schools were distributed according to the variables of sex (males/females), specialization (information technology/linguistics/cultural), and qualification (educational/non-pedagogical). The results indicated that the reality of the role of general secondary school teachers in enhancing the level of awareness of cybersecurity among their students was moderate, and that approval the proposed ways to deepen the role of general secondary school teachers in enhancing the level of cybersecurity awareness among their students were high. The results also indicated that there were no statistically significant differences in the responses of the study sample members due to the sex variable, while statistically significant differences were found in their responses due to the qualification variable.

In favour of those with an educational qualification, and statistically significant differences were found in their responses due to the specialization variable, in favour of those with an information technology specialization.

Keywords: cybersecurity - information security - awareness - cyber risks.

مقدمة البحث

يعد الأمن هو الركيزة الأساسية في بناء أي مجتمع، والعنصر الرئيس في نمو أي نشاط سواء كان نشاط سياسي، أو نشاط تجاري، أو نشاط تعليمي، ومع بروز مجتمع المعلومات، وتقنيات التعليم، ومع تحول التعليم في العصر الحالي باعتماده على التعلم الالكتروني، والتوجه نحو التحول الرقمي أصبح من الضروري حماية الأفراد والمجتمعات من السلبيات المترتبة على ذلك، خاصة وأن العالم يشهد ثورة تقنية أثرت في مختلف المجالات وشملت جميع الفئات العمرية، ورغم ما لهذه الثورة من إيجابيات فإنه لها في المقابل العديد من السلبيات، ومن أبرز هذه السلبيات المخاطرالسيبرانية، ولذا فإن موضوع الأمن السيبراني من المواضيع البحثيَّة التي لم تحظَ بالقدر الكافي من الدِّراسَات، خاصة لدى طلاب المرحلة الثانوية، إذ ظهرت الحاجة إلى ضرورة تنمية وعيهم بالأمن السيبراني.

لقد كان لظهور شبكة الإنترنت وتدفق المعلومات في الفضاء السيبراني أثراً مهمًا في جميع مجالات الحياة، إلا أنها ارتبطت بالعديد من المخاطر التي يُمكن من خلالها إيقاع خسائر فادحة عبر التسبب في خلل بيئة المعلومات والاتصالات الخاصة بمستخدم ما أو بجهة معينة، من خلال التلاعب بالبيانات أو تزييفها، أو محوها من أجهزة الحواسيب (خليفة، ٢٠٢٠، ٢٣)

ولذا بات من الضروري وجود وسيلة آمنة لحماية الفضاء السيبراني الذي يُعد من أساسيات تسخير تقنيات المعلومات والاتصالات في مجالات التنمية لخدمة المجتمعات الإنسانية، ومن هنا ظهرت أهمية الأمن السيبراني لكونه قيمة مضافة ودعامة أساسية لأنشطة الحكومات والأفراد باعتباره يشمل جميع الجوانب التعليمية، والاجتماعية، والاقتصادية،والإنسانية، وممثلًا لقدرة الدولة على حماية مصالحها وشعبها، ومن كونه يرتبط ارتباطًا وثيقًا بسلامة مصادر الثروة المعلوماتية في العصر الحالي، والقدرة على الاتصال والتواصل، ومن ثم تحقيق الإنتاج، والإبداع، والقدرة على المنافسة بين المجتمعات. (البيشي، ٢٠٢١، ٢٥٩)

وتتسع الأساليب الآمنة بشكل كبير لتشمل أنواعًا حديثة تتفق مع حداثة العصر الحالي ومن أبرزها هو الأمن السيبراني، وهو ما يعرف بحماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي مخاطر كالاختراق، أو التعطيل أو الاستخدام أو الاستغلال الغير مشروع (هيئة الاتصالات وتقنية المعلومات، ٢٠٢٢)

وقد أشارت دراسة (المنتشري وحريري، ٢٠٢٠) إلى أن المخاطر السيبرانية تشمل جميع مستخدمي الإنترنت حول العالم أفرادًا ومؤسسات ووزارات، إضافة إلى أنها لا تقتصر على فئة عمرية دون أخرى. وكما توصلت دراسة (قطب، ٢٠٢١) إلى أن زيادة نسبة الجرائم السيبرانية تأتي نتيجة لضعف الوعي بالأمن السيبراني.

مشكلة الدراسة:

أشارت دراسة السواط، والصانع، وأبوعيشة وسليمان (٢٠٢٠)، ودراسة O'Brien (2019) في نتائجها إلى افتقار الطلاب إلى أساسيات الأمن السيبراني، ودراسة Mangold(2016) التي أكَّدت وجود ضعف في الوعي بمفاهيم الأمن السيبراني، وضرورة إكساب الطلاب الوعي بتلك المفاهيم، من خلال الدورات التدريبيَّة، والمعسكرات السيبرانيَّة، وأكْدت نتائج دراسة Sadaghiani (2018) ضرورة مراقبة الطلاب عبر الإنترنت، والتوعية بمخاطر الفضاء السيبراني، وتعليم الطلاب الممارسات الصحيحة، وأكدت دراسة السعيد (٢٠٢٠) عددًا من التوصيات، منها: زيادة التدريب

العملي على مهارات الاستخدام الآمن للكمبيوتر والإنترنت، والوعي بأخلاقيات وآداب السلوك الرقمي.

وأوصت العديد من الدراسات مثل (حمادي،٢٠١٧؛ حلفاية، ٢٠٢٠؛ الشهراني وفلمبان (٢٠٢٠), VON SOLMS,2020، خورشيد، ٢٠٢١، Alzubaidi, 2021, Amankwa. E, 2021) بأهمية توعية المتعلمين منذ مرحلة رياض الأطفال ومروراً بمراحل التعليم المختلفة بكيفية حماية أنفسهم باعتبارهم من مستخدمي الإنترنت المعرضين للخطر.

إضافة لما سبق أكدت العديد من المؤتمرات على ضرورة تعزيز الأمن السيبراني لدى جميع أفراد المجتمع خاصة الشباب، كمؤتمر مستقبل الأمن السيبراني العالمي ٢٠٢١م بالأردن، ومؤتمر هاك ٢٠٢١م بالرياض، ومؤتمر ومعرض الذكاء الاصطناعي لتكنولوجيا الدفاع والأمن السيبراني الأول ٢٠٢١ بالأردن، ومؤتمر، رابطة CMAI الدولية للأمن السيبراني بالهند ٢٠٢١(نقلاً عن الصواط، ٢٠٢٢، ٥).

وفي ضوء ما سبق تتأكد مخاطر غياب الأمن السيبراني وتبدو الحاجة الملحة لتعزيزه ومن هنا تتضح مشكلة الدراسة الحالية في الكشف عن واقع دور معلمي المرحلة الثانوية في تعزيز مستوى الوعي بالأمن السيبراني لدى طلابهم وتحديد السبل المقترحة لتعميقه، وهذا ما تستهدفه الدراسة من خلال محاولتها الإجابة عن الأسئلة الآتية.

أسئلة الدراسة: سعت الدراسة للإجابة عن الأسئلة الآتية:

١. ما واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم؟
٢. ما السبل المقترحة لتعميق واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم؟
٣. ما مدى تأثير متغيرات النوع (ذكور/ إناث) والمؤهل (تربوي/ غير تربوي) والتخصص (تكنولوجيا معلومات/ لغوي/ ثقافي) في رؤية عينة الدراسة لواقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم والسبل المقترحة لتعميقه؟

أهداف الدراسة: هدفت الدراسة تحقيق ما يلي:

١. الكشف عن واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم.
٢. تقديم السبل المقترحة لتعميق واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم.
٣. بيان مدى تأثير متغيرات النوع (ذكور/ إناث) والمؤهل (تربوي/ غير تربوي) والتخصص (تكنولوجيا معلومات/ لغوي/ ثقافي) في رؤية عينة الدراسة لواقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم والسبل المقترحة لتعميقه.

أهمية الدراسة: تنطلق أهمية الدراسة من عدة اعتبارات أبرزها ما يلي:

١. تزايد المخاطر والانتهاكات السيبرانية التي يتعرض لها العالم بمختلف فئاته العمرية سواء على المستوى الفردي أم على المستوى المؤسسي.
٢. توصية العديد من الدراسات والمؤتمرات بإجراء مزيد من الدراسات حول الأمن السيبراني وكيفية تعزيزه لدى جميع فئات المجتمع.
٣. يعد طلاب المرحلة الثانوية من الفئات الأكثر استخداماً لشبكة الإنترنت والأكثر عرضة للمخاطر السيبرانية مما يتطلب تعزيز وعيهم بالأمن السيبراني.

٤. يمكن للدراسة أن تفيد معلمي المرحلة الثانوية بما تكشف عنه من نتائج توقفهم على واقع دورهم في تعزيز الأمن السيبراني لدى طلابهم ومن ثم العمل على تعزيزه.
٥. أهمية ما تقدمه من مقترحات لتعميق دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم.
٦. يمكن للدراسة أن تفيد مخططي ومطوري مناهج التعليم بالمرحلة الثانوية بما تتوصل إليه من نتائج يمكن الأخذ بها في عمليات تخطيط وتطوير المناهج بما يعمق من دورها في تعزيز الوعي بالأمن السيبراني لدى المتعلمين.
٧. يمكن أن تلفت انتباه الكثير من فئات المجتمع لخطورة غياب الأمن السيبراني وضرورة العمل على تعزيزه.

حدود الدراسة: اقتصرت الدراسة على الحدود التالية:

١. الحدود الموضوعية: واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني ومقترحات تعميقه.
٢. الحدود البشرية: معلمي ومعلمات المرحلة الثانوية العامة المحددين بعينة الدراسة.
٣. الحدود المكانية: مدارس المرحلة الثانوية العامة بمحافظات (القاهرة/ الغربية/ المنيا).
٤. الحدود الزمانية: العام الدراسي ٢٠٢٣م.

مصطلحات الدراسة:

الأمن السيبراني:

يُعرف الأمن السيبراني اصطلاحًا بأنه: "الممارسات التي تلعب دورًا رئيسًا في تأمين أنظمة المعلومات. من خلال مراقبة أحداث الأمان والكشف عنها والتحقيق فيها وتحليلها والاستجابة لها". (الجندي ومحمد، ٢٠١٩، ٢٣).

ويُعرف إجرائيًا في هذه الدراسة بأنه: مجموعة من المعايير والضوابط والمهارات التقنية التي ينبغي أن يمتلكها طلاب المرحلة الثانوية من أجل المحافظة على خصوصيتهم عبر شبكة الإنترنت وحماية بياناتهم الشخصية وأجهزتهم الإلكترونية من أي هجمات فيروسية أو مخاطر سيبرانية كالتحرش الإلكتروني والتنمر الإلكتروني وانتحال الشخصيات والابتزاز الإلكتروني وسرقة كلمات المرور والحسابات الشخصية ونحو ذلك.

الدراسات السابقة :تعرض الدراسة فيما يلي بعض الدراسات ذات الصلة بموضوعها مرتبة زمنياً من الأحدث للأقدم على النحو التالي:

١. دراسة سراج (٢٠٢٢): هدفت إجراء تحليل بعدي لنتائج بعض دراسات وبحوث سابقة ذات صلة بالأمن السيبراني في المجال التربوي في الفترة ما بين (٢٠١٥: ٢٠٢١)، وتحديد حجم أثر المعالجات التجريبية المستخدمة فيها، والتعرف على العوامل المؤثرة في نشر ثقافة الأمن السيبراني في المجال التربوي، والتعرف على تأثير الأمن السيبراني على نواتج التعلم (المعرفي - الوجداني- المهاري)، وتمثلت عينة الدراسة في (٧٤) دراسة ذات صلة بالأمن السيبراني في المجال التربوي ثم تم اختيار ٢٥ دراسة في الفترة ما بين (٢٠١٥: ٢٠٢١) واستبعاد (٤٩) دراسة لأنها دراسات وصفية والمنهج المستخدم: منهج التحليل البعدي، واستخدمت الباحثة: استمارة ترميز لتوثيق دراسات وبحوث ذات صلة بالأمن السيبراني في المجال التربوي وأبعادها(عنوان الدراسة، اسم الباحث، السنة، الهدف، الأدوات، المنهج، المشاركون، النتائج). (إعداد /الباحثة)، الأسلوب الإحصائي: متوسط حجم الأثر، وتوصلت النتائج إلى ما يلي: أكثر الدراسات التي تناولت مفاهيم الأمن السيبراني في المجال التربوي قد تطرقت للتنمر

الإلكتروني، تنوع البرامج في دراسات الأمن السيبراني ما بين الإرشاد والتدريب والبرامج الوقائية ولكن أكثرها برامج إرشادية، تنوع محتوى البرامج ما بين التعلم المدمج، الثقافة الرقمية، الحوسبة السحابية، الدعم النفسي الإيجابي، أدوات حرب الجيل الخامس، ومنظور الخدمة العامة وتنوعت نواتج التعلم من خلال الكفايات التعليمية التكنولوجية، حل المشكلات، تعلم اللغة الانجليزية، المواطنة الرقمية، والاندماج الرقمي، وقد قدمت الدراسة برنامجاً تدريبياً مقترحا لتحسين مفاهيم الأمن السيبراني في المجال التربوي.

٢. دراسة غوص والشريف (٢٠٢٢): هدفت التعرُّف على قياس فاعليَّة توظيف التطبيقات الذكيَّة القائمة على الرسوم المتحركة، في تقديم وحدة مقترحة عن الأمن السيبراني، على التحصيل المعرفي والاتجاه نحوه. وتحقيقًا لذلك اتبعت الدِّراسَة المنهج شبه التجريبي، وتمثلت أداتا الدِّراسَة في: اختبار تحصيلي، ومقياس اتجاه. وتوصلت الدِّراسَة إلى النتائج التالية: وجود فرق ذي دلالةٍ إحصائيَّة عند مستوى ($\alpha \leq ٠,٠١$) بين متوسِّطي درجات طالبات المجموعتين التجريبيَّة والضابطة في التطبيق البعدي لمستويات التذكُّر، والفهم، والتطبيق، وكذلك الدرجة الكليَّة للاختبار التحصيلي، لصالح المجموعة التجريبيَّة. وأوصت الدِّراسَة بضرورة تضمين وحدة عن الأمن السيبراني، في منهج الحاسب الآلي للمرحلة المتوسِّطة، والاستفادة من التطبيقات الذكيَّة في توضيح مفاهيم الأمن السيبراني، واستخدام نظريات التعلُّم الموقفي في تصميم محتوى وأنشطة منهج الحاسب الآلي في المرحلة المتوسِّطة.

٣. دراسة فرج (٢٠٢٢): هدفت الدراسة إلى بيان دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطام بن عبد العزيز، وتحديد الفروق في وجهات نظر أفراد العينة نحو دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي للجامعة تبعاً لمتغيرات: (الكلية، التخصص، سنوات الخبرة)، وتحقيقاً لذلك استخدمت الدراسة المنهج الوصفي، وصممت استبانة تكونت من (٢٦) فقرة توزعت إلى ثلاثة مجالات، وطُبقت على عينة من أعضاء هيئة التدريس بالجامعة بلغت (١٢٥) عضواً، وخلصت الدراسة إلى أن دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطام بن عبد العزيز من وجهة نظر أعضاء هيئة التدريس حصل على متوسط عام (٣,٥٥ من ٥) أي بدرجة متوسطة، وبالنسبة للمحاور؛ حصل محور الدواعي المجتمعية لتعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي للجامعة على أعلى متوسط (٣,٧٠)، يليه محور الدواعي المعرفية لتعزيز ثقافة الأمن السيبراني بالجامعة وحصل على متوسط عام (٣,٥١)، وأخيراً محور الدواعي التقنية وحصل على متوسط (٣,٤٦)، كما بينت النتائج عدم وجود فروق ذات دلالة إحصائية تبعاً لمتغير الكلية، والرتبة العلمية، فيما وجدت فروق تعزى لمتغير سنوات الخبرة، وتوصى الدراسة بأهمية إذكاء الوعى بالأمن السيبراني لدى الطلبة، وإدراك منافع البرمجيات المتاحة لمكافحة المخاطر السيبرانية، وتصميم حملات للتوعية بالمخاطر السيبرانية.

٤. دراسة الصواط (٢٠٢٢): هدفَت التَعرُّف على درجة إسهام بعض منصات التعلم الإلكترونية مفتوحة المصدر في تنمية الوعي بالأمن السيبراني من وجهة نظر الطلبة بجامعة أم القرى. ولتحقيق هذا الهدف اعتمدت الدراسة على المنهج الوصفي المسحي، وطُبقت على عينة عشوائية مكونة من (٧٠٠) طالب وطالبة بجامعة أم القرى وجميع فروعها، وتمثلت أداة الدراسة في استبانة إلكترونية لجمع البيانات، وتوصلت أهم نتائج الدراسة إلى أن درجة استخدام طلبة جامعة أم القرى للمنصات الإلكترونية مفتوحة المصدر جاءت بدرجة متوسطة، كما أشارت إلى أن درجة الوعي بالأمن السيبراني جاءت بدرجة مرتفعة، إضافة إلى

عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (a≤ 0.05)بين متوسطات استجابة أفراد عينة الدراسة حول درجة استخدام المنصات الإلكترونية مفتوحة المصدر تعزى إلى متغير (الجنس، المرحلة الدراسية، التخصص)، وعدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (a≤ 0.05) بين متوسطات استجابة أفراد عينة الدراسة حول درجة الوعي بالأمن السيبراني تعزى إلى متغير(الجنس، المرحلة الدراسية، التخصص)، كما أظهرت النتائج وجود علاقة ارتباطية بين درجة استخدام منصات التعلم الإلكترونية مفتوحة المصدر وبين درجة الوعي بالأمن السيبراني لدى طلبة جامعة أم القرى.

٥. دراسة (Alzubaidi, 2021): هدفت قياس المستوى الحالي للوعي بالأمن السيبراني في المملكة العربية السعودية، في شروط ممارسات الأمن السيبراني، ومستوى الوعي، والإبلاغ عن الحوادث. حيث تم استخدام المنهج الكمي المسحي، وتمثلت عينتها في (١٢٣٠) مواطن سعودي، استخدمت أداة الاستبانة، وكان من أبرز نتائجها أن ٣١,٧٪ استخدموا شبكات Wi-Fi العامة للوصول إلى الإنترنت، استخدم ٥١٪ معلوماتهم الشخصية لإنشاء كلمات المرور الخاصة بهم، ولم يكن لدى ٣٢,٥٪ أي فكرة عن التصيد الاحتيالي الهجمات، ٢١,٧٪ كانوا ضحية للجرائم الإلكترونية بينما ٢٩,٢٪ منهم فقط أبلغوا عن الجريمة، مما يعكس مستويات وعيهم. وأوصت الدراسة بضرورة رفع مستوى الوعي للمجتمع السعودي.

٦. دراسة الحربي وعاصف (Asifa&Alharbi, 2021): هدفت التعرف إلي مستوى الوعي بالأمن السيبراني وامتثال المستخدمين بين الطلاب الجامعيين في جامعة المجمعة. حيث تم استخدام المنهج الكمي، وتمثلت عينتها في (٥٧٦) طالبا من جامعة المجمعة، استخدمت أداة الاستبانة، وكان من أبرز نتائجها أن معظم المشاركين ليس لديهم دراية بأساسيات مفهوم الأمن السيبراني ولم يعرفوا كيف يديرون بياناتهم رغم أن ٩٢٪ منهم قد حضروا برنامج رسمي للتوعية الأمنية، تتزايد هجمات التصيد الاحتيالي يوميًا وتستهدف المستخدمين الذين لديهم معرفة قليلة أو معدومة بالأمن السيبراني.

٧. دراسة الشهراني وفلمبان (٢٠٢٠): هدفت التعرف على أثر تصميم الألعاب الإلكترونية لتعزيز مفاهيم الأمن السيبراني حيث تم استخدام المنهج التجريبي بتصميم شبه التجريبي باستخدام برنامجGame Maker، وتمثلت عينتها في (١٧) طالبة من الصف الثاني المتوسط تم اختيارهم بطريقة عشوائية بمدينة جدة، أجري عليهم الاختبار القبلي ومن ثم تقسيمهم إلى أربع مجموعات لتصميم الألعاب الإلكترونية وفق كل مفهوم من مفاهيم الأمن السيبراني وتم إجراء الاختبار قبل دراسة البرنامج وبعده وبعد الانتهاء تم تقييم التصاميم واختبارهم الاختبار البعدي، واستخدمت أدوات تمثلت في اختبار معرفي لقياس مفاهيم الأمن السيبراني، وبطاقة تقييم منتج لتقييم تصاميم الألعاب الإلكترونية، وكان من أبرز نتائجها وجود فروق ذات دلالة إحصائية بين متوسط درجات الطالبات في الاختبار القبلي والبعدي نحو مفاهيم الأمن السيبراني، وأوصت بزيادة الوعي المجتمعي بمفاهيم الأمن السيبراني وبالمخاطر السيبرانية وطرق الوقاية منها من خلال الوسائل المختلفة.

٨. دراسة جبرة (Gabra et al, 2020): هدفت التعرف على درجة وعي الطلاب بالأمن السيبراني في الجامعات النيجيرية، وأيضا إلى معرفة كيفية إدراك الطلاب في هذه الدولة النامية للهجمات الإلكترونية وكيف يمكنهم التخفيف من الهجمات ومعرفة ما إذا كان برنامج التوعية بالأمن السيبراني جزءًا من برنامج الجامعة. حيث تم استخدام المنهج المسحي، تمثلت عينتها في (٣٧٦) طالباً من الجامعات النيجيرية، استخدمت أداة الاستبانة، وكان من أبرز النتائج أن

الطلاب ادعوا أن لديهم معرفة أساسية بالأمن السيبراني، لكنهم ليسوا على دراية بكيفية حماية بياناتهم، كما أن معظم الجامعات ليس لديها برنامج توعية نشط للأمن السيبراني لتحسين معرفة الطلاب حول كيفية حماية أنفسهم من أي تهديدات.

٩. دراسة نينكيو وآخرون (Nyinkeu et al, 2018, 1): هدفت تحديد مفاهيم الأمن السيبراني التي ينبغي تعزيزها لدى طلاب تكنولوجيا المعلومات. حيث تم استخدام المنهج المسحي، وتمثلت عينتها في (٤٠) طالب، استخدمت أداة المقابلة، وكان من أبرز نتائجها استجابات أفراد العينة جاءت بدرجة مرتفعة عن أهمية تعزيز مفاهيم الأمن السيبراني وأمن الشبكات، وأوصت الدراسة بضرورة التركيز على المفاهيم المتعلقة باستخدام شبكة الإنترنت والاهتمام بالتربية السيبرانية وإدراجها في المقررات الدراسية.

١٠. دراسة (Mangold, 2016): هدفت قياس فاعليَّة البرامج التعليميَّة للطلاب، في زيادة المعرفة بالأمن السيبراني، من أجل تطوير متطلَّبات البرامج المستقبليَّة في التدريب الصيفي. حيث استُخدم المنهج شبه التجريبي، وطبق الاختباران القبلي والبعدي على العينة المكونة من (٣٧) طالبًا في ثانويَّة فلوريدا. حيث تم استخدام أداة مسح تم تطويرها في هذه الدِّراسَة. أظهرت نتائج الدِّراسَة أن برنامج التدريب الصيفي أدى إلى زيادة متوسِّط المعرفة بالأمن السيبراني بنسبة (٣٦,١ ٪)، وأوصت الدِّراسَة بإقامة الدورات التدريبيَّة والمعسكرات السيبرانيَّة لتلبية الطلب المتزايد على المختصين في الأمن السيبراني، من خلال الوصول إلى الطلاب في المراحل الثانويَّة والكليات.

التعليق على الدراسات السابقة:

باستقراء الدراسات السابقة التي تم عرضها يتضح إجماعها على أهمية الأمن السيبراني وضرورة تعزيزه لدى جميع الفئات العمرية، وتزايد المخاطر المترتبة على غيابه، ويلاحظ من العرض السابق تنوع ما استهدفته الدراسات السابقة سواء بقياس واقع الوعي بالأمن السيبراني أو المخاطر المترتبة عليه أو علاقته ببعض المتغيرات، أو تصميم برامج تعليمية لتعزيزه، كما يلاحظ تنوع المراحل التعليمية والفئات العمرية التي استهدفتها الدراسات السابقة، إضافة لما سبق يلاحظ غلبة الجانب الوصفي على الدراسات السابقة مع الاعتماد على مقياس الوعي بالأمن السيبراني أو الاستبانة في جمع البيانات، وتأتي هذه الدراسة متفقة مع الدراسات السابقة من حيث تناول موضوع الأمن السيبراني، ومتفقة مع الدراسات التي استخدمت المنهج الوصفي واعتمدت على الاستبانة في جمع البيانات، وتختلف الدراسات الحالية عن الدراسات السابقة في توجهها العام المتمثل في الكشف عن واقع دور المعلمين في تعزيز وعي طلابهم بالأمن السيبراني بجانب إضافة السبل المقترحة لتعميقه، كما تختلف الدراسة الحالية في مجتمعها وعينتها، واستفادت الدراسة الحالية من الدراسات السابقة في تدعيم الإحساس بمشكلتها وفي تناول بعض المفاهيم النظرية بالإضافة للاستفادة منها في بناء وتصميم الأداة وفي تفسير ومناقشة النتائج.

الإطار النظري:

١. مفهوم الأمن السيبراني:

يعد الأمن السيبراني أو ما يطلق عليه أمن المعلومات والحاسب الآلي، هو فرع من فروع التكنولوجيا المتخصصة في حماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية التي تهدف في الغالب إلى الوصول للمعلومات الحساسة، أو تغييرها، أو إتلافها أو ابتزاز المستخدمين للحصول على الخدمات أو الأموال أو السيطرة على العمليات التجارية (مصطفى، ٢٠٢٢، ٧٢٢).

ويُعرف الأمن السيبراني بأنه: مجموعة من الوسائل التقنية والإدارية والتنظيمية

والتشغيلية الرامية لمنع الاستخدام غير القانوني وغير المصرح به، وسوء استخدام واسترجاع المعلومات الإلكترونية وأنظمة المعلومات والاتصالات، ويهدف الأمن السيبراني ضمان توافر واستمرارية عمل المعلومات وتعزيز الحماية والسرية وخصوصية البيانات الخاصة بالأفراد والمؤسسات الوطنية. (الجنفاوي، ٢٠٢١، ٨١)

كما يُعرف بأنه: "مجموعة من الأدوات والوسائل اللازمة لحماية البريد الإلكتروني والبيانات الرقمية الشخصية والمعلومات والأجهزة المحمولة وتعزيز سريتها وخصوصيتها وتشفيرها واتخاذ الإجراءات في حماية الأفراد من مخاطر الفضاء الإلكتروني حيث يتضمن: حماية البيانات والمعلومات- التشفير- حماية البريد الإلكتروني- أمن الأجهزة المحمولة" (الشهراني وفلمبان، ٢٠٢٠، ٦١٨).

والأمن السيبراني: "مجموعة من الأدوات التنظيميَّة والتقنيَّة والإجرائيَّة، والممارسات الهادفة إلى حماية الحواسيب والشبكات، وما بداخلها من بيانات من الاختراقات، أو التلف، أو التغير، أو تعطل الوصول للمعلومات، أو الخدمات" (البار والسميري، ٢٠١٩,١٢).

كما يُعرف بأنه: "مجموعة من القدرات التقنية والعمليات التي يقوم بها الأفراد لتأمين وحماية الأنظمة الحاسوبية الإلكترونية (الأجهزة والبرامج والشبكات والبيانات) من الوصول غير القانوني للقراصنة والمجرمين السيبرانيين" (Ani et al, 2016, p.170).

وفي ضوء ما سبق يمكن القول بأن الأمن السيبراني يتضمن مجموعة الخطوات والإجراءات والمهارات المتطلبة لحماية المؤسسات والأفراد أنفسهم عند استخدامهم لشبكة الإنترنت من أي مخاطر سيبرانية تستهدف حساباتهم الشخصية، أو أجهزتهم الإلكترونية، أو انتحال شخصياتهم، أو الحصول على بيانات ومعلومات عنهم دون إذن منهم أو موافقة شخصية على ذلك.

٢. أهمية وأهداف الأمن السيبراني:

أجمعت العديد من الدراسات (صائغ، ٢٠١٨، ٤٣، المنتشري، ٢٠٢٠، ١٠٣، السواط وآخرون، ٢٠٢٠، ٣٩٢، وقطب، ٢٠٢١، ٣٠٧) على أهمية الأمن السيبراني، وتتمثل في:

- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف جميع الأجهزة الحكومية، ومؤسسات القطاعين الخاص والعام.
- توفير بيئة موثوقة وآمنة للتعاملات في مجتمع المعلومات.
- توفر المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الانترنت المختلفة.
- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات والمخاطر المختلفة.

إضافة إلى ما سبق ذكر الربيعة (٢٠١٧، ٥٦) إلى أن من أهداف الأمن السيبراني هو حماية مصالح الأفراد والمجتمعات وأمنها الوطني والبنى التحتية الحساسة فيها، كما تقوم باتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الانترنت المختلفة.

وتكمن أهمية الأمن السيبراني في كونه يمثل درعا من دروع الأمن السيبراني فيما ذكره كلا من: (السمحان، ٢٠٢٠، ١١؛ العريشي، ٢٠١٨، ٣٤١، الصواط، ٢٠٢٢، ٢٣) على النحو التالي:

- حماية المعلومات وسلامتها واتساقها من خلال منع العبث البشري لتحقيق توافر البيانات وجاهزيتها عند الحاجة.

- حماية المعدات والشبكة ككل من التطفل لتصبح حاجزًا وقائيًا للبيانات والمعلومات.
- استكشاف نقاط الضعف لدى النظام وإصلاحها.
- استخدام وتطوير أدوات مفتوحة المصدر لتنفيذ مبادئ الأمن السيبراني.
- توفير بيئة عمل آمنة للغاية أثناء العمل عبر الإنترنت.
- ضرورة حماية البنية التحتية لشبكة المعلومات لتحقيق استمرارية الأعمال.

من خلال ما سبق يتضح أن أهمية الأمن السيبراني تكمن في المتطلبات الضرورية اللازمة لحماية المعلومات الحساسة والبنى التحتية للدولة والمواطنين من أي عمليات غير مصرح بها وذلك للمحافظة على الأمن الوطني.

٣. خصائص الأمن السيبراني:

يتسم الأمن السيبراني بعدد من الخصائص التي يجب توفرها لضمان حماية المعلومات وهي كما ذكرها: (الصحفي وعسكول، ٢٠١٩، ٥١٣؛ المشاقبة والسرحان، ٢٠٢٠، ٦٧؛ Cains et al, 2021) على النحو التالي:

- الاكتشاف والتتبع: تعني القدرة على تتبع مسار نشاط أو حدث معين للوصول إلى منشئ النشاط ويكون ذلك من خلال عدم الإنكار، وتشخيص الخطأ، واكتشاف وتتبع الجرائم الإلكترونية، ووضع إجراءات للتغلب عليها.
- السرعة وقلة الأدلة: يوفر الأمن السيبراني تقنيات حديثة قادرة على التغلب على الجرائم الإلكترونية بسرعة عالية.
- السرية والأمن: تتمثل في عدم إفشاء المعلومات أو عرضها لأشخاص غير مصرح لهم إلا في حال وجود تصريح لهم للوصول إليها وذلك بوضع تدابير تحمي المعلومات وأنظمتها من خلال ضمان سريتها.
- التحقق من الهوية وتصريحها: تتمثل في التأكد من هوية المستخدم أو الجهاز أو العملية لتبادل البيانات إذ يجب على الطرفين التأكد من هوية الآخر وهناك بعض الإجراءات للتحقق من ذلك من خلال السماح بإعطاء التراخيص اللازمة مثل كلمات المرور والتوقيعات الرقمية للوصول إلى الموارد التقنية والأصول المعلوماتية
- سلامة المعلومات وتوافرها: القدرة على حماية المعلومات من أي تعديل أو تخريب أو وصول غير مصرح به وذلك لضمان الوصول للمعلومة الصحيحة والمحافظة على استمراريتها وتقديمها للمستخدمين.

٤. مهارات الأمن السيبراني:

يتضمن الأمن السيبراني العديد من المهارات ذكرها كلا من: (عبد الودود، ٢٠١٨؛ الجندي ومحمد، ٢٠١٩، ٢١؛ Brecht, ٢٠٢١، الصواط، ٢٠٢٢، ٢٦، ٢٧) على النحو التالي:

- مهارة البحث: يعني استخدام محركات البحث بطريقة منهجية صحيحة وذلك من خلال التأكد من عنوان URL إذا كان الموقع يتضمن https فهو آمن وإذا كان http بدون s فيجب الحذر منه.
- مهارة تحليل البيانات: تعني القدرة على اكتساب المعرفة والمهارة بتحليل البيانات الضخمة التي تحتاجها المؤسسة.
- مهارة التحليل الأمني: تعني فحص أنظمة الحاسب الآلي وتحليلها للتنبؤ بالمشكلات الأمنية لتبني بروتكولات أمان أكثر حماية.

- مهارة التعامل مع الأنظمة والتطبيقات: تعني كيفية تشغيل قواعد البيانات وخوادم الويب وصيانة الأنظمة وتحسين أمان التطبيقات.
- مهارة التطوير أثناء التشغيل: تعني التدخل السريع وإكمال المهام الأمنية المعقدة أثناء تشغيل البرنامج.
- مهارة كتابة الأكواد والبرمجة: تعني التعامل بأهم أنظمة وآليات البرمجة والتشفير في مجال الحاسب.
- مهارة تكنولوجيا المعلومات والشبكات: تعني اكتساب المعرفة بكل ما يتعلق بتكنولوجيا المعلومات لفهم كيفية حدوث الهجمات والتقليل منها، والمعرفة بضوابط الأمان لحماية البيانات من التهديدات السيبرانية.
- مهارة تقييم التهديدات: تعني القدرة على تقييم التهديدات واكتشافها والتقليل من خطورتها.
- مهارة التعامل مع الهجمات: تعني التدخل المبكر بإنشاء خطط فعالة للحوادث وإنجاز المهام الأمنية في الوقت المناسب.
- مهارة اختبار الاختراق: تعني استخدم التقنيات لاكتشاف الضعف الأمني للمؤسسات لتحسين إجراءات الأمان.
- مهارة التواصل: تعني التواصل والعمل مع المبرمجين لتطوير تطبيقات وبرمجيات حول الأمن السيبراني.

٥. أبعاد الأمن السيبراني:

للأمن السيبراني عدة أبعاد مختلفة فتشمل الجوانب السياسية، والاقتصادية، والاجتماعية، والإنسانية، وذلك لارتباطه بسلامة البيانات وأمن المعلومات، التي تعتبر ثروة العصر فهي منبع الإنتاج والإبداع والابتكار، وتمكن من التواصل بين الأفراد في مختلف الدول (حمدان، ٢٠٢١، ٢٧).

ويرتبط الأمن السيبراني بأبعاد مختلفة تهدف إلى تحقيق منظومة أمن متكاملة تعمل على حماية الدولة وشعبها وتتمثل تلك الأبعاد فيما أشار إليه (جبور، ٢٠١٦، ٢٦٢؛ الجنفاوي، ٢٠٢١، ٧٨؛ الشايع، ٢٠١٩، ٧٩) على النحو التالي:

- البعد التقني: تتمثل في حماية البنى التحتية والاتصالات والمعلومات والتطبيقات والشبكات من أي عمليات غير مصرح بها.
- البعد السياسي: تقوم على حماية نظام الدولة العسكري والسياسي حيث يمكن أن تستخدم التقنيات في بث معلومات قد يحدث من خلالها تهديدات تؤدي إلى زعزعة أمنها.
- البعد الاقتصادي: تتمثل في مجالين حماية اقتصاد الدولة المعرفي ومجال التجارة الإلكترونية من خلال فتح سوق حر على شبكات الإنترنت.
- البعد القانوني: تقوم على حماية مجتمع المعلومات من الهجمات التي تحدث داخل الفضاء السيبراني وذلك من خلال تنفيذ القوانين والتشريعات.
- البعد الاجتماعي: تتمثل في حماية القيم والمعتقدات الدينية والهوية الثقافية للمجتمع وتوفير سبل الراحة للمواطن في حياته اليومية وتطوير نشاطه في الفضاء السيبراني وذلك من خلال نشر ثقافة الأمن السيبراني.
- البعد التوعوي: تتمثل في التدريب الأمني لبناء مهارات الأمن السيبراني لدى الطلبة وتشجيعهم على الاستخدام الصحيح للإنترنت ودفاعهم عن خصوصياتهم في الفضاء السيبراني.

٦. أبرز المخاطر السيبرانية:

تُعرف المخاطر السيبرانية بانها "عبارة عن أحداث الكترونية محتملة ينتج عنها نتائج غير مرغوب فيها تسبب ضرراً للأنظمة أو للمؤسسة، وقد تنشأ هذه التهديدات داخلياً أو خارجياً ومن الأفراد أو المؤسسات" (بانقا، ٢٠١٩، ١٣)

وتتمثل تلك المخاطر فيما ذكره كلا من: (ذيب القحطاني، ٢٠١٥، ٣٤؛ المنتشري، ٢٠٢٠، ١٠٧، الصواط، ٢٠٢٢، ٢٤، ٢٥) على النحو التالي:

١- المخاطر الداخلية: هي المخاطر الناتجة عن الأخطاء الفنية وعيوب التصميم والتشغيل للبرامج والثغرات في الأجهزة والشبكات وأنظمة أمن المعلومات دون أي تدخل بشري.

٢- المخاطر الخارجية: هي المخاطر الناتجة عن العنصر البشري سواء كان بطريقة مقصودة أو غير مقصودة، وتتمثل فيما يلي:

- مخاطر تستهدف أجهزة الحاسب والهواتف المحمولة: كالبرمجيات الخبيثة والفيروسات وتهديدات الهاتف المحمول التي تؤدي إلى تشفير البيانات أو استبدال المعلومات بأخرى.
- مخاطر تستهدف مستخدمي الإنترنت.
- التشهير الإلكتروني: يعني بث معلومات غير صحيحة عن الأشخاص بهدف إلحاق الضرر الأدبي أو المعنوي بالشخص أو الجهة المقصودة والإساءة إليهم بالتشهير بهم وتختلف طرق التشهير بإنشاء منشور آخر عن هذا الشخص ينشر فيه أخبار ومعلومات غير صحيحة، أو ببث أخبار وفضائح ملفقة، ولا يقتصر التشهير على الأفراد فقط، بل يمكن أن يمتد إلى الأنظمة التعليمية والسياسية والدينية ويكون ذلك من خلال وسائل التواصل الاجتماعي.
- التصيد الإلكتروني: يحدث من خلال استخدام الرسائل الإلكترونية لتظهر كما لو كانت تنتمي إلى جهة رسمية وذلك من خلال خداع الضحية للكشف عن معلوماتهم السرية مثل كلمات السر ومعلومات الحساب المصرفي وغيرها من المعلومات الشخصية.
- التنمر الإلكتروني: يعني الاستهزاء بالأشخاص وإيذائهم بشكل متكرر ومتعمد وذلك من خلال وسائل التواصل الاجتماعي.
- التجسس الإلكتروني: يحدث عن طريق بعض البرامج المتصلة بالإنترنت والتي تكون عادة بشكل مجاني حيث تتضمن برامج لتجسس تبدأ في مراقبة نشاط المستخدم للوصول لمعلوماته السرية.
- الاحتيال الإلكتروني: يحدث من خلال استخدام شخصية أحد المشاهير أو الأقارب للحصول على معلوماته الشخصية.
- الابتزاز الإلكتروني: يعني الحصول على معلومات أو صور إما بالموافقة أو باختراق جهاز الضحية ثم استخدامها ضده مقابل المال.
- الهندسة الاجتماعية: يحدث عن طريق التحايل على الضحية بغرض الحصول على معلومات حساسة، أو إقناع الضحايا بتنفيذ بعض الإجراءات لاختراق أجهزتهم والإضرار بها.
- سرقة كلمات المرور: يحدث عن طريق تخمين كلمة المرور لشخص المستهدف من خلال استخدام تاريخ ميلاده أو أسمة أو رموز يسهل تخمينها.

إضافة لما سبق ترى الدراسة وجود العديد من المخاطر السيبرانية التي قد تؤثر سلبا على المتعلمين تتمثل في دخول المهاجمين إلى المواقع وأنظمة المعلومات بشكل غير مشروع لتدميرها أو التلاعب بالمعلومات وسرقة البحوث العلمية والاختراعات والاعتداء على حقوق المؤلفين وأيضا

الأضرار الصحية التي تنتج عن الاستخدام الدائم للإنترنت وغيرها من المخاطر.

٧. الجرائم والانتهاكات السيبرانيَّة:

في ظلِّ التسهيلات التي تمنحها شبكة الإنترنت، قام البعض باستغلالها في ارتكاب أعمال غير مشروعة لتنفيذ الجرائم السيبرانيَّة cyber Crime كما عرَّفها الفنتوخ (٢٠١٢، ٨٢) بأنها: نشاط إجرامي يستخدم أجهزة الكمبيوتر، أو وسائل الاتصالات الحديثة، كإرسال الفيروسات، وسرقة الأموال، ونشر معلومات سريَّة من أجل الحصول على مكاسب ماديَّة، ولإثبات المهارات الفنيَّة، أو بهدف التسلية، وتكون من أفراد ضد مؤسسات أو شركات، وحتى أفراد داخل وخارج الدولة، ولا يشترط وجودهما في نفس المكان، مما يجعل الجريمة السيبرانيَّة جريمة عابرة للحدود، ويصعب تعقُّبها، أو إيجاد دليل يثبت الجريمة الإلكترونيَّة، والامتناع عن الإبلاغ عنها من قبل المؤسسات تجنبًا لهزِّ ثقة العملاء.

وهناك عدَّة أنواع من الجرائم، منها ما يمسُّ الجانب الوطني: وتكون ضدَّ الدولة وأمنها واستقرارها كالتحريض السياسي أو الاحتيال الاقتصادي والمالي، وتعطيل الأعمال الحكوميَّة، أو العبث بالمعلومات وإخفائها.

الجانب الأخلاقي: جرائم ضدّ الفرد، كالسب والتشهير والابتزاز الإلكتروني، وهي محاولة الحصول على مكاسب ماديَّة بالإكراه، أو إيقاع الضرر الجسدي والمعنوي، من خلال محترفين ومواقع تحتوي على موادَّ خارج حدود الأخلاق والذوق العام (العوادي، ٢٠١٦، ٩٢).

الجانب التجاري: والهدف منها الاطلاع على وثائق ومنتجات الشركات المنافسة، ومحاولة ضرب اقتصاد الشركات.

الحروب السيبرانيَّة: ووفق دراسة نعمة وكلنتر (٢٠٢٠، ٦٤)) يتَّضح أن هناك فرقًا بين الجريمة السيبرانيَّة والحرب السيبرانيَّة كما تسمى الهجمات السيبرانيَّة، وتعني التسلل إلى مواقع إلكترونيَّة حساسة غير مرخَّص الدخول إليها من أجل الحصول على مزايا اقتصاديَّة أو سياسيَّة، حيث تقوم بها دولة ضدَّ دولة أخرى، بهدف التأثير والإضرار بنظم المعلومات، وإرباك كامل للأنظمة المدنيَّة والعسكريَّة، واختراق الأنظمة المصرفيَّة، وتخريب الشبكات التي تتحكَّم بالبنية التحتيَّة الأساسيَّة في الدولة، وشلِّ حركة الطيران ومحطات الوقود والكهرباء والمياه، وغيرها من المنشآت الحيويَّة.

٨. متطلبات تعزيز الوعي بالأمن السيبراني:

لتنمية الأمن السيبراني وتعزيزه توجد العديد من الإجراءات التي تتخذها العديد من مؤسسات المجتمع، ولكن هنا سنسلط الضوء على الإجراءات التي تقدم من قبل الإدارات التعليمية بمستوياتها المختلفة كما أوضحتها المنتشري (٢٠٢٠، ١١١) ومنها ما يلي:

- أن تضع خطط للتوعية بالأمن السيبراني على مستوى المدارس بشكل عام، وتقوم بالتحذير من المخاطر السيبرانية، وتشمل جميع المعلمين والطلبة.
- تعميم سياسات واضحة للتعامل مع التكنولوجيا، وتشمل الأمن السيبراني، والتأكد من تطبيقها في جميع المدارس، والإشراف على ذلك من قبل الجهات المختصة كوزارة التعليم.
- وجود خطة عمل محددة وواضحة لدى المدرسة للتعامل مع الأخطار والانتهاكات السيبرانية.
- عقد دورات تدريبية للمعلمين لتوعيتهم بالإجراءات التي تمكن الطلاب والأطفال من اتباعها عند تعرضهم ووقوعهم كضحايا للمخاطر السيبرانية.

- اعتبار الوعي بالأمن السيبراني من المهارات اللازمة في الحياة، وإتاحته في القضايا المثارة أثناء التدريس، وكذلك في الأنشطة المدرسية.
- إدراج موضوع الأمن السيبراني ضمن أدلة المعلمين.

ومن هنا يبرز أهمية وعي المعلمين بشكل عام بمفهوم الأمن السيبراني وإجراءاته لحماية أنفسهم وتوعية طلابهم ومن ثم القيام بدورهم الفعال في تقليل الجرائم الالكترونية إلى أقصى حد ممكن في المجتمع (صائغ، ٢٠١٨، ٥١)، بالإضافة لقدرتهم على تعزيزه لدى طلابهم.

منهجية الدراسة وإجراءاتها:

منهج الدراسة: استخدمت الدراسة المنهج الوصفي باعتباره الأنسب لوصف وتشخيص واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم واستطلاع رأيهم حول السبل المقترحة لتعميقه.

مجتمع الدراسة: يتكون مجتمع الدراسة من معلمي ومعلمات المرحلة الثانوية العامة بمحافظات (القاهرة/ الغربية/ المنيا).

عينة الدراسة: اقتصرت الدراسة على عينة بلغت (٤١٧) معلماً ومعلمة بالمرحلة الثانوية موزعين وفق متغيرات النوع (ذكور/ إناث) والتخصص (تكنولوجيا معلومات/ لغوي/ ثقافي) والمؤهل (تربوي/ غير تربوي)، ويوضح الجدول التالي توزيع العينة وفق متغيراتها.

جدول (١) يوضح توزيع أفراد العينة حسب النوع، والمؤهل، والتخصص، والمحافظة

المتغير		التكرار	النسبة المئوية
النوع	ذكور	210	50.4
	إناث	207	49.6
المؤهل	تربوي	375	89.9
	غير تربوي	42	10.1
التخصص	تكنولوجيا معلومات	36	8.6
	لغوي	187	44.8
	ثقافي	194	46.5
المحافظة	القاهرة	153	36.7
	الغربية	137	32.9
	المنيا	127	30.5
المجموع		417	100

أداة الدراسة: استخدمت الدراسة استبانة من إعداد الباحث تم بناؤها في ضوء الإطار النظري والدراسات السابقة بالإضافة للاستعانة بآراء الخبراء والمتخصصين في المجال، وتكونت الاستبانة من محورين، شمل المحور الأول العبارات التي تقيس واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم، وشمل المحور الثاني العبارات التي تتضمن السبل المقترحة لتعميق دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم، وتكون كل محور من (٢٠) عبارة، وأمام كل عبارة تدرج ثلاثي يعبر عن درجة الموافقة بحيث تتراوح ما بين مرتفعة وتعطى (٣) درجات، ومتوسطة وتعطى (٢) درجتان، ومنخفضة وتعطى (١) درجة واحدة فقط، وتتراوح الدرجات على كل محور ما بين (٢٠) إلى (٦٠) درجة بينما تتراوح على الاستبانة مجملة ما بين

(٤٠) إلى (١٢٠) درجة، وتدل الدرجة المرتفعة على وجود واقع قوي ومرتفع من تعزيز معلمي المرحلة الثانوية للوعي بالأمن السيبراني لدى طلابهم وكذلك موافقة قوية ومرتفعة على السبل المقترحة لتعميقه، بينما تدل الدرجة المنخفضة على العكس.

صدق أداة الدراسة:

١- صدق المحكمين: للتحقق من صدق الاستبانة تم عرض الاستبانة على (٨) من المحكمين ذوى الاختصاص والخبرة من أعضاء هيئة التدريس في مجال أصول التربية وعلم النفس التعليمي للقيام بتحكيمها، وقد طلب منهم إبداء آرائهم وملاحظاتهم حول الاستبانة وفقراتها، وكذلك من حيث ترابط كل فقرة بالمحور التي تندرج تحته، ومدى وضوح الفقرة وسلامة صياغتها؛ وذلك بتعديل الفقرات أو حذف غير المناسب منها أو إضافة ما يرونه مناسبًا من فقرات، وبناء على التعديلات والمقترحات التي أبداها المحكمون، قام الباحث بإجراء التعديلات اللازمة التي اتفق عليها غالبية المحكمين والتي بلغت نسبة الاتفاق عليها (٩٠%) فأكثر، من تعديل بعض الفقرات وحذف وإضافة عبارات أخرى، حتى استقرت الاستبانة على صورتها الحالية مكونة من(٤٠) عبارة على محورين لكل محور (٢٠) عبارة.

٢- الصدق الذاتي: بعد تحكيم الاستبانة والالتزام بتعديلات السادة المحكمين تم تطبيق الاستبانة على عينة استطلاعية بلغت (٦٠) معلمًا من معلمي المرحلة الثانوية العامة، وبعد تفريغ الاستبانات وتبويبها، تم حساب الصدق الذاتي باستخدام حساب معامل (ارتباط بيرسون) بين درجة كل محور والدرجة الكلية للاستبانة، وكانت درجة الاتساق الداخلي كما بالجدول التالي:

جدول (١) يوضح معامل الارتباط بين درجة كل محوروالدرجة الكلية للاستبانة(ن=٦٠)

المحور	معامل الارتباط
1	0.805**
2	0.816**

** دال عند مستوى ٠,٠١

يتضح من الجدول (١) أن معاملات الارتباط للدرجة الكلية للمحوري الاستبانة مع الدرجة الكلية للاستبانة موجبة وقوية وتراوحت ما بين(٠,٨٠٥) إلى(٠,٨١٦), وهما قيمتان دالتان إحصائياً عند مستوى (٠,٠١). مما يدل على قوة ارتباط المحورين والاستبانة وهو ما يؤكد صدق الاستبانة، وبذلك أصبحت الاستبانة تتمتع بدرجة عالية من الاتساق الداخلي.

ثبات أداة الدراسة: اعتمد الباحث في حساب ثبات الاستبانة على طريقتي معامل الفا كرونباخ والتجزئة النصفية وذلك بعد التطبيق على العينة الأساسية، ويتضح ذلك من خلال الجدول التالي:

جدول (٢) معاملات الثبات لإجمالي الاستبانة(ن=٦٠)

المحور	عدد عبارات المحور	معامل الفا كرونباخ	التجزئة النصفية	
			الارتباط بين نصفى للمقياس	معامل الثبات بعد التصحيحGuttman
الأول	٢٠	٠,٨٣٩	٠,٨٠٢	٠,٨١٥
الثاني	٢٠	٠,٨٢٠	٠,٨٠٤	٠,٨١٨

المحور	عدد عبارات المحور	معامل الفا كرونباخ	التجزئة النصفية	
			الارتباط بين نصفى للمقياس	معامل الثبات بعد التصحيحGuttman
مجموع الاستبانة	٤٠	٠,٩٢٩	٠,٨٤٢	٠,٨٦٧

يتضح من الجدول (٢) أن قيمة معامل ألفا كرونباخ لثبات الاستبانة قد بلغت (٠,٩٢٩) مرتفعة، حيث تراوحت القيم على المحورين ما بين(٠,٨٢٠- ٠,٨٣٩) وهي قيم مرتفعة، كما بلغ معامل الثبات بعد التصحيح لGuttman (٠,٨٦٧)، وتراوحت القيم على المحورين (٠,٨١٥- ٠,٨١٨)، مما يشير إلى الثبات المرتفع للاستبانة، ويمكن أن يكون ذلك مؤشرًا جيدًا لتعميم نتائجها.

تصحيح الاستبانة:

تعطى الاستجابة(مرتفعة) الدرجة(٣)، والاستجابة (متوسطة) تعطي الدرجة (٢)، والاستجابة (منخفضة) تعطي الدرجة (١)، وقد تحدد مستوى الموافقة لدى عينة الدراسة التي يمكن من خلالها الحكم على الموافقة من حيث كونها مرتفعة، أم متوسطة، أم منخفضة من خلال الجدول التالي:

جدول (٣) يوضح مستوى المو افقة لدى عينة الدراسة

مستوى المو افقة	المدى
منخفضة	من ١وحتى (١ + ٠,٦٦) أي ١,٦٦
متوسطة	من ١,٦٧وحتى (١,٦٧ + ٠,٦٦) أي ٢,٣٣
مرتفعة	من ٢,٣٤وحتى (٢,٣٤ + ٠,٦٦) أي ٣

الأساليب الإحصائية المستخدمة في الدراسة:

بعد تطبيق الاستبانة وتجميعها، تم تفريغها في جداول لحصر التكرارات ولمعالجة بياناتها إحصائيًا من خلال برنامج الحزم الإحصائية (SPSS) Statistical Package for Social Sciences الإصدار الخامس والعشرين. وقد استخدم الباحث مجموعة من الأساليب الإحصائية التي تستهدف القيام بعملية التحليل الوصفي والاستدلالي لعبارات الاستبانة، وهي: معامل ارتباط بيرسون، والنسب المئوية في حساب التكرارات، والمتوسطات الحسابية والانحرافات المعيارية واختبار التاء لعينتين مستقلتين (t – test Independent Simple)، واختبار تحليل التباين أحادي الاتجاه (One Way ANOVA)، واختبار LSD للمقارنات الثنائية البعدية.

نتائج الدراسة وتفسيرها ومناقشتها:

نتائج الإجابة عن السؤال الأول الذي نص على ما يلي: ما واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم؟

للإجابة عن هذا السؤال تم حساب الأوزان النسبية والانحرافات المعيارية. والرتبة لكل عبارة، كما بالجدول الآتي:

جدول (٤) الوزن النسبي ومستوى المو افقة على المحور الأول الخاص بالكشف عن و اقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبر اني لدى طلابهم من وجهة نظرهم(ن=٤١٧)

م	العبارة	الوزن النسبي	الانحراف المعياري	الرتبة	مستوى المو افقة

م	العبارة	الوزن النسبي	الانحراف المعياري	الترتيب	مستوى الموافقة
١٧	أعرف طلابي بالحقوق وقوانين حماية المستهلك عبر شبكة الإنترنت	٢,٢٤٩٤	٠,٧٤٠٤	٣	متوسطة
١٩	أدرب طلابي على كيفية الالتزام بالقوانين والمعايير المنظمة لاستخدام شبكة الإنترنت	٢,٢١٨٢	٠,٨٣٣٧	٤	متوسطة
١٤	أحذر طلابي من انتحال الشخصيات عبر شبكة الإنترنت	٢,٢٠١٤	٠,٨٧٠٣	٥	متوسطة
١	أحذر الطلاب من التعامل مع المواقع المجهولة عبر شبكة الإنترنت	٢,١٩٦٦	٠,٨٥١٩	٦	متوسطة
٨	أوعي طلابي بحقوق الملكية الفكرية وكيفية الحفاظ عليها عبر الإنترنت	٢,١٦٧٩	٠,٨٦٦٤	٧	متوسطة
٩	أدرب طلابي على كيفية استخدام البرامج الأكثر أماناً عبر شبكة الإنترنت	٢,١٦٠٧	٠,٩٤٣٤	٨	متوسطة
١٢	أحذر طلابي من الإفصاح عن بياناتهم الشخصية لأي جهة غير موثقة لديهم عبر شبكة الإنترنت	٢,١٥٨٣	٠,٩٥٠١	٩	متوسطة
٥	أكسب طلابي مهارات الحفاظ على بياناتهم وحساباتهم الشخصية عبر الإنترنت	٢,١٣٩١	٠,٨٥٤٨	١٠	متوسطة
٤	أوعي طلاب بكيفية حماية أنفسهم من الابتزاز الإلكتروني	٢,١٣١٩	٠,٩٤٠٢	١١	متوسطة
٧	أوعي طلاب بكيفية تشفير المواقع التي تروج لأفكار وممارسات غير أخلاقية	٢,١١٧٥	٠,٩٣٤٤	١٢	متوسطة
١٨	أوعي طلابي بجرائم الاحتيال الاقتصادي عبر شبكة الإنترنت وكيفية حماية أنفسهم منها	٢,٠٩٥٩	٠,٨١٧٧	١٣	متوسطة
٢٠	أوعي طلابي بضرورة الفحص المستمر لأجهزتهم الإلكترونية لاكتشاف الأخطاء أو التهديدات السيبرانية والتعامل معها مبكراً	١,٩٦٦٤	٠,٨٨١٩	١٤	متوسطة
١١	أدرب طلابي على كيفية اكتشاف حالات التجسس الإلكتروني عند التعرض لها وكيفية وقاية أنفسهم منها	١,٦٩٣٠	٠,٨٥٣٠	١٥	متوسطة
١٣	أدرب طلابي على استخدام محركات البحث بطريقة منهجية صحيحة وذلك من خلال التأكد من عنوان **URL** إذا كان الموقع يتضمن **https** فهو آمن وإذا كان **http** بدون **s** فيجب الحذر منه	١,٥٨٥١	٠,٧٩٢٤	١٦	منخفضة
١٦	أدرب طلابي على التواصل الإيجابي الفعال عبر شبكة الإنترنت	١,٥٧٠٧	٠,٨٤٩٤	١٧	منخفضة
٦	أدرب طلاب على كيفية حماية أجهزتهم الإلكترونية من الهجمات الفيروسية	١,٥٦٨٣	٠,٨٦٩٢	١٨	منخفضة
١٠	أعرف طلابي بالإجراءات القانونية التي ينبغي عليهم اتباعها عند التعرض لمخاطر سيبرانية	١,٥٢٠٤	٠,٨٤٣٦	١٩	منخفضة
٢	أدرب طلاب على كيفية وقاية أنفسهم من التحرش	١,٥٠٨٤	٠,٨٥٢٣	٢٠	منخفضة

م	العبارة	الوزن النسبي	الانحراف المعياري	الرتبة	مستوى الموافقة
إجمالي المحور	الجنسي عبر الإنترنت مجموع الأوزان النسبية (٣٩,٧٨)	متوسط الأوزان النسبية (١,٩٨٩٠)	النسبة المئوية (٦٦,٣٠)		متوسطة

يوضح الجدول السابق نتائج المحور الأول الخاص بالكشف عن واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم، وذلك في ضوء التوزيع الإحصائي وفقًا للوزن النسبي ومستوى الموافقة على العبارة والرتبة، حيث يشير الجدول إلى أن واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم جاء متوسطاً، حيث بلغ مجموع الأوزان النسبية (٣٩,٧٨)، وبلغ متوسط الأوزان النسبية (١,٩٨٩٠)، وجاءت النسبة المئوية (٦٦,٣٠).

تشير النتيجة السابقة إلى أن معلمي المرحلة الثانوية يؤدون بعض الممارسات لتعزيز وعي طلابهم بالأمن السيبراني، ولكن هذه الممارسات بحاجة لتطوير حيث إن مستواها جاء متوسطاً، ولعل هذا يمكن عزوه لضعف وعي بعض المعلمين بمفاهيم الأمن السيبراني ومتطلبات تعزيزه خاصة من غير المتخصصين في مجال تكنولوجيا التعليم، يضاف لما سبق أن المعلمين في الغالب يكون جهدهم مركز فيما يتعلق بالبرامج والمقررات الدراسية باعتبارهم المهمة الأهم بالنسبة لهم وينظرون لما عداها على أنها مهام ثانوية، يضاف لما سبق تعدد الضغوط والمهام المنوطة بالمعلمين والتي قد تشغلهم عن أداء هذا الدور بدرجة مرتفعة.

ويدعم النتيجة السابقة ما أكدته نتائج دراسة (قطب، ٢٠٢١) التي توصلت إلى أن زيادة نسبة الجرائم السيبرانية نتيجة للقصور في تعزيز الوعي بالأمن السيبراني.

كما تأتي النتيجة السابقة مدعومة بما أشارت إليه دراسة السواط، والصانع، وأبوعيشة وسليمان (٢٠٢٠)، ودراسة O'Brien (2019) إلى افتقار الطلاب إلى أساسيات الأمن السيبراني، وقد أكَّد ذلك ما توصلت إليه الدِّراسَات السابقة من نتائج، وما قدمته من توصيات، كما في دراسة Mangold(2016) التي أكَّدت وجود ضعف في الوعي بمفاهيم الأمن السيبراني، وضرورة إكساب الطلاب الوعي بتلك المفاهيم، من خلال الدورات التدريبيَّة، والمعسكرات السيبرانيَّة، وأكدت نتائج دراسة Sadaghiani (2018) ضرورة مراقبة الطلاب عبر الإنترنت، والتوعية بمخاطر الفضاء السيبراني، وتعليم الطلاب الممارسات الصحيحة، وأكدت دراسة السعيد (٢٠٢٠) عددًا من التوصيات، منها: زيادة التدريب العملي على مهارات الاستخدام الآمن للكمبيوتر والإنترنت، والوعي بأخلاقيات وآداب السلوك الرقمي.

وفيما يتعلق بترتيب العبارات يتضح ما يلي:

- أكثر العبارات التي تعكس واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم، جاءت في الترتيب الأول: أُدرب طلابي على كيفية التميز بين الحقيقة والإشاعة عبر شبكة الإنترنت، بوزن نسبي(٢,٢٧٥٨) وهي درجة متوسطة.
- وجاء في الترتيب الثاني: أُكسب طلابي مهارات الوقاية من التنمر الإلكتروني، بوزن نسبي(٢,٢٥٤٢) وهي درجة متوسطة.
- وجاء في الترتيب الثالث: أُعرف طلابي بالحقوق وقوانين حماية المستهلك عبر شبكة الإنترنت، بوزن نسبي(٢,٢٤٩٤) وهي درجة متوسطة.
- وجاء في الترتيب الرابع: أُدرب طلابي على كيفية الالتزام بالقوانين والمعايير المنظمة لاستخدام

شبكة الإنترنت، بوزن نسبي(٢,٢١٨٢) وهي درجة متوسطة.

- وجاء في الترتيب الخامس: أُحذر طلابي من انتحال الشخصيات عبر شبكة الإنترنت، بوزن نسبي(٢,٢٠١٤) وهي درجة متوسطة.

في حين كانت أقل العبارات التي تعكس واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم، جاءت في الترتيب العشرين: أُدرب طلاب على كيفية وقاية أنفسهم من التحرش الجنسي عبر الإنترنت، بوزن نسبي (١,٥٠٨٤) وهي درجة منخفضة.

- وجاء في الترتيب التاسع عشر: أُعرف طلابي بالإجراءات القانونية التي ينبغي عليهم اتباعها عند التعرض لمخاطر سيبرانية، بوزن نسبي(١,٥٢٠٤) وهي درجة منخفضة.
- وجاء في الترتيب الثامن عشر: أُدرب الطلاب على كيفية حماية أجهزتهم الإلكترونية من الهجمات الفيروسية، بوزن نسبي (١,٥٦٨٣) وهي درجة منخفضة.
- وجاء في الترتيب السابع عشر: أُدرب طلابي على التواصل الإيجابي الفعال عبر شبكة الإنترنت، بوزن نسبي (١,٥٧٠٧) وهي درجة منخفضة.
- وجاء في الترتيب السادس عشر: أُدرب طلابي على استخدام محركات البحث بطريقة منهجية صحيحة وذلك من خلال التأكد من عنوان URL إذا كان الموقع يتضمن https فهو آمن وإذا كان http بدون s فيجب الحذر منه، بوزن نسبي (١,٥٨٥١) وهي درجة منخفضة.

نتائج الإجابة عن السؤال الثاني الذي نص على ما يلي: ما السبل المقترحة لتعميق واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم؟

للإجابة عن هذا السؤال تم حساب الأوزان النسبية والانحرافات المعيارية. والرتبة لكل عبارة، كما بالجدول الآتي:

جدول (٥) الوزن النسبي ومستوى المو افقة على المحور الثاني الخاص بالسبل المقترحة لتعميق و اقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبر اني لدى طلابهم من وجهة نظرهم(ن=٤١٧)

م	العبارة	الوزن النسبي	الانحراف المعياري	الرتبة	مستوى المو افقة
٣٥	استطلاع آراء المعلمين حول احتياجاتهم لتعزيز وعي طلابهم بالأمن السيبراني والعمل على تلبيتها	٢,٨١٢٩	٠,٤٣٦٩	٣	مرتفعة
٣٣	عرض نماذج توضيحية لمخاطر غياب الأمن السيبراني يتم تعميمها على المعلمين والطلاب	٢,٧٦٧٤	٠,٤٢٨٧	٤	مرتفعة
٢٩	التقويم المستمر لأداء المعلم بوجه عام وفيما يتعلق بتعزيز وعي طلابه بالأمن السيبراني بوجه خاصة لاكتشاف نقاط القوة والعمل على تعزيزها ونقاط الضعف والعمل على الحد منها	٢,٧٤٥٨	٠,٦٠٢٦	٥	مرتفعة
٣٠	توفير دليل إرشادي شامل لدور المعلم في تعزيز وعي طلابه بالأمن السيبراني يتاح لكل	٢,٧١٢٢	٠,٦١٥٢	٦	مرتفعة

م	العبارة	الوزن النسبي	الانحراف المعياري	الترتيب	مستوى الموافقة
	المعلمين				
٢٨	تزويد المعلم بالأدوات والتجهيزات التي تساعده في تعزيز وعي طلابه بالأمن السيبراني	٢,٦٦١٩	٠,٥٣٥٦	٧	مرتفعة
٢٥	وضع خطط للتوعية بالأمن السيبراني على مستوى المدارس بشكل عام	٢,٦٤٩٩	٠,٦٣٣٤	٨	مرتفعة
٣٤	منح المعلمين مزيداً من الصلاحيات والتفويضات التي تعمق من دورهم في تعزيز وعي طلابهم بالأمن السيبراني	٢,٦٤٢٧	٠,٥١٨٣	٩	مرتفعة
٢٧	تخصيص جزء من البرنامج اليومي بالمدرسة للتوعية بالمفاهيم المستجدة ومنها الأمن السيبراني	٢,٦٣٣١	٠,٦٣٧١	١٠	مرتفعة
٣١	تكريم المعلمين المتميزين في تعزيز وعي طلابهم بالأمن السيبراني	٢,٦٣٠٧	٠,٧١٢٤	١١	مرتفعة
٣٨	التوسع في عمل مشروعات بحثية تتعلق بالأمن السيبراني وكيفية وقاية الطلاب منه على مستوى المدرسة	٢,٦٠٦٧	٠,٥٢٢٣	١٢	مرتفعة
٢٦	تضمين مفاهيم الأمن السيبراني ضمن البرامج والمقررات الدراسية	٢,٥٧٥٥	٠,٦٤٦٥	١٣	مرتفعة
٤٠	إشراك المعلمين والطلاب مع الإدارة في صنع واتخاذ القرارات الخاصة بالأمن السيبراني وكيفية تعزيزه	٢,٥٤٩٢	٠,٧٢٢٦	١٤	مرتفعة
٢١	تدريب وتأهيل المعلمين على أيدي خبراء الأمن السيبراني لاكتساب المهارات المتطلبة ليقوموا بدورهم في تعزيز وعي طلابهم بالأمن السيبراني	٢,٥٣٢٤	٠,٧٢٣٦	١٥	مرتفعة
٢٢	عقد دورات تدريبية للمعلمين لتوعيتهم باحتياجات الطلاب لتعزيز وعيهم بالأمن السيبراني	٢,٤٩٤٠	٠,٧٢٤٣	١٦	مرتفعة
٢٤	تواصل المعلمين مع أولياء الأمور من أجل الاشتراك معاً في تعزيز وعي الطلاب بالأمن السيبراني	٢,٢٩٥٠	٠,٦٨٧٧	١٧	متوسطة
٣٢	تنفيذ أنشطة عملية بمشاركة المعلمين وخبراء التكنولوجيا لتدريب الطلاب على اكتساب مهارات الأمن السيبراني	٢,٢٨٧٨	٠,٧١٣٠	١٨	متوسطة
٣٩	تبادل الخبرات بين مختلف المدارس والإدارات التعليمية في مجال تعزيز الوعي	٢,٢٨٠٦	٠,٧٠٠٦	١٩	متوسطة

م	العبارة	الوزن النسبي	الانحراف المعياري	الرتبة	مستوى الموافقة
٢٣	دعم الإدارة لدور المعلمين في تعزيز وعي طلابهم بالأمن السيبراني بالأمن السيبراني لدى الطلاب	٢,٢١١٠	٠,٥٦٦٣	٢٠	متوسطة
إجمالي المحور	مجموع الأوزان النسبية (٥١,٧٥)	متوسط الأوزان النسبية (٢,٥٨٧٤)	النسبة المئوية (٨٦,٢٥)		مرتفعة

يشير الجدول السابق إلى أن موافقة أفراد عينة الدراسة على السبل المقترحة لتعميق واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم جاءت مرتفعة، حيث بلغ مجموع الأوزان النسبية (٥١,٧٥)، وبلغ متوسط الأوزان النسبية (٢,٥٨٧٤)، وجاءت النسبة المئوية (٨٦,٢٥).

ويمكن عزو النتيجة السابقة لكون السبل التي تم اقتراحها لتعميق واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم تم بناؤها وصياغتها في ضوء ما أشارت إليه الأدبيات التربوية والدراسات السابقة ذات الصلة بالموضوع، بالإضافة للاسترشاد بآراء الخبراء والمتخصصين في المجال، كما أنه تم مراعاة التنوع والشمول في هذه المقترحات بحيث تغطي جميع الأبعاد المتطلبة للوعي بالأمن السيبراني، وتناسب طبيعة المرحلة التعليمية، بجانب مراعاتها لتكاتف جميع الجهود لمساعدة المعلمين في تعزيز وعي طلابهم بالأمن السيبراني.

وتتفق هذه النتيجة مع ما أشارت إليه دراسة المنتشري (٢٠٢١) التي أكدت أنه لتنمية الأمن السيبراني وتعزيزه توجد العديد من الإجراءات التي تتخذها العديد من مؤسسات المجتمع، ومنها يلي: أن تضع خطط للتوعية بالأمن السيبراني على مستوى المدارس بشكل عام، وتقوم بالتحذير من المخاطر السيبرانية، وتشمل جميع المعلمين والطلبة، تعميم سياسات واضحة للتعامل مع التكنولوجيا، وتشمل الأمن السيبراني، والتأكد من تطبيقها في جميع المدارس، والإشراف على ذلك من قبل الجهات المختصة كوزارة التعليم، وجود خطة عمل محددة وواضحة لدى المدرسة للتعامل مع الأخطار والانتهاكات السيبرانية، عقد دورات تدريبية للمعلمين لتوعيتهم بالإجراءات التي تمكن الطلاب والأطفال من اتباعها عند تعرضهم ووقوعهم كضحايا للمخاطر السيبرانية، اعتبار الوعي بالأمن السيبراني من المهارات اللازمة في الحياة، وإتاحته في القضايا المثارة أثناء التدريس، وكذلك في الأنشطة المدرسية، إدراج موضوع الأمن السيبراني ضمن أدلة المعلمين.

وفيما يتعلق بترتيب العبارات يتضح ما يلي:

- أكثر العبارات التي تعكس السبل المقترحة لتعميق واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم، جاءت في الترتيب الأول: جعل تعزيز الوعي بالأمن السيبراني ضمن المهام الرسمية التي يكلف بها المعلمون، بوزن نسبي(٢,٨٣٢١) وهي درجة مرتفعة.
- وجاء في الترتيب الثاني: تحليل الواقع لتحديد نقاط القوة والضعف والفرص والتهديدات والانطلاق من ذلك في تعميق دور المعلمين في تعزيز وعي طلابهم بالأمن السيبراني، بوزن نسبي(٢,٨٢٧٣) وهي درجة مرتفعة.
- وجاء في الترتيب الثالث: استطلاع آراء المعلمين حول احتياجاتهم لتعزيز وعي طلابهم بالأمن السيبراني والعمل على تلبيتها، بوزن نسبي(٢,٨١٢٩) وهي درجة مرتفعة.

- وجاء في الترتيب الرابع: عرض نماذج توضيحية لمخاطر غياب الأمن السيبراني يتم تعميمها على المعلمين والطلاب، بوزن نسبي(٢,٧٦٧٤) وهي درجة مرتفعة.
- وجاء في الترتيب الخامس: التقويم المستمر لأداء المعلم بوجه عام وفيما يتعلق بتعزيز وعي طلابه بالأمن السيبراني بوجه خاصة لاكتشاف نقاط القوة والعمل على تعزيزها ونقاط الضعف والعمل على الحد منها، بوزن نسبي(٢,٧٤٥٨) وهي درجة مرتفعة.

في حين كانت أقل العبارات التي تعكس السبل المقترحة لتعميق واقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم من وجهة نظرهم، جاءت في الترتيب العشرين: دعم الإدارة لدور المعلمين في تعزيز وعي طلابهم بالأمن السيبراني، بوزن نسبي (٢,٢١١٠) وهي درجة متوسطة.

- وجاء في الترتيب التاسع عشر: تبادل الخبرات بين مختلف المدارس والإدارات التعليمية في مجال تعزيز الوعي بالأمن السيبراني لدى الطلاب، بوزن نسبي(٢,٢٨٠٦) وهي درجة منخفضة.
- وجاء في الترتيب الثامن عشر: تنفيذ أنشطة عملية بمشاركة المعلمين وخبراء التكنولوجيا لتدريب الطلاب على اكتساب مهارات الأمن السيبراني، بوزن نسبي (٢,٢٨٧٨) وهي درجة منخفضة.
- وجاء في الترتيب السابع عشر: تواصل المعلمين مع أولياء الأمور من أجل الاشتراك معاً في تعزيز وعي الطلاب بالأمن السيبراني، بوزن نسبي (٢,٢٩٥) وهي درجة منخفضة.
- وجاء في الترتيب السادس عشر: عقد دورات تدريبية للمعلمين لتوعيتهم باحتياجات الطلاب لتعزيز وعيهم بالأمن السيبراني، بوزن نسبي (٢,٤٩٤٠) وهي درجة مرتفعة.

نتائج الإجابة عن السؤال الثالث الذي نص على ما يلي: ما مدى تأثير متغيرات النوع (ذكور/ إناث) والمؤهل (تربوي/ غير تربوي) والتخصص (تكنولوجيا معلومات/ ثقافي/ لغوي) في رؤية عينة الدراسة لواقع دور معلمي المرحلة الثانوية في تعزيز الوعي بالأمن السيبراني لدى طلابهم والسبل المقترحة لتعميقه؟

للإجابة عن هذا السؤال تم استخدام اختبار ت في حالة متغير النوع والمؤهل، واختبار تحليل التباين أحادي الاتجاه في حالة متغير التخصص، والجداول التالية تبين ذلك:

أولاً: الفروق على محوري الاستبانة بحسب النوع (ذكور/ إناث):

جدول (٦) يوضح الفروق بين أفراد العينة بحسب متغير النوع باستخدام اختبار التاء لعينتين مستقلتين t – test.

المحور	النوع	ن	المتوسط	الانحراف المعياري	قيمة التاء	مستوى الدلالة
المحور الأول	ذكور	٢١٠	٣٨,٦٥	١٢,٦٦	١,٧٨٥-	٠,٠٧٥
	إناث	٢٠٧	٤٠,٩٢	١٣,٣٠		غير دالة
المحور الثاني	ذكور	٢١٠	٥١,٤٤	٨,٢٧	٧٧٤.-	٠,٤٣٩
	إناث	٢٠٧	٥٢,٠٦	٨,٢٠		غير دالة

يتضح من الجدول (٦) عدم وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة من معلمي المرحلة الثانوية العامة على محوري الاستبانة الأول والثاني تبعًا لمتغير النوع (ذكور/ إناث)، حيث جاءت قيمة (ت) للمحورين غير دالة إحصائيًا عند مستوى دلالة (٠,٠٥). ويمكن تفسير ذلك في ضوء أن معلمي ومعلمات المرحلة الثانوية يعملون في بيئة تعليمية متشابهة

ويدرسون نفس البرامج والمقررات الدراسية، وتتاح لهم نفس الظروف والإمكانات، ويعملون وفق لوائح وقوانين واحدة، ولديهم نفس المؤهلات والإمكانات، وبالتالي جاءت رؤيتهم متشابهة دون وجود فروق دالة إحصائياً في رؤيتهم لواقع دور معلمي المرحلة الثانوية في تعزيز وعي طلابهم بالأمن السيبراني ومتطبات تعميقه.

وتتفق هذه النتيجة مع دراسة الصواط (٢٠٢٢) التي توصلت لعدم وجود فروق دالة إحصائياً في استجابات عينتها حول استخدامهم منصات التعلم الإلكترونية والوعي بالأمن السيبراني تعزى لمتغير النوع.

ثانياً: الفروق على محوري الاستبانة بحسب المؤهل (تربوي/ غير تربوي):

جدول (٧) يوضح الفروق بين أفراد العينة بحسب متغير المؤهل باستخدام اختبار التاء لعينتين مستقلتين t – test.

المحور	المؤهل	ن	المتوسط	الانحراف المعياري	قيمة "ت"	مستوى الدلالة
المحور الأول	تربوي	٣٧٥	٤٠,٦٥	١٢,٥٢	٤,١٧٧	٠,٠٠٠١ دالة
	غير تربوي	٤٢	٣١,٩٨	١٤,٨٠		
المحور الثاني	تربوي	٣٧٥	٥٣,١٧	٦,١٨	١٢,٣٠١	٠,٠٠٠١ دالة
	غير تربوي	٤٢	٣٩,٠٥	١٢,٤٩		

يتضح من الجدول (٧) وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة من معلمي المرحلة الثانوية العامة على محوري الاستبانة الأول والثاني تبعًا لمتغير المؤهل (تربوي/ غير تربوي)، حيث جاءت قيمة (ت) للمحورين دالة إحصائيًا عند مستوى دلالة (٠,٠٥)، وجاءت الفروق لصالح الحاصلين على مؤهل تربوي. ويمكن تفسير ذلك في ضوء عامل الخبرة الذي يتمتع به ذوي التأهيل التربوي بحكم أن الدراسة التربوية تمكنهم من اكتساب العديد من المهارات والكفايات التدريسية التي تعمق من ممارساتهم المهنية مع طلابهم وتعمق من تمكنهم من ممارسة العديد من الأدوار ومنها دورهم في تعزيز وعي طلابهم بالأمن السيبراني، وكذلك رؤيتهم لمقترحات تعميقه.

ثالثاً: الفروق على محوري الاستبانة بحسب التخصص (ثقافي/ تكنولوجيا ومعلومات/ لغوي)

جدول (٨) يوضح نتائج اختبار تحليل التباين أحادي الاتجاه لإظهار دلالة الفروق بين استجابات أفراد العينة المستفتاة نحو مدى الموافقة على محوري الاستبانة حسب متغير التخصص

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة "ف"	مستوى الدلالة
الأول	بين المجموعات	١٣٧٢٤,٠٣٧	٢	٦٨٦٢,٠١٩	٥٠,٠٥١	٠,٠٠٠١ دالة
	داخل المجموعات	٥٦٧٥٩,٦٦٥	٤١٤	١٣٧,١٠١		
	المجموع	٧٠٤٨٣,٧٠٣	٤١٦			
الثاني	بين المجموعات	٢٨٥٤,٥٩٣	٢	١٤٢٧,٢٩٦	٢٣,٣١٧	٠,٠٠٠١ دالة
	داخل	٢٥٣٤١,٩٦٨	٤١٤	٦١,٢١٢		

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة "ف)	مستوى الدلالة
	المجموعات					
	المجموع	٢٨١٩٦,٥٦١	٤١٦			

يتضح من الجدول (٨) وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة من معلمي المرحلة الثانوية العامة تبعًا للتخصص حيث بلغت قيمة الفاء، بالنسبة لمحوري الاستبانة، (٥٠,٠٥١)، (٢٣,٣١٧)، وهما قيمتان دالتان إحصائيًا عند مستوى دلالة (٠,٠٥). ولتَعرُّف اتجاه دلالة الفروق وفقًا للتخصص؛ تم استخدام اختبار "LSD" للمقارنات الثنائية البعدية، كما يوضحه الجدول التالي:

جدول (٩) يوضح نتائج اختبار "LSD" للمقارنات الثنائية البعدية لعينة الدراسة تبعًا لمتغير التخصص (ن=٤١٧).

المحور	المجموعة (أ)	المجموعة (ب)	الفرق بين المتوسطات (أ-ب)	الخطأ المعياري	الدلالة الإحصائية
الأول	ثقافي	لغوي	٥,٠٣٤٥١*	١,٢٠٠	٠,٠٠٠١
	تكنولوجيا معلومات	لغوي	٢١,١٠٧٢٥*	٢,١٣١	٠,٠٠٠١
		ثقافي	١٦,٠٧٢٧٤*	٢,١٢٥	٠,٠٠٠١
الثاني	ثقافي	لغوي	٧,٩١٨٧٥*	١,٤٢٤	٠,٠٠٠١
	تكنولوجيا معلومات	لغوي	٣,٥٩٥٩٣*	١,٤٢٠	٠,٠١٢
		ثقافي	٤,٣٢٢٨١*	٠,٨٠٢	٠,٠٠٠١

* تعني أن الفرق بين المتوسطات دالة عند مستوى معنوية ٠,٠٥

يتضح من الجدول (٩) ما يلي:

- توجد فروق ذات دلالة إحصائية بين استجابات أفراد العينة تبعًا لمتغير عدد التخصص (تكنولوجيا معلومات- ثقافي – لغوي)، بالنسبة لمحوري الاستبانة، لصالح أفراد العينة ذوي تخصص تكنولوجيا معلومات مقارنة بذوي التخصص اللغوي والثقافي حيث جاءت قيمة الفرق بين متوسطاتهم دالة إحصائيًا عند مستوى دلالة (٠,٠٥).
- أيضًا أظهرت النتائج دلالة فروق لصالح ذوي التخصص الثقافي مقارنة بالتخصص اللغوي، حيث جاءت قيمة الفرق بين متوسطاتهما دالة إحصائيًا عند مستوى دلالة (٠,٠٥).

وتبدو النتيجة السابقة منطقية، ويمكن عزوها لطبيعة تخصص تكنولوجيا المعلومات، وما يتضمنه من معارف ومهارات تكسب المعلمين العديد من المهارات والكفايات التي ترفع من وعيهم بكيفية التعامل مع المستجدات التكنولوجية وما يترتب عليها من آثار كالأمن السيبراني، ومن الطبيعي إن توافر هذه المعارف والمهارات لديهم يسهم بدرجة كبيرة في تعميق رؤيتهم لواقع دورهم في تعزيز وعي طلابهم بالأمن السيبراني وتحديد مقترحات تعميقه.

توصيات الدراسة:

١. التوسع في برامج التنمية المهنية أثناء الخدمة للمعلمين لإكسابهم المهارات والكفايات التي تتطلبها المتغيرات والمستجدات التربوية باستمرار ومن بينها توعية الطلاب ببعض القضايا المعاصرة كالأمن السيبراني.

٢. التركيز في برامج الإعداد الأولي للطلاب المعلمين (طلاب كليات التربية) على تدريبهم لاكتساب مهارات التوظيف الإيجابي للمستحدثات التكنولوجية في العملية التعليمية وتلاشي ما يترتب عليها من سلبيات ونقل هذه المهارات لمتعلميهم.
٣. دمج مفاهيم الأمن السيبراني والمهارات المتطلبة للوعي بها ضمن برامج الأنشطة الطلابية لطلاب المرحلة الثانوية بما يعزز من وعيهم به.
٤. عمل برامج توعية للأسرة من خلال وسائل الإعلام لإكسابهم المهارات المتطلبة لتعزيز وعيهم ووعي أبنائهم بالأمن السيبراني وكيفية الحد من مخاطر غيابه.
٥. العمل على استقطاب أعضاء المجتمع المحلي للمشاركة في التوعية بمفاهيم الأمن السيبراني وتعزيز الوعي بمتطلباته من خلال تقديم الدعم المادي والمعنوي المتطلب لذلك.

مقترحات الدراسة:

١. مخاطر ضعف مستوى الوعي بالأمن السيبراني وآليات التغلب عليها من وجهة نظر أعضاء هيئة التدريس بالجامعات المصرية.
٢. مستوى الوعي بالأمن السيبراني وعلاقته بمستوى المسئولية الاجتماعية لدى طلاب المرحلة الثانوية.
٣. دور أعضاء هيئة التدريس بالجامعات المصرية في تعزيز وعي طلابهم بالأمن السيبراني من وجهة نظرهم في ضوء بعض المتغيرات.
٤. تصور تربوي مقترح لتعزيز وعي طلاب الجامعات المصرية بالأمن السيبراني في ضوء خبرات بعض الدول.
٥. دور المناهج الدراسية في تعزيز مستوى الوعي بالأمن السيبراني لدى طلاب تكنولوجيا التعليم بالجامعات المصرية.

قائمة المراجع:

البار، عدنان مصطفى والسميري، عيسى رفاعي. (٢٠١٩). أساسيات الأمن السيبراني، جدة.

بانقا، علم الدين. (٢٠١٩). مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية : دراسة حالة دول مجلس التعاون الخليجي. المعهد العربي للتخطيط،الكويت،.(63)

البيشي، منير. (٢٠٢١). الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس. مجلة الجامعة الإسلامية بفلسطين، ٢٦(٦)، ٣٥٣-٣٧٢.

جبور، منى. (٢٠١٦). السيبرانية: هاجس العصر. *مجلة المكتبات والمعلومات والتوثيق في العالم العربي*، (٥). ٢٦٢-٢٦٣.

الجندي، علياء. محمد، نهير. (٢٠١٩). دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة. *عالم التربية*، ٣(٦٧). ١٤-٦٧.

الجنفاوي، خالد. (٢٠٢١). التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت. المجلة العربية للآداب والدراسات الإنسانية، المؤسسة العربية للتربية والعلوم والآداب، القاهرة(١٩). ٧٥- ١٢٣.

حمادي، ألاء محمدرحيم. (٢٠١٧). الجريمة السيبرانية ومخاطرها على الأطفال (الإشكاليات والحلول) (دراسة تحليلية في ضوء الإحصائيات الدولية والعربية والوطنية). مجلة كلية التربية للبنات،جامعة بغداد،العراق، ٢٨(٤)،١١٠٤-١١١٩.

حمدان، سماح محمدسامي. (٢٠٢١). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته بالإجراءات الاحترازية للحماية من الهجمات الإلكترونية في ظل جائحة كورونا. المجلة العربية للعلوم الاجتماعية،المؤسسة العربية للإستشارات العلمية وتنمية الموارد البشرية، القاهرة،١(١٩)، ١٨-٦٩.

خليفة، إيهاب. (٢٠٢٠). الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس. العربي للنشر والتوزيع، القاهرة.

خورشيد، عصمت مصباح يوسف. (٢٠٢١). تطبيقات أدب الطفل في تعليم الاتيكيت الرقمي لمرحلة الطفولة المبكرة (دراسة وصفية). مجلة بحوث عربية في مجالات التربية النوعية، رابطة التربويين العرب، مصر، ٢١(٢١)، ٩٥-١١٨.

الربيعة، صالح. (٢٠١٧). الأمن الرقمي وحماية المستخدم من مخاطر الانترنت. هيئة الاتصالات وتقنية المعلومات.

سراج، شيماء أحمد محمد أحمد. (٢٠٢٢). التحليل البعدي لدراسات الأمن السيبراني في المجال التربوي، المجلة العربية للعلوم التربوية والنفسية، المؤسسة العربية للتربية والعلوم والآداب، مصر،٢٦(٦)، ٣٥٣-٣٧٢.

السمحان، منى عبدالله صالح. (٢٠٢٠). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية، جامعة المنصورة، ١(١١١). ٢-٢٩.

السواط، حمد، والصانع، نورة، وأبو عيشة، زاهدة وسليمان، إيناس (٢٠٢٠). العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف. مجلة البحث العلمي في التربية، كلية البنات للآداب والعلوم والتربية، جامعة عين شمس، ٢١(٤)، ٢٧٨-٣٠٦

الشايع، خالد. (٢٠١٩). الأمن السيبراني مفهومة وخصائصه وسياساته. الدار العالمية.

الشهراني، بيان. فلمبان، فدوى. (٢٠٢٠). أثر برنامج تدريبي قائم على تصميم ألعاب تعليمية إلكترونية باستخدام برنامج Game Marek لإكساب مفاهيم الأمن السيبراني لدى طالبات المرحلة المتوسطة. مجلة البحث العلمي في التربية، كلية البنات للآداب والعلوم والتربية، جامعة عين شمس ، ٩(٢١). ٦١٤-٦٥١.

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

الصحفي، مصباح أحمدحامد وعسكول، سناء صالح. (٢٠١٩). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. مجلة البحث العلمي في التربية، كلية البنات للآداب والعلوم والتربية، جامعة عين شمس، ٢٠(١٠)، ٤٩٣-٥٣٤.

الصواط، شروق عبد الله طائل. (٢٠٢٢). درجة إسهام بعض منصات التعلم الإلكترونية مفتوحة المصدر في تنمية الوعي بالأمن السيبراني من وجهة نظر الطلبة بجامعة أم القرى،[رسالة ماجستير غير منشورة]، كلية التربية، جامعة أم القرى.

عبد الودود، مها. (٢٠١٨). أهمية أمن المعلومات والتهديدات الممكنة ووسائل المحافظة على أمن المعلومات. الموسوعة العربية الشاملة.

العريشي، جبريل حسن. الدوسري، سلمى عبدالرحمن. (٢٠١٨). دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع. مجلة مكتبة الملك فهد الوطنية، ٢٤(٢). ٣٠٢-٣٧٣.

العوادي، أوس مجيد غالب. (٢٠١٦). الأمن المعلوماتي السيبراني. مركز البيان للدراسات والتخطيط.

غوص، أميرة عبد الرحمن حسن، والشريف، باسم نايف محمد. (٢٠٢٢). فاعليَّةُ تَوظيفِ بعضِ التَّطبيقاتِ التّعليميَّةِ الذَّكِيَّة في تقديم وحدَّة مقترَحة عن الْأَمْنِ السيبراني على التَّحصيل

المعرفي والْاتِّجاهات نحوهُ لدى طالباتِ المرحلةِ المتوسِّطةِ بِالمدينَةِ المُنوَّرةِ، مجلة التربية، كلية التربية بنين، جامعة الأزهر بالقاهرة، ٣(١٩٥)، يوليو، ٦٨٥- ٧٣٤.

فرج، علياء عمر كامل. (٢٠٢٢). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي - جامعة الأمير سطام بن عبد العزيز نموذجاً، مجلة كلية التربية، جامعة سوهاج،ج١(٩٤).٥٠٩- ٥٣٧.

الفنتوخ، عبد القادر بن عبد الله. (٢٠١٢). الجريمة في الإنترنت: وطرق الحماية منها. العبيكان للنشر.

القحطاني، ذيب. (٢٠١٥). أمن المعلومات. مكتبة الملك فهد الوطنية،مدينة الملك عبدالعزيز للعلوم والتقنية.

قطب، بشائر حامد.حلبي، آمال سعد الدين حسين. (٢٠٢١). دور الصحف السعودية في تنمية الوعي بالأمن السيبراني: دراسة على القائم بالاتصال. المجلة العربية للإعلام والاتصال، الجمعية السعودية للإعلام والاتصال، جامعة الملك سعود،(25) ، .295-335

المشاقبة، محمد ناصر موسي. السرحان، حنين عبدالمهدي سالم. (٢٠٢٠). أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية.مجلة المفرق. ١-٩٩.

مصطفى، إسلام مصطفى جمعة. (٢٠٢٢). جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)، كليةالحقوق،جامعةالقاهرة، ١٢(٣)، ٧١٧- ٧٥٤.

المنتشري، فاطمة يوسف وحريري، رندة. (٢٠٢٠). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية، المؤسسة العربية للتربية والعلوم والآداب والتربية، القاهرة، ٤ (١٣)، ١٤٠-٩٥.

نعمة، أحمد عبيس، وكلنتر، زهراء عماد محمد (٢٠٢٠). تكييف الهجمات السيبرانيَّة في ضوء القانون الدولي. مجلة الكوفة للعلوم القانونيَّة والسياسيَّة: جامعة الكوفة - كليَّة القانون، مج١٣, (٤٤)، ٤٩ - ٧٤.

هيئة الاتصالات وتقنية المعلومات (٢٠٢٢). الأمن السيبراني. https://www.citc.gov.sa/ar/Digitalknowledge/Pages/cyber-security.aspx

رومنة المراجع

Al-Bar, Adnan Mustafa and Al-Sumairi, Issa Rifai (2019). Fundamentals of Cybersecurity, Jeddah.

Banqa, Alam Al-Din (2019). The Risks of Electronic (Cyber) Attacks and Their Economic Impacts: A Case Study of the Gulf

Cooperation Council Countries. Arab Planning Institute, Kuwait, (63).

Al-Bishi, Munir (2021). Cybersecurity in Saudi Universities and Its Impact on Enhancing Digital Trust from the Perspective of Faculty Members. Journal of the Islamic University of Palestine, 26(6), 353-372.

Jabour, Mona (2016). Cybersecurity: The Obsession of the Age. Journal of Libraries, Information and Documentation in the Arab World, (5), 262-263.

Al-Jundi, Alia. Muhammad, Nahir (2019). The Role of Applied Cybersecurity Practice in Developing Skills and Accuracy of Practical Application of Information Security among Female University Students. World of Education, 3(67), 14-67.

Al-Janfawi, Khaled. (2021). The Digital Transformation of National Institutions and Cybersecurity Challenges from the Perspective of Academic Police Officers in Kuwait. The Arab Journal of Arts and Humanities, Arab League Educational, Cultural and Scientific Foundation, Cairo (19), pp. 75-123.

Hamadi, Alaa Mohammed Rahim. (2017). Cybercrime and its Risks to Children (Problems and Solutions) (An Analytical Study in Light of International, Arab, and National Statistics). Journal of the College of Education for Girls, University of Baghdad, Iraq, 28(4), 1104-1119.

Hamdan, Samah Mohammed Sami. (2021). Family Members' Awareness of the Concept of Cybersecurity and Its Relationship to Precautionary Measures to Protect Against Cyberattacks in Light of the COVID-19 Pandemic. The Arab Journal of Social Sciences, Arab Foundation for Scientific Consultations and Human Resources Development, Cairo, 1(19), 18-69.

Khalifa, Ihab. (2020). Cyberwarfare: Preparing to Lead Military Battles in the Fifth Field. Al-Arabi for Publishing and Distribution, Cairo.

Khorshid, Ismat Misbah Youssef. (2021). Applications of Children's Literature in Teaching Digital Etiquette to Early Childhood (A Descriptive Study). Arab Journal of Research in the Fields

of Specific Education, Arab Educators Association, Egypt, 21(21), 95-118.

Al-Rabiah, Saleh. (2017). Digital Security and User Protection from Internet Risks. Communications and Information Technology Commission.

Seraj, Shaimaa Ahmed Mohamed Ahmed. (2022). Meta-Analysis of Cybersecurity Studies in the Educational Field. Arab Journal of Educational and Psychological Sciences, Arab League Educational, Cultural and Scientific Organization, Egypt, 26(6), 353-372.

Al-Samhan, Mona Abdullah Saleh. (2020). Requirements for Achieving Cybersecurity for Administrative Information Systems at King Saud University. Journal of the Faculty of Education, Mansoura University, 1(111), 2-29.

Al-Sawat, Hamad, Al-Sanea, Zahida Abu Aisha, and Suleiman, Enas (2020). The Relationship between Cybersecurity Awareness and National, Moral, and Religious Values among Elementary and Intermediate School Students in Taif. Journal of Scientific Research in Education, Girls' College of Arts, Sciences, and Education, Ain Shams University, 21(4), 278-306.

Al-Shaya, Khaled. (2019). Cybersecurity: Concept, Characteristics, and Policies. Al-Dar Al-Alamiya.

Al-Shahrani, Bayan. Felemban, Fadwa. (2020). The Effect of a Training Program Based on Designing Electronic Educational Games Using the Game Marek Program on Instilling Cybersecurity Concepts among Intermediate School Students. Journal of Scientific Research in Education, Girls' College of Arts, Sciences, and Education, Ain Shams University, 9(21), 614-651.

Sayegh, Wafaa Hassan Abdel Wahab. (2018). Family members' awareness of the concept of cybersecurity and its relationship to their security precautions against cybercrimes. The Arab Journal of Social Sciences, Arab Foundation for Scientific Consultations and Human Resources Development, Cairo, 3(14), 18-70.

Al-Sahafi, Misbah Ahmed Hamed and Askoul, Sanaa Saleh. (2019). The level of cybersecurity awareness among secondary

school computer teachers in Jeddah. Journal of Scientific Research in Education, Girls' College of Arts, Sciences, and Education, Ain Shams University, 20(10), 493-534.

Al-Sawat, Shorouk Abdullah Tael. (2022). The degree of contribution of some open-source e-learning platforms in raising cybersecurity awareness from the students' perspective at Umm Al-Qura University, [unpublished master's thesis], College of Education, Umm Al-Qura University.

Abdul-Wadud, Maha. (2018). The importance of information security, possible threats, and means of maintaining information security. The Comprehensive Arab Encyclopedia.

Al-Arishi, Gabriel Hassan. Al-Dosari, Salma Abdel-Rahman. (2018). The Role of Higher Education Institutions in Promoting a Culture of Information Security in Society. King Fahd National Library Journal, 24(2), pp. 302-373.

Al-Awadi, Aws Majeed Ghaleb. (2016). Cyber Security. Al-Bayan Center for Studies and Planning.

Ghous, Amira Abdul Rahman Hassan, and Al-Sharif, Basem Nayef Mohammed. (2022). The Effectiveness of Employing Some Smart Educational Applications in Delivering a Proposed Cybersecurity Unit on Cognitive Achievement and Attitudes Towards It among Intermediate School Female Students in Medina. Journal of Education, Faculty of Education for Boys, Al-Azhar University, Cairo, 3(195), July, pp. 685-734.

Farag, Alia Omar Kamel. (2022). Motives for Promoting a Culture of Cybersecurity in Light of the Digital Transformation - Prince Sattam bin Abdulaziz University as a Model, Journal of the Faculty of Education, Sohag University, Vol. 1 (94), 509-537.

Al-Fantookh, Abdul Qader bin Abdullah. (2012). Cybercrime and Methods of Protection. Al-Obeikan Publishing.

Al-Qahtani, Theeb. (2015). Information Security. King Fahd National Library, King Abdulaziz City for Science and Technology.

Qutb, Bashayer Hamid. Halabi, Amal Saad Eddin Hussein. (2021). The Role of Saudi Newspapers in Raising Cybersecurity Awareness: A Study of the Communicator. Arab Journal of

Media and Communication, Saudi Media and Communication Association, King Saud University, (25), 335-295.

Al-Mashqaba, Muhammad Nasser Musa. Al-Sarhan, Hanin Abdul-Mahdi Salem. (2020). The Impact of Implementing a Cybersecurity Policy on the Quality of Accounting Information in Banks

Alharbi, Talal. Tassaddiq, Asifa. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data Cogn. Comput, 5 (23). 2-15.

Alzubaidi, Abdulaziz. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1). 2-13.

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security, 12(4), 233-249.

Brecht, Daniel. (2021, April 29). Top 10 most in-demand cybersecurity skills for 2021.

Cains, Mariana. Flora, Liberty. Taber, Danica. Henshel, Diane. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation.

Gabra, Adamu. Sirat, Maheyzah. Hajar, Siti. Dauda, Ibrahim. (2020). Cyber security awareness among university students: acase study. Readers Insight, 3(11).

Mangold, L. V. (2016). An analysis of knowledge gain in youth cybersecurity education programs (Order No. 10250476).

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.

O'Brien, C. (2019). Teachers' perceptions about use of digital games and online resources for cybersecurity basics education: A case study (Order No. 13807207).

Sadaghiani-Tabrizi, A. (2018). Integrating cybersecurity education in K-6 curriculum: Schoolteachers, IT experts, and parents' perceptions (Order No. 10749961).

Uchenna, P. Ani, Daniel. Mary, Hongmei. Tiwari, Ashutosh. (2016). Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure. Springer International Publishing Switzerland, (501). 170- 181.

Von Solms, R., & Von Solms, S. (2020). Cyber safety education in developing countries.