درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني للمعلمين والموجهين الطلابيين بمدارس تعليم الليث

إعداد

أ/ عبد الكريم بن سلمان الثقفي

درجة الماجستير في الإدارة التربوية والتخطيط، كلية التربية، جامعة أم القرى، المملكة العربية السعودية

مجلة الدراسات التربوية والانسانية. كلية التربية. جامعة دمنهور

المجلد السابع عشر - العدد الأول (يناير) ، لسنة 2025م

درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني للمعلمين والموجهين الطلابيين بمدارس تعليم الليث

أ/ عبد الكريم بن سلمان الثقفي[1]

المستخلص:

هدفت هذه الدراسة إلى معرفة درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين والموجهين الطلابيين، واعتمدت الدراسة على المنهج الوصفي بالأسلوب المسحي؛ وتمثلت أداة جمع البيانات الرئيسية لهذه الدراسة في الاستبيان. وأجريت على عينة مكونة من (320) معلماً و(70) موجهاً طلابياً، بمدارس التعليم العام بإدارة تعليم الليث. وباستخدام الأساليب الإحصائية (التكرارات والمتوسط الحسابي والانحراف المعياري – معامل ألفا كرونباخ – معامل الارتباط واختبار تحليل التباين (ANOVA)) عبر برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS) توصلت الدراسة إلى أن درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث من وجهة نظر المعلمين والموجهين الطلابيين بشكل عام كانت مرتفعة وذلك بمتوسط (3.43) وأن درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين جاءت في المرتبة الأولى بدرجة مرتفعة تليها بمتوسط (3.74) تليها درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين بدرجة مرتفعة أيضاً وبمتوسط (3.40).

الكلمات المفتاحية: المعلمين، مديري المدارس، الوعي، الأمن السيبراني.

---

[1] درجة الماجستير في الإدارة التربوية والتخطيط، كلية التربية، جامعة أم القرى، المملكة العربية السعودية

البريد الإلكتروني: althaqafy1441@gmail.com

The degree of school principals' contribution to raising cybersecurity awareness among teachers and student mentors in Al-Laith Education Schools

Abdul Karim Al-Thaqafi
Educational Administration and Planning, College of Education , Umm Al-Qura University, KSA.
Email: althaqafy1441@gmail.com

Abstract:

This study aimed to identify the degree to which school principals contribute to raising the level of awareness of cyber security in Al-Layth schools among teachers, student mentors, from the point of view of teachers and student councilors. The study relied on the descriptive approach using the survey method. The main data collection tool for this study was the questionnaire. It was conducted on a sample of (320) teachers and (70) student counselor, in general education schools in the Al-Laith Education Department. Using statistical methods (frequencies, mean, standard deviation - Cronbach's alpha coefficient - correlation coefficient and analysis of variance (ANOVA)) via (SPSS) The study found that the degree of contribution of school principals in raising the level of awareness of cybersecurity in Al-Laith schools from the point of view of teachers and student councilors in general was high, with an average of (3.43), and that the degree of contribution of school principals in raising the level of awareness of cyber security in Al-Laith schools among teachers was in the range of First place with an average of (3.74), followed by the degree of contribution of school principals in raising the level of awareness of cyber security in Al-Laith Schools among students with an average of (3.40).

Keywords: teachers, School principals, awareness, cyber security.

مقدمة الدراسة:

يشهد المجتمع العالمي اليوم، تطوراً كبيراً في العملية التكنولوجية انعكست آثارها على مختلف المجالات والقطاعات مما فرض على جميع المؤسسات، ومنها المؤسسات التعليمية حتمية الاستجابة للمتطلبات التكنولوجية المعاصرة والتفاعل معها. وتظهر القيادة المدرسية كعمل قيادي يسعى إلى تحقيق أهدافه المنشودة واستيعاب كافة المستجدات والمستحدثات التي استوجبت ضرورة الاتجاه نحو الأخذ بآلياتها المختلفة ومواكبتها والاستفادة منها ولتحقيق ذلك يجب استخدام كافة أدوات التكنولوجيا ووسائل الاتصال الحديثة وأصبح مديري المدارس أمام تحديات مستمرة في التنظيم البشري والعلاقات الإنسانية وتعقيداتها بل إن أهم ما يميز عمل مديري المدارس اليوم هو القدرة على استخدام أساليب تطبيقية في مجال المعرفة، خاصة في ظل تنامي الاعتماد على التعليم الإلكتروني كجزء أساسي من منظومة التعليم.

ونتيجةً للإسهام الفعال الذي يقوم به مديرو المدارس؛ لتحقيق أهداف المدرسة والقيام بكافة الأعباء الموكلة إليهم فمن الضروري إدخال التقنية في القيادة ؛لأنها تساعد مديري المدارس على التغلب على كثير من الصعوبات التي تواجههم في الجوانب الفنية والإدارية وتوفير الوقت للتفكير في الجوانب التطويرية لاتخاذ قرارات سليمة بدلاً من الانشغال في جوانب إدارية روتينية، وهنا تبرز أهمية إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني خاصة في ظل الاعتماد على التعليم الإلكتروني كأحد أهم المستحدثات التربوية للعملية التربوية المعاصرة الذي أصبح سمة أساسية لكثير من المؤسسات التعليمية الحديثة وذلك لما للتعليم الإلكتروني من إسهام كبير في المساهمة لجيل من الخريجين القادرين على التعامل مع متطلبات القرن الجديد (الحربي، 2022).

ومع تزايد اعتماد المجتمع على البنية التحتية الرقمية فإن التكنولوجيا مازالت عرضة للتأثر؛ حيث تتعرض سرية البنية التحتية لتكنولوجيا المعلومات والاتصالات وسلامتها وتوفرها للتهديدات السيبرانية، بما في ذلك الاحتيال الإلكتروني، وسرقة البيانات والمعلومات الشخصية، والملكية الفكرية، وتعطيل الخدمات؛ لذلك فقد صدر الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني وهي الجهة المختصة في المملكة بالأمن السيبراني (فرج، 2022).

وعلى الرغم من الجهود التي تبذل من حكومة المملكة إلا أن المعلمين يتعرضون لانتهاكات ومخاطر سيبرانية دون أن يكون لديهم دراية بتلك المخاطر والانتهاكات، هناك العديد

من التهديدات الإلكترونية التي تعرضت لها المملكة العربية السعودية، ومنها قطاع التعليم بشكل خاص، حيث بلغت نسبة الخسائر الإلكترونية في هذا المجال 14 % وتعد أكبر نسبة مقارنة بالقطاعات الأخرى، وهنا تبرز الأهمية التربوية للأمن السيبراني، وهو ما يدعو إلى ضرورة رفع مستوى الوعي بأهمية الأمن السيبراني لدى هؤلاء المعلمين لضمان سرية وخصوصية الوثائق التعليمية والحفاظ على سلامتها بشكل مستمر وضرورة تضافر الجهود من قبل المدرسة ووزارة التعليم في هذا الشأن (المنتشري، 2020).

وللمعلم الحق الكامل في الحفاظ على خصوصية معلوماته وبياناته وترشيد استخدامها، ومن صور انتهاكاها في الفضاء السيبراني: إدخال معلومات وهمية، وانتحال الشخصية بهدف حصول المعتدي على مبالغ مالية، والتجسس الإلكتروني بتتبع العيوب واصطياد الأخطاء، والتنصت ومحاولة الوصول إلى السجلات الخاصة والاعتداء على الحياة الخاصة، لذا يعد التثقيف وتوعية المعلمين بأهمية الأمن السيبراني وماهيته التي تتضمن حماية البريد الإلكتروني وحماية البيانات والمعلومات الخاصة وأمن الأجهزة المحمولة جزءًا أساسياً من حركة التحول الرقمي، وركيزة أساسية لدعم رؤية المملكة 2030 لتطوير التحول الرقمي، وبناءًا على ذلك فإن تعليمه والتوعية بأهميته أصبح ضرورة ملحه خاصة مع التطور التكنولوجي وتطور المعلومات التي تؤثر في حياة الفرد اليومية، مما يزيد من أهمية تعليم الأمن السيبراني والتوعية بمفاهيمه ومهاراته (الشهراني، فلمبان، 2020).

وتبرز أهمية تعزيز مفهوم الأمن السيبراني وحماية شبكات وأنظمة تقنية المعلومات والتقنيات التشغيلية وخاصة في المؤسسات التعليمية بهدف التأسيس حماية البنى التحتية بالقطاعات التي لها الأولوية، وهو ما تضمنته رؤية المملكة 2030، وكذلك تحديد إسهام مديري المدارس في تبني برامج إعداد وتأهيل المعلمين لرفع مستوى الوعي بالأمن السيبراني بالمدارس (الخضري، وآخرون، 2020).

ويستخلص مما سبق أن تنوع وسائل وأجهزة الاتصالات والشبكات الإلكترونية وتفاوت خصائصها وطبيعتها في ظل التطور التكنولوجي لها؛ أدى إلى انتشار تبادل المعلومات بين العالم بشكل تسبب في زيادة العبء المالي على الدول التي تسعى إلى تحقيق الأمن المطلوب للفرد والمجتمع في ظل الاستخدام الكبير للشبكات الإلكترونية وأجهزة الحاسب الآلي وتطبيقاته، والأجهزة الذكية، ويعتبر الأمن بمثابة الركيزة الأساسية للمجتمع، مع بروز مجتمع المعلومات والشبكات الإلكترونية، والفضاء السيبراني، فقد أصبح الأمن السيبراني قيمة مضافة، ودعامة

للمجتمع مما فرض تحديات وأدوار جديدة لمديري المدارس الأمر الذي استوجب معه ضرورة رفع مستوى الوعي بالأمن السيبراني بمدارس التعليم، لحماية المعلومات المهمة والحساسة لدى المعلمين والمؤسسات التربوية، وكذلك تثقيف المعلمين والطلاب بعدم التعرض للانتهاكات والمخاطر السيبرانية، وتوفير طرق الوقاية ضد الهجمات السيبرانية؛ للحفاظ على أمن المؤسسة التعليمية والمعلم، هذا ما دفع بإحساس الباحث إلى إجراء البحث الحالي بعنوان" إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث".

مشكلة الدراسة وأسئلتها:

انطلاقاً من جهود المملكة في اطلاق المركز الوطني الإرشادي للأمن السيبراني، والتوجهات الهادفة إلى تعزيز الوعي بالأمن السيبراني، والتي تمثلت في إنشاء الهيئة الوطنية للأمن السيبراني التي تأسست في 31 أكتوبر 2017م. من أجل رفع مستوى الوعي السيبراني وتجنب المخاطر السيبرانية وتقليل آثارها وإصدار التنبيهات بآخر وأخطر الثغرات، وإطلاق حملات وبرامج توعوية، والتعاون مع المراكز الإرشادية الأخرى، كذلك تم إطلاق الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز تحت مظلة اللجنة الأولمبية السعودية للعمل على تقديم أنشطة وبرامج تساهم في زيادة وعي المجتمع بالأمن السيبراني وتشجيع الشباب للاحتراف في مجال الأمن السيبراني، وتطوير البرمجيات وفقاً للمعايير العالمية، وإنشاء كلية الأمن السيبراني والبرمجة والذكاء الاصطناعي بالرياض(فرج، 2022).

وكذلك بينت بعض الدراسات السابقة ضعف الوعي بجوانب الأمن السيبراني والإهتمام به لدى من يعملون بالمؤسسات التعليمية وذلك كدراسة بنت إبراهيم (2021) التي بينت نتائجها عن ضعف الوعي بجوانب الأمن السيبراني في التعليم عن بعد لدى معلمات العلوم بالمرحلة الابتدائية في المملكة العربية السعودية. ودراسة التيماني (2021) التي بينت أن الاهتمام الحكومي بموضوع الأمن السيبراني بدأ بشكل مبكر قبل أن يدرك الأفراد في المجتمع هذا المفهوم.

وأكدت العديد من الدراسات على الحاجة إلى تعزيز الأمن السيبراني. منها دراسة Mark, L. K., & Nguyen, T. T. T. (2017) التي أكدت على ضرورة توفير بيئات تعليمية آمنة عبر الإنترنت، وغير متصلة بالإنترنت للأطفال، بالإضافة إلى زيادة وعيهم الذاتي بأمان الإنترنت والمعرفة. ودراسة Chandarman and Van Niekerk (2017)

التي بينت الحاجة إلى حملات لتنمية الوعي بالأمن السيبراني، والتي تستهدف علاج نقاط الضعف المحددة لدى المستخدمين.

وتفعيلاً لدور المؤسسات التربوية لنشر ثقافة ورفع مستوى الأمن السيبراني وقعت وزارة التعليم مع الهيئة الوطنية للأمن السيبراني اتفاقية لتعزيز التعاون المشترك في مجالات التعليم والبحث العلمي والتدريب والتوعية في مجال الأمن السيبراني، بما يسهم في تأهيل الكوادر الوطنية وبناء القدرات في مجال الأمن السيبراني من أجل رفع الوعي بالأمن السيبراني(الهيئة الوطنية للأمن السيبراني، 2022)

وقد أظهرت العديد من الدراسات السابقة أهمية الأمن السيبراني وضرورة تعزيزه في المؤسسات التعليمية كدراسة فرج (2022) التي بينت نتائجها أهمية تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي، ودراسة المنيع (2022) التي أكدت على أهمية توعية العاملين بمخاطر استخدام الأجهزة الشخصية، المتمثلة في الهاتف المحمول لنقل أو تخزين معلومات سريَّة خاصة بالعمل.

وعليه ومكن القول في ضوء ما سبق أن مشكلة الدراسة تتحدد في الإجابة عن السؤال الرئيسي التالي: ما درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث؟ ويتفرع من هذا السؤال الأسئلة الفرعية التالية:

1. ما درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين؟
2. ما درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين؟

أهداف الدراسة: هدفت الدراسة إلى تحديد:

1. درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين.
2. درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين بمدارس تعليم الليث.

أهمية الدراسة:

الأهمية النظرية:

–قد تسهم في إثراء المكتبات المحلية والعربية في مجال ممارسة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني من وجهة نظر المعلمين والموجهين الطلابيين.

–قد تسد الفجوة البحثية في مجال ممارسة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني من وجهة نظر المعلمين والموجهين الطلابيين، نظراً لندرة الدراسات العربية والدراسات التي أجريت في المملكة العربية السعودية والتي تناولت إسهام الإدارة المدرسية في تعزيز الأمن السيبراني.

الأهمية التطبيقية:

–قد تسهم في جذب اهتمام الباحثين لإجراء المزيد من الدراسات حول موضوع الأمن السيبراني.

–قد يستفيد من نتائجها المدارس في معرفة أهمية وكيفية رفع درجة الوعي بأهمية إسهام الإدارة المدرسية في تعزيز الأمن السيبراني داخل المدرسة.

–قد يستفيد من نتائج الدراسة صانعي القرار في المؤسسات التربوية للأخذ بها عند بناء تصور مستقبلي.

حدود الدراسة: تمثلت حدود الدراسة فيما يلي:

–الحدود الموضوعية: بيان درجة ممارسة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث.

–الحدود المكانية: أجريت الدراسة على المدارس الحكومية بمدارس تعليم الليث.

–الحدود البشرية: عينة من المعلمين والموجهين الطلابيين بمدارس تعليم الليث.

–الحدود الزمانية: أجريت الدراسة خلال الفصل الدراسي الثاني من العام الدراسي 1445هـ.

مصطلحات الدراسة:

الأمن السيبراني: عرفته الهيئة الوطنية للأمن السيبراني (2018) بأنه حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها وما تقدمه من خدمات، وما تحويه من بيانات من اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي نحوها.

الوعي بالأمن السيبراني : (Security Cyber of Awareness) الوعي هو: إدراك الإنسان لذاته وما يحيط به إدراكا مباشرا، وهو أساس كل معرفة. كما يشير الوعي إلى الفهم وسلامة الإدراك، ويقصد بهذا الإدراك إدراك الإنسان لنفسه وللبيئة المحيطة به، وهو استجابة الفرد لمثيرات تقييم الذات والثقة بالنفس والتأمل الذاتي والوعي الوجداني (بخيت، 2019).

التعريف الإجرائي: درجة إدراك مديري مدارس تعليم الليث أهمية جهودهم وممارساتهم من أجل رفع مستوى الوعي لدى المعلمين بالأمن السيبراني في جميع الاجراءات والتدابير والتقنيات والأدوات المستخدمة لحماية سلامة الشبكات والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به، ويشمل كذلك حماية الأجهزة والبيانات المتعلقة بالمدرسة.

الإطار النظري:

1.مفهوم الأمن السيبراني:

يعبر مفهوم الأمن السيبراني عن "مجموعة الآليات والإجراءات والوسائل والأطر، التي تستهدف حماية البرمجيات، وأجهزة الكمبيوتر، من الهجمات والاختراقات والتهديدات لما تحويه من معلومات، وقد ارتبطت نشأته بظهور الهجمات والاختراقات منذ منتصف الخمسينات من القرن الماضي، وتزايدت أهميته مع ظهور وانتشار شبكة الإنترنت وما تبعها من تطور في عمليات الحفظ والتخزين ونقل المعلومات الكترونيًا" (جاب الله، ٢٠٢١، ص. 52).

وفي ذات السياق يشير عسيري وآخرون (2021، ص. 69) إلى أن الأمن السيبراني: "يعبر عن حماية الأجهزة والأنظمة التقنية، ووسائل التخزين التابعة لها، والتعامل الآمن مع خدمات الإنترنت، والبرمجيات ضد أي دخول غير مصرح له، أو تعديل أو إتلاف أو نشر البيانات الموجودة بها من غير إذن مسبق، وأما الوعي بالأمن السيبراني فهو مجموعة المعارف والمهارات والسلوك الفعلي والعلاقات المتبادلة بينها التي تساعد الأفراد على حماية أجهزتهم، ووسائل التخزين الخاصة بهم، بكافة أنواعها، والتعامل الآمن مع خدمات الإنترنت والبرمجيات".

كما يشار إليه بأنه "جميع الجهود التي يتم بذلها، والتي تستهدف حماية البريد الإلكتروني والبيانات الرقمية الشخصية، والمعلومات، والأجهزة المحمولة، وتعزيز خصوصيتها، وتشفيرها، واتخاذ الإجراءات التي تعمل على حماية الطلاب من مخاطر الفضاء السيبراني" (فرج، 2021، ص. 515).

كما يشير الأمن السيبراني إلى "جميع الإجراءات والتدابير والتقنيات والأدوات المستخدمة من قبل الأفراد والمؤسسات بهدف حماية الشبكات، والبرامج، والبيانات، من الهجوم، او التلف، أو الوصول غير المسموح به" (المنيع، 2022، ص. 163).

ويشير السعادات والتميمي (2022) إلى الأمن السيبراني باعتبار أنه: "الإحساس والدراية بالأعمال والممارسات غير المشروعة، والتي تهدف للاختراق أو التعطيل أو التعديل أو الاستغلال غير المصرح به للبيانات أو المعلومات، بهدف الحماية والوقاية منها" (ص. 264).

وعرفت الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية (2022) الأمن السيبراني بأنه: "العمل على تعزيز حماية الشبكات، وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، مراعية في ذلك الأهمية الحيوية المتزايدة للأمن السيبراني في حياة المجتمعات، وحماية مصالح المملكة الحيوية، وحماية أمنها الوطني، وحماية البنى التحتية الحساسة في المملكة" (ص. 1).

ويتضح أن الأمن السيبراني مجموعة من الإجراءات التي يتم اتخاذها من أجل المحافظة على المعلومات والبيانات الإلكترونية، وصد الهجمات والاختراقات التي ينفذها مجرموا الإنترنت، وعدم الوقوع ضحية سواءً على مستوى الأفراد أو المؤسسات، لأي أحد من شأنه أن يتلاعب بالمحتوى الرقمي الخاص بالفرد، أو المؤسسة، أو يستخدمه استخدامًا غير لائق، أو ليس من صلاحياته.

2.أهداف الأمن السيبراني:

تسعى العديد من الدول والمؤسسات في مختلف المجالات إلى تعزيز الأمن السيبراني، وذلك من أجل تحقيق العديد من الأهداف، والتي يُمكن إيجازها فيما يلي (الربيعة، 2017، ص. 3):

–ضمان توافر استمرارية عمل نظم المعلومات.
–حماية مصالح الدول الحيوية وأمنها الوطني، والبنى التحتية الحساسة فيها.
–اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.
–تعزيز حماية الشبكات وأنظمة المعلومات.
–تعزيز حماية وسرية وخصوصية البيانات الشخصية.

ويضيف كل من (صائغ، 2018، ص. 22) ما يلي:

-توفير بيئة آمنة تتمتع بقدر كبير من الموثوقية في مجتمع المعلومات.

-تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات.

-التصدي لهجمات وحوادث أمن المعلومات، والتي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.

-توفير المتطلبات اللازمة للحد من الجرائم السيبرانية، والتي تستهدف المستخدمين.

-مقاومة البرمجيات الخبيثة، وما تستهدفه من إحداث أضرار بالغة بالمستخدمين، وأنظمة المعلومات.

-الحد من التجسس، والتخريب الإلكتروني، على مستوى الحكومات والأفراد.

-التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة بأنواعها، وسد الثغرات الموجودة بأنظمة المعلومات

ومن خلال ما سبق يتضح أن الأمن السيبراني له العديد من الأهداف، فبدونه يصبح الأفراد والمؤسسات في خطر، ومن هنا فإن أهم أهداف الأمن السيبراني حماية الأفراد والمؤسسات من الاختراق، أو الابتزاز، أو التجسس والحد من الجرائم الإلكترونية.

3.أهمية الأمن السيبراني:

تتمثل أهمية الأمن السيبراني والوعي به فيما يلي:

-ضرورة حفظ الوثائق، والمعلومات، التربوية، والحفاظ على سريتها، وخصوصيتها، ومتابعة ومراقبة وتطوير وضبط نظام المعلومات، والأمن في المدارس، ومراقبة أي محاولات للتسلل إلى شبكات المعلومات بالمدرسة (Stewart & Shilingford, 2011, p. 8).

-ارتباطه بجميع الجوانب التعليمية والاجتماعية، والاقتصادية، والإنسانية، وقدرته على تعزيز أمن الدول، وذلك من خلال حماية أفرادها على كافة المستويات (جبور، 2012، ص. 22).

-الحد من الأضرار المادية والنفسية والمعنوية التي تؤثر على المعلم والمؤسسة التربوية، الناتجة عن التعرض للجرائم الإلكترونية، والوقوع كضحية لأحد أشكال الجرائم السيبرانية (Wilson, 2014, p.5).

–مواجهة الجرائم التي قد تتسبب في إيقاع خسائر فادحة، مما يؤدي لشلل بيئة المعلومات والاتصالات الخاصة بمستخدم معين، أو بجهة معينة، كالتلاعب في البيانات أو تزييفها أو محوها من أجهزة الحواسيب (خليفة، ٢٠١٧، ص. 139).

–يعتبر توفر الأمن السيبراني عامل أساسي للتنمية الاقتصادية المستدامة، حيث سهلت التطورات التكنولوجية حدوث نمو اقتصادي كبير للدول؛ ومع ذلك فإن المؤسسات تواجه العديد من المخاطر الناتجة عن اعتمادها على الخدمات الرقمية، أبرزها المخاطر المتعلقة بالأمن السيبراني. (Vasiu & Vasiu, 2018, p. 173) .

–ضمان سرية وأمن المعلومات: والتي تعني التأكد من أن المعلومات لا تكشف، ولا يُطلع عليها من قبل أشخاص غير مخولين بذلك.

–التكاملية، وسلامة المحتوى، والذي يتعلق بأن محتوى المعلومات صحيح ولم يُعدل، وعلى نحو خاص، ولم يغير، ولم يُعبث به، عن طريق تدخل غير مشروع.

–استمرارية توافر المعلومات أو الخدمة.

–عدم إنكار التصرف المرتبط بالمعلومات ممن قام به، ويُقصد به ضمان إنكار الشخص المتصل بالمعلومات أو مواقعها بقيامه بتصرف ما، بحيث تتوافر قدرة إثبات هذا التصرف، وأن شخصًا ما في وقت معين قد قام به، وكذلك عدم قدرة مستلم رسالة معينة على إنكار استلامه لهذه الرسالة (الصحفي والعسكول، 2019، ص. 497).

–تنمية وعي المعلمين بالانتهاكات والمخاطر السيبرانية، ومدى خطورتها، وحثهم على ضورة رفع مستوى الوعي لديهم بأهمية الأمن السيبراني، وضرورة تضافر الجهود من قبل المدرسة ووزارة التعليم في هذا الشأن (المنتشري وحريري، 2020، ص. 103).

وبناء على ما سبق فإن الأمن السيبراني أصبح ذو أهمية كبيرة خاصة في عصر النهضة التكنولوجية، والذي صاحبه التطور الكبير للتكنلوجيا، وفي المقابل تطورت فيه الجرائم المرتبطة بها، والتي تواجه بالأمن السيبراني، لكونه يحافظ على الخصوصية، والسرية، كما يحافظ على حقوق الأفراد والمنشآت، ويضمن الحفاظ على المعلومات دون تغيير، ويحمي الجميع من الوقوع في براثن مجرمي الإنترنت.

4.متطلبات تحقيق الأمن السيبراني:

تتمثل متطلبات تحقيق الأمن السيبراني في الآتي (القحطاني والعنزي، ٢٠١١، ص. 92):

-تحديد إجراءات العمل في الشبكات المعلوماتية: حيث لابد أن تكون إجراءات العمل في تلك الشبكات واضحة ومحددة، من حيث ما هو مسموح أو غير مسموح، فيما يتعلق بالأمن المعلوماتي على الشبكة.

-توفير الآليات اللازمة لتنفيذ سياسات العمل: بحيث يكون هناك وضوح ودقة حول كيفية التنفيذ لهذه السياسات، وتحديد العقوبات التي ستوقع في حالة حدوث اختراق.

-المورد البشري: ضرورة الاهتمام بإسناد إدارة وتشغيل الشبكات المعلوماتية للعناصر البشرية الكفء، والمدربة والمؤهلة للتعامل مع التقنيات والتكنولوجيا الحديثة، وعدم إفساح المجال للهواة وغير المتخصصين للعبث بمقدرات الهيئات الحكومية بالدول، أو بخصوصيات الأفراد.

-تحديث الأوضاع الأصلية لمعدات الشبكات: حيث يتم كل فترة تغيير الأوضاع الأصلية للمعدات المرتبطة بشبكات المعلومات كإجراء احترازي، مما يساعد على منع الاختراق من الخارج.

-المراقبة: ضرورة الحرص على توفير المراقبة والمتابعة اللازمة والمستمرة للأنشطة المعلوماتية على الشبكة بشكل دقيق، بهدف اكتشاف أية أنشطة مشبوهة، أو حركات غير طبيعية، ضمن نطاق الشبكة، والعمل على تفادي تفاقم الأوضاع.

-حسن اختيار مواقع نقاط الشبكة: فلا بد من الدقة عند اختيار نقاط الاتصال بشبكات المعلومات، وأن تكون هذه النقاط في مواقع جيدة، ومؤمنة ومحمية من الاختراق، وإنشاء بروتوكولات للتحقق والتشفير، وأن يتم اختيار البرامج المعروفة والمشهورة عالميًا في هذا الإطار.

5.عناصر الأمن السيبراني:

توجد ثلاثة عناصر أساسية يعتمد عليها الأمن السيبراني، وتتمثل في السرية، وصحة المعلومات وسلامتها، والتكامل وتوافر البيانات، ويمكن تفصيلها فيما يلي المناسب (Borky et al., 2019, p. 349):

–السرية: ويقصد بسرية المعلومات الحفاظ عليها، ويتم ذلك من خلال منح الإذن للمخول لهم فقط بالوصول لتلك المعلومات والبيانات، ومنع الأشخاص غير المخول لهم الوصول لتلك المعلومات، مع ضرورة التأكيد على عدم الإفصاح عنها، أو تسريبها لأشخاص آخرين غير متخصصين أو مخول لهم ذلك.

–تكامل وسلامة المعلومات: وتعني الحفاظ على المحتوي من التعديل، أو التغيير، أو الحذف، أو الإضافة، إلا من خلال الأشخاص المؤهلين والمتخصصين بالإشراف على هذا المحتوى.

–توافر المعلومات وإتاحتها: ويقصد به توافر المعلومات من قبل الأشخاص المتخصصين والمشرفين على تقديمها واتاحتها في الوقت

ويشير الحربي (2022، ص. 87) إلى تلك العناصر بأنها: (الإتاحة، والسلامة، والسرية) وهي كما يلي:

–توفر المعلومات متى ما احتجنا إليها، وضمان إتاحة جميع الموارد المخزنة لها.

–يجب أن تكون المعلومات صحيحة، وسليمة، من التعديلات غير المشروعة.

–سرية البينات: بحيث لا يصل إليها إلا الأشخاص المصرح لهم فقط.

يتضح مما سبق أن للأمن السيبراني ثلاثة عناصر أساسية، حتى يتحقق الأمن السيبراني، وأنه ينبغي الحفاظ على المعلومات والبيانات بكل الوسائل الممكنة، حتى لا تتعرض للاختراقات، ومن ثم يصبح الفرد فريسة سهلة للمستهدفين، وأصحاب المصالح، ولذا ينبغي تطبيق تلك العناصر الثلاثة من السرية، وعدم السماح لأحد بالتعديل فيها، وإتاحتها في الوقت المناسب، وللفئة المطلوب لها هذه المعلومات.

6.خصائص الأمن السيبراني:

إذا كانت الجريمة الإلكترونية تتم وفق منهجية وأساليب حديثة، وذات بعد تكنولوجي، أعلى من الجرائم التقليدية؛ فإنه يصبح من الضروري جدًا أن يتحقق الأمن السيبراني من أجل التغلب على هذه المشكلة، ومواكبة التطور التكنولوجي، ولذلك فقد تميز الأمن السيبراني بعدة خصائص من أبرزها ما يلي(الملاحي، ٢٠١٥، ص. 67):

–الاكتشاف والتعقب: فالأمن السيبراني يهدف إلى اكتشاف الجريمة الإلكترونية، وتعقب أثرها، وبالتالي التغلب عليها.

-السرعة وغياب الدليل: تتمثل صعوبات إثبات الجرائم الإلكترونية في استخدام المخترقين وسائل تقنية حديثة ومتطورة باستمرار، ولذلك فإنه من الضروري أن يتحقق الأمن السيبراني بتقنيات حديثة عالية تفوق تقنياتهم وخبراتهم، حتى يمكن التقليل من تلك التعديات.

-ضعف الأجهزة الأمنية والقضائية في التعامل مع الجرائم الإلكترونية: وذلك بسبب نقص الخبرة الرقمية لدى الأجهزة الأمنية، وهذا يعزز دور الأمن السيبراني في تحقيق الأمن الرقمي للمؤسسات، لاسيما المؤسسات التعليمية، والمدارس في حماية البيانات والبنى التحتية لهذه المؤسسات.

-كما أضاف Stallings & Brown (2018, p. 2) بعض الخصائص للأمن السيبراني، وهي على النحو التالي:

-السرية: وتعني حماية المعلومات الحساسة من الوصول غير المصرح به.

-الانتماء: ضمان أن المعلومات تنتمي فقط إلى الأشخاص الذين لهم الحق في الوصول إليها.

-التوفر: ضمان توفر المعلومات والخدمات المتعلقة بها عند الحاجة إليها.

-المصداقية: ضمان صحة المعلومات وعدم تعرضها للتلاعب أو التزوير.

ويضيف Whitman & Mattord (2021, p. 4) الخصائص التالية:

-الاستجابة: من خلال القدرة على التعرف على الأحداث الأمنية والاستجابة السريعة لها بطريقة مناسبة.

-الاستجابة للكوارث: وتعني القدرة على استعادة البيانات، والخدمات المتعلقة بها بعد وقوع كارثة، مثل الهجمات السيبرانية أو الأعطال الفنية.

-الشفافية: وتعني القدرة على تعقب الأنشطة الرقمية وتحليلها بشكل دقيق وشفاف، بما في ذلك تحديد مصادر الهجمات السيبرانية والتحقق من الامتثال للسياسات والمعايير الأمنية.

-الحماية متعددة الطبقات: حيث يتم استخدام طبقات متعددة من الأمن لحماية الأصول الرقمية، بدءًا من الأجهزة والبرامج والشبكات والبيانات.

-الإدارة المرنة للهوية والوصول: القدرة على إدارة الوصول إلى الموارد الرقمية بطريقة مرنة ومتكيفة مع احتياجات المؤسسة والمستخدمين.

وبالتالي يتضح أن الأمن السيبراني هو أمن بالمعنى الحقيقي، حيث يحمي حقوق الأفراد والمؤسسات، من الاختراق أو التجسس، كما أن الأمن السيبراني به خاصية الاكتشاف والتعقب، للمجرمين، والذي يحاولون التعدي على حقوق الآخرين وابتزازهم، وانتهاك حقوقهم، ولذا فالأمن السيبراني مطلب واقعي، وضرورة حتمية، في ظل التقدم التكنولوجي.

7.الأمن السيبراني في العملية التعليمية:

هيأت مواقع التواصل الاجتماعي لمستخدميها عالمًا خاصًا بهم، وعلى الأخص بين المراهقين من الطلاب، وانتشر ذلك على وجه الخصوص بعد ظهور الجيل الرابع من الهواتف الذكية، ومن أكثر مواقع الشبكات الاجتماعية شعبية وانتشارًا بين الجميع لاسيما الطلاب موقع فيسبوك (Face Book) وموقع تويتر (Twitter) وموقع لينكدان (Linkedin) والمدونات الإليكترونية (Weblogs) وتطبيق سناب شات (Snap chat) وتطبيق واتساب (Whats App) وانستجرام (Instagram) واليوتيوب (YouTube) حتى أصبحت وسائل التواصل الاجتماعي سواءً المذكورة أو غيرها، جزءً لا يتجزأ من الحياة اليومية المعاصرة، والتي لا يمكن الاستغناء عنها في بعض الأحيان، لما لها من فائدة سواءً على الصعيد الاجتماعي، أو الثقافي، أو المهني في بعض الأحيان (De Andrea, et al., 2012, p. 15)

وفي إطار التغير والتطور السريع في شتى المجالات، برزت الحاجة إلى الوسائل التي تحقق التواصل، داخل العملية التعليمية، بين المعلمين والمديرين والطلاب، ومن ثم ظهرت المنصات التعليمية، ومنها منصة مدرستي، حيث تزايد الحديث عنها، وتصاعد البحث حول استخداماتها المتعددة، واكتشاف إمكاناتها المجهولة، على الرغم من وجود بعض تلك المنصات منذ سنوات، إلا أن استخدامها الاستخدام الأمثل ظل محكومًا بتوافر الشبكات، والحواسيب، وغيرها (العتيبي وآخرون، 2022، ص. 385).

هذا بالإضافة إلى أن التدفق الهائل للمعلومات، وانتشار التكنولوجيا، واعتماد العديد من المؤسسات التعليمية عليها في تسيير أعمالها، ومن ثم ظهر معه تهديد جديد لم يكن معروفًا من قبل، حيث اتجه العديد من الأشخاص إلى اختراق الشبكات، والتلاعب بالمعلومات، وإيذاء أصحابها بطرق وأساليب متعددة، حيث انتشر ما يعرف بالجرائم السيبرانية (Chang et al., 2013, p. 881).

ومن ثم اتجهت العديد من الدول إلى تبني ما يعرف بالأمن السيبراني، وتوفيره لجميع مستخدمي الإنترنت، وبصفة خاصة طلاب المدارس، وكان من أهم تلك المبادرات مبادرة دول الاتحاد الأوروبي، والتي ساهمت في وضع مبادئ للاستخدام الآمن لشبكات المعلومات، وكذلك الإطار الأوروبي للاستخدام الآمن للأجهزة المحمولة، وبحلول عام 2009م تم إدراج مفاهيم الأمن السيبراني ضمن المناهج الدراسية، وذلك في 24 دولة أوروبية، وكذلك الحال في الولايات المتحدة حيث تولت وزارة الأمن الداخلي هذا الملف، وأصبحت مسئولة عن تعزيز ونشر الوعي بالأمن السيبراني، ومن ثم فقد تم تأسيس التحالف الوطني للأمن السيبراني (Von Solms & Von Solms, 2015, p. 15).

ولم تكن المؤسسات التعليمية وعلى رأسها المدارس والجامعات بمعزل عن هذا الاهتمام، حيث أكدت دراسة (Spiering, 2013) على أهمية إعداد خطة لتنمية قدرات الإدارة المدرسية والمعلمين فيما يتعلق بالوعي بالأمن السيبراني، وأشارت دراسة (Goran, 2017) إلى أهمية رفع مستوى الوعي بالأمن السيبراني لدى المعلمين والطلاب، وكذلك دراسة (المنتشري، 2019) أكدت على أهمية رفع مستوى الوعي بالأمن السيبراني لدى المعلمات، والمشرفات، والعاملات في ميدان التوجيه والإرشاد التربوي.

ولمدير المدرسة دورٌ فعالٌ في نجاح وتقدّم المدرسة، وتحقيقها لأهدافها، حيث أشارت نتائج البحوث إلى وجود ترابط قوي بين القيادة الفعالة، ومدى نجاح المدرسة في تحقيق أهدافها، حيث إن نجاح إدارة المدرسة وفعاليتها يرتبط بنجاح وفعالية قيادتها المدرسية، وهذا يعتمد بشكل كبير على ما يتمتع به مدير المدرسة من مهارات وسمات، ومن ثم فقد اتجهت جهود الفكر التربوي إلى تحديد خصائص القيادة الناجحة في الفترة الأخيرة، ومدى قدرتها على استخدام المهارات التكنولوجية، وغرس الوعي بالأمن السيبراني في كل منسوبي المدرسة، ومن ثم تم وضع معايير ثابتة يمكن على أساسها اختيار مدراء المدارس بحيث يكونون قادرين على أداء أدوارهم بكفاءة، وفاعلية، ومن ثم زاد الاهتمام بالعامل الإنساني دون إهمال الجوانب الأخرى والطرق والمهارات المطلوبة (Walsh & Ken, 2015, p. 2).

ومن ثم يتضح أهمية الوعي بالأمن السيبراني، وأنه ضرورة حتمية في عصر انتشار التكنولوجيا، وهناك العديد من الدراسات التي أظهرت أهمية الوعي بالأمن السيبراني، وحثت على انتشاره، والاهتمام به، لاسيما لدى العاملين في الميدان التربوي، والطلاب.

الدراسات السابقة:

هدفت دراسة (Fazil, et.al 2023)، للتعرف على واقع تعزيز الوعي بالسلامة على الإنترنت والأمن السيبراني بين طلاب المدارس الثانوية والثانوية في أفغانستان: دراسة حالة بمقاطعة بدخشان، مع التركيز على الشباب في مقاطعة بدخشان، أفغانستان، ولتحقيق هذا الغرض، تم اختيار 170 طالبًا وطالبة من مختلف المستويات الدراسية في المدارس العامة والخاصة في مقاطعة بدخشان بأفغانستان بدقة. تم تسهيل جمع البيانات من خلال استبيان مسح شامل يضم 16 سؤالًا قائمًا على مقياس ليكرت. وقد خلصت الدراسة إلى أن واقع تعزيز الوعي بالسلامة على الإنترنت والأمن السيبراني بين طلاب المدارس الثانوية والثانوية في أفغانستان: دراسة حالة بمقاطعة بدخشان كان متوسطاً، مع التأكيد على الأهمية القصوى لغرس الوعي فيما يتعلق بالممارسات الرقمية المسؤولة المتعلقة بالخصوصية والأمن وحقوق التأليف والنشر، مع دعوة مقنعة للمشاركة الفعالة للآباء. وتساهم الدراسة بشكل كبير في تعزيز مجتمع أكثر أمانًا ومسؤولية وقائماً على المعرفة. والدعوة إلى تنمية المعرفة الرقمية ومبادئ السلامة عبر الإنترنت عبر مختلف الفئات العمرية ومجالات الدراسة.

وهدفت دراسة Ravendran, et al. (2023) إلى تقييم معرفة تطبيق الركائز التسع للثورة الصناعية الرابعة في التعليم لدى معلمي STEM في ماليزيا، وتتمثل الركائز الأساسية التسع للثورة الصناعية الرابعة في: الروبوتات المستقلة، والواقع المعزز، وتكامل النظام، والتصنيع الإضافي، والأمن السيبراني، والحوسبة السحابية، والبيانات الضخمة والتحليلات، وإنترنت الأشياء، والمحاكاة، وتم استخدام منهج الدراسة الكمي، من خلال استبيان المسحي، لإجراء الدراسة، وتم اختيار حجم عينة من 200 مدرس STEM في المدارس الثانوية في ماليزيا من خلال تقنية بسيطة لأخذ العينات العشوائية، وتم استخدام متوسط الدرجات لتقييم المعرفة، وأظهرت نتائج الدراسة أن المعلمين على دراية كبيرة بتطبيق المحاكاة، والواقع المعزز، والروبوتات المستقلة في التعليم، وفي الوقت نفسه، يتمتع المعلمون بمعرفة متوسطة في تطبيق الأمن السيبراني، والتصنيع الإضافي، وإنترنت الأشياء في التعليم، وأخيرًا، سجل المعلمون مستوى منخفضًا من المعرفة تجاه تطبيق الحوسبة السحابية، والتكامل الأفقي والرأسي، وكذلك البيانات الضخمة والتحليلات، في التعليم.

هدفت دراسة العقلاء وعلي (2022) إلى الكشف عن درجة الوعي بمفاهيم الأمن السيبراني لدى معلمي ومعلمات الحاسب الآلي بمدينة حائل، واعتمدت الدراسة على المنهج الوصفي المسحي، وتم تطبيق استبانة إلكترونية على عينة عشوائية مكونة من (١٨٤) معلم ومعلمة حاسب آلي بالمرحلتين المتوسطة والثانوية بمدينة حائل، وأظهرت الدراسة أن درجة وعي معلمي ومعلمات الحاسب الآلي في مدينة حائل بماهية الأمن السيبراني جاءت متوسطة، كما أنها أشارت إلى أن درجة وعيهم بطرق المحافظة على نظام الأمن السيبراني جاءت متوسطة أيضا، مع وجود فروق ذات دلالة إحصائية في وعي معلمي ومعلمات الحاسب الآلي بالأمن السيبراني تعزى متغيرات للجنس لصالح المعلمات، كما أن معلمي ومعلمات المرحلة المتوسطة لديهم وعي بالأمن السيبراني أعلى من معلمي ومعلمات المرحلة الثانوية وبفارق دال إحصائيا، ولا توجد فروق ذات دلالة إحصائية في وعي معلمي ومعلمات الحاسب الآلي بمفاهيم الأمن السيبراني تعزى لمتغير الخبرة أو المؤهل الأكاديمي، بينما توجد فروق ذات دلالة إحصائية في وعي معلمي ومعلمات الحاسب بمفاهيم الأمن السيبراني تعزى لمتغير الدورات التدريبية، لصالح من تلقى دورة تدريبية واحدة فأكثر.

وهدفت دراسة Karimnia, Maennel & Shahin (2022) إلى تحليل مستوى الوعي الحالي بالأمن السيبراني لدى طلاب المدارس الثانوية في إيران، من خلال إجراء مسح لعينة بلغت (616)، وتطوير برنامج توعية للطلاب الذين تتراوح أعمارهم ما بين 16 و 18 عامًا باستخدام نموذج ADDIE الحساس ثقافيًا، وتم تنفيذ البرنامج وتقييم فعاليته من خلال طرق الاختبار القبلي والبعدي، وتم اتباع المنهج التكاملي، وأظهرت النتائج انخفاض مستويات المعرفة بالنظافة الإلكترونية، والاستخدام المفرط لشبكات VPN وأن المحاضرات هي طريقة التعلم المفضلة، كما أظهرت النتائج زيادة في المعرفة العامة بشأن الأمن السيبراني عقب الانتهاء من البرنامج.

كذلك هدفت دراسة: (Witsenboer, 2022)، بعنوان: قياس الوعي بالأمن السيبراني عبر الإنترنت لدى طلاب المدارس الابتدائية والثانوية في هولندا، حيث استخدمت الدراسة استبيان الجوانب الإنسانية لأمن المعلومات (HAIS-Q) الذي تم التحقق منه بشكل أساسي من قبل (Parsons et al. 2017) واستبيان (Arachchilage & Love, 2014)، للعناصر الإضافية. وقد كشفت هذه الدراسة أن مستوى بالأمن السيبراني عبر الإنترنت لدى طلاب المدارس الابتدائية والثانوية في هولندا كان متوسطاً، أن المناهج المدرسية الهولندية بالكاد تولي

اهتماما لموضوع الأمن السيبراني عبر الإنترنت لدى طلاب المدارس الابتدائية والثانوية في هولندا وأن الطلاب يكتسبون سلوكهم عبر الإنترنت بشكل رئيسي من خلال الخبرة والتعليمات على الإنترنت ومن خلال أولياء الأمور ومن خلال الأشقاء. بالإضافة إلى ذلك، طور العديد من الطلاب سلوكًا متهورًا بمرور الوقت.

وهدفت دراسة أنديجاني وفلمباوي (2021) إلى تعرّف ممارسات تعزيز الوعي بثقافة الأمن السيبراني وتوصياتها في المملكة العربية السعودية، وتعرّف الفئات المستهدفة بتعزيز الوعي بثقافة الأمن السيبراني، واتبعت الدراسة السبع مراحل لمنهج المراجعة المنهجية للدراسات السابقة، ووضحت الدراسة العوائد وأهمية الدراسة الاجتماعية والبيئية والاقتصادية والثقافية والمحلية والدولية، وتوصلت الدراسة إلى تفاوت درجات الوعي من درجة منخفضة إلى درجة عالية لدى المعلمات، والقيادة المدرسية، والتعرض للانتهاكات السيبرانية، والوعي بمخاطر البيئة السيبرانية، ودور القيادة المدرسية في تعزيز الوعي بثقافة الأمن السيبراني، كما اتضح أن درجة الوعي لدى طلاب وطالبات التعليم العام للمرحلة الابتدائية والمتوسطة في التعامل الآمن مع خدمات تصفح الإنترنت والقيم الوطنية والأخلاقية والدينية مرتفعة بدرجة كبيرة، وأن درجة الوعي بالأمن السيبراني لدى الطلاب والطالبات تتفاوت من درجة منخفضة إلى درجة عالية.

وهدفت دراسة عسيري وآخرون (2021) لتعرف مستوى الوعي بالأمن السيبراني، ومستوى الانتماء الوطني لدى طلبة المرحلة الثانوية بمدينتي مكة وجدة بمنطقة مكة المكرمة، كما سعت الدراسة أيضاً لمعرفة الفروق في الانتماء بين أفراد الدراسة والذي يعزى لاختلاف خصائصهم الديموغرافية كالجنس والمدينة والتخصص والمرحلة الدراسية، بالإضافة إلى الكشف عن العلاقة بين الوعي بالأمن السيبراني وقيم الانتماء الوطني، وكذلك معرفة الإسهام الذي يسهمه متغير الوعي بالأمن السيبراني في قيم الانتماء الوطني وذلك باختبار نموذج خطي بينهما بأسلوب الانحدار الخطي البسيط، وتكونت العينة من (714) طالباً وطالبة، ولغرض جمع البيانات تم تطوير مقياس الوعي بالأمن السيبراني مكون من مجالين، الأول حماية الأجهزة ووسائل التخزين، والثاني التعامل الآمن مع خدمات الإنترنت والبرامج، بينما تكون مقياس الانتماء الوطني من مجال واحد فقط، وكانت مستويات ثبات المقياسين مقبولة لأجل أغراض هذه الدراسة، وجاء في نتائج الدراسة، أن الطلاب لديهم مستوى وعي متوسط في التعامل مع الأجهزة ووسائل التخزين، ومستوى وعي عالٍ في التعامل الآمن مع خدمات الإنترنت والبرامج، وكذلك

مستوى وعي عال على المقياس ككل، كما حققوا مستوى عالٍ أيضاً على مقياس الانتماء الوطني، وفيما يخص الفروق بين أفراد العينة، كانت مشاعر الانتماء لدى الإناث أكبر من الذكور، كما عكس طلبة الصف الثاني ثانوي مشاعر انتماء أكبر من نظرائهم في الصف الأول والثالث ثانوي، بينما لم توجد فروق مهمة بين العينة تعزى لمتغيرات المدينة، أو التخصص، كما أشارت النتائج لوجود علاقة طردية ذات دلالة إحصائية بين الوعي بالأمن السيبراني وقيم الانتماء، وأن الوعي بالأمن السيبراني يتنبأ بقيم الانتماء الوطني.

استهدفت دراسة بنت إبراهيم (2021) الكشف عن فاعلية برنامج تدريبي مقترح لتنمية الوعي بجوانب الأمن السيبراني في التعليم عن بعد لدى معلمات العلوم بالمرحلة الابتدائية في المملكة العربية السعودية، واستخدمت المنهج التجريبي ذو التصميم شبه التجريبي ذي المجموعة الواحدة، وتمثلت أداة الدراسة في مقياس الوعي بجوانب الأمن السيبراني في التعليم عن بعد، وشمل مجتمع الدراسة معلمات العلوم بالمرحلة الابتدائية، وتكونت عينة الدراسة من (30) معلمة، وطبق مقياس الوعي بجوانب الأمن السيبراني في التعليم عن بعد قبليًا، وبعد تدريب المعلمات على البرنامج المقترح خلال الفصل الدراسي الأول لعام 1441– 1442هـ، بواقع (10) جلسات تدريبية، ثم طبق المقياس بعديا، وأسفرت نتائج الدراسة عن وجود فرق ذي دلالة إحصائية عند مستوى (0,05) بين متوسطي درجات المعلمات في التطبيقين القبلي والبعدي لمقياس الوعي، لصالح التطبيق البعدي، ويدل هذا على فاعلية البرنامج التدريبي المقترح.

التعليق على الدراسات السابقة:

اتفقت الدراسة الحالية مع الدراسات السابقة في تناولها للأمن السيبراني وفي المنهج المستخدم في كثير منها وهو المنهج الوصفي، إلا أنها تختلف عنها في تناول درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث وهو ما تنفرد به الدراسة الحالية.

كما تتفق الدراسة الحالية مع الدراسات السابقة في المنهج المستخدم، وهو المنهج الوصفي، كما تتفق مع بعضها في العينة، وهم مديرو المدارس، وكذلك في الأداة، حيث تستخدم الاستبانة كأداة لها.

وتميزت الدراسة الحالية عن الدارسات السابقة في تناولها لإسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث، وهو ما لم تتطرق إليه أي دراسة سابقة على حسب علم الباحث.

ومن خلال الاطلاع على بعض الدراسات السابقة المرتبطة بموضوع الدراسة الحالية "إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث"، ومراجعة أدبياتها ومحتوياتها يمكن حصر أوجه الاستفادة من تلك الدراسات كالتالي:

–كتابة الإطار النظري المتعلق بكل من مديري المدارس، والوعي بالأمن السيبراني.

–معرفة الخلفية النظرية المرتبطة بإسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث.

–تعرّف المنهجية العلمية المستخدمة.

–الاستفادة منها في إعداد أدوات الدراسة والمنهج المستخدم.

–تحديد الأساليب الإحصائية المناسبة لمعالجة البيانات الخاصة بنتائج الدراسة.

–مناقشة نتائج الدراسة، وكتابة التوصيات وتقديم بحوث مقترحة في ضوء الدراسات السابقة المرتبطة بإسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث، والاستفادة منها في تدعيم الإطار النظري وتحليل وتفسير نتائج الدراسة الحالية.

منهجية الدراسة وإجراءاتها:

منهج الدراسة: اعتمدت الدراسة على المنهج الوصفي بأسلوبه المسحي؛ لملاءمته لطبيعة البحث الحالي.

مجتمع وعينة الدراسة: يتكون مجتمع الدراسة من معلمي وموجهي الطلاب بمدارس التعليم العام بإدارة تعليم الليث بمراحلها الثلاث (ابتدائي – متوسط – ثانوي) والبالغ عددهم (1972) فرداً. وذلك بواقع (1886) معلماً و(86) موجهاً طلابياً، وذلك حسب إحصائية شؤون المعلمين التابعة لإدارة التعليم بمحافظة الليث. خلال العام الدراسي لعام 1444– 1445هـ. وقد تم اعتماد معادلة ستيفن ثامبسون لتحديد حجم العينة المناسب. وشملت عينة الدراسة (320) معلما و(70) موجهاً طلابياً، من معلمي وموجهي الطلاب بمدارس التعليم العام بإدارة تعليم الليث بمراحلها الثلاث (ابتدائي – متوسط – ثانوي)، تم اختيارهم بطريقة العينة الميسرة، حيث استفاد الباحث

من نماذج قوقل ضمن تطبيق (Google Forms) في توزيع رابط الاستبانة على مجتمع الدراسة.

أداة الدراسة وصدقها وثباتها: يتكون الاستبيان من جزأين:

الجزء الأول: اشتمل على البيانات الأولية لعينة الدراسة وتشمل الخصائص الديموغرافية للعينة (المرحلة الدراسية – المؤهل العلمي – سنوات الخبرة – الدورات التدريبية في التقنية).

الجزء الثاني: اشتمل على ثلاث محاور على النحو التالي:

- **المحور الأول:** درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين، واشتمل على (14) عبارة
- **المحور الثاني:** درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين، واشتمل على (15) عبارة

صدق وثبات أداة الدراسة:

أولاً: صدق الصدق الظاهري (صدق المحكمين):

للتأكد من صدق أداة الدراسة (الاستبيان) وقدرته على قياس متغيرات الدراسة، قام الباحث بعرض الاستبيان في صورته الأولية على عدد (17) محكماً من أعضاء هيئة التدريس بعدد من جامعات المملكة العربية السعودية وإدارات التعليم، وطلب منهم إبداء آرائهم وملاحظاتهم في مدى مناسبة عبارات، ومدى وضوحها، وانتمائها للبعد الذي وضعت فيه، وقد أبدى المحكمون عددٍ من الملحوظات والمرئيات التي قام الباحث بعد ذلك بالتعديل عليها بناءً على نسبة الاتفاق بين المحكمين باستخدام معادلة "كوبر" ليمكن القول بأن الاستبيان صادقًا من حيث المحتوى. وتمت مراجعته مع المشرف على الدراسة والخروج بصيغة نهائية وأخذ الموافقة النهائية على تنفيذها.

ثانياً: الصدق الداخلي (الاتساق):

للتأكد من صدق الاتساق الداخلي لأداة الدراسة قام الباحث بحساب درجة ارتباط كل عبارة من عبارات الاستبيان مع الدرجة الكلية للاستبيان باستخدام معامل ارتباط بيرسون الخطي والجدول التالي يوضح النتائج:

جدول (1) معاملات ارتباط بيرسون لحساب الاتساق الداخلي لعبارات أداة الدراسة

العبارة	معامل الارتباط	العبارة	معامل الارتباط	العبارة	معامل الارتباط	العبارة
1	(**)0.664	10	(**)0.443	19	(**)0.548	28
2	(**)0.854	11	(**)0.551	20	(**)0.612	29
3	(**)0.752	12	(**)0.828	21	(**)0.478	
4	(**)0.464	13	(**)0.631	22	(**)0.557	
5	(**)0.873	14	(**)0.791	23	(**)0.597	
6	(**)0.537	15	(**)0.838	24	(**)0.419	
7	(**)0.388	16	(**)0.768	25	(**)0.890	
8	(**)0.767	17	(**)0.695	26	(**)0.791	
9	(**)0.581	18	(**)0.513	27	(**)0.753	

(**) دالة احصائياً عند مستوى معنوية (0.01) – (*) دالة احصائياً عند مستوى معنوية (0.05)

يتضح من الجدول (1) أن معاملات الارتباط بين عبارات الاستبيان مع الدرجة الكلية جاءت جيدة ودالة احصائياً عند (0.01) وهي قيم ارتباط موجبة وجيدة. كما قام الباحث بحساب الاتساق الداخلي للاستبيان عن طريق حساب معاملات ارتباط بيرسون بين كل عبارة من عبارات كل محور من محاور الاستبيان مع الدرجة الكلية للمحور الذي تنتمي إليه والنتائج موضحة في الجدول التالي:

جدول (2) معاملات ارتباط عبارات كل محور من محاور الاستبيان مع الدرجة الكلية للمحور الذي تنتمي إليه

المحور الأول				المحور الثاني			
رقم العبارة	درجة الارتباط	رقم العبارة	درجة الارتباط	رقم العبارة	درجة الارتباط	رقم العبارة	درجة الارتباط
1	(**)0.414	9	(**)0.535	1	(**)0.369	9	(**)0.398
2	(**)0.502	10	(**)0.522	2	(**)0.421	10	(**)0.444
3	(**)0.609	11	(**)0.676	3	(**)0.621	11	(**)0.702
4	(**)0.877	12	(**)0.536	4	(**)0.489	12	(**)0682
5	(**)0.616	13	(**)0.470	5	(**)0.552	13	(**)04560
6	(**)0.594	14	(**)0.527	6	(**)0.620	14	(**)0.827
7	(**)0.413			7	(**)0.393	15	(**)0619
8	(**)0.422			8	(**)0.521		

**معامل الارتباط دال عند (0.01)

من الجدول (2) نجد أن قيم معاملات الارتباط بين عبارات المحور الاول: "درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين" مع الدرجة الكلية للمحور كانت جميعها دالة احصائياً عند (0.01) وتراوحت بين (0.877 – 0.413). كما نجد أن قيم معاملات الارتباط بين عبارات المحور الثاني: "درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الطلاب"مع الدرجة الكلية للمحور كانت جميعها دالة احصائياً عند (0.01) وتراوحت بين (0.722 – 0.358) كذلك نجد أن قيم معاملات الارتباط بين عبارات المحور الثالث "درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين" مع الدرجة الكلية للمحور كانت جميعها دالة احصائياً عند (0.01) وتراوحت بين (0.827 – 0.369) وهي درجات موجبة ومرتفعة. وبالتالي فإن هذه القيم تشير إلى أن الاستبيان يتمتع بدرجة مقبولة من الاتساق الداخلي.

ثبات أداة الدراسة:

تم التحقق من ثبات أداة الدراسة (الاستبيان) في الدراسة الحالية باستخدام معامل كرونباخ ألفا (Cronbach Alpha) والجدول التالي يبين النتائج:

جدول رقم (3) معامل الفا كرونباخ لمحاور أداة الدراسة

البعد	عدد العبارات	معامل ألفا كرونباخ
درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين	14	0.871
درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين	15	0.821
الدرجة الكلية للاستبيان	**29**	**0.931**

من الجدول (3) نجد أن معاملات ألفا كرونباخ لأبعاد الاستبيان تراوحت بين (0.821–0.871) وبلغت قيمة معامل الفا كرونباخ للاستبيان ككل (0.931) وهي قيم عالية جداً تدل على أن الاستبيان يتسم بدرجة جيدة من الثبات.

نتائج الدراسة ومناقشتها وتفسيرها:

نتائج الإجابة عن السؤال الأول الذي نص على ما يلي: "ما درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين؟" وللإجابة على هذا السؤال قام الباحث بحساب المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية لاستجابات عينة الدراسة حول عبارات المحور الأول من أداة الدراسة، كما بالجدول التالي:

جدول (4) المتوسطات الحسابية والانحرافات المعيارية لاستجابات عينة الدراسة حول درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين

م	العبارة	المتوسط الحسابي	الانحراف المعياري	درجة الممارسة
1	معالجة الثغرات في الأنظمة التقنية.	4.12	0.9	مرتفعة جداً
2	تطوير المصادر المفتوحة لتحقيق مبادئ الأمن السيبراني.	2.59	0.93	منخفضة
3	المحافظة على سلامة البيانات.	3.7	0.74	مرتفعة
4	تجهيز البيانات المطلوبة.	4.19	0.74	مرتفعة
5	حماية الأجهزة والشبكات من الاختراقات.	4.15	0.89	مرتفعة جداً
6	الحد من التجسس الإلكتروني على مستوى المدرسة.	3.63	0.88	مرتفعة
7	تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة.	3.93	0.78	مرتفعة
8	مواجهة الهجمات المستهدفة لأمن المعلومات.	3.68	0.83	مرتفعة
9	توفير بيئة آمنة تتمتع بقدر كبير من الموثوقية في المعلومات الخاصة بالمدرسة.	3.12	0.83	متوسطة
10	التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة بأنواعها.	3.65	0.85	مرتفعة
11	تنظيم دروات تدريبية للتوعية بالأمن السيبراني	3.54	1.01	مرتفعة
12	اختيار كلمة مرور قوية للحسابات الشخصية.	3.75	0.67	مرتفعة
13	توعية المعلمين بجهود هيئة الأمن السيبراني باستمرار	4.14	0.89	مرتفعة جداً
14	إشراك المعلمين في وضع الخطط والبرامج التوعوية الهادفة إلى تعزيز الأمن السيبراني داخل المدرسة.	4.22	1.02	مرتفعة جداً
	المتوسط العام	**3.74**	**0.85**	**مرتفعة**

يتضح من الجدول (4) أن المتوسط العام لاستجابات عينة الدراسة حول درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين بلغ (3.74) وبلغ الانحراف المعياري الكلى (0.85) والمتوسط يقع ضمن الفترة (من 3.40 إلى أقل من 4.20) والمتوسط ضمن هذه الفترة من التدرج الخماسي يشير إلى أن درجة إسهام مديري

المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين وجهة نظر المعلمين والموجهين الطلابيين مرتفعة.

وبترتيب متوسطات استجابات عينة الدراسة حول عبارات محور درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين نجد أن العبارة (إشراك المعلمين في وضع الخطط والبرامج التوعوية الهادفة إلى تعزيز الأمن السيبراني داخل المدرسة) جاءت في المرتبة الأولى بمتوسط (4.22) وبدرجة ممارسة مرتفعة جداً،. وفي المرتبة الثانية حلت العبارة (تجهيز البيانات المطلوبة) وذلك بمتوسط (4.19) وبدرجة ممارسة مرتفعة.

وفي المرتبة الثالثة نجد العبارة (حماية الأجهزة والشبكات من الاختراقات) بمتوسط (4.15) وفي المرتبة الرابعة نجد العبارة (توعية المعلمين بجهود هيئة الأمن السيبراني باستمرار) بمتوسط (4.14). وحلت العبارة (معالجة الثغرات في الأنظمة التقنية) في المرتبة الخامسة بمتوسط (4.12) تليها العبارة (تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة) بمتوسط (3.93) وفي المرتبة السابعة نجد العبارة (اختيار كلمة مرور قوية للحسابات الشخصية) بمتوسط (3.75) وفي المرتبة الثامن نجد العبارة (المحافظة على سلامة البيانات) تليها العبارة (مواجهة الهجمات المستهدفة لأمن المعلومات) بمتوسط (3.68) ثم العبارة (التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة بأنواعها) بمتوسط (3.65) وفي المرتبة الحادية عشر نجد العبارة (الحد من التجسس الإلكتروني على مستوى المدرسة.) بمتوسط (3.63) وفي المرتبة الثانية عشرة نجد العبارة (تنظيم دروات تدريبية للتوعية بالأمن السيبراني) بمتوسط (3.53).

وفي المرتبة قبل الأخيرة نجد العبارة (توفير بيئة آمنة تتمتع بقدر كبير من الموثوقية في المعلومات الخاصة بالمدرسة) بمتوسط (3.12) وبدرجة ممارسة متوسطة. وفي المرتبة الأخيرة نجد العبارة (تطوير المصادر المفتوحة لتحقيِق مبادئ الأمن السيبراني) بمتوسط (2.59) وبدرجة موافقة منخفضة.

ويمكن تفسير هذه النتيجة التي أشارت إلى أن درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى المعلمين وجهة نظر المعلمين والموجهين الطلابيين مرتفعة، بأن مديري المدارس في ظل التطور الرقمي والمعلوماتي المعاصر

يديرون مدارسهم في بيئة معقدة تقنياً ومواجهه بالعديد من التهديدات السيبرانية لا سيما وأن المملكة العربية السعودية بعد رؤية 2030 اتخذت خطوات جبارة في طريق التحول الرقمي، وبالتالي كان لابد من مواجهة التحديات والمخاطر التي تصاحب ذلك التحول، الأمر الذي يجعل مديري المدارس يحرصون على توعية المعلمين ورفع مستويات معرفتهم بالأمن السيبراني ومخاطره وكيفية حماية المدرسة ونظامها من الاختراقات والحرص على أن يتم العمل دون تهديد أو اختراق.

وتأتي هذه النتيجة مخالفة لما توصلت اليه دراسة المنتشري (2020) التي بينت أن دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات ولدى طالبات المدرسة يتحقق بدرجة قليلة من وجهة نظر المعلمات.

نتائج الإجابة عن السؤال الثاني الذي نص على ما يلي: "ما درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين؟" وللإجابة على هذا السؤال قام الباحث بحساب المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية لاستجابات عينة الدراسة حول عبارات المحور الثاني من أداة الدراسة، كما بالجدول التالي:

جدول (5) المتوسطات الحسابية والانحرافات المعيارية لاستجابات عينة الدراسة حول درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين

م	العبارة	المتوسط الحسابي	الانحراف المعياري	درجة الممارسة
1	طلب تحديث كلمة المرر باستمرار.	3.71	0.76	مرتفعة
2	التوجيه بعدم ترك الأجهزة مفتوحة دون استخدام.	3.41	0.78	مرتفعة
3	تصميم برامج توعوية لتعزيز الأمن السيبراني وأليات تعزيزه.	3.72	0.93	مرتفعة
4	توجيه الطلاب بعدم الإفصاح عن البيانات الشخصية نهائيا.	4.22	0.71	مرتفعة جداً
5	وضع ضوابط لحماية الأصول المعلوماتية المدرسية من الوصول غير المسموح به.	3.34	0.68	متوسطة
6	توضيح الإجراءات اللازم اتباعها لحماية البيئة المادية للمعلومات.	3.13	0.75	متوسطة
7	توضيح الإجراءات اللازم اتباعها للاستخدام الآمن لشبكة الإنترنت .	4.14	0.76	مرتفعة
8	تبيين الإجراءات اللازم اتباعها في حال التعرض لأحدى الجرائم السيبرانية.	3.31	0.82	متوسطة
9	استضافة المختصين في الأمن السيبراني بهدف توضيح آليات تجنب تداعياته.	2.28	1.68	منخفضة
10	التنسيق مع الهيئة الوطنية للأمن السيبراني لتنظيم برامج توعوية بالأمن السيبراني داخل المدرسة.	2.3	1.65	منخفضة

م	العبارة	المتوسط الحسابي	الانحراف المعياري	درجة الممارسة
11	فحص جهاز الحاسوب ووسائط التخزين المادية بشكل دوري للتأكد من خلوها من الفيروسات والبرمجيات الخبيثة.	2.15	0.87	منخفضة
12	تحديث برامج التشغيل ومتصفح شبكة الإنترنت بشكل دوري.	4.13	0.86	مرتفعة
13	التحذير من عدم تحميل برامج أو تطبيقات من مواقع مجهولة المصدر.	3.54	0.96	مرتفعة
14	التأكيد على أهمية قراءة التعليمات الخاصة بالبرامج والتطبيقات التي يتم تحميلها قبل الاستمرار.	4.21	0.93	مرتفعة جداً
	المتوسط العام	**3.40**	**0.94**	**مرتفعة**

يتضح من الجدول (8) أن المتوسط العام لاستجابات عينة الدراسة حول درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين بلغ (3.40) وبلغ الانحراف المعياري الكلى (0.94) والمتوسط يقع ضمن الفترة (من 3.40 إلى أقل من 4.20) والمتوسط ضمن هذه الفترة من التدرج الخماسي يشير إلى أن درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين من وجهة نظر المعلمين والموجهين الطلابيين مرتفعة.

بترتيب متوسطات استجابات عينة الدراسة حول عبارات محور درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين نجد أن العبارة (حماية الأجهزة والشبكات من الاختراقات) جاءت في المرتبة الأولى بمتوسط (4.22) وبدرجة ممارسة مرتفعة جداً، وفي المرتبة الثانية حلت العبارة (التأكيد على أهمية قراءة التعليمات الخاصة بالبرامج والتطبيقات التي يتم تحميلها قبل الاستمرار) وذلك بمتوسط (4.21) وبدرجة ممارسة مرتفعة جداً. وفي المرتبة الثالثة نجد العبارة (توضيح الإجراءات اللازم اتباعها للاستخدام الآمن لشبكة الإنترنت) بمتوسط (4.14) وفي المرتبة الرابعة نجد العبارة (تحديث برامج التشغيل ومتصفح شبكة الإنترنت بشكل دوري) بمتوسط (4.13). وحلت العبارة (تصميم برامج توعوية لتعزيز الأمن السيبراني وأليات تعزيزه) في المرتبة الخامسة بمتوسط (3.72) تليها العبارة (طلب تحديث كلمة المرر باستمرار) بمتوسط (3.71) وفي المرتبة السابعة نجد العبارة (التحذير من عدم تحميل برامج أو تطبيقات من مواقع مجهولة المصدر) بمتوسط (3.54) وفي المرتبة الثامنة نجد العبارة (التوجيه بعدم ترك الأجهزة مفتوحة دون استخدام.) بمتوسط (3.41) تليها العبارة (وضع ضوابط لحماية الأصول المعلوماتية المدرسية من الوصول غير المسموح

بـه.) بمتوسـط (3.34) ثـم العبـارة (تبيين الإجـراءات الـلازم اتباعهـا فـي حـال التعـرض لأحـدى الجرائم السيبرانية) بمتوسط (3.31) وفي المرتبة الحادية عشر نجد العبارة (توضيح الإجراءات اللازم اتباعها لحماية البيئة المادية للمعلومات) بمتوسط (3.13) وفي المرتبة الثانية عشرة نجد العبارة (التنسيق مع الهيئة الوطنية للأمن السيبراني لتنظيم برامج توعوية بالأمن السيبراني داخل المدرسة) بمتوسط (2.30). وفي المرتبة قبل الأخيرة نجد العبارة (استضافة المختصين في الأمن السيبراني بهدف توضيح آليات تجنب تداعياته) بمتوسط (2.28) وبدرجة ممارسة منخفضة. وفي المرتبة الأخيرة نجد العبارة (فحص جهاز الحاسوب ووسائط التخزين المادية بشكل دوري للتأكد من خلوها من الفيروسات والبرمجيات الخبيثة) بمتوسط (2.15) وبدرجة موافقة منخفضة.

ويعزو الباحث هذه النتيجة التي أشارت إلى أن درجة إسهام مديري المدارس في رفع مستوى الوعي بالأمن السيبراني بمدارس تعليم الليث لدى الموجهين الطلابيين من وجهة نظر المعلمين والموجهين الطلابيين مرتفعة. إلى تقدير مديري المدارس لأهمية الأمن السيبراني باعتبار أن المدرسة بشكل عام والموجهين الطلابيين معنيين بالمساعدة في بناء جيل رقمي يتقن استخدام تقنيات الاتصال المختلفة منذ سنوات عمره المبكرة، يعرف كيف يبحر في الفضاء السيبراني دون أن يعرض نفسه أو أنظمته التي يستخدمها لخطر الاختراق والجرائم السيبرانية. بالإضافة إلى حاجة الموجهين الطلابيين أنفسهم لامتلاك الوعي بالأمن السيبراني لضمان سرية وخصوصية الوثائق التعليمية والحفاظ على سلامتها بشكل مستمر، ومتابعة ومراقبة وتطوير وضبط نظام المعلومات والأمن في المدرسة، ومراقبة أي محاولات للتسلل إلى شبكات المعلومات الخاصة بالمدرسة كمؤسسة تربوية.

التوصيات:

- ضرورة اتخاذ وزارة التعليم التدابير والسياسيات اللازمة لضمان حصول جميع المعلمين والموجهين الطلابيين والطلاب على مستوى عال من الوعي بالأمن السيبراني من خلال التدريب وتشجيع البحث العلمي في مجال الأمن السيبراني.
- تنفيذ تعليم الأمن السيبراني كجزء من المناهج الدراسية في مدارس التعليم العام بالمملكة العربية السعودية، وذلك بإدخاله ضمن مناهج الحاسب.

- إجراء برامج تدريبية للتوعية بالأمن السيبراني، مع منح المعلمين والموجهين الطلابيين الأولوية في البرامج التدريبية التي ستنفذها وزارة التعليم. ومن خلال حصول المعلمين والموجهين على هذا النوع من البرامج التدريبية، سيكون لدى طلاب المدارس الوعي الكافي بالاستخدام الآمن للإنترنت وتقليل مخاطر الجرائم الإلكترونية.
- ضرورة قيام الجامعات بإعداد المعلمين الخريجين الجدد بتعلم موضوعات الأمن السيبراني وممارسات الحوسبة الآمنة، من خلال اضافته للمواد الدراسية والتطبيقات العملية ضمن الكلية.
- منح الحوافز المادية والمعنوية المناسبة التي تعمل على دعم وتشجيع الموظفين المتميزين والمبدعين في مجال الأمن السيبراني.
- التنسيق بين إدارات التعليم والجهات المختصة المعنية بالأمن السيبراني في المملكة العربية السعودية لتقديم برامج تسهم في رفع مستوى وعي المعلمين، الطلاب والموجهين الطلابيين بالأمن السيبراني بالإضافة إلى آليات حماية البيئة المادية لشبكة الإنترنت.

قائمة المراجع:

أولا: المراجع العربية:

أنديجاني، دلال صالح، وفلمبان، فدوى ياسين. (2021). ممارسات تعزيز الوعي بثقافة الأمن السيبراني وتوصياتها في المملكة العربية السعودية. *المجلة العربية للمعلومات وأمن المعلومات، (4)، 75- 102.*

بنت إبراهيم، منال حسن محمد. (2021). الوعي بجوانب الأمن السيبراني في التعليم عن بعد .*المجلة العلمية لجامعة الملك فيصل – العلوم الإنسانية والإدارية، 22(2)، 299- 307.*

التيماني، مداخل زيد عبدالرحيم. (2021). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني .*مجلة الخدمة الاجتماعية، (67)، 1- 23.*

جاب الله، وليد عبدالرحيم. (2021). الأمن السيبراني بين الاحتكار والاستثمار. *مجلة الديمقراطية، 21(82) ، 49- 53.*

جبور، منى الأشقر. (2012). *الأمن السيبراني: التحديات ومستلزمات المواجهة. اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني*. جامعة الدول العربية: المركز العربي للبحوث الفضائية والقانونية، بيروت، أغسطس، 27- 28.

الحربي، أيمن. (2022). مقدمة في الأمن السيبراني. واحة امان، معهد البحوث والدراسات الاستشارية، أم القرى، متاح على: https://cutt.us/pS1rk

خليفة، إيهاب. (2017). *القوى الإلكترونية كيف يمكن أن تدير الدول شئونها في عصر الإنترنت* . القاهرة: العربي للنشر والتوزيع.

الربيعة، صالح بن علي. (2017). *الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت* . الرياض: هيئة الاتصالات وتقنية المعلومات.

السعادات، خليل بن إبراهيم، والتميمي، ندى بنت عبدالله بن سعود. (2022). رفع الوعي بالأمن السيبراني لدى المعلمين في ضوء مبادئ تعليم الكبار. *آفاق جديدة في تعليم الكبار، جامعة عين شمس – مركز تعليم الكبار، (32)، 255- 280.*

الشهراني، بيان ناصر محمد، وفلمبان، فدوى ياسين. (2020). 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، 21(9)، 614- 651.*

صائغ، وفاء بنت حسن. (2018). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم المنية من الجرائم الإلكترونية. *المجلة العربية للعلوم الاجتماعية، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية، 14(3)، 18- 70.*

الصحفي، مصباح أحمد حامد، والعسكول، سناء صالح. (2019). 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، 10(20)، 493- 534.*

العتيبي، محمد، والعبدلي، عبد الله، والبارقي، أحمد. (2022). دراسة تقويمية لمنصة مدرستي من وجهة نظر الطلاب والمعلمين وقادة المدارس. المجلة العربية للعلوم التربوية والنفسية، المؤسسة العربية للتربية والعلوم والآداب، مصر، 6(27)، 385- 424.

عسيري، محمد بن جابر، والبقمي، سعود بن سعد محمد، وآل مناخرة، الحسن بن يحيى. (2021). العلاقة بين الوعي بالأمن السيبراني وقيم الانتماء الوطني لدى طلبة المرحلة الثانوية بمنطقة مكة المكرمة. *مجلة جامعة الملك عبدالعزيز – الآداب والعلوم الإنسانية، جامعة الملك عبدالعزيز، 29(8)، 61- 92.*

العقلاء، رؤى أحمد صالح، وعلي، نور الدين عيسى آدم. (2022). درجة الوعي بمفاهيم الأمن السيبراني لدى معلمي ومعلمات الحاسب الآلي بمدينة حائل. *دراسات عربية في التربية وعلم النفس، رابطة التربويين العرب، (144)، 277- 300.*

فرج، علياء عمر. (2021). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي جامعة الأمير سطام بن عبد العزيز نموذجًا. *مجلة كلية التربية، جامعة سوهاج، 1(94)، 510- 539.*

القحطاني، سالم بن سعيد، والعنزي، حمود بن محمد. (2011). *تبادل المعلومات بين الأجهزة الأمنية في المملكة العربية السعودية: دراسة ميدانية*، أطروحة دكتوراه، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، السعودية.

الملاحي، فؤاد. (2015). *الأمن السيبراني*. قطر: وزارة الإعلام، مجلة الدوحة.

المنتشري، فاطمة يوسف. (2020). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للعلوم التربوية والنفسية، 4(17)، 457- 484.*

المنتشري، فاطمة يوسف، وحريري، رنده. (2020). درجة وعى معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للتربية النوعية، المؤسسة العربية للتربية والعلوم والآداب، (14)، 95- 140.*

المنتشري، فاطمة. (2019). *وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بالأمن السيبراني*. رسالة ماجستير غير منشورة، جدة، كلية العلوم الصحية والسلوكية والتعليم، جامعة دار الحكمة.

المنيع، الجوهرة بنت عبد الرحمن. (2022). متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030. *مجلة كلية التربية، جامعة أسيوط، 38(1)، 156– 196.*

الهيئة الوطنية للأمن السيبراني. (2018). الضوابط الأساسية للأمن السيبراني. المملكة العربية السعودية، متاح على: https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

الهيئة الوطنية للأمن السيبراني. (2022). المملكة العربية السعودية. متاح على: https://nca.gov.sa

ثانيا: المراجع الأجنبية:

Borky, J. M., Bradley, T. H., Borky, J. M., & Bradley, T. H. (2019). Protecting information with cybersecurity. Effective Model-Based Systems Engineering, 345-404.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. The African Journal of Information and Communication, 20, 133-155.

Chang, XU., Pei, S. & Su, N. (2013). research on real-time network forensics based on improved data mining algorithm. Applied Mechanics and Materials. 380, 1881- 1885.

DeAndrea, D. C., Ellison, N. B., LaRose, R., Steinfield, C., & Fiore, A. (2012). Serious social media: On the use of social media for improving students' adjustment to college. The Internet and higher education, 15(1), 15-23.

Fazil, Abdul Wajid & Musawer Hakimi &, Saidamin Sajid & Quchi, Mohammad Mustafa & Khudai Qul Khaliqyar (2023). Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province, *American Journal of Education and Technology (AJET),* Volume 2 Issue 4, Year 2023.

Goran, I. (2017). Cyber security risks in public high school. Unpublished master thesis. City university of New York: John Jay college of criminal justice.

Karimnia, R., Maennel, K., & Shahin, M. (2022, February). Culturally-sensitive Cybersecurity Awareness Program Design for Iranian High-school Students. In ICISSP (pp. 121-132).

Mark, L. K., & Nguyen, T. T. T. (2017). An invitation to internet safety and ethics: School and family collaboration. Journal of Invitational Theory and Practice, 23, 62-75.

Ravendran, S., Karpudewan, M., Ali, M. N., & Fah, L. Y. (2023). Measuring teachers' knowledge on the applications of the nine pillars of the fourth industrial revolution (4ir) in education. mojes: Malaysian Online Journal of Educational Sciences, 11(2), 50-64.

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

Stallings, W., & Brown, L. (2018). Computer security: principles and practice, pearson education. *Inc., Upper Saddle River, New Jersey*.

Stewart, K., & Shilingford, N. (2011). Cybergirls Sumer camp: Exposing middle school females to Internet security. In University of Minnesota-2011 Colloquium Abstracts & Papers.

Vasiu, I., & Vasiu, L., (2018). Cybersecurity as an Essential Sustainable Economic Development Factor. European Journal of Sustainable Development. 7(4), 171-178.

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

Walsh, Ken, (2015). Leading and managing the future school – developing organizational and management structure in secondary schools. Unpublished Master Dissertation. National College for School Leadership. UK.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security.* Cengage learning.

Wilson, C. E. (2014, June). Cybersecurity Education: The Emergence of an Accredited Academic Discipline?. In Journal of The Colloquium for Information Systems Security Education (Vol. 2, No. 1, pp. 13-13).

Witsenboer, Jacob Willem Abraham & Sijtsma, Klaas & Scheele, Fedde (2022).Measuring cyber secure behavior of elementary and high school students in the Netherlands, *Journal of Computers & Education 186 (2022) 104536.*