المجلة الدولية للدراسات التربوية والنفسية

المجلد العاشر، العدد الثالث، 655:635
كانون الأول (2021)

بحث رقم 7

واقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية

مشاعل بنت شبيب بن مطيران الظويفري

ماجستير اقتصاديات التعليم وتخطيطه- وزارة التعليم- المملكة العربية السعودية
mashael1alzuwifri@outlook.sa

استلام البحث: 2021/7/8 مراجعة البحث: 2021/7/20 قبول البحث: 2021/8/12

DOI: https://doi.org/10.31559/EPS2021.10.3.7

المجلة الدولية للدراسات التربوية والنفسية
International Journal of Educational & Psychological Studies (EPS)
Journal Homepage: https://www.refaad.com/views/EPSR/Home.aspx
ISSN: 2520-4149 (Online) 2520-4130 (Print)
www.refaad.com

واقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية

مشاعل شبيب مطيران الظويفري المطيري
ماجستير اقتصاديات التعليم وتخطيطه- وزارة التعليم- المملكة العربية السعودية
mashael1alzuwifri@outlook.sa

DOI: https://doi.org/10.31559/EPS2021.10.3.7 **قبول البحث:** 2021/8/12 **مراجعة البحث:** 2021/7/20 **استلام البحث:** 2021/7/8

الملخص:

هدفت الدراسة التعرف على واقع الأمن السيبراني وآليات تفعيله في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية؛ ولتحقيق ذلك؛ تم استخدام المنهج الوصفي التحليلي، وتصميم استبانة مكونة من (46) فقرة، موزعة على ثلاثة مجالات، تم توزيعها على عينة مكونة من (418) من القيادة المدرسية (القادة والقائدات والمعلمين والمعلمات) بمدارس التعليم العام بالمدينة المنورة، وقد توصلت الدراسة إلى أن واقع الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة جاء بدرجة عالية، وبمتوسط حسابي (3.62)، وبنسبة (72%)، وأن التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة جاءت بدرجة مرتفعة أيضًا، وبمتوسط حسابي (4.15)، وبنسبة مئوية (83%)، كما أشارت نتائج الدراسة إلى عدم وجود فروق دالة إحصائياً بين متوسط استجابات أفراد عينة الدراسة في التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة باختلاف متغير النوع، أو الوظيفة، أو المؤهل العلمي، أو عدد سنوات الخبرة، أو عدد الدورات التدريبية في مجال تكنولوجيا المعلومات. كما توصلت الدراسة إلى عدد من الآليات المقترحة لزيادة فاعلية الأمن السيبراني في مدارس التعليم العام من أهمها، نشر الوعي بالأمن السيبراني لدى القيادات والمعلمين، وتعزيز وعي الطلاب بمخاطر الروابط الضارة، وتوفير دليل تفاعلي عن أخلاقيات الأمن السيبراني؛ وقد أوصت الدراسة بضرورة استخدام منسوبي المدارس استخدام كلمة مرور معقدة لحسابات الدخول المهمة، وعدم استخدم البريد الإلكتروني الرسمي في التسجيل والاشتراك في مواقع التواصل الاجتماعي أو التطبيقات الإلكترونية.

الكلمات المفتاحية: التعليم عن بعُد؛ منصة مدرستي؛ الأمن السيبراني.

1. المقدمة:

شهد العالم حدثًا جللاً يُهدد التعليم بأزمة هائلة، ربما كانت هي الأخطر خلال العقدين السابقين، إذ أن جائحة كورونا (COVID-19) ، وما نتج عنها من إغلاق للمؤسسات التربوية كالمدارس والجامعات، وضعت التعليم وغيره من القطاعات أمام تحدٍ حقيقي، وقد حالت هذه الظروف والأحداث الطارئة دون تواجد الطلبة والمعلمين في بيئة التعلم المعتادة (قاعة دراسية)، وتم فرض التباعد الاجتماعي، والتباعد الجسدي والتباعد المكاني، (عبد القادر، 2021)؛ من أجل ذلك، وحفاظاً على حياة الإنسان وصحته؛ علقت الدراسة، وتوقفت العملية التعليمية، وصار لزاماً مواجهة هذه الأزمة وتحدياتها والحد من آثارها السلبية بأكبر قدر ممكن. (محمود، 2020)

وبعد أن طال تأثير هذه الجائحة قطاع التعليم العام بكآفة مراحله ومستوياته، وامتد تأثيره إلى النظم التعليمية في جميع أنحاء العالم؛ وهذا الأمر الذي أدى إلى إغلاق المدارس والجامعات على نطاق واسع، أعلنت اليونسكو أن إغلاق المدارس والجامعات قد ألحق الضرر بأكثر من (1.5) مليار ونصف متعلم في (191) بلداً، وفقًا لتاريخ 20 أبريل 2020، والذي يمثل ذروة الأزمة، أي ما يقرب من(91.3%) من الطلاب الملتحقين بالمدارس والجامعات على مستوى العالم. ومن هنا كانت الحاجة ماسة إلى البحث عن آلية لتقديم التعليم ومواجهة الأزمات والتغلب عليها. فكان التواصل عن بُعد هو الملاذ

الوحيد في ظل استمرار الجائحة وتعذر التعليم التقليدي (وجهًا لوجه)، بحيث يبقى الناس في منازلهم ويمارسون حياتهم عبر وسائل التكنولوجيا والاتصالات، فيتلقى المتعلمون دروسهم، ويقدم الأساتذة دروسهم، وتستمر الحياة إلى حين تجاوز هذه الأزمة. (فيلالي، 2020)

وقد ذكر الدهشان (2020) أن منظمة اليونسكو نصحت الدول المتضررة بضرورة اللجوء إلى التعليم عن بُعد، وطرحت وسائل لمساعدة المؤسسات، والدول التي ترغب في العمل بنظام التعليم عن بُعد؛ وذلك من خلال توفير نماذج للتطبيقات التي يمكن من خلالها إجراء الاتصالات مع الطلاب مثل تطبيق سكايب، وتطبيق هانج أوت، والتطبيقات التي توفر مواد للقراءة وتعلم اللغة للطلاب؛ والمواقع التي توفر خدمات التعلم عن بُعد مثل الموقع العربي "إدراك" بالإضافة إلى المواقع التي يمكن للطلاب الحصول على فيديوهات تعليمية من خلالهما مثل يوتيوب، إذ تحولت التطبيقات الذكية إلى منصات تعليمية، وشهدت شركات التقنية، ومنصات التعليم رواجاً كبيراً في مجتمعات التعلم بتقديم المبادرات والحلول لقطاع التعليم.

وفي هذا الإطار اعتمدت بعض الدول على منصات تعليمية موجودة لديها بالفعل، وقامت بتطويرها لاستيعاب أكبر قدر ممكن من الطلاب، فيما قامت دول أخرى بإطلاق منصات تعليمية جديدة، ومن هذه الدول المملكة العربية السعودية التي قامت بإطلاق منصة مدرستي وانفقت عليها الكثير من أجل تقديم تجربة ناجحة في التعليم عن بُعد. وعلى الرغم من الإنفاق السخي والاستثمار الكبير في منصة مدرستي إلا أنها تعرضت لمخاطر سيبرانية عدة؛ مما أدى إلى توقفها عدة مرات بفعل هذه المخاطر، وقد يرجع ذلك إلى أن هذه تجربة جديدة على كثير من الطلاب والمعلمين، ولم يحسنوا استخدام ما لديهم من بيانات، بالإضافة إلى أن الاعتماد على التعليم الإلكتروني في مرحلة التعليم العام كان ضعيفاً جداً خلال السنوات الماضية، وكان هناك بعض التخوف من التعامل مع الأنظمة الإلكترونية لدى قطاع كبير من الطلاب والمعلمين. (يوسف، 2020)

وفي هذا الصدد لوحظ أن البعض يستخدم مواقع الإنترنت بدون المعرفة لما قد يتعرض له من مخاطر وتهديدات. وقد أكد جليسون (Gleeson, 2014) على ذلك بأنه كلما ارتفع استخدام الأفراد للإنترنت زادت احتمالية تعرضهم للأذى، واختراق أنظمة المعلومات التي قد ينتج عنها تسريب بيانات الملايين من المستخدمين. كما أكد الصحفي (2019) على أن هذه المخاطر تكمن في الدخول غير المشروع على شبكات الحاسب ونظم المعلومات ونشر الفيروسات وإتلاف البرامج، وتزوير المستندات ومهاجمة المراكز المالية والبنوك، وقد يكون على شكل إرهاب إلكتروني ينشر الشائعات والأكاذيب؛ ليفسد الأفراد والمجتمعات من خلال بث الأفكار التي تهدد العقيدة والوطن ووحدته والأخلاق والقيم، إضافة إلى نشر الرذيلة والإباحية والأفكار المنحرفة التي تستهدف المراهقين وتشوه ثقافتهم وأفكارهم.

ومن أجل ما قد يترتب على تلك المخاطر من خسائر مادية واقتصادية واجتماعية؛ فقد اتجهت الكثير من الدول المتقدمة إلى تبني مبادرات هادفة لتوفير الأمن السيبراني لجميع مستخدمي الإنترنت، وخاصة طلبة المدارس (المنتشري، 2020)، ومن أجل تحقيق أقصى استفادة من المنصات التعليمية في قطاع التعليم العام، ولتقليص الهدر الحاصل فيها جراء استخدامها بطريقة غير آمنة، وفي ضوء المخاطر والتهديدات أصبح الأمن السيبراني حديث العالم بأسره، بل وأصبح جزءًا أساسيًا من أي سياسات أمنية أو اقتصادية أو سياسية أخرى، إذ أصبح صناع القرار في مختلف الدول يضعون مسائل الأمن السيبراني كأولوية في سياستهم (الصحفي، 2019)؛ وقد جاءت هذه الدراسة لبحث الآليات المقترحة لزيادة فاعلية الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة.

الأمن السيبر اني:

ولّد التطور الهائل الذي طرأ على تكنولوجيا المعلومات خلال العقدين السابقين؛ ما يسمى اليوم الفضاء السيبراني، وهو مصطلح أشمل من الإنترنت، حيث وفر فرصاً لجميع الناس للوصول إلى المعلومات التي يريدونها في جميع المجالات من وإلى أي مكان في العالم، وتشير القواعد والأنظمة التي تحكم الفضاء السيبراني إلى أن هناك خلايا للجرائم السيبرانية في جميع أنحاء العالم وقضايا الجريمة السيبرانية في تزايد مستمر، وتزداد صعوبة ملاحقة مرتكبيها (حيمد، 2019)، ومع تطورت تكنولوجيا المعلومات (IT) الخاصة بصناعة الشبكات العالمية، مثل: الإنترنت أصبحت المنظمات معتمدة على سلامة وأمن شبكات الكمبيوتر الخاصة بهم وأجهزة الحوسبة التنظيمية الخاصة بهم. ومع ذلك أصبحت أجهزة الحوسبة التنظيمية مثل: أجهزة الكمبيوتر المكتبية، والمحمولة، والهواتف الذكية، أهدافًا بشكل متزايد للهجمات الإلكترونية. (Alexander, 2017)

ويشير الأمن السيبراني إلى الآلية التي تعتمد على الحاسوب لحماية المعدات والمعلومات والخدمات من الوصول غير القانوني وغير المصرح به (مانيطه، 2017). وترتكب الجرائم السيبرانية بواسطة استخدام الحاسوب والإنترنت، بيد أن ذلك لا يعني حصر مرتكبي جرائم الإنترنت في طبقة أو فئة معينة أو جنس معين، فمرتكبو الجريمة قد يكونون من البالغين، أو الأحداث سواءً من المتعلمين والمثقفين، من الفقراء والأغنياء، أم من الرجال والنساء. (الردفاني، 2014)

ويمكن تعريف الأمن السيبراني Cybersecurity بأنه: "النشاط الذي يؤمن حماية الموارد البشرية، والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة" (جبور، 2012). كما يعرف بأنَّه أمن الفضاء الإلكتروني، أو أمن البيئة الافتراضية الإلكترونية المعبرة عن سيادة وحق الدولة في الدفاع وحماية فضائها السيبراني المتعلق بالأمن القومي والمصالح والأهداف الحيوية (الجمل، 2020). وبالتالي قد يعبر عن التدابير المتخذة لحماية الكمبيوتر أو الشبكة من الوصول غير المصرح به للحفاظ على أمن وسلامة المعلومات المخزنة داخلها بالأمن السيبراني، كما قد يتضمن التدخلات الفنية التي تحمي البيانات ومعلومات الهوية والأجهزة من الوصول غير المصرح به

أو الضرر بما في ذلك أمن الأصول في الفضاء الإلكتروني، وبالتالي يمكن النظر إلى الأمن السيبراني على أنه تنظيم وجمع للموارد والعمليات والهياكل المستخدمة لحماية أصول محددة في الفضاء السيبراني والأنظمة التي تدعم الفضاء الإلكتروني من الأحداث التي لا تتوافق بحكم القانون مع حقوق الملكية الفعلية.

وتقع مسؤولية الأمن السيبراني على جميع الأفراد، حيث يتعين على كل مستخدم اتخاذ قرارات مستنيرة حول كيفية وصولهم إلى بياناتهم الخاصة وتخزينها، وكيف يتصرفون عند التفاعل مع أنظمة وشبكات الكمبيوتر. يمكن تحقيق ذلك على أفضل وجه عندما تكون هناك ثقافة العمل داخل مؤسستهم التي تدعم الأمن السيبراني بشكل أفضل. هذا يعني أن المؤسسة هي الهيئة الحاكمة والتنفيذية بحاجة إلى توفير القيادة التي تضمن للموظفين والطلاب والباحثين حماية أنفسهم والمؤسسة وأصحاب المصلحة من عواقب انتهاكات أمن المعلومات العرضية والهجمات السيبرانية الضارة. (Chapman, 2019)

تهديدات الأمن السيبر اني:

لقد تزايدت الجرائم المرتكبة بواسطة تقنيات المعلومات والاتصال، لاسيما عن طريق الإنترنت، وجسامة الخسائر المادية والبشرية، وتلك المتعلقة باستقرار الدول وأمن الشعوب التي تتسبب فيها، خاصة بعدما شهد الإقبال على استخدام هذه التقنيات (الراظي، 2019). وقد كشفت دراسة حديثة في مجال تكنولوجيا المعلومات أن الجرائم السيبرانية ستكلف العالم ما يقارب من (6) تريليونات دولار سنوياً في عام 2021م، وهذا ضعف المبلغ في عام 2015م، فهذه التكاليف نابعة من الأضرار والآثار الكثيرة التي تُخلفها الجرائم السيبرانية، ومنها سرقة البيانات أو تخريبها وسرقة الأموال؛ وفقد الإنتاجية؛ وسرقة الملكية الفكرية؛ والاختلاس والاحتيال؛ والاختلالات التجارية؛ واختراق الأنظمة، والإضرار بالسمعة. (فوزي، 2019)

والتهديد الأمني في هذا الإطار يتمثل في الهجمات السيبرانية التي تقوض من قدرات وظائف الشبكة المعلوماتية من خلال استغلال أحد نقاط الضعف ما يمنح المهاجم القدرة على التلاعب بالنظام، وهي عملية الاستغلال المتعمد لأنظمة الكمبيوتر والشبكات المعتمدة على التكنولوجيا من خلال البرمجيات الضارة، ويمكن حصر أهم هذه التهديدات في الآتي:

- **الأنشطة غير المصرح بها**: التي تستهدف مسح أو تعديل أو إعاقة نظام التشغيل (ملاك، 2016)، وتشمل جرائم الدخول غير المشروع إلى نظام معلوماتي أو المكوث فيه، مع التعرض للبيانات المعلوماتية وإعاقة عملها، وقد تتضمن الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح، أو ترخيص مسبق يتيح القيام بالمعالجة، وإنشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليها. (الردفاني، 2014)
- **البرمجيات الخبيثة:** وتتمثل في التخمين والخداع والبرمجيات الخبيثة والنفاذ لملف تخزين كلمات المرور والتحكم بالأجهزة. (بونيف، 2019)
- **محاولات الاختراق**: وتستهدف هذه الهجمات البنية التحتية للنظام من شبكات اتصالات وأغذية وصرافة، فكلما كانت البُنى التحتية مرتبطة بشكل كبير بالإنترنت كان تأثير هذه الهجمات أقوى على النظام، وتحاول المنظمات تشديد الرقابة على الكهرباء لكونها المشغل الأساسي لكل الأنظمة، ويجب أن يكون هناك خطط منظمة لحماية البنى التحتية من أي هجوم. (السرحان والمشاقبة، 2020)
- **الاحتيال الإلكتروني**: يتخذ الاحتيال الإلكتروني أشكالًا متعددة؛ منها: إيهام الضحية (المجني عليه) بوجود مشروع كاذب، وقد يتخذ اسم أو صفة كاذبة؛ تمكنه من الاستيلاء على الضحية؛ فيتم التواصل مع الضحية من خلال اتصال الجاني بالضحية عن طريق الشبكة؛ أو قد يتعامل الجاني مباشرة مع بيانات الحاسب، فيستعمل البيانات الكاذبة التي تساعده في الخداع والاحتيال عليه. (المنتشري، 2020)
- **انتحال اسم المجال:** يستغل هذا النوع من الهجمات أوجه القصور في بروتوكولات الاستقبال والإرسال لمحاولة التسلل إلى النظام حيث أن آلية عمل معظم البروتوكولات تعد من المعلومات العامة التي يسهل على الجميع معرفتها، فتشمل الهجمات إعادة توجيه الرسائل، أو منع إرسالها إلى طرف معين. (السرحان والمشاقبة، 2020)
- **الدخول والتعديل:** تتضمن هذه الجرائم كل من قدم أو أنتج أو وزع أو حاز بغرض الاستخدام جهازاً أو برنامجاً معلوماتيًا، أو أي بيانات معلوماتية معدة، أو كلمات سر أو أكواد دخول؛ وذلك بغرض اقتراف الجرائم السيبرانية. (الردفاني، 2014)
- **هجمات مستهدفة:** هو القيام باختراق شبكة أو جهاز إلكتروني؛ بهدف سرقة المعلومات المخزّنة فيه، والتي عادة ما تكون على درجة كبيرة من الأهمية؛ سواءً أكانت معلومات عسكرية؛ أم اقتصادية؛ أم صناعية؛ أم تجارية، أم غيرها، وهو ما يترتب عليه آثار إستراتيجية فادحة في الطرف المستهدف. (العيسى، 2019)
- **تسريب البيانات:** أن أشهر الجرائم انتشارًا هي جرائم الدخول غير المشروع إلى البريد الإلكتروني للآخرين، وإنشاء مواقع للتشهير. (فوزي، 2019)
- **الهندسة الاجتماعية**: تشير إلى عملية تلاعب بالبشر وخداعهم بهدف الحصول على بيانات أو معلومات؛ كانت ستظل خاصة وآمنة، ولا يمكن الوصول إليها بهدف اختراق النظام. (الصحفي، 2019)
- **التنمر الإلكتروني:** يُقصد به استخدام تكنولوجيا الاتصالات لأغراض التحرش والمضايقة والإزعاج، والتهديد، والابتزاز، وقدانتشر التنمر الإلكتروني كأحد أشكال المخاطر السيبرانية بصورة كبيرة مع انتشار الأجهزة اللوحية والهواتف الذكية. (المنتشري، 2020)

زيادة فاعلية الأمن السيبر اني:

لضمان حماية البيانات والمعلومات، هناك جملة من العناصر الضرورية لزيادة فاعلية الأمن السيبراني حصرها الصانع (2020) في: السرية والأمن: أي التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك؛ والتكاملية وسلامة المحتوى: وذلك بالتأكد من أن محتوى المعلومات صحيح، ولم يتم تعديله أو تدميره أو تغييره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواءً في مرحلة التعامل الداخلي، أو المعلومات، أو عن طريق التدخل غير المشروع؛ واستمرارية توفر المعلومات أو الخدمة: أي بالتأكد من استمرارية عمل النظام المعلوماتي واستمرارية القدرة على التفاعل مع المعلومات، وأن المستخدم لن يتعرض لمنع الدخول إلى النظام.

في هذا الصدد قدمت الهيئة الوطنية للأمن السيبراني العديد من التوصيات بهذا الشأن منها ما يلي (الهيئة الوطنية للأمن السيبراني، 2021): تعزيز الصمود السيبراني لتمكين العاملين والموظفين من أداء أعمالهم عن بُعد دون الحاجة للحضور إلى مقر العمل، وفي هذا الإطار أُطلِقت قائمة بضوابط الأمن السيبراني للعمل عن بعد، تضمنت: التوعية بالأمن السيبراني؛ وإدارة هويات الدخول والصلاحيات؛ وحماية الأنظمة وأجهزة معالجة المعلومات؛ وإدارة أمن الشبكات؛ والتشفير؛ ومراقبة الأمن السيبراني، وإدارة الحوادث. كما قدمت عدداً من البرامج والمبادرات الوطنية التي قد تساهم في رفع مستوى وفاعلية الأمن السيبراني مثل:

- المركز الوطني الإرشادي للأمن السيبراني: من أجل رفع مستوى الوعي بالأمن السيبراني، وتجنب المخاطر السيبرانية، وتقليل آثارها أُطلِق المركز الوطني الإرشادي للأمن السيبراني؛ ليعمل على إصدار التنبيهات بآخر وأخطر الثغرات.
- الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز: من أجل قدرات محلية احترافية في الأمن السيبراني، وتطوير البرمجيات والدرونز أُطلِق الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز تحت مظلة اللجنة الأولمبية السعودية؛ للعمل على تقديم أنشطة وبرامج تسهم في زيادة وعي المجتمع بالأمن السيبراني والبرمجة والدرونز ودعم، وتشجيع الشباب للاحتراف في هذا المجال.
- الأكاديمية الوطنية للأمن السيبراني: مبادرة أطلقتها وزارة الاتصالات وتقنية المعلومات بالتعاون مع صندوق تنمية الموارد البشرية "هدف"؛ لرفع مستوى القدرات الرقمية الوطنية في مختلف مجالات التقنية الحديثة لمواكبة متطلبات التحول الرقمي، وتشمل عدّة مسارات (تحليل بيانات الذكاء الاصطناعي، الحوسبة السحابية، تطوير الويب والتطبيقات، تصميم وتطوير الألعاب، البرامج التنفيذية).
- مبادرة حصين: أُطلِقت مبادرة حصين من أجل تعزيز الأمن السيبراني على المستوى الوطني، وتُعنى بحماية البريد الإلكتروني من الانتحال والاستخدام غير المصرح به، فهي تعمل على تمكين الجهات من: معرفة مستوى تطبيق مبادرة حصين للجهة، إنشاء سجلات أسماء النطاق، استطلاع لسجلات أسماء النطاق، توعية الجهات الوطنية بأهمية تفعيل توثيق أسماء للنطاقات، وطرق تنفيذها.

كما قامت الهيئة الوطنية للأمن السيبراني على مستوى المملكة بتقديم ضوابط للعمل عن بعد خلال حالة الاستعداد لمواجهة جائحة كورونا (COVID-19) تمثلت في:

- التوعية بالأمن السيبراني، ويتم ذلك من خلال التعامل الأمن مع التصفح والاتصال بالإنترنت، والتعامل الأمن مع خدمات البريد الإلكتروني ووسائل التواصل الاجتماعي وغيرها.
- إدارة هويات الدخول والصلاحيات، من خلال تطبيق التحقق من الهوية متعدد العناصر لعمليات الدخول عن بُعد، والمراجعة الدورية لهويات الدخول والصلاحيات المستخدمة للعمل عن بُعد، وغيرها.
- حماية الأنظمة وأجهزة معالجة المعلومات، من خلال تحديد وحصر الأصول التقنية والأنظمة الخاصة بالجهة المستخدمة للعمل عن بُعد، وتحديث الحزم الأمنية للأصول التقنية والأنظمة المستخدمة للدخول عن بُعد بشكلٍ دوري، والحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة على أجهزة المستخدمين والخوادم المستخدمة في عمليات الدخول عن بُعد باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن.

الأمن السيبر اني في وزارة التعليم:

الأمن السيبراني هو الحل الأمثل لمتابعة الاستخدام الواسع للإنترنت وتطبيقاته، وأنظمته المختلفة للتقليل من المخاطر التي تنشأ من سوء الاستخدام؛ حيث توجد محتويات غير مشروعة وغير مرغوب بها ذات تأثير سلبي على أخلاقيات وقيم المجتمع وتؤدي إلى تغييرات في شخصية الأفراد، وميل البعض منهم لسلوكيات منحرفة؛ وبالتالي كثرة الجرائم من خلال التقليد، أو ممارسة ألعاب معينة تشجع على ذلك؛ ولهذا فلا بد من بناء مجتمع واعي مسؤول ومدرك؛ لهذه المخاطر ليستطيع التعامل معها وثقاً لقواعد السلامة مع إدراكه للعواقب القانونية للتصرفات اللامسؤلية والتي تعرض الآخرين للخطر، أو للسرقات. (الصانع، 2020)

وفي سبيل التوعية بمخاطر الأمن السيبراني؛ قامت وزارة التعليم بتوعية منسوبيها من المعلمين وأولياء الأمور والطلاب بضرورة الاحتفاظ بمعلوماتهم، وعدم إفشاء هذه المعلومات أو إعطائها لأي شخص كان، وبالاشتراك مع هيئة الأمن السيبراني تقوم وزارة التعليم بإرسال رسائل نصية مفادها الحظر من تمكين أي شخص لا نعرفه من البيانات المتعلقة بمنصة مدرستي، وفي سبيل ذلك وقعت وزارة التعليم الهيئة والوطنية 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. (وزارة التعليم، 2020).

وترجع أهمية هذا التعاون الإستراتيجي مع وزارة التعليم لتحقيق أهداف الهيئة، ومستهدفات الإستراتيجية الوطنية للأمن السيبراني، المتمثلة في تأهيل الكوادر الوطنية المتخصصة في الأمن السيبراني؛ لسد الاحتياج الوطني في هذا المجال، وكذلك دعم وتشجيع البحث العلمي؛ ليكون نواة لقدرات وطنية تلبي الاحتياج المتزايد لمنتجات وخدمات وحلول الأمن السيبراني؛ وذلك لتعزيز الأمن السيبراني للمملكة، واستثمار الفرص المتاحة في هذا المجال، وتتضمن مجالات التعاون في هذه الاتفاقية، دعم التعاون المشترك في برامج التعليم العالي والتدريب، وبناء القدرات في مجال الأمن السيبراني، ورفع جودة مخرجات برامج التعليم العالي في الأمن السيبراني وزيادة عدد الخريجين منها، كذلك دعم وتشجيع البحث العلمي في هذا المجال، بالإضافة إلى رفع مستوى الوعي بالأمن السيبراني في التعليم بقطاعيه العام والعالي، يُذكر أن وزارة التعليم والهيئة الوطنية للأمن السيبراني نفذتا عدداً من المبادرات المشتركة خلال الفترة الماضية، كمبادرة "الابتعاث في الأمن السيبراني"، و"الإطار السعودي للتعليم العالي في الأمن السيبراني"، وأيضاً برامج التدريب الموجهة لخريجي الجامعات السعودية. (وزارة التعليم، 2020)

وقد أطلقت الهيئة الوطنية للأمن السيبراني ممثلة بالمركز الوطني الإرشادي للأمن السيبراني، بالتعاون مع وزارة التعليم حملة بعنوان (#بأمان_نتعلم)؛ وذلك في إطار جهود المركز في رفع الوعي والمعرفة بالأمن السيبراني؛ لتجنب المخاطر السيبرانية، وتقليل آثارها عن طريق إصدار التنبيهات بآخر وأخطر الثغرات والمنشورات التوعوية. وتهدف هذه الحملة التي تتزامن مع بداية كل عام دراسي خلال السنوات القليلة الماضية إلى رفع الوعي بالأمن السيبراني، وتقليل المخاطر التي قد يتعرض لها الطالب أثناء ممارسة مهامه التعليمية اليومية باستخدام شبكة الإنترنت، حيث نشر المركز الدليل الإرشادي للتعليم عن بُعد الذي يساهم في تحصين شبكة المنزل ضد الاختراقات. كما نشر المركز على حسابه في «تويتر» عدداً من الإرشادات التوعوية في التواصل الاجتماعي والتصيد الإلكتروني الذي قد يتعرض له الطلاب عن طريق وسائل التواصل الاجتماعي، والتي تستغل الظروف الراهنة للوصول للمستخدمين، إضافة إلى ذلك، فقد نشر المركز الممارسات الأمنية الصحيحة التي تستهدف طلاب المدارس، الطلاب الجامعيين، وكذلك المعلمين وأعضاء هيئة التدريس والمدربين.

يذكر أن المركز الوطني الإرشادي للأمن السيبراني يعمل على تعزيز جهود المملكة في رفع مستوى الوعي بالأمن السيبراني، ويهدف إلى رفع مستوى الوعي بالأمن السيبراني لدى أفراد المجتمع والقطاع الخاص والجهات الوطنية، ونشر التحذيرات الدورية للثغرات الأمنية ومشاركة التنبيهات لحماية الأفراد والمنشآت والحفاظ على الأمن السيبراني الوطني، كما يعمل على بناء أوجه التعاون والشراكات محلياً ودولياً، والتعرف على أفضل الممارسات في مجال التوعية بالأمن السيبراني لتفعيل البرامج التثقيفية التي تخاطب مختلف المستويات، إضافة إلى نشر أفضل الممارسات للتعامل مع الثغرات الأمنية، ومن أهداف الحملة حسب (الهيئة الوطنية للأمن السيبراني، 2021): رفع الوعي بالأمن السيبراني، وتقليل المخاطر التي قد يتعرض لها الطالب أثناء ممارسة مهامه التعليمية اليومية بالإنترنت، وتحصين شبكة المنزل ضد الاختراقات، وإيضاح أبرز الإجراءات الوقائية الواجب مراعاتها؛ لتحصين الحاسب الآلي والأجهزة الذكية، وإرشادات في الخصوصية حول أساسيات تجهيز، وتخصيص مكان في المنزل لتلقي الدروس الافتراضية.

وامتداد لدور وزارة التعليم في تنمية الوعي بالأمن السيبراني قامت بتوعية منسوبيّ التعليم عن طريق تقديم إرشادات لهم في التعامل مع بياناتهم المتعلقة بمنصة مدرستي وضرورة أن تكون هذه البيانات خاصة بهم فقط، وعدم تمكين أي شخص منها؛ وذلك من خلال الرسائل النصية والتوجيهات المباشرة، كل ذلك في سبيل رفع الوعي بأهمية الأمن السيبراني ومحو الأمية الرقمية من خلال التصفح الأمن للمحتوى وطرق مشاركته واستخدامه، إذ يعتمد الوعي بالأمن السيبراني على معرفة الأفراد بالطرق الأساسية التي يمكنهم من خلالها حماية أنفسهم وبياناتهم وأجهزتهم. يمكن العثور على أساس هذا الوعي في تطوير المهارات الأساسية للتكنولوجيا ومحو الأمية الرقمية، حيث يتم تضمين المهارات والكفاءات المتعلقة بالوعي بالأمن السيبراني كجزء من الدورات التدريبية في المعرفة الرقمية أو الحاسوبية أو المعلوماتية، أو كعناصر للتعلم مدى الحياة. (Bhatnagar,2020)

كما تم تطبيق المهارات المتعلقة بالوعي بالأمن السيبراني بشكل أكبر، مع التركيز على الكفاءات مثل: الإدارة الجيدة لكلمات المرور باستخدام كلمات مرور آمنة مختلفة، وتخزين كلمات المرور بأمان باستخدام مدير كلمات المرور، والمصادقة الثنائية، والتعرف على محاولات التصيد الاحتيالي، واكتشاف رسائل البريد الإلكتروني الضارة، واستخدام المصدر المفتوح (Frydenberg, 2020). وعلى هذا أبدت وزارة التعليم الاهتمام بالأمن السيبراني للمدرسة والعاملين بها بالإضافة إلى الدور الذي يُمكن أن تؤديه في التوعية في مجال الأمن السيبراني؛ ويشير "كريتزنجلر وآخرون" (Kritizingler et. al, 2017) المذكور في (المنتشري وحريري، 2020) إلى بعض تلك لأدوار على النحو الآتي:

- وضع خطط على مستوى المدارس بشكلٍ عام للتوعية بالأمن السيبراني؛ والتحذير من المخاطر والانتهاكات السيبرانية؛ بما يشمل الطلبة والمعلمين.
- التأكد من تطبيق جميع المدارس لسياسات واضحة بالنسبة للتعامل مع التكنولوجيا الرقمية؛ بما يشمل الأمن السيبراني، ويجب تعميم تلك السياسات على جميع المدارس، والإشراف على تطبيقها من قبل بعض الجهات المختصة في وزارة التعليم.
- أن يكون لدى وزارة التعليم خطة عمل واضحة للتعامل مع المخاطر والانتهاكات السيبرانية، وأن تتضمن تلك الخطة الجهات والمؤسسات التي يُمكن التواصل معها لمواجهة تلك المخاطر والانتهاكات.

- عقد دورات تدريبية لجميع المعلمين في المجالات التالية: الوعي بالأمن السيبراني لدى المعلمين، الإجراءات التي يُمكن للمعلمين اتباعها في حال وقوعهم ضحية للمخاطر والانتهاكات السيبرانية.
- التعاون مع بعض المؤسسات الأكاديمية كالجامعات، أو المؤسسات الاقتصادية ومؤسسات المجتمع المدني في وضع خطط التوعية بالأمن السيبراني، وتوفير المصادر والدعم اللازم للتدريب ونشر الوعي بالأمن السيبراني.
- إشراك الآباء في خطط وبرامج عمل المدرسة ذات الصلة بالأمن السيبراني.
- العمل على نشر العناية بموضوع الأمن السيبراني على نطاق واسع؛ وذلك من خلال عقد ورشات عمل ندوات أيام مفتوحة مخصصة للأمن السيبراني»، وضع ملصقات، أو توزيع كتيبات، أو نشرات للتوعية، أو عبر مواقع التواصل الاجتماعي.
- إدراج موضوع الأمن السيبراني ضمن أدلة المعلمين.
- إدراج الوعي بالأمن السيبراني ضمن المهارات الحياتية اللازمة للطلبة، ومناقشته ضمن القضايا المثارة أثناء التدريس والأنشطة المدرسية.

1.1. مشكلة الدراسة:

اتجهت المملكة العربية السعودية إلى التعليم عن بُعد في مرحلة التعليم العام، عقب انتشار جائحة كورونا (COVID-19)، فبادرت بإنشاء منصة "مدرستي"، كنظام إلكتروني بديل عن التعليم التقليدي (وجهًا لوجه)، حيث يضم الكثير من الأدوات التعليمية الإلكترونية التي تدعم عمليات التعليم والتعلم، وتسهم في تحقيق الأهداف التعليمية للمناهج والمقررات الدراسية، كما تدعم اكتساب المهارات والقيم والمعارف للطلاب والطالبات لتتواءم مع المتطلبات الرقمية للحاضر والمستقبل الذي ازداد معه استخدام الأجهزة الإلكترونية على اختلافها؛ لاستخدام المنصات التعليمية، والدخول على مواقع الإنترنت والبحث عن مصادر التعلم المختلفة.

ولكي تحقق هذه المنصة الأهداف المنوطة بها عكفت المملكة على تطويرها باستمرار، وإدخال التعديلات عليها؛ لتسهيل التعامل مع أدواتها وتوظيفها؛ لتحقيق أهدافها، وأنفقت- في سبيل ذلك- ميزانية ضخمة، لكن لكون استخدام هذه المنصات ما زال جديدًا وفي طور البداية وتحت التجريب، فقد تم اختراقها عدة مرات، كما رصدت بعض التجاوزات من غير المنتمين للتعليم العام، حيث إن التوسع في استخدام الفضاء السيبراني يزيد من حجم الأصول المعرضة للهجمات السيبرانية المباشرة؛ لذا يستوجب اتخاذ المزيد من الضوابط الإضافية الرامية إلى تقليل احتمالية المخاطر السيبرانية الناتجة عن ذلك، أو على الأقل تقليل تأثيرها، وقد أصبح ما تم الإشارة إليه في الآونة الأخيرة ظاهرة مجتمعية، برزت على شكل روابط تطلب بيانات حسابات ميكروسوفت ومنصة مدرستي، وهذا مؤشر على أن الطلاب قد يتعرضون لمخاطر الأمن السيبراني، مما دعا وزارة التعليم إلى مناشدة أولياء الأمور بعدم الإفصاح عن أي معلومات تتعلق بمنصة مدرستي. (وزارة التعليم،2020)

من أجل ذلك قامت الوزارة بإرسال الكثير من التحذيرات للطلاب وأولياء الأمور بعدم إفشاء بيانات الدخول وعدم إعطائها لأي شخص، للإحالة دون تمكين أي شخص منها، ومع ذلك هناك الكثير من الجرائم السيبرانية التي انتشرت في السنوات الأخيرة مع ما قامت به الهيئة الوطنية للأمن السيبراني من تحذير بالمخاطر والتهديدات التي يتعرض لها مستخدمو منصة مدرستي، وقد نشرت هذه التحذيرات، إضافة إلى الإجراءات والاحترازات الواجب اتباعها حيال ذلك على موقعها الإلكتروني (الهيئة الوطنية للأمن السيبراني، 2020)، كما تقوم الهيئة الوطنية للأمن السيبراني بإرسال رسائل نصية لمستخدمي منصة مدرستي بهدف توعيتهم وعدم إفشاء معلوماتهم والمحافظة على سرية البيانات.

وعلى الرغم من الجهود الكبيرة التي بذلتها المملكة العربية السعودية في مجال الأمن السيبراني، وما زالت تبذلها، إلا أن الأمن السيبراني يعد من المواضيع البحثية الحديثة التي لم تحظ بالقدر الكافي من العناية على مستوى البحث العلمي في المؤسسات التعليمية داخل المملكة العربية السعودية وخارجها. وقد أكدت عدة دراسات على ذلك منها: دراسة الصحفي (2019) التي توصلت إلى وجود ضعف وقصور في الوعي بمفاهيم الأمن السيبراني لدى المعلمات في مدارس التعليم العام في المملكة العربية السعودية، كما أكدت دراسة المنتشري وحريري (2020) على تدني دور القيادة المدرسية في تعزيز الأمن السيبراني في مدارس التعليم العام بجدة. وكذلك بالرغم من الإنفاق السخي الذي تم إنفاقه على منصة مدرستي، وعلى المواقع التعليمية التابعة لها، إلا أنه تتعرض لبعض الاختراقات، وتهدر من مكتسباتها، وهذا من شأنه أن يؤثر على العملية التعليمية، وبالتالي يعد هدرًا وفاقداً كبيراً على جميع الأصعدة.

وفي ظل تدني ثقافة الأمن السيبراني للطلاب والطالبات، وعدم وعيهم بالمخاطر التي يمكن أن يتعرضوا لها من خلال استخدام الإنترنت ، فكان من الضروري توعية الإداريين والمعلمين والطلبة والعاملين في جميع المراحل التعليمية، وتحذيرهم من الجرائم السيبرانية الموجهة؛ التي قد تستهدف بنية الأوطان ووحدتها المبنية على وحدة العقيدة والأخلاق والقيم المثلى، ومن أجل الاستفادة من المنصة والحد من الهدر التعليمي الذي قد يحدث، جاءت هذه الدراسة للإجابة عن السؤال الرئيس التالي: ما واقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية؟

2.1. أسئلة الدراسة:

تمثلت أسئلة الدراسة فيما يلي:

1. ما واقع الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية؟
2. ما التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية؟
3. هل توجد فروق ذات دلالة إحصائية ($\alpha \leq 0.05$) بين متوسط استجابات أفراد عينة الدراسة في التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة تبعًا لمتغير النوع، أو الوظيفة، أو المؤهل العلمي، أو عدد سنوات الخبرة، أو عدد الدورات التدريبية في مجال تكنولوجيا المعلومات؟
4. ما الآليات المقترحة لزيادة فاعلية الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية؟

3.1. أهمية الدراسة:

تنبع أهمية الدراسة من أهمية الموضوع الذي تناقشه، فقد أدى التقدم الرقمي المعاصر إلى تطورات هائلة غير مسبوقة في عالم التكنولوجيا، شملت جميع مجالات النشاط الإنساني، بما في ذلك الأنشطة الحياتية اليومية وصولاً إلى المجالات العلمية والتربوية والسياسية والاقتصادية، وغير ذلك من مجالات، ورافق ذلك مع تدفق المعلومات المختلفة عبر شبكة الإنترنت، وانتشار وسائل الوصول لمصادر المعلومات، بما في ذلك الحواسيب المكتبية، والمحمولة، والهواتف الذكية، مما أدى إلى ظهور العديد من المشكلات الأمنية التي تتعلق باستخدامات الإنترنت، وكذلك التوسع الكبير في استخدام الإنترنت من قبل طلاب المرحلة قبل الجامعية في ظل اعتماد المملكة العربية السعودية على التعليم عن بُعد في مرحلة التعليم العام؛ ولذا تبرز أهمية الدراسة في النقاط الآتية:

1. إلقاء الضوء على واقع الأمن السيبراني في مدارس التعليم العام بالمملكة العربية السعودية الأمر الذي يضع أمام صناع القرار الواقع الفعلي لمستوى فاعلية الأمن السيبراني في مدارس التعليم العام بالمملكة العربية السعودية.
2. قد تسهم نتائج الدراسة الحالية في التعرف على الأمن السيبراني، وزيادة وعي المجتمع بمفهوم الأمن السيبراني، ومخاطر الانتهاكات السيبرانية.
3. قد يُستفاد من الآليات المقترحة في زيادة فاعلية الأمن السيبراني في مدارس التعليم العام بالمدينة المنورة، من حيث تقليص الهدر الحاصل في منصة مدرستي، والعمل على الاستفادة القصوى من الإمكانيات الضخمة التي توفرها المنصة.
4. كما تكتسب الدراسة أهميتها من تناولها لموضوع الأمن السيبراني في التعليم العام، حيث تم الاعتماد على التعليم عن بُعد في المملكة العربية السعودية بين عامي 2020 و2021، وهذا بدوره يتطلب رفع الوعي لدى منسوبي التعليم العام بمخاطر الأمن السيبراني.
5. قد تكون الدراسة الحالية نواة لأبحاث ودراسات مستقبلية تتبنى اتجاهات حديثة في التعلم.

4.1. حدود الدراسة:

تتمثل حدود الدراسة المكانية، والبشرية، والزمنية في الآتي:

- **الحدود المكانية:** تتحدد الحدود المكانية في مدارس التعليم العام بالمدينة المنورة – المملكة العربية السعودية.
- **الحدود البشرية:** تتحدد الحدود البشرية في القادة، والمعلمين، والقائدات، والمعلمات بمدارس التعليم العام بالمدينة المنورة – المملكة العربية السعودية.
- **الحدود الزمنية:** طبقت الدراسة خلال شهري فبراير ومارس 2021م -1442هـ.
- **الحدود الموضوعية:** الأمن السيبراني في المدارس: واقعه، تحدياته وأليات تفعيله.

5.1. مصطلحات الدراسة:

- **الأمن السيبراني (Cybersecurity):** يعريف بأنه "النشاط الذي يحمي الموارد المالية والبشرية التي ترتبط بالاتصالات، ويخفف من حدة الأضرار والخسائر التي تحدث في حال وجود قرصنة أو مخاطر أو تهديدات، ويحاول إصلاح ما أفسدته هذه الهجمات، وهو التدخلات التقنية والتدابير المتخذة لحماية أجهزة الكمبيوتر والشبكات، ونزاهة المعلومات المخزنة داخل هذه الأجهزة" (الصانع، 2020).

  ويعرف الأمن السيبراني إجرائياً بأنه: جميع الإجراءات التي يقوم بها القادة والمعلمون والقائدات والمعلمات بغرض حماية شبكات المعلومات، ضد كآفة الأعمال والممارسات التي تستهدف التلاعب بتلك المعلومات، وحمايتها من الاختراق ومن البرمجيات الخبيثة والفيروسات، إضافة إلى مقاومة التنمر، والتحكم في الوصول غير المصرح به، وغيرها من الممارسات الإلكترونية السلبية.
- **فاعلية الأمن السيبراني(Effectiveness of Cybersecurity):** هو مدى قدرة المستخدمين على حماية بياناتهم وفاعلية الإجراءات التي يتم تنفيذها من قبل المعلمين وقادة وقائدات المدارس للتصدي لمخاطر الأمن السيبراني (الصانع، 2020). وقد تبنت الباحثة تعريف الصانع كتعريف إجرائي في هذه الدراسة.

6.1. الدراسات السابقة:

بعد الاطلاع على الأدب النظري وما تضمنه من دراسات سابقة حول موضوع الدراسة، تم اختيار مجموعة من الدراسات وثيقة الصلة بموضوع

الدراسة الحالية، وتم ترتيبها تنازلياً من الأحدث إلى الأقدم على النحو الآتي:

- **دراسة المنتشري (2020)** والتي هدفت إلى معرفة دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، واتبعت الدراسة المنهج الوصفي التحليلي، وتم إعداد استبانة، وتم تطبيقها على عينة مكونة من (420) معلمة في عدد من المدارس الحكومية بمدينة جدة، وأظهرت نتائج الدراسة أن دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات ولدى طالبات المدرسة يتحقق بدرجة موافقة قليلة من وجهة نظر المعلمات، ويُمكن ملاحظة أن هذه الفقرات تتعلق بالدور التوعوي؛ والخاص باستباق وقوع الطالبات كضحايا للجرائم السيبرانية؛ وتدور تلك الفقرات حول تنظيم أيام مفتوحة؛ أو ندوات أو دورات تدريبيه؛ للتعريف بالأمن السيبراني، أو نشرات توعوية للتعريف بأخلاقيات الأمن السيبراني، وفي ضوء تلك النتائج تقدمت الدراسة بتصور مقترح لدور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات والطالبات، وجاءت آليات تطبيقه عبر التنسيق مع الجهات المختصة المعنية بالأمن السيبراني في المملكة العربية السعودية، واشتمل على آليات خاصة بكل من: المعلمات، والطالبات، والمعلمات والطالبات معاً، بالإضافة إلى آليات حماية البيئة المادية لشبكة الإنترنت.
- **وهدفت دراسة الصانع (2020)** إلى معرفة درجة وعي المعلمين بالأمن السيبراني وعلاقته بتطبيق أساليب حديثة لحماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية لديهم، وتكونت العينة من (104) معلماً ومعلمة في مدارس مدينة الطائف الحكومية والأهلية، واستخدمت الدراسة المنهج الوصفي الارتباطي، وتم بناء مقياس لتحديد درجة الوعي بالأمن السيبراني لدى المعلمين، وأساليب حماية الطلبة من مخاطر الإنترنت، وأساليب لتعزيز القيم والهوية الوطنية لدى الطلبة. وأظهرت نتائج الدراسة ارتفاع وعي المعلمين بالأمن السيبراني في مجال حماية الأجهزة الخاصة والمحمولة من مخاطر الاختراق الإلكتروني والهجمات السيبرانية، وفي درجة استخدامهم لأساليب حماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية بمدنية الطائف. ووجدت علاقة ارتباطية موجبة ومتوسطة بين وعي المعلمين بالأمن السيبراني واستخدامهم لأساليب حماية الطلبة من مخاطر الإنترنت، ولأساليب تعزيز القيم والهوية الوطنية، فيما لم توجد فروق ذات دلالة إحصائية بين استجابات المعلمين حول الوعي بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت، بينما وجدت فروق ذات دلالة إحصائية بين استجابات المعلمين حول أساليب تعزيز القيم والهوية الوطنية تبعاً لنوع المدرسة لصالح المدارس الحكومية، ولم توجد فروق ذات دلالة إحصائية بين استجابات المعلمين حول الوعي بالأمن السيبراني، وأساليب حماية الطلبة من مخاطر الإنترنت ، وأساليب تعزيز القيم والهوية الوطنية تبعا للجنس، والتخصص، والمؤهل العلمي، وسنوات الخبرة في التدريس.
- **وقامت الهيئة الوطنية للأمن السيبراني (2020)** بتقصي الآثار الناجمة عن جائحة كورونا (COVID-19) على مستوى المملكة العربية السعودية، بعد أن انتشرت في أنحاء العالم، وأصبحت أكثر وضوحًا وفتكاً في حياة الناس، وبات من الضروري تعزيز الأمن السيبراني لمواجهة آثارها السلبية على الحالة الاجتماعية والاقتصادية والتعليمية، وذلك من أجل القيام باستثمارات تستمرّ حتى ما بعد هذه الأزمة. توصّلت نتائج الدراسة إلى ما يلي: مع زيادة نسبة العمل عن بُعد، شهد سطح الهجمات السيبرانية المتوفّر لمنفّذي التهديدات مجالات جديدة؛ إن الخبرات المحدودة في مجال الأمن السيبراني سيكون لها آثار على المدى القصير في توظيف الكوادر المؤهلة في المجال وعلى المدى البعيد في تنمية قدراتهم؛ وإنّ المستويات المرتفعة للضغوطات وعدم اليقين تقدّم فرصًا جديدة لهجمات التصيّد وبرمجيات الفدية.
- **وتناولت دراسة المنتشري، وحريرى (2020)** درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، ولتحقيق أهداف الدراسة تم اتباع المنهج الكمي الوصفي التحليلي، وتم إعداد استبانة، وتم تطبيق الاستبانة على عينة عشوائية مكونة من (392) من معلمات المرحلة المتوسطة بمدينة جدة، وأظهرت النتائج أن معلمات المرحلة المتوسطة على درجة متوسطة من الوعي بكل من مفاهيم الأمن السيبراني، ومخاطر الأمن السيبراني، وانتهاكات الأمن السيبراني، كما دلت الاستجابات على درجة وعي منخفضة جدًا لدى المعلمات في الكثير من مفاهيم الأمن السيبراني، وعدم اتخاذ التدابير والإجراءات اللازمة لحماية جهاز الحاسب، أو الملفات الشخصية، أو الصور بل وما يتعلق بمشاركة المعلومات بشكل آمن وغياب المفاهيم الخاصة بإمكانية التجسس والاختراق والسطو على البيانات، كما تبيَّن عدم وجود فروق ذات دلالة إحصائية تعزى إلى متغيري المؤهل الدراسي، وعدد سنوات الخبرة بين استجابات المعلمات في حين أظهرت النتائج وجود فروق ذات دلالة إحصائية تعزى إلى متغير دورات تدريبية في الأمن السيبراني.
- **وهدفت دراسة الصحفي (2019)** الكشف عن مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة، استخدمت الباحثة المنهج الكمي، وتكونت عينة الدراسة من (104) من معلمات الحاسب للمرحلة الثانوية بمدينة جدة، أكدت الدراسة على وجود ضعف وقصور لدى معلمات الحاسب الآلي- في الوعي بمفاهيم الأمن السيبراني، وتبيَّن أن هناك ثغرات تشريعية في النظم القانونية العربية فيما يتعلق بالقضايا المتعلقة بتحقيق الأمن والثقة في الفضاء الإلكتروني، كما توصلت الدراسة إلى أنه يمكن توفير التوعية، وتأكيد ضمان المعلومات في شكلٍ جذاب، كما تبيَّن عدم وجود فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد عينة الدراسة في درجة وعي معلمات الحاسب بالأمن السيبراني تعزى لمتغيرات الدراسة: سنوات الخبرة-المؤهل العلمي-الدورات التدريبية.
- **وهدفت دراسة صائغ (2018)** إلى التعرف على وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية، واعتمد البحث على المنهج الوصفي التحليلي لتحقيق هدفه. وجاءت أدوات البحث متمثلة في استبانة للتعرف على وعي أفراد الأسرة بمفهوم الأمن

السيبراني وعلاقته باحتياطاتهم الأمنية للوقاية من الجرائم الإلكترونية، وطبقت على عينة قوامها (215) من سكان منطقة مكة المكرمة في المملكة العربية السعودية، وخلصت الدراسة إلى مجموعة من النتائج من أهمها: أنه توجد علاقة ذات دلالة إحصائية في وعي أفراد الأسرة بمفهوم الأمن السيبراني وبين الاحتياطات الأمنية التي يتخذونها للوقاية من الجرائم الإلكترونية، كما لا توجد فروق ذات دلالة إحصائية في الممارسات التي يقوم بها أفراد الأسر لحماية أنفسهم من الجرائم الإلكترونية تُعزى للمتغيرات الدراسة: النوع، والعمل، والعمر، ومستوى التعليم، ومتوسط دخل الأسرة.

- **استعرضت دراسة هولي وآخرين (Kurtz et al., 2018)** نتائج الدراسة التي أجراها مركز أبحاث التعلم في الولايات المتحدة، وشملت عينة الدراسة (503) فرد من مديري المدارس ومساعديهم في عدد من المدارس الأمريكية، وتم إعداد استبانة لاستطلاع آرائهم حول استخدام الطلبة للإنترنت وتعرضهم للجرائم السيبرانية، وأعْربَ أكثر من نصف قادة المدارس عن قلقهم الشديد بشأن استخدام وسائل التواصل الاجتماعي للطلاب خارج المدرسة، والتنمر الإلكتروني، وإرسال محتوى جنسي عبر الإنترنت، وعدم قدرة الطلبة على التحقق من موثوقية الأخبار على الإنترنت، وأشارت النتائج إلى أن القيادة المدرسية تواجه تحديات متعددة في العملية التعليمية في عصر الثورة الرقمية.
- **وأجرى كوريجان وروبرتسون،(Corrigan & Robertson,2015)** دراسة هدفت إلى معرفة دور قادة المدارس في مواجهة الجرائم السيبرانية في كندا، وتم استطلاع آراء تسعة من مديري المدارس الكندية، وأظهرت نتائج الدراسة أن قادة المدارس يؤدون أدواراً متعددة في تعزيز الأمن السيبراني، والتحرك الفوري في حال وقوع أي جرائم سيبرانية، والتنسيق مع أولياء الأمور لمتابعة تلك الجرائم، كما أوضحت الدراسة دور قادة المدارس في وضع سياسات تدعم الاستخدام الآمن للإنترنت، والاستجابة للأحداث السيبرانية التي قد تحدث خارج نطاق المدرسة.

من خلال استعراض الدراسات السابقة يلاحظ أن بعضاً منها عُني بدراسة الوعي بالأمن السيبراني؛ مثل دراسة المنتشري وحريرى (2020)، وهدفت التعرف إلى درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني، ودراسة الصانع (2020) التي هدفت إلى معرفة درجة وعي المعلمين بالأمن السيبراني. وتناولت بعض الدراسات دور القائدات في تعزيز الأمن السيبراني، مثل دراسة المنتشري (2020) التي هدفت إلى تعرف دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة، ودراسة هولي وآخرين (Kurtz et al., 2018) التي هدفت إلى التعرف على دور القادة في تحديد الطلاب ممن تعرضوا للجرائم السيبرانية. كما تنوعت الدراسات في الأماكن والبيئات التي أجريت فيها، سواء كانت الداخلية (محلية) أو الخارجية، فيلاحظ أن معظم الدراسات المحلية أجري في مدن رئيسة وكبيرة مثل دراسة المنتشري (2020) التي أجريت في جدة، ودراسة صائغ (2018) التي أجريت في مكة المكرمة، أما الدراسات الخارجية فقد أجريت دراسة كوريجان وروبرتسون،(Corrigan & Robertson,2015) في كندا، ودراسة هولي وآخرين (Kurtz et al., 2018) التي أجريت في أمريكيا. وقد اتضح أن الدراسة الحالية تتفق مع الدراسات السابقة في تناول محور الأمن السيبراني مثل دراسة المنتشري (2020)، ودراسة المنتشري وحريرى (2020)، ودراسة هولي وآخرين (Kurtz et al., 2018). وقد تميزت الدراسة الحالية عن الدراسات السابقة كونها تجرى في ظل الهجمات الإلكترونية المتعددة التي ظهرت مؤخراً، كما أنها تجري في المملكة العربية السعودية في ظل تبني المملكة إجراءات احترازية في أمن المعلومات، وما يزيد الدراسة الحالية أهمية هي أن التعليم اليوم، ولا سيما التعليم العام تحول كلياً إلى تعليم رقمي حيث يتم تدريس طلاب مدارس التعليم العام عن بُعد.

2. إجراءات الدراسة:

1.2. منهج الدراسة:

اعتمدت هذه الدراسة المنهج الوصفي التحليلي أسلوباً لها، حيث يعد المنهج الوصفي التحليلي لمناسبته لطبيعة الدراسة القائمة، ويعد هذا المنهج من أهم مناهج البحث العلمي وأكثرها شيوعاً واستخداماً تبعاً للمرونتة الكبيرة من أهم مناهج البحث العلمي والأكثر استخداماً لمرونته الكبيرة. (عبيدات، 2011)

2.2. مجتمع الدراسة:

تكون مجتمع الدراسة من القادة والمعلمين والقائدات والمعلمات بمدارس التعليم العام بالمدينة المنورة، المملكة العربية السعودية، وقد بلغ حجم المجتمع الكلي لعام 1442 (21.302) من القادة والمعلمين والقائدات والمعلمات.

3.2. عينة الدراسة:

تم اختيار عينة الدراسة بالطريقة العشوائية من مجتمع الدراسة المتمثل في أعضاء الإدارة المدرسية والمعلمين المعلمات بمدارس التعليم العام بالمدينة المنورة، بالمملكة العربية السعودية. وقد بلغ عددها (418) من القادة والقائدات والمعلمين المعلمات كما هو موضح في جدول (1).

جدول (1): خصائص أفراد عينة البحث

المتغير	الفئات	العدد	النسبة
النوع	ذكر	223	%53
	أنثى	195	%47
الوظيفة	قائد	109	%27
	قائدة	93	%22
	معلم	114	%27
	معلمة	102	%24
المؤهل العلمي	بكالوريوس	188	%45
	بكالوريوس+ دبلوم تربوي	106	%25
	ماجستير	86	%21
	دكتوراه	38	%9
عدد سنوات الخبرة	أقل من 5 سنوات	65	%16
	من (5-10) سنوات	68	%16
	أكثر من 10 سنوات	285	%68
عدد الدورات التدريبية في مجال تكنولوجيا المعلومات	دورتين فأقل	245	%59
	(3-5)دورات	79	%19
	أكثر من 5 دورات	94	%22

4.2. أداة الدراسة:

لتحقيق هدف الدراسة المتمثل في التعرف على واقع التعامل مع آليات الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة، والتعرف على التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة، والبحث عن الآليات المقترحة؛ لزيادة فاعلية الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة، وبناءً على الدراسات السابقة والأدبيات التي تناولت موضوع الدراسة مثل دراسة المنتشري (2020)، ودراسة صائغ (2018). وتم إعداد استبانة موجهة إلى القادة والمعلمين والقائدات والمعلمات في مدارس التعليم العام، وتكونت الاستبانة من المعلومات العامة عن أفراد عينة البحث متمثلة في متغيراتهم الشخصية والوظيفية (النوع، الوظيفة، المؤهل العلمي، عدد سنوات الخبرة، عدد الدورات التدريبية في مجال تكنولوجيا المعلومات) بالإضافة إلى اشتمالها على ثلاثة مجالات هي:

- المجال الأول: واقع التعامل مع آليات الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة، وتكون من (15) فقرة.
- المجال الثاني: التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة، وتكون من (14) فقرة.
- المجال الثالث: الآليات المقترحة لزيادة فاعلية الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة، وتكون من (17) فقرة.

وقد كانت الإجابات على كل فقرة مكونة من 5 اختيارات حيث الدرجة 5 تعني موافقة بشدة و1 تعني غير موافقة بشدة حسب مقياس ليكرت الخماسي (Scale Likert)، كما هو موضح في جدول (2) الآتي:

جدول(2): مقياس ليكرت الخماسي (Scale Likert) المستخدم في الدراسة

التصنيف	مو افقة بشدة				غير مو افقة بشدة
الدرجة	5	4	3	2	1
متوسط الدرجة	4.20-5	3.40-4.20	2.60-3.40	1.80-2.60	1.00-1.80
التقدير	موافقة بشدة (عالية جداً)	موافق (عالية)	موافق إلى حد ما (متوسطة)	غير موافق (منخفضة)	غير موافق بشدة (منخفضة جداً)

5.2. صدق الأداة:

1.5.2. الصدق الظاهري:

تم التأكد من صدق المحتوى الظاهري لعبارات الاستبانة، من خلال عرضها في صورتها الأولية على مجموعة من المحكمين المختصين والخبراء التربويين في مجال الإدارة التربوي واقتصاديات التعليم وتخطيطه والأمن السيبراني وأمن وخصوصية المعلومات وعلم النفس في كل من جامعة طيبة، وجامعة الملك عبد العزيز، وجامعة جدة، وجامعة الأمير مقرن، وجامعة حفر الباطن، ووزارة التعليم، والهيئة الوطنية للأمن السيبراني، وبلغ عددهم (11) محكمًا لإبداء الرأي حول العبارات المعروضة في الاستبانة، وتحديد درجة انتمائها للمحور الخاص بها، وكذلك صلاحية عرضها، كما تم ترك مساحة بعد كل محور للمحكم، ليبدي رأيه، أو يطرح عبارة يرى أنها تناسب المحور، وغير مدونة في القائمة. وقد اتفق المحكمون على انتماء أغلب العبارات لمجالها، وجاءت ملاحظاتهم بين التعديل والدمج أو الحذف أو الإضافة، وتم الأخذ بجميع ملاحظاتهم ومقترحاتهم، وتم تعديل الأداة بناءً على آراء المحكمين.

2.5.2. صدق البناء لأداة الدراسة:

بعد التأكد من الصدق الظاهري لأداة البحث، قامت الباحثة بتطبيقها ميدانياً على عينة استطلاعية عشوائية قوامها (40) من القادة والمعلمين، والقائدات والمعلمات لهم نفس خصائص العينة النهائية، كما قامت الباحثة بحساب صدق الأداة؛ وذلك باستخدام طريقة الصدق البنائي التي تعتمد على حساب معامل الارتباط بين كل فقرة من فقرات أداة الدراسة، والدرجة الكلية للمجال الذي تنتمي إليه، كما تم التحقق من صدق الاتساق الداخلي للمجالات مع الدرجة الكلية للأداة بحساب معاملات الارتباط لمجالات الأداة مع الأداة ككل تبعاً لاستجابات أفراد العينة.

- **صدق الاتساق الداخلي لفقرات الاستبانة مع الدرجة الكلية لكل بعد:**

تم حساب معاملات الارتباط بين كل فقرة والمجال الذي تنتمي إليه الفقرة، كما هو مبين في جدول (3):

جدول (3): معامل ارتباط بيرسون (Pearson's Correlation) بين الفقرة والبعد التي تنتمي إليه

المجال الأول: و اقع التعامل مع آليات الأمن السيبر اني		المجال الثاني: التحديات التي تواجه تفعيل الأمن السيبر اني		المجال الثالث: الآليات المقترحة لزيادة فاعلية الأمن السيبر اني	
NO.	R	NO.	R	NO.	R
1	.414**	1	.750**	1	.767**
2	.426**	2	.782**	2	.857**
3	.477**	3	.647**	3	.721**
4	.727**	4	.698**	4	.765**
5	.684**	5	.756**	5	.905**
6	.588**	6	.767**	6	.696**
7	.637**	7	.824**	7	.740**
8	.741**	8	.654**	8	.846**
9	.739**	9	.827**	9	.838**
10	.774**	10	.616**	10	.772**
11	.840**	11	.498**	11	.843**
12	.743**	12	.635**	12	.793**
13	.701**	13	.653**	13	.860**
14	.680**	14	.333*	14	.794**
15	.707**			15	.811**
				16	.679**
				17	.774**

** دالة إحصائياً عند مستوى معنوية 0.01، * دالة إحصائياً عند مستوى معنوية 0.05.

يتضح من جدول (3) أن جميع قيم معاملات الارتباط موجبة، وجميعها ذات دلالة إحصائية عند مستوى الدلالة (0.01)، عدا الفقرة رقم (14) من المحور الثاني جاءت دالة إحصائياً عند مستوى دلالة (0.05)، وتشير هذه النتيجة إلى صدق الاتساق الداخلي لفقرات أداة الدراسة الدراسة، وأن الفقرات ذات علاقة ارتباطية دالة إحصائياً بالمجال الذي تنتمي إليه.

- **صدق البناء الداخلي لمجالات أداة الدراسة:**

تم حساب معاملات الارتباط باستخدام معامل ارتباط بيرسون (Pearson's Correlation) للمجالات مع الدرجة الكلية للاستبانة تبعاً لاستجابات أفراد العينة، كما هو مبين في جدول (4) التالي.

جدول (4): معامل ارتباط بيرسون (Pearson's Correlation) بين البعد والدرجة الكلية للاستبانة

م	المجال	عدد الفقرات	معامل بيرسون
1	المجال الأول: واقع التعامل مع آليات الأمن السيبراني في مدارس التعليم العام	15	.631**
2	المجال الثاني: التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام	14	.513**
3	المجال الثالث: الآليات المقترحة؛ لزيادة فاعلية الأمن السيبراني في مدارس التعليم العام	17	.701**

** دال إحصائياً عند مستوى الدلالة (0.01).

يتضح من جدول (4) أن قيم معاملات الارتباط لمجالات أداة الدراسة مع الدرجة الكلية لها كانت دالة إحصائيًا عند مستوى الدلالة (0.01)، وجميعها قيم موجبة.

6.2. ثبات أداة الدراسة:

يدل الثبات على " المدى الذي تظل فيه أداة القياس ثابتة في قياس ما تقيس" (سليمان وأبو علام، 2010، ص596). وللتحقق من ثبات أداة الدراسة تم حساب معامل الاتساق الداخلي معادلة كرونباخ ألفا (Cronbach's ALPHA)، وجاءت النتائج، كما هو مبين في جدول (5) الآتي:

جدول (5): معامل ألفا كرونباخ (Cronbach's ALPHA) لمحاور أداة الدراسة

المجال	عدد الفقرات	معامل كرونباخ الفا
المجال الأول: واقع التعامل مع آليات الأمن السيبراني في مدارس التعليم العام	15	0.901
المحور الثاني: التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام	14	0.904
المحور الثالث: الآليات المقترحة؛ لزيادة فاعلية الأمن السيبراني في مدارس التعليم العام	17	0.958
الاستبانة ككل	**46**	**0.893**

يتضح من جدول (5) أن أداة الدراسة ككل تتمتع بدرجة ثبات عالية، فقد بلغت قيمة معامل كرونباخ ألفا (Cronbach's ALPHA) للاستبانة ككل (0.893)، كما بلغت للمجال الأول (0.901) وللمجال الثاني (0.904)، وللمجال الثالث (0.958)، مما يدل على أن الأداة ككل تتمتع بدرجة مرتفعة من الثبات ويمكن الموثوق في نتائجها.

3. نتائج الدراسة ومناقشتها:

1.3. النتائج المتعلقة بالسؤال الأول:

للإجابة على هذا السؤال والذي ينص على: **ما و اقع الأمن السيبر اني في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية؟** تم حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة، وتم ترتيب فقرات المجال الأول حسب المتوسطات الحسابية تنازلياً كما هو موضح في جدول (6).

جدول (6): المتوسطات الحسابية والانحر افات المعيارية والنسبة المئوية لاستجابات أفراد عينة الدراسة على المحور الأول "و اقع التعامل مع آليات الأمن السيبر اني"

رقم الفقرة	الفقرات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	الترتيب	الاستجابة
8	أحرص على استخدام متصفح آمن للإنترنت.	4.02	0.79	80%	1	عالية
3	أستخدم الروابط الرسمية التي تنشرها وزارة التعليم في موقعها الرسمي (منصة مدرستي).	3.94	0.79	79%	2	عالية
11	أستخدم برمجيات معتمدة وموثوقة؛ لحماية الحاسب من الاختراق.	3.93	0.83	79%	3	عالية
4	أحرص على عدم فتح أيّ مرفقات أو روابط مرفقة مع رسائل إلكترونية مجهولة المصدر.	3.90	0.95	78%	4	عالية
12	أحرص على عدم الإفصاح عن كلمة المرور الخاص بي لأي أحد.	3.85	0.98	77%	5	عالية
10	ألغي الاشتراك في التطبيقات التي تتضمن إعلانات لحماية بياناتي الشخصية والمالية.	3.75	0.89	75%	6	عالية
1	أؤيد طلب المدرسة من منسوبيها تغيير كلمة المرور الخاصة بهم بشكلٍ دوري.	3.74	0.97	75%	7	عالية
9	لا أستخدم التطبيقات المجهولة التي تقدم خدمات مجانية للمعلمين.	3.65	1.06	73%	8	عالية
6	أتجنب إرسال معلوماتي الشخصية عبر الرسائل أو البريد الإلكتروني.	3.57	1.12	71%	9	عالية
2	أستخدم كلمة مرور معقدة لحسابات الدخول المهمة مثل الدخول لشبكة الوزارة وتختلف عن كلمات المرور المستخدمة في مواقع التواصل الاجتماعي او مواقع التسوق الإلكتروني.	3.39	1.09	68%	10	متوسطة
7	لا استخدم البريد الإلكتروني الرسمي في التسجيل والاشتراك في مواقع التواصل الاجتماعي او التطبيقات.	3.36	1.21	67%	11	متوسطة
14	أحتفظ بنسخة احتياطية من ملفاتي في ذاكرة خارجية، لتفادي السرقة أو التلف.	3.35	1.21	67%	12	متوسطة
5	عند استخدام الأجهزة والتطبيقات الإلكترونية، يجب ان أقوم بتعديل سياسات الخصوصية الافتراضية، من خلال إعدادات الخصوصية، بما يضمن تطبيق مستوى عالي من الخصوصية.	3.33	1.16	67%	13	متوسطة
15	أُفعّل خدمات الوصول لموقعي بشكلٍ مؤقت أثناء استخدام بعض التطبيقات التي تتطلب ذلك.	3.26	1.24	65%	14	متوسطة
13	أستخدم التشفير (من خلال تعيين كلمة مرور) لملفاتي المهمة التي أقوم بإرسالها من خلال شبكة الإنترنت.	3.23	1.26	65%	15	متوسطة
المجال ككل	**و اقع الأمن السيبر اني في مدارس التعليم العام**	**3.62**	**0.81**	**72%**		عالية

يتضح من جدول (6) أن المتوسط العام للمجال الأول "واقع الأمن السيبراني في مدارس التعليم العام بالمدينة المنورة" بلغ (3.62) بانحراف معياري بلغ (0.81)، ودرجة استجابة عالية، وبنسبة مئوية (72%) . وجاء في الثلاثة مراتب الأولى الفقرات رقم (8، 3، 11)، وفي الثلاثة مراتب الأخيرة الفقرات رقم (13، 5.15) وجاء في المرتبة الأولى الفقرة رقم(8) "أحرص على استخدام متصفح آمن للإنترنت، "بمتوسط حسابي بلغ (4.02)، وانحراف معياري بلغ (0.79)، وبنسبة مئوية (80%) ودرجة استجابة عالية، وجاء في المرتبة الثانية الفقرة رقم 3"أستخدم الروابط الرسمية التي تنشرها وزارة التعليم في موقعها الرسمي (منصة مدرستي)، " بمتوسط حسابي بلغ (3.94)، وانحراف معياري بلغ (0.79)، ودرجة استجابة عالية، وجاء في المرتبة الثالثة الفقرة رقم (11) "أستخدم برمجيات معتمدة وموثقة؛ لحماية الحاسب من الاختراق. " بمتوسط حسابي بلغ (3.93)، وانحراف معياري بلغ (0.83)، ودرجة استجابة عالية، وتعزو الباحثة هذه النتائج إلى وعي منسوبي وزارة التعليم بالاعتماد على الروابط الرسمية للوزارة كما أن الوزارة توفر لهم تطبيقات

ميكروسوفت الأصلية فلا حاجة لديهم لاستخدام تطبيقات غير أصلية.

وجاء في المرتبة الثالثة عشر الفقرة رقم 14 " أحتفظ بنسخة احتياطية من ملفاتي في ذاكرة خارجية، لتفادي السرقة أو التلف، " بمتوسط حسابي بلغ (3.35)، وانحراف معياري بلغ (1.21)، ودرجة استجابة متوسطة، وجاء في المرتبة الرابعة عشر الفقرة رقم 5 " عند استخدام الأجهزة والتطبيقات الإلكترونية، يجب ان أقوم بتعديل سياسات الخصوصية الافتراضية، من خلال إعدادات الخصوصية، بما يضمن تطبيق مستوى عالٍ من الخصوصية. " بمتوسط حسابي بلغ (3.33)، وانحراف معياري بلغ (1.16)، ودرجة استجابة متوسطة، وجاء في المرتبة الخامسة عشر الفقرة رقم 15 " أُفعّل خدمات الوصول لموقعي بشكلٍ مؤقت أثناء استخدام بعض التطبيقات التي تتطلب ذلك" بمتوسط حسابي بلغ (3.26)، وانحراف معياري بلغ (1.24)، ودرجة استجابة متوسطة، تعزو الباحثة هذه النتيجة إلى قلة خبرة الكثير من المستخدمين بالدخول على إعدادات الخصوصية وتعديلها، وكذلك عدم استخدام التأكد بخطوتين لعدم أخذ وقت طويل.

مما سبق يتضح أن واقع الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة جاء بمستوى مرتفع بنسبة (72%)، وعلى الرغم من ذلك يمكن القول إن هذه النسبة لا تصبو إلى الوعي بالأمن السيبراني المنشود، وقد اختلفت هذه النتيجة مع النتيجة التي توصلت لها دراسة دراسة المنتشري (2020)، التي أظهرت درجة موافقة قليلة من وجهة نظر المعلمات حول دور القيادة المدرسية في تعزيز الأمن السيبراني، كما اختلفت مع دراسة الصحفي (2019) التي أكدت على وجود ضعف وقصور لدى معلمات الحاسب الآلي في الوعي بمفاهيم الأمن السيبراني.

2.3. النتائج المتعلقة بالسؤال الثاني:

للإجابة على هذا السؤال والذي ينص على ما التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية؟ تم حساب المتوسطات الحسابية، والانحرافات المعيارية لاستجابات أفراد عينة الدراسة، وتم ترتيب هذه الفقرات حسب المتوسطات الحسابية تنازليًا.

جدول (7): المتوسطات الحسابية والانحرافات المعيارية والنسبة المئوية لاستجابات أفراد عينة الدراسة على المجال الثاني "التحديات التي تواجه تفعيل الأمن السيبراني"

رقم الفقرة	الفقرات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	الترتيب	الاستجابة
7	قلة وعي بعض الطلاب حول مخاطر الأمن السيبراني.	4.32	0.74	86%	1	عالية جداً
8	ضعف السيطرة على الطلاب، ومنعهم من دخول المواقع غير الموثوق بها.	4.32	0.77	86%	2	عالية جداً
14	قلة الوعي بقانون الجرائم المعلوماتية.	4.30	0.81	86%	3	عالية جداً
4	قلة وجود مختصين في المدارس للتعامل مع مخاطر الأمن السيبراني.	4.27	0.75	85%	4	عالية جداً
11	انتشار إعلانات تصيديه تدعي وجود تحديث مجاني ومزيف لمايكروسوفت تيمز (منصة مدرستي).	4.26	0.78	85%	5	عالية جداً
9	قلة البرامج التدريبية الموجهة للمعنيين بالعملية التعليمية حول مخاطر الأمن السيبراني.	4.25	0.77	85%	6	عالية جداً
10	انتشار العديد من التطبيقات التعليمية غير الموثوق بها.	4.25	0.76	85%	7	عالية جداً
6	قلة وعي بعض المعلمين حول مخاطر الأمن السيبراني.	4.18	0.83	84%	8	عالية
5	قلة وعي بعض القادة المدارس حول مخاطر الأمن السيبراني.	4.13	0.86	83%	9	عالية
2	عدم توفير المدرسة لبرمجيات حماية مواكبة لما يستجد من مخاطر الأمن السيبراني بشكل دوري.	4.10	0.77	82%	10	عالية
1	ضعف تفعيل آليات التعامل مع مخاطر الأمن السيبراني في المدارس.	4.08	0.77	82%	11	عالية
12	انتهاك خصوصية المعلمين عن طريق نشر فيديوهات خاصة بهم من (فيديوهات مقتبسة من الدروس) عبر وسائل التواصل الاجتماعي.	4.06	0.84	81%	12	عالية
3	تعرض منصة مدرستي لاختراقات من قبل الطلاب أو من أفراد خارج المدرسة.	3.83	0.96	77%	13	عالية
13	التعرض إلى تهديدات عبر مواقع التواصل الاجتماعي (واتساب، تويتر، تليجرام، يوتيوب، سناب شات، .... فيسبوك).	3.65	1.05	73%	14	عالية
المجال ككل	**التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة**	**4.14**	**0.64**	**83%**		**عالية**

يتضح من جدول (7) أن المتوسط العام للمجال الثاني: التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة بلغ (4.14) بانحراف معياري بلغ (0.64)، ودرجة استجابة عالية، وبنسبة مئوية (83%). وجاء في المراتب الثلاثة الأولى الفقرات رقم (14، 7،8)، وفي الثلاث مراتب الأخيرة الفقرات رقم (12, 3,13)، حيث جاء في المرتبة الاولى الفقرة رقم 7 "قلة وعي بعض الطلاب حول مخاطر الأمن السيبراني، "بمتوسط حسابي بلغ (4.32)، وانحراف معياري بلغ (0.74)، وبنسبة مئوية (86%)، ودرجة استجابة عالية جداً، وجاء في المرتبة الثانية الفقرة رقم (8) "ضعف السيطرة على الطلاب، ومنعهم من دخول المواقع غير الموثوق بها " بمتوسط حسابي بلغ (4.32)، وانحراف معياري بلغ (0.77)، وبنسبة مئوية (86%)، ودرجة استجابة عالية جداً، وجاء في المرتبة الثالثة الفقرة رقم (14) " قلة الوعي بقانون الجرائم المعلوماتية، " بمتوسط حسابي بلغ (4.30)، وانحراف معياري بلغ (0.81)، وبنسبة مئوية (86%)، ودرجة استجابة عالية جداً. وتعزو الباحثة هذه النتيجة وهذا الاتفاق حول قلة وعي الطلاب وعدم السيطرة عليهم إلى صعوبة تحقيق ذلك إلا بالتعاون مع أولياء الأمور وتوعيتهم بطرق حماية أبنائهم والرقابة عليهم نظرا لصعوبة إمكانية سيطرة المعلمين على الطلاب والتحكم في طريقة تصفحهم للمواقع المختلفة، وتعد هذه التحديات غاية في الصعوبة التي لا يمكن تخطها إلا بتوعية أولياء الأمور والطلاب معاً.

وجاء في المرتبة الثانية عشر الفقرة رقم (12) " انتهاك خصوصية المعلمين عن طريق نشر فيديوهات خاصة بهم من (فيديوهات مقتبسة من الدروس) عبر وسائل التواصل الاجتماعي، "بمتوسط حسابي بلغ (4.06)، وانحراف معياري بلغ (0.84)، وبنسبة مئوية (81%)، ودرجة استجابة عالية، وجاء في المرتبة الثالثة عشر الفقرة رقم (3) " تعرض منصة مدرستي لاختراقات من قبل الطلاب أو من أفراد من خارج المدرسة، " بمتوسط حسابي بلغ (3.83)، وانحراف معياري بلغ (0.96)، وبنسبة مئوية (77%)، ودرجة استجابة عالية، وجاء في المرتبة الرابعة عشر الفقرة رقم (13) " التعرض إلى تهديدات عبر مواقع التواصل الاجتماعي، (واتساب، تويتر، تليجرام، يوتيوب، سناب شات، .... فيسبوك)، " بمتوسط حسابي بلغ (3.65)، وانحراف معياري بلغ (1.05)، وبنسبة مئوية (73%)، ودرجة استجابة عالية، وتعزو الباحثة هذه النتيجة إلى أن بعض المعلمين والقادة لم تكن لهم تجربة أو دور الدوائر المقربة منهم في انتهاك خصوصياتهم وسرقة البيانات.

مما سبق يتضح أن التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة جاءت بمستوى مرتفع بنسبة مئوية بلغت (83%)، وترى الباحثة أن هذه النسبة تمثل إشكالية كبرى في منظومة التعليم عن بُعد، ولابد من إيجاد حلول لمواجهة هذه التحديات، وقد اتفقت هذه النتيجة مع النتائج التي توصلت إليها دراسة المنتشري، وحريرى (2020)، التي أشارت إلى على درجة وعي منخفضة جدًا (أي أن التحديات مرتفعة) لدى المعلمات في الكثير من مفاهيم الأمن السيبراني، التي تمثلت في عدم اتخاذ التدابير والإجراءات اللازمة لحماية جهاز الحاسب، أو الملفات الشخصية، أو الصور بل وما يتعلق بمشاركة المعلومات بشكل آمن، وغياب المفاهيم الخاصة بإمكانية التجسس والاختراق والسطو على البيانات.

3.3. النتائج المتعلقة بالسؤال الثالث:

للإجابة على هذا السؤال والذي ينص على " هل توجد فروق ذات دلالة إحصائية ($\alpha \leq 0.05$) بين متوسط استجابات أفراد عينة الدراسة في التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة تبعًا لمتغير النوع، أو الوظيفة، أو المؤهل العلمي، أو عدد سنوات الخبرة، أو عدد الدورات التدريبية في مجال تكنولوجيا المعلومات؟". ومن أجل التعرف على الفروق في استجابات أفراد عينة الدراسة؛ تم استخدم اختبار– ت T –Test لعينتين مستقلتين؛ للكشف عن دلالة الفروق الإحصائية لمتوسطات استجابات أفراد عينة الدراسة التي تعزى لمتغير: النوع، وتحليل التباين الأحادي One Way ANOVA، للكشف عن مستوى دلالة الفروق الإحصائية لمتوسطات استجابات أفراد عينة الدراسة التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة التي تعزى لمتغيرات: الوظيفة، والمؤهل العلمي، وعدد سنوات الخبرة، وعدد الدورات التدريبية في مجال تكنولوجيا المعلومات، وقد تم عرض النتائج المتعلقة بكل متغير على حدة كلى النحو التالي:

- **متغير النوع:**

جدول (8): نتائج اختبار"ت" (T-Test) لدلالة الفروق بين متوسطات استجابات أفراد عينة الدراسة على التحديات التي تواجه تفعيل الأمن السيبر اني في مدارس التعليم العام بمنطقة المدينة المنورة تبعاً لمتغير النوع

الفئات	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة ت	مستوى الدلالة
ذكور	223	4.16	0.67	0.93	0.56
إناث	195	4.12	0.62		

يتضح من جدول (8)، أن قيمة (ت) غير دالة إحصائياً عند مستوى دلالة (0.05) لمجال التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة، وذلك تبعاً لمتغير النوع الاجتماعي. وهذا يشير إلى أن استجابات القادة والمعلمين متقاربة مع استجابات القائدات والمعلمات من حيث نظرتهم للتحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة. وذلك لأن المعلمين والمعلمات والقائدات والقادة يمارسون عملهم تحت مظلة وزارة التعليم المسؤولة بشكل مباشر أو غير مباشر عن توعية المرؤوسين فيها فيما يتعلق بالأمن السيبراني. وتتفق هذه النتيجة مع نتائج دراسة الصانع (2020) التي توصلت إلى عدم وجود فروق ذات دلالة إحصائية بين استجابات المعلمين حول الوعي بالأمن السيبراني، وأساليب حماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية تبعا لمتغير الجنس.

- **متغير الوظيفة**

جدول (9): نتائج تحليل التباين الأحادي (One Way ANOVA) لدلالة الفروق بين متوسطات استجابات أفراد عينة الدراسة على التحديات التي تواجه تفعيل الأمن السيبر اني في مدارس التعليم العام بمنطقة المدينة المنورة تبعاً لمتغير الوظيفة

مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	مستوى الدلالة
بين المجموعات	2.742	3	0.914	2.222	0.085
داخل المجموعات	170.286	414	0.411		
المجموع	**173.028**	**417**			

يتضح من جدول (9) أن قيمة (ف) غير دالة إحصائيا عند مستوى دلالة (0.05) لمجال (التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة)، التي تعزى لاختلاف متغير الوظيفة. وهذا يشير إلى أن استجابات القادة والقائدات متقاربة مع استجابات المعلمين والمعلمات من حيث نظرتهم للتحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة.

- **متغير المؤهل العلمي:**

جدول (10): نتائج تحليل التباين الأحادي (One Way ANOVA) لدلالة الفروق بين متوسطات استجابات أفراد عينة الدراسة على التحديات التي تواجه تفعيل الأمن السيبر اني في مدارس التعليم العام بمنطقة المدينة المنورة تبعاً لمتغير المؤهل العلمي

مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	مستوى الدلالة
بين المجموعات	0.334	3	0.111	0.267	0.849
داخل المجموعات	172.694	414	0.417		
المجموع	**173.028**	**417**			

يتضح من جدول (10) أن قيمة (ف) غير دالة إحصائياً عند مستوى دلالة (0.05) لمجال التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة، تعزى لاختلاف متغير المؤهل العلمي. وهذا يشير إلى أن استجابات القادة والمعلمين متقاربة مع بعضها البعض بغض النظر عن المؤهل العلمي الذي لديهم (سواء كان بكالوريوس، أم بكالوريوس مع دبلوم، أم ماجستير، أم دكتوراه) من حيث نظرتهم للتحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة. وتتفق هذه النتيجة مع نتيجة دراسة الصانع (2020) التي توصلت إلى عدم وجود فروق ذات دلالة إحصائية بين استجابات المعلمين حول الوعي بالأمن السيبراني، وأساليب حماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية تبعا لمتغير المؤهل العلمي.

- **متغير عدد سنوات الخبرة:**

جدول (11): نتائج تحليل التباين الأحادي (One Way ANOVA) لدلالة الفروق بين متوسطات استجابات أفراد عينة الدراسة على التحديات التي تواجه تفعيل الأمن السيبر اني في مدارس التعليم العام بمنطقة المدينة المنورة تبعاً لمتغير عدد سنوات الخبرة

مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	مستوى الدلالة
بين المجموعات	0.602	2	0.301	0.725	0.485
داخل المجموعات	172.426	415	0.415		
المجموع	**173.028**	**417**			

يتضح من جدول (11) أن قيمة (ف) غير دالة إحصائياً عند مستوى دلالة (0.05) لمجال التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة تعزى لاختلاف متغير عدد سنوات الخبرة. وهذا يشير إلى أن استجابات القادة والمعلمين متقاربة مع بعضها البعض بغض النظر عن عدد سنوات الخبرة التي لديهم (سواء كانت أقل من 5 سنوات، أم من (5-10) سنوات، أم أكثر من 10 سنوات) من حيث نظرتهم للتحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة. وتتفق هذه النتيجة مع نتيجة دراسة الصانع (2020) التي توصلت إلى عدم وجود فروق ذات دلالة إحصائية بين استجابات المعلمين حول الوعي بالأمن السيبراني، وأساليب حماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية تبعا لمتغير سنوات الخبرة.

- **متغير عدد الدورات التدريبية في مجال تكنولوجيا المعلومات:**

جدول (12): نتائج تحليل التباين الأحادي (One Way ANOVA) لدلالة الفروق بين متوسطات استجابات أفراد عينة الدراسة على التحديات التي تواجه تفعيل الأمن السيبر اني في مدارس التعليم العام بمنطقة المدينة المنورة تبعاً لمتغير عدد الدورات التدريبية في مجال تكنولوجيا المعلومات

مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	مستوى الدلالة
بين المجموعات	0.861	2	0.431	1.038	0.355
داخل المجموعات	172.167	415	0.415		
المجموع	**173.028**	**417**			

يتضح من جدول (12) أن قيمة (ف) غير دالة إحصائياً عند مستوى دلالة (0.05) لمجال التحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة تعزى لاختلاف متغير عدد الدورات التدريبية في مجال تكنولوجيا المعلومات. وهذا يشير إلى أن استجابات القادة والمعلمين متقاربة مع بعضها البعض بغض النظر عن عدد الدورات في مجال تكنولوجيا المعلومات التي خضعوا لها (سواء كانت دورتين فأقل، أم (3-5) دورات، أم أكثر من 5 دورات) من حيث نظرتهم للتحديات التي تواجه تفعيل الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة. وقد اختلفت هذه النتيجة مع النتيجة التي توصلت لها دراسة دراسة المنتشري، وحريرى (2020)، التي أظهرت وجود فروق ذات دلالة إحصائية تعزى إلى متغير دورات تدريبية في الأمن السيبراني، واتفقت مع النتيجة التي توصلت لها دراسة وهدفت دراسة الصحفي (2019)، التي أشارت إلى عدم وجود فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد عينة الدراسة في درجة وعي معلمات الحاسب بالأمن السيبراني تعزى إلى متغير الدورات التدريبية.

4.3. النتائج المتعلقة بالسؤال الرابع:

للإجابة على هذا السؤال والذي ينص على "ما الأليات المقترحة لزيادة فاعلية الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة؟"، تم حساب المتوسطات الحسابية والانحرافات المعيارية، والنسبة المئوية لاستجابات أفراد عينة الدراسة، وتم ترتيب هذه الفقرات حسب المتوسطات الحسابية تنازلياً.

جدول (13): المتوسطات الحسابية والانحر افات المعيارية والنسبة المئوية لاستجابات أفراد عينة الدراسة على المجال الثالث (الأليات المقترحة لزيادة فاعلية الأمن السيبر اني في مدارس التعليم العام بمنطقة المدينة المنورة)

رقم الفقرة	الفقرات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	الترتيب	الاستجابة
5	نشر الوعي بالأمن السيبراني لدى القيادات والمعلمين والطلاب حول آليات التعامل مع شبكة الإنترنت، والمنصات التعليمية.	4.62	0.56	%92	1	عالية جداً
9	تعزيز وعي الطلاب بمخاطر الروابط الضارة عند تصفح الإنترنت.	4.62	0.54	%92	2	عالية جداً
11	توفير دليل تفاعلي عن أخلاقيات الأمن السيبراني، ومفاهيمه لمستخدمي منصة مدرستي.	4.62	0.57	%92	3	عالية جداً
12	رفع الوعي بمفاهيم ومخاطر وانتهاكات الأمن السيبراني من خلال عرض فيديوهات تعريفية موجزة على منصة مدرستي.	4.62	0.55	%92	4	عالية جداً
8	رفع وعي الطلاب بأهمية التحقّق من المصادر الموثوق بها؛ لحصولهم على معلومات تتعلق بدراستهم.	4.61	0.55	%92	5	عالية جداً
10	إرسال رسائل نصية توعوية بمفاهيم ومخاطر وانتهاكات الأمن السيبراني.	4.61	0.55	%92	6	عالية جداً
13	وضع إجراءات، وسياسات لحفظ الأمن السيبراني داخل المدرسة، وفقا للضوابط الأساسية الصادرة من الهيئة الوطنية للأمن السيبراني.	4.61	0.55	%92	7	عالية جداً
14	توعية منسوبيّ المدرسة بمفاهيم الأمن السيبراني.	4.61	0.57	%92	8	عالية جداً
15	وضع قوانين صارمة؛ للتعامل مع المتنمرين عبر منصة مدرستي والتوعية بقانون الجرائم المعلوماتية.	4.61	0.57	%92	9	عالية جداً
4	عقد دورات تدريبية بالشراكة مع الجامعات؛ لتوعية منسوبي التعليم العام بالأمن السيبراني.	4.59	0.60	%92	10	عالية جداً
1	توفير برامج توعوية للتعريف بالأمن السيبراني، وآليات تعزيزه في المدارس.	4.57	0.60	%91	11	عالية جداً
16	تشكيل فريق قانوني مختص بقضايا التنمر الإلكتروني عبر منصة مدرستي.	4.57	0.60	%91	12	عالية جداً
2	اتباع الضوابط الأساسية في الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني	4.54	0.59	%91	13	عالية جداً
17	تخصيص ميزانية مخصصه للأمن السيبراني تتناسب مع ما يتم صرفه على التقنية والخدمات الإلكترونية وتضمن استدامة أنشطة الأمن السيبراني.	4.54	0.69	%91	14	عالية جداً
6	عقد دورات تدريبية بإشراف معلّمي الحاسب الآلي لتوعية منسوبيّ المدرسة بالأمن السيبراني.	4.52	0.62	%90	15	عالية جداً
3	توفير خبراء ومختصين في الأمن السيبراني؛ لفحص الأجهزة والبرمجيات بصفة دورية في المدارس.	4.51	0.67	%90	16	عالية جداً
7	تضمين مفاهيم الأمن السيبراني بمقرر تكنولوجيا التعليم ببرامج إعداد المعلمين والمعلمات.	4.48	0.66	%90	17	عالية جداً
المجال ككل	**الآليات المقترحة لزيادة فاعلية الأمن السيبر اني في مدارس التعليم العام بمنطقة المدينة المنورة**	**4.58**	**0.51**	**%92**		عالية جداً

يتضح من جدول (13) أن المتوسط العام للمجال الثالث (الآليات المقترحة لزيادة فاعلية الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة) بلغ (4.58) بانحراف معياري بلغ (0.51)، ودرجة استجابة عالية جداً، ونسبة مئوية (92%)، حيث جاء ذلك في الثلاثة مراتب الأولى الفقرات رقم(5، 9، 11)، وجاء في الثلاثة مراتب الأخيرة الفقرات رقم (6، 3، 7) ، حيث جاء في المرتبة الأولى الفقرة رقم (5) "نشر الوعي بالأمن السيبراني لدى القيادات والمعلمين والطلاب حول آليات التعامل مع شبكة الإنترنت ، والمنصات التعليمية، "بمتوسط حسابي بلغ (4.62)، وانحراف معياري بلغ (0.56)، ونسبة مئوية (92%)، ودرجة استجابة عالية جداً. وجاء في المرتبة الثانية الفقرة رقم (9) " تعزيز وعي الطلاب بمخاطر الروابط الضارة عند تصفح الإنترنت " بمتوسط حسابي بلغ (4.62)، وانحراف معياري بلغ (0.54) ونسبة مئوية (92%)، ودرجة استجابة عالية جداً. وجاء في المرتبة الثالثة الفقرة رقم (11) " توفير دليل تفاعلي عن أخلاقيات الأمن السيبراني، ومفاهيمه لمستخدمي منصة مدرستي. " بمتوسط حسابي بلغ (4.62)، وانحراف معياري بلغ (0.57)، ونسبة مئوية (92%)، ودرجة استجابة عالية جداً، وجاء في المرتبة الخامسة عشر الفقرة رقم (6) " عقد دورات تدريبية بإشراف معلّمي الحاسب الآلي لتوعية منسوبيّ المدرسة بالأمن السيبراني، " بمتوسط حسابي بلغ (4.52) وانحراف معياري بلغ (0.62)، ونسبة مئوية (90%)، ودرجة استجابة عالية جداً، وجاء في المرتبة السادسة عشر الفقرة رقم (3) " توفير خبراء ومختصين في الأمن السيبراني؛ لفحص الأجهزة والبرمجيات بصفة دورية في المدارس، " بمتوسط حسابي بلغ (4.51)، وانحراف معياري بلغ (0.67)، ونسبة مئوية (90%)، ودرجة استجابة عالية جداً، وجاء في المرتبة السابعة عشر الفقرة رقم (7) " تضمين مفاهيم الأمن السيبراني بمقرر تكنولوجيا التعليم ببرامج إعداد المعلمين والمعلمات. " بمتوسط حسابي بلغ (4.48)، وانحراف معياري بلغ (0.66)، ونسبة مئوية (90%)، ودرجة استجابة عالية جداً.

وتعزو الباحثة موافقة أفراد عينة البحث على جميع المقترحات بدرجة عالية جدًا، إلى الحاجة الماسة والملحة لوجود آليات لزيادة فاعلية الأمن السيبراني في مدارس التعليم العام، ولشعور منسوبي وزارة التعليم بالمخاطر التي تحيط بالعملية التعليمية، والبحث عن كل السبل لتفعلها.

مما سبق يتضح أن أفراد عينة البحث موافقون بنسبة 92% على الآليات المقترحة لزيادة فاعلية الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنورة.

5.3. التوصيات:

في ضوء النتائج التي توصلت إليها الدراسة، تم اقتراح مجموعة من التوصيات على النحو الآتي:

1. **رفع الوعي بالأمن السيبر اني من خلال:**
   - توفير برامج توعوية للتعريف بالأمن السيبراني، وآليات تعزيزه في المدارس.
   - توعية منسوبيّ المدرسة بمفاهيم الأمن السيبراني.
   - نشر الوعي بالأمن السيبراني لدى القيادات والمعلمين والطلاب حول آليات التعامل مع شبكة الإنترنت والمنصات التعليمية.
   - رفع الوعي مخاطر الأمن السيبراني وانتهاكاته من خلال عرض فيديوهات تعريفية موجزة على منصة مدرستي.
   - رفع وعي الطلاب بأهمية التحقّق من المصادر الموثوق بها؛ لحصولهم على معلومات تتعلق بدراستهم.
   - تعزيز وعي الطلاب بمخاطر الروابط الضارة عند تصفح الإنترنت.
   - توفير دليل تفاعلي عن أخلاقيات الأمن السيبراني ومفاهيمه لمستخدمي منصة مدرستي.
   - إرسال رسائل نصية توعوية بمفاهيم الأمن السيبراني ومخاطره وانتهاكاته.
   - عقد دورات تدريبية بإشراف معلّمي الحاسب الآلي لتوعية منسوبي المدرسة بالأمن السيبراني.
   - عقد دورات تدريبية بالشراكة مع الجامعات؛ لتوعية منسوبي التعليم العام بالأمن السيبراني.
   - تضمين مفاهيم الأمن السيبراني بمقرر تكنولوجيا التعليم ببرامج إعداد المعلمين والمعلمات.
2. **تشريع بعض القو انين الخاصة بالأمن السيبر اني من خلال:**
   - وضع إجراءات وسياسات لحفظ الأمن السيبراني داخل المدرسة، وفقا للضوابط الأساسية الصادرة من الهيئة الوطنية للأمن السيبراني.
   - وضع قوانين صارمة؛ للتعامل مع المتنمرين عبر منصة مدرستي والتوعية بقانون الجرائم المعلوماتية.
   - تشكيل فريق قانوني مختص بقضايا التنمر الإلكتروني عبر منصة مدرستي.
   - اتباع الضوابط الأساسية في الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني
   - تخصيص ميزانية مخصصة للأمن السيبراني تتناسب مع ميزانية التقنية والخدمات الإلكترونية، لتضمن استدامة أنشطة الأمن السيبراني.
   - توفير خبراء ومختصين في الأمن السيبراني؛ لفحص الأجهزة والبرمجيات بصفة دورية في المدارس.
3. **زيادة فاعلية الأمن السيبر اني من خلال:**
   - استخدام كلمة مرور معقدة لحسابات الدخول المهمة مثل الدخول لشبكة الوزارة، وينبغي أن تختلف عن كلمات المرور المستخدمة في مواقع التواصل الاجتماعي او مواقع التسوق الإلكتروني.
   - عدم استخدم البريد الإلكتروني الرسمي في التسجيل والاشتراك في مواقع التواصل الاجتماعي أو التطبيقات.

- ضرورة الاحتفاظ بنسخة احتياطية من الملفات في ذاكرة خارجية؛ لتفادي السرقة أو التلف.
- استخدام التشفير (من خلال تعيين كلمة مرور) للملفات المهمة التي يقوم بها منسوبي وزارة التعليم إرسالها من خلال شبكة الإنترنت.
- تعديل سياسات الخصوصية الافتراضية، من خلال إعدادات الخصوصية، بما يضمن تطبيق مستوى عالٍ من الخصوصية، عند استخدام الأجهزة والتطبيقات الإلكترونية.
- تفعيل خدمات الوصول للموقع بشكلٍ مؤقت أثناء استخدام بعض التطبيقات التي تتطلب ذلك.

4. العمل على تخطي التحديات التي تواجه تفعيل الأمن السيبر اني في مدارس التعليم العام من خلال:

- العمل على زيادة وعي الطلبة حول مخاطر الأمن السيبراني.
- إيجاد آلية للسيطرة على الطلاب، ومنعهم من دخول المواقع غير الموثوق بها.
- العمل على زيادة الوعي بقانون الجرائم المعلوماتية.
- توفير عدد كافٍ من المختصين في المدارس للتعامل مع مخاطر الأمن السيبراني.
- الالتزام بتوجيهات وزارة التعليم وعدم الوقوع في الإعلانات التصيدية التي تدعي وجود تحديث مجاني ومزيف لمايكروسوفت تيمز، ومنصة مدرستي.
- العمل على زيادة البرامج التدريبية الموجهة للمعنيين بالعملية التعليمية حول مخاطر الأمن السيبراني.
- عمل قوائم بالتطبيقات التعليمية الموثوق بها، ونشرها على موقع المنصة، والمراجعة الدورية لتلك التطبيقات لرصد سلوكها.

6.3. المقترحات:

- إجراء دراسة مماثلة للدراسة الحالية في مختلف إدارات التعليم بالمملكة العربية السعودية.
- إجراء دراسة مماثلة للدراسة الحالية على جامعات المملكة العربية السعودية.
- إجراء دراسة حول العلاقة بين الوعي بالأمن السيبراني والثقافة التكنولوجية لدى المعلمين.

المراجع:

أولاً: المراجع العربية:

1. بونيف، سامي (2019). دور الإستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية: الردع السيبراني أنموذجا. *المجلة الجزائرية للحقوق والعلوم السياسية: المركز الجامعي أحمد بن يحي الونشريسي تيسمسيلت - معهد العلوم القانونية والإدارية:* 4(7): 121 - 135.
2. الجمل، حازم (2020). الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة 2030. *مجلة البحوث الأمنية: كلية الملك فهد الأمنية - مركز الدراسات*
3. حيمد، محمد (2019). رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة. *المجلة العربية الدولية للمعلوماتية: اتحاد الجامعات العربية - جمعية كليات الحاسبات والمعلومات:* 7(12): 83 - 100.
4. الدهشان، جمال (2020). مستقبل التعليم بعد جائحة كورونا: سيناريوهات استشرافية. *المجلة الدولية للبحوث في العلوم التربوية: المؤسسة الدولية لآفاق المستقبل،* 3(4): 105 – 169.
5. الراظي، سيدي (2019). الجريمة السيبرانية وتكاملية النص الوطني، الإقليمي والدولي. *مجلة القانون والأعمال: جامعة الحسن الأول - كلية العلوم القانونية والاقتصادية والاجتماعية - مختبر البحث قانون الأعمال،* (47): 24 - 34.
6. الردفاني، محمد (2014). تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية. *المجلة العربية للدراسات الأمنية: جامعة نايف العربية للعلوم الأمنية،* 30(61): 157 – 192.
7. السرحان، حنين؛ المشاقبة، محمد (2020). *أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية* (رسالة ماجستير غير منشورة). جامعة آل البيت، المفرق.
8. سليمان، أمين؛ أبو علام، رجاء (2010). *القياس والتقويم في العلوم الإنسانية أسسه وأدواته وتطبيقاته*. القاهرة، دار الكتاب الحديث.
9. صائغ، وفاء (2018). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية. *المجلة العربية للعلوم الاجتماعية: المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية،* 14(3): 18 – 70.
10. الصانع، نورة (2020). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. *مجلة كلية التربية: جامعة أسيوط - كلية التربية،* 36(6): 41 - 90.
11. الصحفي، مصباح (2019). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. *مجلة البحث العلمي في*

التربية؛ جامعة عين شمس - كلية البنات للآداب والعلوم والتربية، 20(10): 493 - 534.

12. عبد القادر، محمود (2021). أزمة جائحة كورونا (كوفيد 19) وإشكاليات التعليم عن بعد: تحديات ومتطلبات. *المجلة التربوية*: جامعة سوهاج - كلية التربية، (83): 1 - 17.
13. عبيدات، ذوقان (2011). *البحث العلمي مفهومه وأدواته وأساليبه*، عمان: دار الفكر للنشر والتوزيع.
14. العيسى، طلال (2019). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر. *مجلة الزرقاء للبحوث والدراسات الإنسانية: جامعة الزرقاء - عمادة البحث العلمي*، 19(1): 81 - 95.
15. فوزي، إسلام. (2019). الأمن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سوسيولوجي. *المجلة الاجتماعية القومية: المركز القومي للبحوث الاجتماعية والجنائية*، 56(2): 99 - 139.
16. فيلالي، مريم. (2020). قراءات تحليلية للتعليم الافتراضي وقت الأزمات: كوفيد-19 أنموذجاً. *مجلة دراسات في العلوم الإنسانية والاجتماعية: مركز البحث وتطوير الموارد البشرية - رماح*، 3(4): 58 - 98.
17. مانيطه، يوسف (2017). نظرة عامة عن الجريمة الإلكترونية في الفضاء السيبراني. *المجلة الليبية العالمية: جامعة بنغازي-كلية التربية بالمرج*، (32): 1 - 10.
18. محمود، عبد الرازق (2020). تطبيقات الذكاء الاصطناعي: مدخل لتطوير التعليم في ظل تحديات جائحة فيروس كورونا (COVID-19). *المجلة الدولية للبحوث في العلوم التربوية: المؤسسة الدولية لآفاق المستقبل*، 3(4): 171 - 224.
19. ملاك، قارة (2016). الجريمة المعلوماتية في القطاع البنكي وأساليب مكافحتها: إشارة لحالة الجزائر. *مجلة جامعة الأمير عبد القادر للعلوم الإسلامية: جامعة الأمير عبد القادر للعلوم الإسلامية*، (39): 411 - 430.
20. المنتشري، فاطمة (2020). دور القيادة المدرسية في تعزيز الأمن السيبرانى في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للعلوم التربوية والنفسية؛ المؤسسة العربية للتربية والعلوم والآداب*، 17(1): 457 - 484.
21. المنتشري، فاطمة، وحريري، رندة (2020). درجة وعى معلمات المرحلة المتوسطة بالأمن السيبرانى في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للتربية النوعية؛ المؤسسة العربية للتربية والعلوم والآداب*، 14(1): 95 - 140.
22. الهيئة الوطنية للأمن السيبراني (2020). الإستراتيجية الوطنية للأمن السيبراني. المملكة العربية السعودية. https://nca.gov.sa/
23. وزارة التعليم (2020). المملكة العربية السعودية. https://www.moe.gov.sa
24. وزارة التعليم (2020). المملكة العربية السعودية. https://www.moe.gov.sa/ar/Pages/default.aspx.
25. يوسف، يوسف (2020). اتجاهات الطلاب نحو التعليم الإلكتروني في ظل جائحة فيروس كورونا: دراسة تطبيقية على عينة من طلاب كلية الاتصال والإعلام بجامعة الملك عبد العزيز بجدة. مجلة *الحكمة للدراسات الإعلامية والاتصالية*: (21): 11 - 37.

ثانياً: المراجع الأجنبية:

1. Alexander, R. T. (2017). *Can the analytical hierarchy process model be effectively applied in the prioritization of information assurance defense in-depth measures? -a quantitative study* (Doctoral dissertation, Capella University).
2. Bhatnagar, N., & Pry, M. (2020). Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of social media: An Initial Study. *Information Systems Education Journal*, 18(1): 48-58.
3. Chapman, J. (2019). *How Safe is Your Data?: Cyber-security in Higher Education*. Higher Education Policy Institute.
4. Corrigan, L., & Robertson, L. (2015). Inside the Digital Wild West: How School Leaders Both Access and Avoid social media. *International Association for Development of the Information Society*.
5. Frydenberg, M., & Lorenz, B. (2020). Lizards in the Street! Introducing Cybersecurity Awareness in a Digital Literacy Context. *Information Systems Education Journal*, 18(4): 33-45.
6. Gleeson, H. (2014). *The prevalence and impacts of bullying linked to social media on the mental health and suicidal behavior among young people: A review of the literatures*,7,14-16. https://www.education.ie/en/Publications/Education-eports/The-Preva- lence-and-Impact-of-Bullying-linked-to-Social-Media-on-the-Mental- Health-and-Suicidal-Behaviuor-Among-Young-People.pdf
7. Kurtz, H., Lloyd, S., Harwin, A., & Osher, M. (2018). School Leaders and Technology: Results from a National Survey. *Editorial Projects in Education*.

www.refaad.com

المجلة الدولية للدراسات التربوية والنفسية
International Journal of Educational & Psychological Studies (EPS)
Journal Homepage: https://www.refaad.com/views/EPSR/Home.aspx
ISSN: 2520-4149 (Online) 2520-4130 (Print)

The reality of cyber security and increasing its effectiveness in public education schools in Al-Madinah Al-Munawwarah region from the point of view of the school leadership

Mashael Shabib Mutairan AlZuwifri AlMutairi

Master's in Education Economics and Planning, Ministry of Education, KSA
mashael1alzuwifri@outlook.sa

Received : 8/7/2021 **Revised** : 20/7/2021 **Accepted** : 12/8/2021 **DOI** : https://doi.org/10.31559/EPS2021.10.3.7

Abstract: The study aimed to identify the reality of cyber security and increasing its effectiveness in public education schools in Al-Madinah Al-Munawwarah region from the point of view of the school leadership. To achieve the aim of the study, the descriptive and analytical approach was used, and a questionnaire was designed and distributed to a randomly selected sample from the study population of the study represented by leaders and teachers in public education schools in Madinah, Saudi Arabia, and the final sample reached (418). The study reached a set of findings, the most important of which were: Cybersecurity in public education schools in the Medina came at a high level of (72%) and it was found that there are many challenges facing the activation of cybersecurity in public education schools in the Madinah, which came at a high level with a percentage of (83%). The results of the study also indicated that there were no statistically significant differences at a significance level (0.05) for the challenges facing the activation of cybersecurity in public education schools in the Madinah due to the different variables of gender, job, academic qualification, number of years of experience, number of training courses in the field of information technology. As the study concluded the agreement of (92%) of the study sample on the proposed mechanisms to increase the effectiveness of cybersecurity in public education schools in Al Madinah Al Munawara; on top of which was: spreading awareness of cybersecurity among leaders, teachers, and students about the mechanisms of dealing with the Internet and educational platforms and enhancing students' awareness of the dangers of harmful links when surfing the Internet. As well as providing an interactive guide on cybersecurity ethics and its concepts for users of Madrasati platform. The study recommends that school staff should use a complex password for important log-in accounts, such as entering the Ministry's network. Furthermore, refraining from the use of the official e-mail to register and subscribe to social networking sites or electronic applications.

Keywords: *Distance Education; Madrasati Platform; Cybersecurity.*

References:

1. 'bd Alqadr, Mhmwd (2021). Azmh Ja'ht Kwrwna (Kwfyd 19) Weshkalyat Alt'lym 'n B'd: Thdyat Wmttlbat. Almjlh Altrbwyh: Jam't Swhaj - Klyt Altrbyh, (83): 1 - 17.
2. 'bydat, Dwqan (2011). Albhth Al'lmy Mfhwmh Wadwath Wasalybh, 'man: Dar Alfkr Llnshr Waltwzy'.
3. Al'ysa, Tlal (2019). Alms'wlyh Aldwlyh Alnash'h 'n Alhjmat Alsybranyh Fy Dw' Alqanwn Aldwly Alm'asr. Mjlt Alzrqa' Llbhwth Waldrasat Alensanyh: Jam't Alzrqa' - 'madh Albhth Al'lmy, 19(1): 81 - 95.
4. Bwnyf, Samy (2019). Dwr Alestratyjyat Alastbaqyh Fy Mwajht Alhjmat Alsybranyh: Alrd' Alsybrany Anmwdja. Almjlh Aljza'ryh Llhqwq Wal'lwm Alsyasyh: Almrkz Aljam'y Ahmd Bn Yhy Alwnshrysy Tysmsylt - M'hd Al'lwm Alqanwnyh Waledaryh: 4(7): 121 - 135.
5. Aldhshan, Jmal (2020). Mstqbl Alt'lym B'd Ja'ht Kwrwna: Synarywhat Astshrafyh. Almjlh Aldwlyh Llbhwth Fy Al'lwm Altrbwyh: Alm'ssh Aldwlyh Lafaq Almstqbl, 3(4): 105 – 169.
6. Fwzy, Eslam. (2019). Alamn Alsybrany: Alab'ad Alajtma'yh Walqanwnyh: Thlyl Swsywlwjy. Almjlh Alajtma'yh Alqwmyh: Almrkz Alqwmy Llbhwth Alajtma'yh Waljna'yh, 56(2): 99 - 139.
7. Fylaly, Mrym. (2020). Qra'at Thlylyh Llt'lym Alaftrady Wqt Alazmat: Kwfyd-19 Anmwdjaan. Mjlt Drasat Fy Al'lwm Alensanyh Walajtma'yh: Mrkz Albhth Wttwyr Almward Albshryh - Rmah, 3(4): 58 - 98.
8. Alhy'h Alwtnyh Llamn Alsybrany (2020). Alestratyjyh Alwtnyh Llamn Alsybrany. Almmlkh Al'rbyh Als'wdyh. https://nca.gov.sa/

9. Hymd, Mhmd (2019). R'yh Estratyjyh Lmkafht Aljra'm Alsybranyh: Alymn Drash Halh. Almjlh Al'rbyh Aldwlyh Llm'lwmatyh: Athad Aljam'at Al'rbyh - Jm'yt Klyat Alhasbat Walm'lwmat: 7(12): 83 - 100.

10. Aljml, Hazm (2020). Alhmayh Aljna'yh Llamn Alsybrany Fy Dw' R'yt Almmlkh 2030. Mjlt Albhwth Alamnyh: Klyt Almlk Fhd Alamnyh - Mrkz Aldrasat

11. Manyth, Ywsf (2017). Nzrh 'amh 'n Aljrymh Alelktrwnyh Fy Alfda' Alsybrany. Almjlh Allybyh Al'almyh: Jam't Bnghazy-Klyt Altrbyh Balmrj, (32): 1- 10.

12. Mhmwd, 'bd Alrazq (2020). Ttbyqat Aldka' Alastna'y: Mdkhl Lttwyr Alt'lym Fy Zl Thdyat Ja'ht Fyrws Kwrwna (Covid-19). Almjlh Aldwlyh Llbhwth Fy Al'lwm Altrbwyh: Alm'ssh Aldwlyh Lafaq Almstqbl, 3(4): 171 - 224.

13. Mlak, Qarh (2016). Aljrymh Alm'lwmatyh Fy Alqta' Albnky Wasalyb Mkafhtha: Esharh Lhalh Aljza'r. Mjlt Jam't Alamyr 'bd Alqadr Ll'lwm Aleslamyh: Jam't Alamyr 'bd Alqadr Ll'lwm Aleslamyh, (39): 411 - 430.

14. Almntshry, Fatmh (2020). Dwr Alqyadh Almdrsyh Fy T'zyz Alamn Alsybrana Fy Almdars Alhkwmyh Llbnat Bmdynh Jdh Mn Wjht Nzr Alm'lmat. Almjlh Al'rbyh Ll'lwm Altrbwyh Walnfsyh: Alm'ssh Al'rbyh Lltrbyh Wal'lwm Waladab, 17(1): 457 - 484.

15. Almntshry, Fatmh, Whryry, Rndh (2020). Drjt W'a M'lmat Almrhlh Almtwsth Balamn Alsybrana Fy Almdars Al'amh Bmdynh Jdh Mn Wjht Nzr Alm'lmat. Almjlh Al'rbyh Lltrbyh Alnw'yh: Alm'ssh Al'rbyh Lltrbyh Wal'lwm Waladab, 14(1): 95 - 140.

16. Alrazmy, Sydy (2019). Aljrymh Alsybranyh Wtkamlyh Alns Alwtny, Aleqlymy Waldwly. Mjlt Alqanwn Wala'mal: Jam't Alhsn Alawl - Klyt Al'lwm Alqanwnyh Walaqtsadyh Walajtma'yh - Mkhtbr Albhth Qanwn Ala'mal, (47): 24 - 34.

17. Alrdfany, Mhmd (2014). Thqyqat Alshrth Fy Mwajhh Thdyat Aljra'm Alsybranyh. Almjlh Al'rbyh Lldrasat Alamnyh: Jam't Nayf Al'rbyh Ll'lwm Alamnyh, 30(61): 157 – 192.

18. Sa'gh, Wfa' (2018). W'y Afrad Alasrh Bmfhwm Alamn Alsybrany W'laqth Bahtyatathm Alamnyh Mn Aljra'm Alelktrwnyh. Almjlh Al'rbyh Ll'lwm Alajtma'yh: Alm'ssh Al'rbyh Llastsharat Al'lmyh Wtnmyh Almward Albshryh, 14(3): 18 – 70.

19. Alsan', Nwrh (2020). W'y Alm'lmyn Balamn Alsybrany Wasalyb Hmayt Altlbh Mn Mkhatr Alentrnt Wt'zyz Alqym Walhwyh Alwtnyh Ldyhm. Mjlt Klyt Altrbyh: Jam't Asywt - Klyh Altrbyh, 36(6): 41 - 90.

20. Alshfy, Msbah (2019). Mstwa Alw'y Balamn Alsybrany Lda M'lmat Alhasb Alaly Llmrhlh Althanwyh Bmdynh Jdh. Mjlt Albhth Al'lmy Fy Altrbyh: Jam't 'yn Shms - Klyt Albnat Lladab Wal'lwm Waltrbyh, 20(10): 493 - 534.

21. Slyman, Amyn: Abw 'lam, Rja' (2010). Alqyas Waltqwym Fy Al'lwm Alensanyh Assh Wadwath Wttbyqath. Alqahrh, Dar Alktab Alhdyth.

22. Alsrhan, Hnyn: Almshaqbh, Mhmd (2020). Athr Ttbyq Syast Alamn Alsybrany 'la Jwdh Alm'lwmat Almhasbyh Fy Albnwk Altjaryh Alardnyh (Rsalt Majstyr Ghyr Mnshwrh). Jam't Al Albyt, Almfrq.

23. Wzart Alt'lym (2020). Almmlkh Al'rbyh Als'wdyh. https://www.moe.gov.sa

24. Wzart Alt'lym (2020). Almmlkh Al'rbyh Als'wdyh. https://www.moe.gov.sa/ar/pages/default.aspx.

25. Ywsf, Ywsf (2020). Atjahat Altlab Nhw Alt'lym Alelktrwny Fy Zl Ja'ht Fyrws Kwrwna: Drash Ttbyqyh 'la 'ynh Mn Tlab Klyt Alatsal Wale'lam Bjam't Almlk 'bd Al'zyz Bjdh. Mjlt Alhkmh Lldrasat Ale'lamyh Walatsalyh: (21): 11 - 37.