المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد 5 - الإصدار 59
تأريخ النشر: 20 سبتمبر 2024 م

واقع الأمن السيبراني في التعليم وعلاقته بالأمن النفسي من وجهة نظر المعلمات بدولة الكويت

The reality of cybersecurity in education and its relationship to psychological security from the point of view of female teachers in the State of Kuwait

إعداد الدكتورة/ عائشة عبيد الله مبارك قويضي العازمي

دكتوراه الفلسفة في التربية تخصص صحة النفسية، مدرب معتمد ومستشار تربوي، معلمة بوزارة التعليم بالكويت، عضو في جمعية علم النفس الكويتية، دولة الكويت

Email: dr.aishaom@gmail.com

الملخص

هدفت الدراسة إلى التعرف على واقع الأمن السيبراني وعلاقته بالأمن النفسي والتحديات التي تواجه تفعيله في التعليم داخل دولة الكويت والآليات المقترحة لتفعيله في مدارس الكويت من وجهة نظر المعلمات، ولتحقيق أهداف الدراسة تم استخدام المنهج الوصفي الارتباطي واستبانة الأمن السيبراني ومقياس الأمن النفسي بعد ضبط خصائصهما السيكومترية ليناسبا عينة الدراسة، على عينة مكونة من (353) معلمة من معلمات المرحلة الثانوية في محافظة الفروانية في دولة الكويت، وقد توصلت الدراسة إلى ارتفاع وعي المعلمات بأساسيات الأمن السيبراني، كما توصلت إلى عدد من التحديات التي تواجه تفعيل الأمن السيبراني في المدارس منها: عدم توفير المدرسة لبرمجيات حماية حديثة مع قلة وعي بعض المعلمين حول مخاطر الأمن السيبراني وتوصلت إلى عدد من الآليات المقترحة لتفعيل الأمن السيبراني في مدارس دولة الكويت، وأظهرت النتائج وجود علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة (0.05) موجبة بين الوعي بالأمن السيبراني والأمن النفسي عند المعلمات بدولة الكويت. وفي ضوء ما توصلت له الدراسة توصي الباحثة بالتأكيد على ضرورة اهتمام (مركز الأمن الوطني السيبراني NCSC)، وزارتي التربية والتعليم العالي بتطبيق الاستراتيجية الوطنية للأمن السيبراني والعمل بها، وحماية أنظمة المعلومات الإداريـــة بالجامعات والمؤسسات التعليمية، وإدراج مجال الفضاء السيبراني ضمن مناهج التعليم في دولة الكويت، وكذلك تشجيع بحوث ودراسات الأمن السيبراني في أطروحات الماجستير والدكتوراه، وتشجيع مجالات البحث العلمي والابتكار في مجال الأمن السيبراني، وتوعية العاملين بكافة مؤسسات الدولة وتنمية المعايير المهنية الاحترافية لديهم وإرســـاء بنية تحتية للدخول إلى مجال صناعة البرمجيات العالمية والقدرة على منافسة المنتج المستورد، و عقد دورات تدريبية وورش لتوعية الطلبة والمعلمات والعاملين في مجال التعليم بمفهوم الأمن السيبراني، وتعزيز تمويل الأبحاث العلمية في مجال الأمن السيبراني.

الكلمات المفتاحية: الأمن السيبراني، الأمن النفسي، معلمات المرحلة الثانوية

المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد 5 - الإصدار 59
تأريخ النشر: 20 سبتمبر 2024 م

The reality of cybersecurity in education and its relationship to psychological security from the point of view of female teachers in the State of Kuwait

Dr. Aisha Obaidullah Mubarak Qwaidi Al-Azmi

Doctorate of Philosophy in Education, Kuwait

Abstract:

The study aimed to identify the reality of cybersecurity and its relationship to psychosecurity and the challenges to its operationalization in education within Kuwait and the proposed mechanisms for its operationalization in Kuwait schools from the point of view of female teachers. To achieve the study's objectives, the correlative descriptive curriculum, cybersecurity identification and psychometer were used to adjust their psychometric characteristics to fit the sample of the study. 353 female high school teachers in Kuwait's Farawaniyah governorate. The study found that female teachers were more aware of the fundamentals of cybersecurity. It also found a number of challenges facing the operationalization of cybersecurity in schools, including: The school did not provide modern protective software with some teachers' lack of awareness about cybersecurity risks and came up with a number of proposed mechanisms to activate cybersecurity in Kuwait schools. The results showed a statistically significant correlation between cybersecurity awareness and psychosocial security among female teachers in Kuwait. In light of the findings of the study, the researcher recommends emphasizing the need for the National Cyber Security Center (NCSC) and the Ministries of Education and Higher Education to focus on implementing and working with the National Cyber Security Strategy, protecting administrative information systems in universities and educational institutions, including the field of cyberspace in the educational curricula in the State of Kuwait, as well as encouraging cybersecurity research and studies in master's and doctoral theses, encouraging areas of scientific research and innovation in the field of cybersecurity, educating employees in all state institutions and developing their professional standards, establishing an infrastructure to enter the field of the global software industry and the ability to compete with imported products, holding training courses and workshops to educate students, teachers and workers in the field of education about the concept of cybersecurity, and enhancing funding for scientific research in the field of cybersecurity.

Keywords: Cybersecurity, Psychosecurity, Secondary Teachers.

1. المقدمة:

يعتبر الأمن الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور نمو أي نشاط بعيداً عن تحققه، سواء أكان ذلك، على المستوى التقني، أم على المستوى القانوني. وقد تحول الأمن، مع بروز مجتمع المعلومات، والفضاء السيبراني، إلى واحد من الخدمات التي تشكل قيمة مضافة، ودعامة أساسية، لأنشطة الحكومات والأفراد على السواء، كما هو الحال مع التطبيقات الخاصة بالحكومة الإلكترونية، والصحة الإلكترونية والتعليم عن بعد، والاستعلام، والتجارة الإلكترونية وغيرها الكثير. إلا أن الوجوه المتعددة للأمن السيبراني، ومضاعفاتها الخطيرة التي لا تقف عند حدود الإساءة إلى الأفراد والمؤسسات بل تتعداها إلى تعريض سلامة الدول والحكومات. (حنين أبو حسين، 2021، ص1).

لقد انتشرت مؤخرًا نوعية خطيرة من الهجمات والجرائم السيبرانية تعتمد على تقنيات متقدمة (كالحوسبة السحابية والذكاء الاصطناعي وإنترنت الأشياء)، وأجهزة تصنت على شبكات الاتصال، وبرمجيات لتشفير العمليات المشبوهة، وبرمجيات خبيثة لاختراق أنظمة أمن الشبكات والحاسبات لتسخيرها في القيام بعمليات إجرامية وتعاملات مشبوهة دون علم أصحابها فيما يُسمَّى بالشبكات الآلية حيث يمكن أن تضم شبكة آلية واحدة عشرات أو مئات الآلاف أو ملايين الحواسب أو الأجهزة المتصلة بالإنترنت التي يمكن استخدامها لشن هجمات متنوعة، مثل الهجمات الموزّعة لإعاقة الخدمات على شبكات ومواقع مستهدفة لأغراض إجرامية كالتخريب والإرهاب والتهديد والابتزاز(فاطمة أحمد، 2022، ص392).

كما أن الأمور لم تتوقف عند هذا الحد بل تطرقت إلى المؤسسات الأكاديمية كالجامعات والمعاهد البحثية حيث لا يخفى على أحد أن هناك الكثير من الجرائم المعلوماتية التي تتم داخل الجامعات كالسرقات العلمية والقرصنة الإلكترونية التي تتم على مواقع الجامعات ذاتها والاختراقات وما إلى ذلك فكم سمعنا عن أساتذة قاموا بانتحال بحوث وكتابات علمية لآخرين، وكم سمعنا عن مواقع لجامعات تم اختراقها، ومن ثم تظهر أهمية النظافة الرقمية" الممارسات والاحتياطات التي يتخذها المستخدمون بهدف الحفاظ على البيانات الحساسة منظمة ومنظمة وآمنة من السرقة والهجمات الخارجية Tandon, Gaurav, H, (2019).

ويواجه معلم اليوم مجموعة من المتغيرات والتعامل معها يحتاج إلى درجة كفاءة عالية مما يتطلب التطوير الذاتي والتنمية المهنية المستمرة التي تزود المعلم بالعديد من الخبرات والمهارات، وتساعده على مواجهة كل جديد في مهنته مما يتطلب منه اكتساب المهارات لتنمية ذاته، حيث تهدف عملية التنمية المهنية للمعلم إلى تطوير أدائه في ضوء معايير محددة وواضحة ومواكبة للتطورات التكنولوجية التي تشهدها العملية التعليمية، وربطها بالبيئة التي يعيش فيها (أماني حمدي وآخرون، 3131، ص415).

وتأتي الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت نتيجة لإدراكنا للتحديات والتهديدات التي تواجهها الدولة والتي تستوجب تحديد الأسس والإجراءات الواجب اتخاذها وتسخير كافة القدرات التكنولوجية وتأهيل الموارد البشرية وتحسين القدرة على التعامل مع قضايا الأمن السيبراني، وذلك من أجل تعزيز أمن البنية التحتية الوطنية والبيانات الهامة، والحد من مخاطر الفضاء الإلكتروني المهددة لاقتصاد الدولة والأمن الوطني، وتأمين بيئة معلوماتية موثوقة ومرنة وآمنة للقطاع الحكومي والقطاع الخاص والأفراد(الشيخ جابر الصباح، 2020، ص10).

1.1. مشكلة الدراسة

بالنظر إلى قطاع التعليم من ضمن القطاعات السابقة سنجد أن العديد من الجامعات قد تعرضت لهجوم وحوادث اختراق فعلى سبيل المثال: ما حدث في عام 2015 من تعرض جامعة ميتشجان، جامعة كامبريدج وجامعة أكسفورد للهجوم من قبل مجموعة من الهاكرز المحترفين على شبكة الحاسوب الأكاديمية الممولة من القطاع العام (حسني، إسراء، 2015). كذلك ما تعرضت له جامعة" كشمير" في أغسطس 2022 من تسلل كشف عن المعلومات الشخصية لأكثر من مليون طالب وموظف حالي وسابق. كما أعلن مجلس مدرسة Waterloo Public school أن المتسللين وصلوا إلى قاعدة بيانات الطلاب أثناء هجوم إلكتروني وقع في يوليو 2022 (ALLIANCE, 2022).

وشدد رئيس كلية الكويت للعلوم والتكنولوجيا البروفيسور خالد البقاعين على أهمية الدورات التدريبية في تعزيز الوعي بالأمن السيبراني وقدرات الموظفين على مجابهة الهجمات السيبرانية، لافتاً إلى أهمية التخصصات في هذا المجال لحماية مؤسسات الكويت من أي هجمات محتملة مستقبلاً.

وأشار إلى أن تتعرض الكويت ما بين 1000-1500 هجمة إلكترونية يومياً بدرجات خطورة مختلفة منها هجمات للرسائل المزعجة والتصيد الإلكتروني، وذلك خلال ورشة عمل نظمتها السفارة الأميركية لدى الكويت بالتعاون مع كلية الكويت للعلوم والتكنولوجيا حول الأمن السيبراني لطلبة الكلية وموظفي الدولة (2023).

وبتطور التقنية والاتصالات وشبكات المعلومات الحديثة تشكلت منظومة متكاملة من الاحتياجات الحساسة للمحافظة على ممتلكات الدول المتعلقة بالتقنية والاتصال، مما جعل تأهيل المتخصصين في مجال أمن المعلومات ضرورة حتمية تبنتها الجامعات والكليات والمعاهد المتخصصة، في هذه الدراسة سنسلط الضوء على الأمن السيبراني في التعليم كأحدث مجال من مجالات التعلم والتعليم التقنية (لطيفة العمير، 2019، ص3).

عليه يُعد الأمن النفسي من الضرورات اللازمة للمعلم بشكل عام ومعلم علم النفس بشكل خاص، حيث يحتاج المعلم للعوامل التي تساعده على التكيف المهني والتدريسي والتطور الذاتي وفقاً لقدراته وإمكاناته، حيث يرى بعض التربويين أن عوامل ضعف العملية التعليمية قلة امتلاك المعلمين للمهارات الأساسية كالتخطيط واستخدام الوسائل التعليمية والاختبارات والتعزيز وإدارة الصف، ويرتبط الأداء المهني للمعلم بالمناخ المدرسي ودرجة التكيف النفسي داخل البيئة التعليمية ويستطيع المعلم أن يتحسن ويتطور أدائه وما يطرأ عليه من تغير نحو الأفضل عن طريق إيجاد مناخ مدرسي جيد وعلاقتها بمهارات الأداء المهني للمعلم.

ومن ثم تطرح الدراسة التساؤل التالي: **ما واقع الأمن السيبراني في التعليم وعلاقته بالأمن النفسي من وجهة نظر المعلمات بدولة الكويت؟**

ومنه يتفرع الأسئلة التالية:-

- ما واقع الأمن السيبراني في التعليم داخل دولة الكويت من وجهة نظر المعلمات بدولة الكويت؟
- ما التحديات التي تواجه تفعيل الأمن السيبراني في مدارس دولة الكويت من وجهة نظر المعلمات داخل دولة الكويت؟
- ما الآليات المقترحة لتفعيل الأمن السيبراني في مدارس دولة الكويت من وجهة نظر المعلمات بدولة الكويت؟

- هل توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة (0.05) بين الوعي بالأمن السيبراني والأمن النفسي عند المعلمات بدولة الكويت؟

2.1. أهمية الدراسة:

- التعرف على واقع الأمن السيبراني في التعليم داخل دولة الكويت وعلاقته بالأمن النفسي من وجهة نظر المعلمات بدولة الكويت.
- التعرف على التحديات التي تواجه تفعيل الأمن السيبراني في مدارس دولة الكويت وعلاقته بالأمن النفسي من وجهة نظر المعلمات داخل دولة الكويت.
- التعرف على الآليات المقترحة لتفعيل الأمن السيبراني في مدارس دولة الكويت وعلاقته بالأمن النفسي من وجهة نظر المعلمات بدولة الكويت.
- الكشف عن وجود علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة (0.05) بين الوعي بالأمن السيبراني والأمن النفسي عند المعلمات بدولة الكويت.

3.1. مصطلحات الدراسة

الأمن السيبراني:

هو أمن الشبكات والأنظمة المعلوماتية، والبيانات والمعلومات والأجهزة المتصلة بالإنترنت وعليه؛ فهو المجال الذي يتعلق بإجراءات ومقاييس، ومعايير الحماية، المفروض اتخاذها، أو الالتزام بها لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقسى وأسوأ الأحوال (حنين أبو حسين، 2021، ص18).

الأمن السيبراني هو مجموعة من الوسائل والتدابير التكنولوجية التي يتم استخدامها سواء من قبل أشخاص، أو هيئات، أو منظمات، أو أي كيانات أخرى، هدفها حماية كل ما يتعلق بها من بيانات، أو أدوات أو أنظمة وبرامج أو معدات، أو أجهزة سواء أكانت أجهزة حاسب آلي أو الحاسوب الشخصي أو هواتف ذكية غيرها من الدخول غير المصرح به أو المساس بها.

الأمن النفسي Psychological Security

ويُعرف Maslow الأمن النفسي بأنه هو الحاجة إلى الأمن والأمان والاستقرار، والحماية والتحرر من الخوف والقلق والإحساس بعدم الخطر، وشعور الفرد بأنه محبوب ومتقبل من الآخرين وله مكانه بينهم، تشعره بأهميته في المجتمع الذي يعيش فيه(Fenniman, 2010, 33).

وهو شعور مركب يحمل في طياته شعور الفرد بالسعادة والرضا عن حياته بما يحقق له الشعور بالسلامة والاطمئنان، وأنه محبوب ومتقبل من الأخرين بما يمكنه من تحقيق قدر أكبر من الانتماء للآخرين، مع إدراكه لاهتمام الآخرين به وثقتهم فيه حتى يستشعر قدرًا كبيرًا من الدفء والمودة، ويجعله في حالة من الهدوء والاستقرار، ويضمن له قدرًا من الثبات الانفعالي والتقبل الذاتي واحترام الذات، ومن ثم إلى توقع حدوث الأحسن في الحياة مع إمكانية تحقيق رغباته في المستقبل بعيدًا عن خطر الإصابة باضطرابات نفسية أو صراعات أو أي خطر يهدد أمنه واستقراره في الحياة (الخالدي، 2022، ص20).

2. الدراسات السابقة للدراسة.

دراسة (عبد العزيز الغامدي، 2016)

هدفت الدراسة إلى التعرف على مستوى الأمن النفسي لدى عينة مكونة من (60) طلاب وطالبات المرحلة الثانوية وتعرف الفروق بينهم واستخدم الباحث مقياس الأمن النفسي، وأوصت الدراسة بضرورة إقامة برامج تدريبية للطلاب والطالبات تهدف لزيادة مستوى الأمن النفسي لديهم، والاهتمام أكثر بزيادة الوعي لدى الأسر في تنمية الأمن النفسي لدى أبنائهم، فالأسرة هي الوعاء الذي يستقي منه الفرد صفاته النفسية والسلوكية، والعمل على جعل البيئة المدرسية بيئة آمنة نفسياً.

دراسة (حنين أبو حسين، 2020)

هدفت هذه الدراسة إلى التعرف على الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة) ومعرفة مفهوم الفضاء السيبراني وتأثيرها على دول العالم، حيث اعتمدت الدراسة على المنهج الوصفي وتم الاستعانة لغايات الاستدلال، ويعتبر الأمن السيبراني هو مجال متغير باستمرار، مع تطوير التقنيات التي تفتح آفاقا جديدة للهجمات الإلكترونية، وعلى الرغم من أن الانتهاكات الأمنية الكبيرة هي التي يتم الإعلان عنها فقط، إلا أنه لا يزال يتعين على المؤسسات الصغيرة أن تهتم بالانتهاكات الأمنية، حيث قد تكون غالبا هدفا للفيروسات والتصيد الاحتيالي. وقد خلصت الدراسة إلى مجموعة من النتائج كان من أبرزها: أن الأمن السيبراني يقوم على حماية المنظمات والموظفين والأفراد، يجب على المنظمات والخدمات تنفيذ أدوات الأمن السيبراني والتدريب وأساليب إدارة المخاطر وتحديث الأنظمة باستمرار مع تغير التقنيات وتطورها، تبين من الدراسة أن المشرع الأردني لم يعالج في قانون الأمن السيبراني الأردني المسائل التقنية والفنية لحادث الأمن السيبراني من حيث الطبيعة والأثر والتصنيف. الأمر الذي من شأنه التأثير على ضمان الحماية المقررة أو المرجوة للأمن السيبراني وسلامة الفضاء السيبراني الأردني.

كما أوصت الدراسة بضرورة مبادرة المشرع الأردني لإيجاد قواعد قانونية خاصة ناظمة لالتزامات وحالات قيام مسؤولية مقدمي خدمات الأمن السيبراني: الجزائية، والمدنية، وحالات الإعفاء منها. وهو ما سيترك آثارا إيجابية ستؤدي إلى زيادة حجم التبادل المعلوماتي الإلكتروني، وستشجع الإقدام على الاستثمار في هذا القطاع الشرياني، فتعم المنفعة على اقتصادنا الوطني، وأوصت أيضا ضرورة أن تسمح التشريعات، في هذا المجال، باللجوء لدعاوى أو لطلبات وقف بث المضمون الإلكتروني غير المشروع، وأن يتم، بدقة، تحديد الإجراءات الواجب إتباعها لسحبه، أو لمنع وصوله لمستخدمي الشبكة.

دراسة (فاطمة المنتشري، 2020)

هدفت الدراسة إلى معرفة دور القياد المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، وتقديم تصور مقترح لدور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة واتبعت الدراسة المنهج الوصفي التحليلي، وتم إعداد استبانة مكونة من محورين وهما دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات، و دور القيادة المدرسية في تعزيز الأمن السيبراني لدى طالبات المدرسة، 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. وفي ضوء تلك النتائج قدمت 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، الطالبات، المعلمات والطالبات معاً، بالإضافة إلى آليات حماية البيئة المادية لشبكة الإنترنت.

دراسة (نورة الصانع، 2020)

هدفت 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 بمدينة 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.

دراسة (أماني حمدي، وآخرون، 2021)

هدفت الدراسة إلى التعرف على فاعلية برنامج قائم على معايير الأمن النفسي في تنمية الأداءات المهنية لمعلمي علم النفس، حيث تم تحديد معايير الأمن النفسي اللازمة لمعلمي علم النفس بالمرحلة الثانوية والتي تمثلت في الاتزان الانفعالي - التكيف العلاقات الإيجابية مع الآخرين النفسي - التوافق المهني – الوعي التكنولوجي اكتشاف الذات، وتحديد الأداءات المهنية التي يجب تنميتها لدى معلمي علم النفس بالمرحلة الثانوية وتمثلت في أداءات تخطيطية - أداءات تنفيذية – أداءات تخصصية - أداءات تكنولوجية - أداءات اجتماعية - أداءات أخلاقية)، وتمثلت أدوات البحث في اختبار تحصيلي وبطاقة ملاحظة لقياس الجانب المعرفي والجانب الأدائي لدى معلمي علم النفس وتوصل البحث لوجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) بين متوسطي درجات المعلمين مجموعة البحث في التطبيق القبلي والبعدي للاختبار التحصيلي في الموضوعات ككل ولكل موضوع على حدة لصالح التطبيق البعدي، ووجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) بين متوسطي درجات المعلمين مجموعة البحث في التطبيق القبلي والبعدي لبطاقة الملاحظة في الأداءات ككل ولكل أداء على حدة لصالح التطبيق البعدي، مما يشير إلى فعالية البرنامج التدريبي الإلكتروني القائم على معايير الأمن النفسي في تنمية الأداءات المهنية لمعلمي علم النفس في المرحلة الثانوية.

دراسة (مشاعل الظويفري، 2021)

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 استخدام البريد الإلكتروني الرسمي في التسجيل والاشتراك في مواقع التواصل الاجتماعي أو التطبيقات الإلكترونية.

دراسة (فاطمة أحمد، 2022)

تناولت الدراسة موضوع الأمن السيبراني والنظافة الرقمية نظرًا لأهميته الكبير في ظل التحديات الراهنة التي تواجه المستخدمين نتيجة تعاملاتهم مع شبكات الإنترنت والأجهزة حيث تزداد عمليات الاختراق والانتهاكات يومًا بعد يوم ومن ثم كان لازما أن يكون هناك ردعًا لها وهنا يأتي دور الأمن السيبراني والنظافة الرقمية. ومن ثم هدفت هذه الدراسة إلى التعرف على مفهوم كلًا من الأمن السيبراني والنظافة الرقمية، ومعرفة الفرق بينهما، الوقوف على أهم الهجمات التي تعترض عملية الأمن السيبراني وكذا المشكلات التي تواجه النظافة الرقمية. وقد اعتمدت الدراسة على المنهج الوصفي التحليلي، وخرجت بعدة نتائج أهمها أن النظافة الرقمية جزء من الأمن السيبراني، أنه يوجد علاقة فيما بين النظافة الرقمية والأمن السيبراني والذكاء الاصطناعي. وقد أوصت الدراسة بضرورة تكثيف دورات التوعية بموضوع الأمن السيبراني والنظافة الرقمية للحد من الانتهاكات.

دراسة هولي وآخرين (Kurtz et al,2018)

استعرضت 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، وأغرب 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.

دراسة كوريجان وروبرتسون (Robertson & Corrigan, 2015)

هدفت الدراسة 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 الأمن للإنترنت، والاستجابة للأحداث السيبرانية التي قد تحدث خارج نطاق المدرسة.

ومن خلال الدراسات السابقة يتضح أنها إما دراسات استطلاعية قد جاءت مبنية على أراء معينة، أو أنها قد جاءت منصبة على منطقة معينة لدراسة التهديدات التي تعترضها في حين أن الدراسة الحالية دراسة نظرية فهي تركز فقط على الجانب النظري من حيث مفهوم وأهداف وأهمية وخصائص الأمن السيبراني ودور الدولة في مواجهة التحديات والمخاطر التي تواجهها في الأمن السيبراني وذلك بشكل عام دون ربط الموضوع بحدود مكانية معينة.

3. الإطار النظري

1.3. مفهوم الأمن السيبراني

تطلق كلمة سيبراني على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، والفضاء السيبراني يعني الفضاء الإلكتروني (Cyberspace)، وهو يعني كل ما يتعلق بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة (كالواتساب، والفيس بوك، وغيرها من مئات التطبيقات)، وكل الخدمات التي تقوم بتنفيذها كتحويل الأموال عبر النت، والشراء أون لاين، وغيرها من آلاف الخدمات في جميع مجالات الحياة على مستوى العالم (https://www.mah6at.net)

يقصد بالأمن السيبراني "Cyber Security" حماية الأشياء من خلال تكنولوجيا المعلومات مثل الأجهزة والبرمجيات ويشار إليها " ICT " وذلك اختصار Information Communication Technologies

والأمن السيبراني يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني مـــن الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستخدمة تقنيا وتنظيميًا وإداريا في منع الوصول غير المشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية ونظامية، وبذلك فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها، وحمايتها بكل خصوصية وسرية من خلال إتباع التدابير والإجراءات اللازمة لحماية البيانات (منى السمحان، 2020، ص9).

الأمن السيبراني لغوياً: الأمن السيبراني مكون من "لفظتين": الأمن"، و"السيبراني"

الأمن: هو نقيض الخوف، أي بمعنى السلامة والأمن مصدر الفعل أمن أمناً وأماناً.

وأمَنَةً: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه.

السيبراني: مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وكلمة "cyber" لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم."governor" وأشار بعض المؤرخين إلى أن أصلها يرجع إلى عالم الرياضيات الأمريكي (Norbert 1894-1964 Wieners) وذلك للتعبير عن التحكم الآلي.

الأمن السيبراني اصطلاحاً:

هناك العديد من التعاريف التي قدمت لمفهوم الأمن السيبراني، حيث يُعرف بأنه" مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة."

وهذا ما ذهب إليه الكاتبان Neittaanmaki Pekkaho Marti في كتابهما Cyber Security Analytics, Technology and Automation حيث عرفا الأمن السيبراني أنه: "عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة."

بينما عرفه إدوارد أمورسو Amoroso Edward بأنه" وسائل من شأنها الحـــد مـن خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة.

وعرفه غسان على أنه " عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الوصول غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين والمستهلكين في الفضاء السيبراني (غسان، 2019).

وهو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من عتاد وبرمجيات وما تقدمه من خدمات وما تحويه من بيانات من أي اختراق أو تعديل أو تعطيل أو دخول أو استخدام أو استخدام غير مشروع ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي وما إلى ذلك (دليل الهيئة الوطنية للأمن السيبراني، 2019).

إن الأمن السيبراني مجموعة الأدوات والسياسات ومفاهيم الأمن والضوابط والمبادئ التوجيهية ومنهجيات إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتقنيات التي يمكن استخدامها في حماية بيئة الفضاء الإلكتروني وأصول المؤسسات والمستخدمين وتشمل أصول المؤسسات والمستخدمين أجهزة الحاسوب المتصلة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات وكافة المعلومات التي يتم نقلها أو تخزينها في بيئة الفضاء الإلكتروني، ويسعى الأمن السيبراني إلى تحقيق الخصائص الأمنية لأصول المؤسسات والمستخدمين والمحافظة عليها وحمايتها من المخاطر الأمنية ذات الصلة في بيئة الفضاء الإلكتروني، كما تضم الأهداف العامة للأمن السيبراني كل من التيسير والسلامة والسرية (الاستراتيجية الوطنية للأمن السيبراني بالكويت، 2020، ص29).

ويرى "كانونجيا وماندارينو" (Canongia and Mandarino, 2014) أن الأمن السيبراني هو "فن ضمان ووجود واستمرارية مجتمع المعلومات، وضمان وحماية الفضاء الإلكتروني، بما يشمل المعلومات والأصول والبنية التحتية الحيوية" كما يُعرف الأمن السيبراني 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 اعادة الوضع الى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار الى خسائر دائمة (منى جبور، 2012، ص5).

وتجدر الإشارة إلى أن الأمن السيبراني مفهوم أوسع من أمن المعلومات، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمـــن المعلومات لا يهتم بذلك، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية الورقية"، بينما لا يهتم الأمن السيبراني بذلك. (الموسوعة السياسية political-encyclopedia.org/dictionary)

بعض المفاهيم المرتبطة بالأمن السيبراني وذلك حسب (الموسوعة السياسية political-encyclopedia.org/dictionary)

الفضاء السيبراني: عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI، بأنه": فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية. "فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين.

الردع السيبراني: يُعرف الردع السيبراني بأنه" منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية " الهجمات السيبرانية تعرف بأنها " فعلاً يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكّن المهاجم مـــن التلاعـــب بالنظام."

الجريمة السيبرانية: مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها.

ومن بعض المفاهيم أيضاً (دليل الهيئة الوطنية للأمن السيبراني، 2019)

هجوم سيبراني: استغلال غير مشروع لأنظمة الحاسب والشبكات والمنظمات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية، بهدف إحداث أضرار وتشمل أي نوع من الأنشطة الخبيثة التي تحاول الوصول غير المشروع أو تعطيل أو منع أو تدمير النظم المعلوماتية أو المعلومات نفسها.

صمود الأمن السيبراني: القدرة الشاملة للجهة على التصدي للحوادث السيبرانية وامتصاص الأضرار والتعافي منها في الوقت المناسب.

1.1.3. أهمية الأمن السيبراني:

في عالمنا المترابط بواسطة الشبكة، يستفيد الجميع من برامج الدفاع السيبراني. فمثلاً على المستوى الفردي يمكن أن يؤدي هجوم الأمن السيبراني إلى سرقة الهوية أو محاولات الابتزاز أو فقدان البيانات المهمة مثل الصور العائلية كما تعتمد المجتمعات على البنية التحتية الحيوية مثل محطات الطاقة والمستشفيات وشركات الخدمات المالية لذا فإن تأمين هذه المنظمات وغيرها أمر ضروري للحفاظ على عمل مجتمعنا بطريقة آمنة وطبيعية. (مبادرة العطاء الرقمي، 2019)

ومن أهمية الأمن السيبراني:

في عالم اليوم المترابط بواسطة الشبكات، يستفيد الجميع من برامج الدفاع السيبراني. وتتمثل أهمية الأمن السيبراني فيما يلي:

- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها تحقيق وفـــرة البيانات وجاهزيتها عند الحاجة إليها.
- حماية الأجهزة والشبكات ككل من الاختراقات لتكون درع واق للبيانات والمعلومات.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.
- توفير بيئة عمل آمنة جدًا خلال العمل عبر الشبكة العنكبوتية.

كما تتجلى أهمية الأمن السيبراني في قدرته على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التخلص من الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب سوء استخدامها، وكنتيجة حتمية لهذه الأهمية جعلته العديد من الدول على قمة أولوياتها وخصيصا بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، في إشارة صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حروب جديدة هي الحروب الإلكترونية. (الموسوعة السياسية، 2020).

2.1.3. خصائص الأمن السيبراني

1- ضمان الوصول المنطقي إلى الأصول المعلوماتية والتقنية للمؤسسة، وذلك لمنع الوصول غير المصرح به وتقييد الوصول لما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.

2- قدرته على حماية أنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للمؤسسة، وكذلك القدرة على حماية البريد الإلكتروني من المخاطر السيبرانية.

3- لديه قدرة على حماية وإدارة أمن الشبكات.

4- ضمان حماية أجهزة المؤسسة المحمولة بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في المؤسسة.

5- السرية وسلامة البيانات والمعلومات ودقتها وتوافرها وفق السياسات والإجراءات التنظيمية للمؤسسة (الهيئة القومية للأمن السيبراني، 2018).

3.1.3. أهداف الأمن السيبراني

- حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة، وضمان توافر استمرارية عمل نظم المعلومات.
- واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حدٍ سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة، وتعزيز حماية وسرية وخصوصية البيانات الشخصية (الرابغي، 2020).
- حماية شبكة المعلومات من أي هجوم وذلك بمعرفة آخر التقنيات والتكنيكات الموجود في هذا المجال ومن أهمها كشف أهداف رسائل هذا العدو والتعرّف على طبيعة هذا المهاجم وذلك وماذا يريد من خلال معرفة تكنيكاته المستخدمة والأساليب المختلفة لكي يتم العمل على إيقاف هذا الهجوم بأسلوب علمي وتقني مُحكم يمنع هذا الهجوم.
- تأمين البنى التحتية لأمن المعلومات والبيانات الخاصة بالمواطنين، مثلاً عندنا في المملكة لا بد من حماية قوية لجميع ما يتعلّق ببيانات المواطنين وحفظها في مكان آمن، وكذلك جميع أجهزتها ومواردنا الحياتية سواء من ممتلكات إلكترونية من أي محاولة عبث أو اختراق أو تدمير وتوفير الحماية اللازمة. (البكر، 2018)

4.1.3. عناصر الأمن الصناعي

حتى يتحقق الهدف من الأمن السيبراني، لا بد من توفر مجموعة من العناصر مع بعضها البعض لتكمل الدور في ذلك، ومن **أهم أبعاد وعناصر الأمن السيبراني:**

1. **التقنية (technology):** تشكل التكنولوجيا والتقنية دورًا في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.
2. **الأشخاص (People):** يستوجب الأمر لزومًا على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانبِ القيام بعمل نسخ احتياطية للبيانات.

3. الأنشطة والعمليات (Process): يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة (إيمان الحياري، 2019).

2.3. الأمن النفسي

1.2.3. مفهوم الأمن النفسي:

يتضمن الأمن النفسي إحساس الفرد بتقبل الآخرين وشعوره بالانتماء للمجتمع من خلال عملية التوافق مع الذات، وعملية التكيف مع الآخرين والتفاعل معهم. وعليه يجب أن تشمل معايير الأمن النفسي الاستقرار الانفعالي والنفسي والمهني والتكيف والتوافق المدرسي، وتحقيق الذات والشعور بالتقدير الذاتي والفهم النفسي لمشكلات الطلاب، وإقامة علاقات إيجابية مع الآخرين.

والشعور بالطمأنينة النفسية أحد مظاهر الصحة النفسية الإيجابية وأول مؤشراتها، حيث تحدث الكثير من العلماء والمفكرين عن أبرز المؤشرات الإيجابية للصحة النفسية ومنها شعور الفرد بالأمن النفسي والنجاح في إقامة علاقات مع الآخرين وتحقيق التوافق النفسي والبعد عن التصلب والانفتاح على الآخرين (بلال القرالة، 2016، ص8).

2.2.3. أهمية الأمن النفسي:

تتمثل أهمية الأمن النفسي في أنه من المفاهيم الأساسية في علم الصحة النفسية، والأمن النفسي هو الطمأنينة النفسية والانفعالية، والإنسان الآمن نفسياً يكون في حالة توازن، أو توافق واستقرار، وعليه سيتم عرض بعض تعريفات الأمن النفسي تعتقد الباحثة أنها مرتبطة بموضوع الدراسة الحالية. **حيث يعرف الأمن النفسي بأنه:** الحاجة إلى الشعور بأن البيئة الاجتماعية بيئة صديقة للفرد وشعور الفرد بأن الآخرين يحترمونه ويتقبلونه داخل الجماعة مع إدراكه لاهتمام الآخرين به وثقتهم فيه حتى يستشعر بقدر كبير من الدفء ويجعله في حالة من الهدوء والاستقرار، ويضمن له قدر من الثبات الانفعالي والتقبل الذاتي واحترام الذات، ومن ثم إلى توقع حدوث الأحسن في الحياة مع إمكانية تحقيق رغباته في المستقبل مع خلوه من خطر إصابته باضطرابات نفسية أو صراعات أو أي خطر يهدد أمنه واستقراره في الحياة (همت مصطفى، 2016، ص290-289).

3.2.3. عوامل الأمن النفسي:

- أن يشعر الشخص بقيمته الحقيقية ويرى نفسه بنظرة إيجابية (الإيمان بالذات).
- أن يحظى الفرد بعلاقات مثمرة وإيجابية مع الآخرين تتسم بالاهتمام المتبادل من جميع الأطراف.
- قدرة الشخص على رعاية ذاته وتنمية قدراته وتقييم سلوكياته حسب ضوابط ومعايير يقررها لنفسه.
- وعي الفرد ببيئته وبمقومات الحياة حوله وتسخيرها بما يصب في مصلحته.
- أن يستبصر الشخص المستقبل ويكون ذو طموح وأهداف يحرص على تحقيقها.
- أن يكون الشخص على دراية بقدراته ومواهبه ويعمل على بنائها وتطويرها طوال الوقت (ابريعم، 2019).

3.3. الهجمات والمخاطر التي يتعرض لها الأمن السيبراني

بعد الانتشار الكبير للإنترنت والأجهزة الذكية والأجهزة المحمولة.. أصبح من الضروري في وقتنا الحالي الانتباه للأمن السيبراني.. وكيفية حماية أنفسنا في الفضاء الرقمي.. ابتداءً من المنزل إلى العمل وعلى مستوى الدولة ككل.

ويعد الأمن السيبراني من أكثر المواضيع انتشاراً في أيامنا هذه.. وتعلّمه أصبح ضرورة لا بد منها.. نظراً لأن حياتنا اليومية أصبحت أكثر اعتماداً على الأدوات والخدمات المستندة إلى الإنترنت.. والعالم أصبح متصلا بشبكة الإنترنت في عصرنا الحالي.. وبالتالي أصبح الجميع عرضة للهجمات السيبرانية. إن جميع التقنيات بحد ذاتها تعاني من مخاطر كبيرة.. حيث يستغرق الأمر فقط من خمس إلى ست دقائق حتى يتم إختراق أي جهاز حاسوبي.

- **البرامج الضارة:** تُعد البرامج الضارة من أكثر أنواع تهديدات الأمن السيبراني شيوعًا، والتي بمجرد تثبيتها يمكن مراقبة أنشطة المستخدم، وحصول القراصنة على بيانات سرية، وهو ما يساعدهم في اختراق أهداف أخرى داخل الشبكة.

حيث ينجح المهاجمون في تثبيت البرامج الضارة من خلال الطلب من المستخدم اتخاذ إجراء مثل النقر فوق رابط أو فتح مرفق، أو استخدام تلك البرامج نقاط الضعف في المتصفحات أو أنظمة التشغيل لتثبيت نفسها دون علم المستخدم أو موافقته ومن هذه الهجمات (فيروس طروادة- برنامج الفدية- برنامج المسح الضار- برامج التجسس- برنامج الديدان- وغيرها....).

- **هجمات الهندسة الاجتماعية:** يعمل هذا النوع من الخطر على التلاعب بالمستخدمين نفسيًا، ومن ثم قيامهم بالكشف عن معلومات حساسة، أو بأفعال مرغوبة للمهاجم وتشمل تلك الهجمات (التصيد الاحتيالي- التصيد بالحربة- تنزيلات القيادة- برنامج أمان الخوف- صيد الحيتان- برنامج التخويف- وغيرها....)..

- **هجمات سلسلة التوريد:** هجمات سلسلة التوريد هي عبارة عن هجوم إلكتروني ضد منظمة تستهدف روابط ضعيفة في تحديث البرامج الموثوق بها وسلسلة التوريد، وذلك استغلالًا لثقة المؤسسات في بائعيها الخارجيين، فيما يخص التحديثات والتصحيح.

وينطبق هذا الهجوم على أدوات مراقبة الشبكة وأنظمة التحكم الصناعية والآلات الذكية، والأنظمة الأخرى التي تدعم الشبكة مع حسابات الخدمة.

- **رفض الخدمة الموزعة:** في عالم إدارة الأمن السيبراني، يُعد رفض الخدمة الموزعة من أبرز أنواع تهديدات الأمن السيبراني، إذ يهدف إلى التغلب على موارد النظام المُستهدف وجعله يتوقف عن العمل، مما يمنع الوصول إلى مستخدميه، ويستخدم المهاجمون عددًا كبيرًا من أجهزة الكمبيوتر أو الأجهزة الأخرى في شن هجومًا منسقًا ضد النظام المُستهدف، بهدف سرقة البيانات أو التسبب في أضرار أخرى وتُستخدم هجمات رفض الخدمة الموزعة جنبًا إلى جنب مع التهديدات الإلكترونية الأخرى، وتشمل أساليبها على (الروبوتات- هجوم حجب الخدمة- هجوم Smurf).

- **الهجوم الوسيط:** الوسيط المهاجم هو الذي يضع نفسه بين المستخدم والخادم المُستخدم، وذلك عند وصول المستخدم أو الأجهزة إلى نظام بعيد عبر الإنترنت، وهو ما يعرضه إلى سرقة البيانات الحساسة والمساومة عليها وتشمل هجمات الوسيط (اختطاف الجلسات- هجوم إعادة التشغيل- هجوم التنصت- هجوم البلوتوث- انتحال ال IP).

- **هجمات كلمة المرور:** هناك عدة طرق تمكن المهاجم من الوصول إلى كلمة مرور المستخدم، وهي الاتصال بالشبكة أو استخدام الهندسة الاجتماعية أو التخمين أو الوصول إلى قاعدة بيانات كلمات المرور، وتشمل هجمات كلمة المرور على (تخمين كلمة المرور- هجوم القاموس هجوم تمرير التجزئة- هجوم الكرة الذهبية- وغيرها).

- **هجوم ثقب المياه:** يُستخدم هذا النوع من الهجمات لاستهداف المنظمات، إذ تحدث هجمات ثقب المياه عندما تصيب مجموعة مواقع الويب التي تستخدمها منظمة معينة بشكل متكرر، ومن ثم تحميل برامج ضارة من المواقع المصابة.

ويستخدم المهاجمون هجوم ثقب المياه لسرقة المعلومات الشخصية والتفاصيل المصرفية والملكية الفكرية، فضلاً عن الوصول غير المصرح به إلى أنظمة الشركات الحساسة.

وعلى الرغم من ندرة استخدام هجمات ثقب المياه؛ إلا أن معدل نجاحها مرتفعًا، نظرًا لاستهدافها مواقع الويب المشروعة التي لا يمكن إدراجها في القائمة السوداء.

التهديدات المتقدمة المستمرة

يحصل المهاجمون على بيانات حساسة، عند وصولهم بشكل غير مصرح به إلى إحدى الشبكات، دون اكتشاف ذلك لفترة طويلة، وهذا النوع من الهجمات يُطلق ضد المؤسسات الكبيرة وحتى الدول، وغير ذلك من الكيانات الضخمة وتشمل التهديدات المتقدمة المستمرة على (إنشاء حساب جديد- نشاط غير طبيعي- ملفات بيانات غير عادية- وغيرها).

4.3. واقع الأمن السيبراني في التعليم بدولة الكويت

أدى الاهتمام الكبير بمجال الأمن السيبراني إلى تحركات سريعة وقوية في المجال التعليمي على مستويات عالية، فقد أنشأت كليات متخصصة حكومية وخاصة في هذا المجال وانبثقت بعض الوحدات السيبرانية في مجموعة من الجامعات السعودية كما عقدت اتفاقيات عديدة بين وزارة التعليم والجهات ذات الاختصاص لتدريب وتأهيل الطلاب والطالبات على البرمجيات من المستوى التأسيسي حتى مستوى الخبرة والتقدم. كما انطلت دورات معتمدة ومبادرات تطوعية عديدة للتدريب والتأهيل في مجال الأمن السيبراني.

الأمن السيبراني 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 مسئول ومدرك؛ لهذه المخاطر ليستطيع التعامل معها وثقاً لقواعد السلامة مع إدراكه للعواقب القانونية للتصرفات اللامسوؤلية والتي تعرض الآخرين للخطر، أو للسرقات (نورة الصانع، 2020).

مازالت الفرص التعليمية في مجال الأمن السيبراني ضئيلة بالمقارنة مع الطلب العالي للمهنيين المؤهلين القادرين على حمل لواء حماية الثغور الرقمية. كما أحرزت الكويت تقدماً في مؤشر الأمن السيبراني العالمي الصادر عن الاتحاد الدولي للاتصالات، حيث ارتفع ترتيبها من المركز 67 في 2019 إلى المركز الـ65 في 2020 (آخر بيانات للمؤشر). ويعود ذلك الفضل لله، ثم إلى ما بذلته الدولة وأجهزتها والمخلصون فيها من جهود في إقرار السياسات والآليات واستحداث المركز الوطني للأمن السيبراني. لكن يبقى السؤال: أين نحن من تفعيل كل هذه الأدوات والمؤسسات وتحقيق الاستفادة المرجوّة منها؟ كما لا يمكن إغفال أهمية التشريعات في مجال الأمن السيبراني وأمن المعلومات، لكن وبشهادة الكثير من المختصين، فهذه القوانين تحتاج إلى مراجعة جذرية، حيث اهتمت في غالبيتها بإرساء العقوبات، لا تشجيع الممارسات الحميدة والمنشودة، بالإضافة إلى تضييقها على مساحة حرية الرأي والتعبير، وعدم تضمينها إجراءات لحماية المبلغين والمخترقين الأخلاقيين (ضاري الحويل، 2022).

لا يزال الطريق أمامنا طويلاً، لكن هذا لا يدعو إلى اليأس أو الاستسلام، حيث أجمع الخبراء على ضرورة الاستمرار في تعزيز الإمكانات لضمان ودعم صمود مجال الأمن السيبراني في مختلف القطاعات على المستوى الوطني، من خلال الاستثمار

في البنى التحتية والبرمجيات ونظم المعلومات، ورأس المال البشري المتمثل بالجيل القادم من قادة الأمن السيبراني وتطوير مهاراتهم وقدراتهم، ومواءمة المسميات الوظيفية لتتناسب مع طبيعة التخصص. كما شددت التوصيات على أهمية تعزيز الوعي المجتمعي بالسلوك الرقمي الأخلاقي والمهني في العالم الافتراضي. ولم يتم إغفال جزئية دعم إجراء التقييم الدورية الشاملة لمستوى نضج الأمن السيبراني ومرونته لجميع المؤسسات العامة والخاصة والأهلية، بغضّ النظر عن حجمها، بالإضافة إلى تعزيز تمويل الأبحاث العلمية في مجال الأمن السيبراني، والتركيز بشكل خاص على توسيع مشاركة الشركات الصغيرة والمتوسطة في هذه الأبحاث العلمية. بتحقيق هذا قد نصل إلى مرادنا، وإن لم نستطع ذلك، فحتماً سنكون قطعنا شوطاً كبيراً (ضاري الحويل، 2022).

كيف واجهت دولة الكويت الهجمات والتهديدات والتحديات الناتجة عن مخاطر الأمن السيبراني؟

إن الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت هي استجابة لإدراك حكومة دولة الكويت لحجم التهديدات والتحديات الناتجة عن مخاطر الأمن السيبراني والتي تطال الدولة ومؤسساتها وأفرادها ككل، ولرسم خارطة الطريق نحو تعزيز أمن المعلومات بكافة أشكاله للتأكد من تسخير كافة الإمكانيات واتخاذ كافة التدابير اللازمة لذلك (الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت، 2020، ص13).

وتتمثل رؤيتنا في دولة الكويت بحماية مصالح الدولة المعرضة للمخاطر والتهديدات المتعلقة بالأمن السيبراني واتخاذ كافة التدابير الأمنية لتعزيز القدرة على الإدارة والاستجابة لأي طارئ، مما يضمن تحقيق أكبر قيمة اقتصادية واجتماعية من استخدام الفضاء الإلكتروني والاستفادة من الإمكانيات والمزايا التي يوفرها من دون التعرض للمخاطر (الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت، 2020، ص15).

وكانت مهمة الاستراتيجية خلق وتعزيز منظومة الأمن السيبراني الوطني بجميع عناصرها التقنية والتنظيمية والرقابية والإدارية وفي مختلف الجهات الحكومية والقطاع الخاص، وتوفير بيئة فضاء إلكتروني آمنة لتعزيز الأمن والازدهار لجميع الذين يعيشون ويعملون في دولة الكويت. وتقوم استراتيجية الأمن السيبراني على ثلاثة أهداف رئيسية لتمكن حكومة دولة الكويت من تحقيق رؤيتها الخاصة بالأمن السيبراني الوطني.

الهدف الأول: تعزيز ثقافة الأمن السيبراني التي تدعم الاستخدام الآمن والصحيح للفضاء الإلكتروني **ومنها** العمل مع وزارتي التربية والتعليم العالي والمؤسسات التابعة لها على تطوير مناهج أكاديمية وتثقيفية متعلقة بالأمن السيبراني. الجهة المسؤولة: الهيئة العامة للاتصالات وتقنية المعلومات (مركز الأمن الوطني السيبراني NCSC)، وزارتي التربية والتعليم العالي.

الهدف الثاني: حماية ومراقبة الأصول والبنى التحتية الحيوية والمعلومات الوطنية والشبكة المعلوماتية في دولة الكويت **ومنها** إعداد لوائح وضوابط ومعايير الأمن السيبراني للشبكات الحيوية والخدمات الإلكترونية والأنظمة الهامة الجهة المسؤولة: الهيئة العامة للاتصالات وتقنية المعلومات (مركز الأمن الوطني السيبراني NCSC)

الهدف الثالث: إتاحة سبل التعاون والتنسيق وتبادل المعلومات فيما بين مختلف الجهات المحلية والدولية في مجال الأمن السيبراني **ومنها** إعداد لوائح وضوابط ومعايير الأمن السيبراني للشبكات الحيوية والخدمات الإلكترونية والأنظمة الهامة الجهة المسؤولة: الهيئة العامة للاتصالات وتقنية المعلومات (مركز الأمن الوطني السيبراني NCSC).

4. إجراءات الدراسة

1.4. منهج الدراسة

لتحقيق أهداف البحث اعتمدت الباحثة على المنهج الوصفي الارتباطي حيث يتوافق مع الدراسة الحالية والإجراءات المتبعة فيها، بالإضافة إلى أن المنهج الوصفي الارتباطي من أكثر الطرق شيوًعاً واستخداماً لفحص العلاقات بين المتغيرات.

2.4. مجتمع الدراسة

يتكون مجتمع الدراسة الحالية من جميع معلمات المرحلة الثانوية في المدارس الحكومية بمحافظة الفروانية بالكويت والبالغ عددهم (1973) معلمة وفقاً لإحصائيات منطقة الفروانية التعليمية للعام الدراسي 2023- 2024.

3.4. عينة الدراسة

تم أخذ عينة عشوائية بسيطة مكونة من (353) معلمة من معلمات المرحلة الثانوية بمحافظة الفروانية بالكويت بطريقة عشوائية من مجتمع الدراسة.

4.4. أدوات الدراسة

تبنت الباحثة استبانة الأمن السيبراني إعداد (الظويفري،2021) وهي استبانة تم إعدادها بهدف التعرف على واقع الأمن السيبراني عند المعلمات والتحديات التي تواجهه والمقترحات لحل مشكلاته في مدارس الكويت، بالإضافة لمقياس الأمن النفسي (الطمأنينة الانفعالية) من إعداد (د/ زينب شقير، 2005) لقياس مستوى الأمن النفسي عند معلمات المرحلة الثانوية في دولة الكويت، وذلك بعد ضبط الخصائص السيكومترية لكلاً الأداتين حتى تناسبا عينة الدراسة.

5.4. الخصائص السيكومترية لأدوات الدراسة:

1.5.4. استبانة الأمن السيبراني:

1- صدق الأداة:

ويقصد بصدق الأداة أن تقيس الأداة ما وضع لقياسه (أبو سمرة، الطيطي، 2020)، وهو ما يعني أن تكون الأداة قادرة على تحديد واقع الأمن السيبراني عند معلمات المرحلة الثانوية، ولمعرفة مدى صدق الاستبانة قامت الباحثة باستخدام الطريقتين التاليتين:

- **الصدق الظاهري:**

تم عرض الاستبانة على عدد (10) من المحكمين، في صورته الأولية وذلك للتحقق من صلاحية الاستبانة وإبداء الرأي وذلك بالتأكد من:

أ- صلاحية تطبيق الاستبانة.

ب- شمول الاستبانة لجميع المحاور المرتبطة بموضوع البحث.

ت- دقة صياغة مفردات الاستبانة.

كما هو موضح في الجدول (1) تم استخدام معادلة كوبر لحساب معامل الاتفاق بين المحكمين وهي كالتالي:

معامل الاتفاق= (عدد مرات الاتفاق/ (عدد مرات الاتفاق+عدد مرات عدم الاتفاق)) X 100

جدول 1 معامل اتفاق السادة المحكمين على صلاحية عبارات الاستبانة

بنود التحكيم	معامل الاتفاق
مدى مناسبة العبارات لمجموعة البحث	%80
تصحيح الصياغة اللغوية التي تحتاج لذلك	%88
مدى ارتباط عبارات الاستبانة بموضوع البحث	%87
مدى صلاحية الاستبانة للتطبيق	%90

- **صدق الاتساق الداخلي:**

تم حساب صدق الاتساق الداخلي للاستبانة وذلك من خلال حساب معامل ارتباط كل محور من محاور الاستبانة بالدرجة الكلية لها وذلك حسب الجدول (2).

جدول 2 معاملات ارتباط بيرسون بين كل عبارة من عبارات محاور الاستبانة والمحور الخاص بها

م	المحور	معامل الارتباط بالدرجة الكلية	مستوى الدلالة
1	واقع التعامل مع آليات الأمن السيبراني	0.782	0.01
2	التحديات التي تواجه تفعيل الأمن السيبراني	0.885	
3	الآليات المقترحة لزيادة فاعلية الأمن السيبراني	0.610	

بمراجعة الجدول (2) نلاحظ ارتفاع معاملات ارتباط بيرسون بين كل محور والدرجة الكلية للاستبانة حيث تتراوح معاملات الارتباط من (0.610 – 0.885) وهي جميعها دالة عند مستوى دلالة (0.01)، مما يدل على صدق الاستبانة.

2- ثبات الاستبانة:

للتحقق من ثبات الاستبانة تم حساب معامل ألفا كرونباخ لكل محور من محاور الاستبانة وكانت النتائج كما هو موضح في جدول (3).

جدول 3 معامل الثبات ألفا كرونباخ لمحاور المقياس

م	المحور	معامل الثبات ألفا كرونباخ
1	واقع التعامل مع آليات الأمن السيبراني	0.763
2	التحديات التي تواجه تفعيل الأمن السيبراني	0.665
3	الآليات المقترحة لزيادة فاعلية الأمن السيبراني	0.867
	الاستبانة ككل	0.963

يتضح من الجدول (3) أن الاستبانة تتمتع بمعامل ثبات مرتفع (0.963)، وأن معاملات الثبات للمحاور تتراوح بين (0.665 – 0.867)، وهي جميعها معاملات مرتفعة، مما يدل على ثبات عبارات الاستبانة.

ويتضح من فحص الخصائص السيكومترية لاستبانة الأمن السيبراني أن الأداة تتمتع بالصدق والثبات، وأنها صالحة للتطبيق الميداني.

2.5.4. مقياس الأمن النفسي:

1- صدق الأداة:

وهو يعني أن تكون الأداة قادرة على تحديد مستوى الأمن النفسي عند معلمات المرحلة الثانوية، ولمعرفة مدى صدق المقياس قامت الباحثة باستخدام الطريقتين التاليتين:

- الصدق الظاهري:

تم عرض المقياس على عدد (10) من المحكمين، في صورته الأولية وذلك للتحقق من صلاحية المقياس وإبداء الرأي وذلك بالتأكد من:

أ- صلاحية تطبيق المقياس.

ب- شمول المقياس لجميع المحاور المرتبطة بموضوع البحث.

ت- دقة صياغة مفردات المقياس.

كما هو موضح في الجدول (4) تم استخدام معادلة كوبر لحساب معامل الاتفاق بين المحكمين وهي كالتالي:

معامل الاتفاق= (عدد مرات الاتفاق/ (عدد مرات الاتفاق+عدد مرات عدم الاتفاق)) X 100

جدول 4 معامل اتفاق السادة المحكمين على صلاحية عبارات المقياس

بنود التحكيم	معامل الاتفاق
مدى مناسبة العبارات لمجموعة البحث	%77
تصحيح الصياغة اللغوية التي تحتاج لذلك	%95
مدى ارتباط عبارات المقياس بموضوع البحث	%87
مدى صلاحية المقياس للتطبيق	%94

- **صدق الاتساق الداخلي:**

تم حساب صدق الاتساق الداخلي للمقياس وذلك من خلال حساب معامل ارتباط كل محور من محاور المقياس بالدرجة الكلية لها وذلك حسب الجدول (5).

جدول 5 معاملات ارتباط بيرسون بين كل عبارة من عبارات محاور المقياس والمحور الخاص بها

م	المحور	معامل الارتباط بالدرجة الكلية	مستوى الدلالة
1	تكوين الفرد ورؤيته للمستقبل	0.652	0.01

2	الحياة العامة والعملية للفرد	0.780	
3	الحالة المزاجية للفرد	0.800	
4	العلاقات الاجتماعية والتفاعل الاجتماعي للفرد	0.789	

بمراجعة الجدول (5) نلاحظ ارتفاع معاملات ارتباط بيرسون بين كل محور والدرجة الكلية للمقياس حيث تتراوح معاملات الارتباط من (0.652 – 0.800) وهي جميعها دالة عند مستوى دلالة (0.01)، مما يدل على صدق المقياس.

2- ثبات المقياس:

للتحقق من ثبات المقياس تم حساب معامل ألفا كرونباخ لكل محور من محاور المقياس وكانت النتائج كما هو موضح في جدول (6).

جدول 6 معامل الثبات ألفا كرونباخ لمحاور المقياس

م	المحور	معامل الثبات ألفا كرونباخ
1	تكوين الفرد ورؤيته للمستقبل	0.654
2	الحياة العامة والعملية للفرد	0.694
3	الحالة المزاجية للفرد	0.723
4	العلاقات الاجتماعية والتفاعل الاجتماعي للفرد	0.863
	المقياس ككل	0.887

يتضح من الجدول (6) أن المقياس يتمتع بمعامل ثبات مرتفع (0.887)، وأن معاملات الثبات للمحاور تتراوح بين (0.654 – 0.863)، وهي جميعها معاملات مرتفعة، مما يدل على ثبات عبارات المقياس.

ويتضح من فحص الخصائص السيكومترية مقياس الأمن النفسي أن الأداة تتمتع بالصدق والثبات، وأنها صالحة للتطبيق الميداني.

5. نتائج الدراسة:

قبل الإجابة على أسئلة الدراسة تم تصنيف مستويات الإجابة على بنود الأداة وذلك باستخدام المعادلة التالية:

طول الفئة = (أكبر قيمة – أقل قيمة) ÷ العدد الكلية للبدائل

طول الفئة = (5 – 1) ÷ 5 = 0.80

وبناء عليه سوف يتم توزيع الفئات كما هو موضح في الجدول (7)

جدول 7 توزيع فئات الاستجابات وفق التدرج الخاص بأداة البحث

الرتبة	المدى
مرتفعة جدا	من 4.20 –5.00
مرتفعة	من 3.40 – أقل من 4.20

متوسطة	من 2.60 إلى أقل من 3.40
منخفضة	من 1.80 إلى أقل من 2.60
منخفضة جدا	من 1.00 إلى أقل من 1.80

1. للإجابة على السؤال الأول: "ما واقع الأمن السيبراني في التعليم داخل دولة الكويت من وجهة نظر المعلمات بدولة الكويت؟"

تم حساب المتوسط الحسابي والانحراف المعياري لاستجابات أفراد العينة على عبارات محور "واقع التعامل مع آليات الأمن السيبراني" ثم تم ترتيب عبارات المحور حسب ترتيب المتوسطات الحسابية تنازليا كما هو موضح في الجدول (8)

جدول 8 المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة على محور "واقع التعامل مع آليات الأمن السيبراني"

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الرتبة
1	أحرص على عدم الإفصاح عن كلمة المرور الخاص بي لأي أحد	4.592	0.771	مرتفعة جدا
2	أحرص على عدم فتح أيّ مرفقات أو روابط مرفقة مع رسائل إلكترونية مجهولة المصدر.	4.577	0.815	مرتفعة جدا
3	استخدام الروابط الرسمية التي تنشرها وزارة التعليم في موقعها الرسمي.	4.518	0.859	مرتفعة جدا
4	أحرص على استخدام متصفح آمن للإنترنت.	4.512	0.882	مرتفعة جدا
5	أتجنب إرسال معلوماتي الشخصية عبر الرسائل أو البريد الإلكتروني	4.501	0.898	مرتفعة جدا
6	استخدام كلمة مرور معقدة لحسابات الدخول المهمة مثل الدخول لشبكة الوزارة وتختلف عن كلمات المرور المستخدمة في مواقع التواصل الاجتماعي أو مواقع التسوق الإلكتروني.	4.487	0.895	مرتفعة جدا
7	استخدام برمجيات معتمدة وموثوقة؛ لحماية الحاسب من الاختراق.	4.478	0.862	مرتفعة جدا
8	عند استخدام الأجهزة والتطبيقات الإلكترونية، يجب أن أقوم بتعديل سياسات الخصوصية الافتراضية، من خلال إعدادات الخصوصية، بما يضمن تطبيق مستوى عالي من الخصوصية.	4.467	0.885	مرتفعة جدا
9	أحتفظ بنسخة احتياطية من ملفاتي في ذاكرة خارجية، لتفادي السرقة أو التلف.	4.461	0.931	مرتفعة جدا

10	أؤيد طلب المدرسة من منسوبيها تغيير كلمة المرور الخاصة بهم بشكلٍ دوري	4.396	0.870	مرتفعة جدا
11	استخدام التشفير من خلال تعيين كلمة مرور لملفاتي المهمة التي أقوم بإرسالها من خلال شبكة الإنترنت	4.393	0.938	مرتفعة جدا
12	أفعّل خدمات الوصول لموقعي بشكلٍ مؤقت أثناء استخدام بعض التطبيقات التي تتطلب ذلك.	4.390	0.935	مرتفعة جدا
13	ألغي الاشتراك في التطبيقات التي تتضمن إعلانات لحماية بياناتي الشخصية والمالية.	4.359	0.981	مرتفعة جدا
14	لا أستخدم التطبيقات المجهولة التي تقدم خدمات مجانية للمعلمين	4.320	1.00	مرتفعة جدا
15	لا أستخدم البريد الإلكتروني الرسمي في التسجيل والاشتراك في مواقع التواصل الاجتماعي أو التطبيقات.	4.218	1.158	مرتفعة جدا
	الإجمالي	**4.445**		**مرتفعة جدا**

من الجدول (8) لوحظ أن جميع عبارات المحور حصلت على رتبة مرتفعة جداً مع فارق بسيط بين المتوسطات مما يدل على أن واقع الأمن السيبراني في التعليم داخل دولة الكويت من وجهة نظر المعلمات بدولة الكويت مرتفع جداً وهذا يدل على وعي المعلمات بدولة الكويت بمفاهيم وأساسيات الأمن السيبراني.

2. للإجابة على السؤال الثاني: "ما التحديات التي تواجه تفعيل الأمن السيبراني في مدارس دولة الكويت من وجهة نظر المعلمات داخل دولة الكويت؟"

تم حساب المتوسط الحسابي والانحراف المعياري لاستجابات أفراد العينة على عبارات محور "التحديات التي تواجه الأمن السيبراني" ثم تم ترتيب عبارات المحور حسب ترتيب المتوسطات الحسابية تنازليا كما هو موضح في الجدول (9)

جدول 9 المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة على محور التحديات التي تواجه الأمن السيبراني"

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الرتبة
1	عدم توفير المدرسة لبرمجيات حماية مواكبة لما يستجد من مخاطر الأمن السيبراني بشكل دوري.	3.600	0.788	مرتفعة
2	قلة وعي بعض المعلمين حول مخاطر الأمن السيبراني	3.586	0.749	مرتفعة
3	ضعف تفعيل آليات التعامل مع مخاطر الأمن السيبراني في المدارس.	3.563	0.806	مرتفعة

4	قلة الوعي بقانون الجرائم المعلوماتية.	3.512	0.808	مرتفعة
5	انتشار إعلانات تصديه تدعي وجود تحديث مجاني ومزيف لمايكروسوفت تيمز	3.507	0.787	مرتفعة
6	قلة البرامج التدريبية الموجهة للمعنيين بالعملية التعليمية حول مخاطر الأمن السيبراني.	3.501	0.856	مرتفعة
7	قلة وعي بعض القادة المدارس حول مخاطر الأمن السيبراني.	3.415	0.843	متوسطة
8	انتشار إعلانات تصديه تدعي وجود تحديث مجاني ومزيف لمايكروسوفت تيمز	3.431	0.787	متوسطة
9	قلة وجود مختصين في المدارس للتعامل مع مخاطر الأمن السيبراني.	3.428	0.901	متوسطة
10	ضعف السيطرة على الطلاب، ومنعهم من دخول المواقع غير الموثوق بها.	3.438	0.872	متوسطة
11	انتشار العديد من التطبيقات التعليمية غير الموثوق بها.	2.408	0.903	منخفضة
12	تعرض منصة تيمز لاختراقات من قبل الطلاب أو من أفراد خارج المدرسة.	2.342	0.903	منخفضة
13	انتهاك خصوصية المعلمين عن طريق نشر فيديوهات خاصة بهم من)فيديوهات مقتبسة من الدروس) عبر وسائل التواصل الاجتماعي.	2.300	0.950	منخفضة
14	التعرض إلى تهديدات عبر مواقع التواصل الاجتماعي (واتساب، تويتر، تليجرام، يوتيوب، سناب شات، فيسبوك)	2.243	0.992	منخفضة
	متوسط الإجمالي	**3.162**		**متوسطة**

بمراجعة الجدول (9) يتضح أن رتبة المتوسط الإجمالي لمحور "التحديات التي تواجه الأمن السيبراني" جاءت بدرجة متوسطة، وذلك بمتوسط (3.162)، كما جاء في المراتب الست الأولى برتبة مرتفعة الفقرات (10,8,11,3,5,6)، وفي المراتب الأربعة التالية برتبة متوسطة الفقرات (9,5,4,2)، ثم في المراتب الأربعة الأخيرة برتبة ضعيفة الفقرات (7,12,13,14).

كما يتضح أن أعلى فقرة في محور التحديات هي الفقرة "عدم توفير المدرسة لبرمجيات حماية مواكبة لما يستجد من مخاطر الأمن السيبراني بشكل دوري" وذلك بمتوسط (3.600) وذلك يدل على وجود مشكلة في أساسيات الأمن السيبراني في المدارس حيث ترى أفراد العينة أن برمجيات الحماية السيبرانية الحديثة والمحدثة دورياً غير متوفرة بالمدارس مما يجعل بيانات المدارس المخزنة إلكترونيا مثل شؤون الطلبة والعاملين وأعمال الامتحانات وغيرها عرضة للمخاطر انتهاك الأمن السيبراني.

كما يتضح أن أقل فقرة في المحور في الفقرة " التعرض إلى تهديدات عبر مواقع التواصل الاجتماعي (واتساب، تويتر، تليجرام، يوتيوب، سناب شات، فيسبوك)" وذلك بمتوسط (2.243) مما يدل على وعي المستخدمات من المعلمات وهيئة المدارس بهذه التهديدات، وكونها لا تمثل تحدياً أساسيا من التحديات التي تواجه الأمن السيبراني.

والمحور عامة لا يمتلك متوسط ذي رتبة عالية جدا، حيث جاءت أغلب عباراته برتب متوسطة أو منخفضة وهذا يتفق مع إجابة السؤال الأول ويدل على وجود نسبة وعي عالية بمخاطر الأمن السيبراني في التعليم.

3. للإجابة على السؤال الثالث: "ما الآليات المقترحة لتفعيل الأمن السيبراني في مدارس دولة الكويت من وجهة نظر المعلمات بدولة الكويت؟"

تم حساب المتوسط الحسابي والانحراف المعياري لاستجابات أفراد العينة على عبارات محور "الآليات المقترحة لزيادة فاعلية الأمن السيبراني" ثم تم ترتيب عبارات المحور حسب ترتيب المتوسطات الحسابية تنازليا كما هو موضح في الجدول (10)

جدول 10 المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة على محور "الآليات المقترحة لزيادة فاعلية الأمن السيبراني"

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الرتبة
1	وضع قوانين صارمة؛ للتعامل مع المتنمرين عبر منصة تيمز والتوعية بقانون الجرائم المعلوماتية.	4.708215297	0.654846824	مرتفعة جدًا
2	توعية منسوبيّ المدرسة بمفاهيم الأمن السيبراني.	4.648725212	0.727780574	مرتفعة جدًا
3	عقد دورات تدريبية بالشراكة مع الجامعات؛ لتوعية منسوبي التعليم العام بالأمن السيبراني.	4.64305949	0.766903262	مرتفعة جدًا
4	تشكيل فريق قانوني مختص بقضايا التنمر الإلكتروني عبر منصة تيمز.	4.59490085	0.759543115	مرتفعة جدًا
5	نشر الوعي بالأمن السيبراني لدى القيادات والمعلمين والطلاب حول آليات التعامل مع شبكة الإنترنت، والمنصات التعليمية.	4.583569405	0.726496697	مرتفعة جدًا
6	توفير خبراء ومختصين في الأمن السيبراني؛ لفحص الأجهزة والبرمجيات بصفة دورية في المدارس.	4.577903683	0.779910486	مرتفعة جدًا
7	توفير دليل تفاعلي عن أخلاقيات الأمن السيبراني، ومفاهيمه لمستخدمي منصة تيمز.	4.563739377	0.80976965	مرتفعة جدًا
8	تضمين مفاهيم الأمن السيبراني بمقرر تكنولوجيا التعليم ببرامج إعداد المعلمين والمعلمات.	4.560906516	0.809988268	مرتفعة جدًا

9	عقد دورات تدريبية بإشراف معلمي الحاسب الآلي لتوعية منسوبي المدرسة بالأمن السيبراني.	4.555240793	0.79624974	مرتفعة جدًا
10	تعزيز وعي الطلاب بمخاطر الروابط الضارة عند تصفح الإنترنت.	4.552407932	0.705659857	مرتفعة جدًا
11	رفع الوعي بمفاهيم ومخاطر وانتهاكات الأمن السيبراني من خلال عرض فيديوهات تعريفية موجزة على منصة مدرستي.	4.54674221	0.793221914	مرتفعة جدًا
12	توفير برامج توعوية للتعريف ب الأمن السيبراني، وآليات تعزيزه في المدارس.	4.543909348	0.858727595	مرتفعة جدًا
13	اتباع الضوابط الأساسية في الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني	4.543909348	0.828418203	مرتفعة جدًا
14	تخصيص ميزانية مخصصة للأمن السيبراني تتناسب مع ما يتم صرفه على التقنية والخدمات الإلكترونية وتضمن استدامة أنشطة الأمن السيبراني.	4.52407932	0.836057655	مرتفعة جدًا
15	رفع وعي الطلاب بأهمية التحقّق من المصادر الموثوق بها؛ لحصولهم على معلومات تتعلق بدراستهم.	4.458923513	0.868734697	مرتفعة جدًا
16	وضع إجراءات، وسياسات لحفظ الأمن السيبراني داخل المدرسة، وفقا للضوابط الأساسية الصادرة من الهيئة الوطنية للأمن السيبراني.	4.390934844	0.979985783	مرتفعة جدًا
17	إرسال رسائل نصية توعوية بمفاهيم ومخاطر وانتهاكات الأمن السيبراني.	4.373937677	0.927239651	مرتفعة جدًا
	متوسط الإجمالي	**4.551**		**مرتفعة جدًا**

بمراجعة الجدول (10) يتضح أن رتبة المتوسط الإجمالي لمحور " الآليات المقترحة لزيادة فاعلية الأمن السيبراني" حصلت على رتبة مرتفعة جداً مع فارق بسيط بين المتوسطات مما يدل على أن أغلب أفراد العينة موافقات على الآليات المقترحة لزيادة فاعلية الأمن السيبراني.

4. للإجابة على السؤال الرابع "هل توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة (0.05) بين الوعي بالأمن السيبراني والأمن النفسي عند المعلمات بدولة الكويت؟"

تم حساب معامل الارتباط بيرسون بين مجموع استجابات أفراد العينة على محور "واقع التعامل مع آليات الأمن السيبراني" التابع لاستبانة الأمن السيبراني والذي يعبر عن وعي أفراد العينة بالأمن السيبراني وبين مجموع استجابات أفراد العينة على مقياس الأمن النفسي، وهذا ما يوضحه جدول (11).

جدول 11 معامل الارتباط بيرسون بين مجموع استجابات أفراد العينة على محور "واقع التعامل مع آليات الأمن السيبراني" التابع لاستبانة الأمن السيبراني وبين مجموع استجابات أفراد العينة على مقياس الأمن النفسي

المتغيرات	المتوسط	الانحراف المعياري	معامل الارتباط	مستوى الدلالة
الوعي بالأمن السيبراني	66.68	9.572	0.881	<0.01
الأمن النفسي	206.60	24.17		

يتضح من جدول (11) ارتفاع معامل الارتباط بين مستوى الوعي بالأمن السيبراني حيث أنه يساوي (0.881) بمستوى دلالة أقل من (0.01) أي أنه دال إحصائيًا عند مستوى (0.05) وهذا يعني وجود علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة (0.05) بين الوعي بالأمن السيبراني والأمن النفسي عند المعلمات بدولة الكويت.

6. مناقشة النتائج والتوصيات:

1.6. مناقشة النتائج

أولًا: مناقشة نتائج السؤال الأول: ما واقع الأمن السيبراني في التعليم داخل دولة الكويت من وجهة نظر المعلمات بدولة الكويت؟

أظهرت النتائج الإحصائية حصول محور واقع التعامل مع آليات الأمن السيبراني على رتبة (مرتفعة جدا) مما يؤكد وعي المعلمات بدولة الكويت بمفاهيم وأساسيات الأمن السيبراني.

ثانياً: مناقشة نتائج السؤال الثاني: ما التحديات التي تواجه تفعيل الأمن السيبراني في مدارس دولة الكويت من وجهة نظر المعلمات داخل دولة الكويت؟

أظهرت النتائج الإحصائية أن أبرز تحديات الأمن السيبراني في مدارس الكويت تتمثل في:

- عدم توفير المدرسة لبرمجيات حماية مواكبة لما يستجد من مخاطر الأمن السيبراني بشكل دوري.
- قلة وعي بعض المعلمين حول مخاطر الأمن السيبراني.
- ضعف تفعيل آليات التعامل مع مخاطر الأمن السيبراني في المدارس.
- قلة الوعي بقانون الجرائم المعلوماتية.
- انتشار إعلانات تصديه تدعي وجود تحديث مجاني ومزيف لمايكروسوفت تيمز.
- قلة البرامج التدريبية الموجهة للمعنيين بالعملية التعليمية حول مخاطر الأمن السيبراني.

ثالثاَ: مناقشة نتائج السؤال الثالث: ما الآليات المقترحة لتفعيل الأمن السيبراني في مدارس دولة الكويت من وجهة نظر المعلمات بدولة الكويت؟

أظهرت النتائج الإحصائية موافقة أفراد العينة برتبة مرتفعة جدا على الآليات المقترحة في الاستبانة وهي كالتالي:

- وضع قوانين صارمة؛ للتعامل مع المتنمرين عبر منصة تيمز والتوعية بقانون الجرائم المعلوماتية.
- توعية منسوبيّ المدرسة بمفاهيم الأمن السيبراني.

- عقد دورات تدريبية بالشراكة مع الجامعات؛ لتوعية منسوبي التعليم العام بالأمن السيبراني.
- تشكيل فريق قانوني مختص بقضايا التنمر الإلكتروني عبر منصة تيمز.
- نشر الوعي بالأمن السيبراني لدى القيادات والمعلمين والطلاب حول آليات التعامل مع شبكة الإنترنت، والمنصات التعليمية.
- توفير خبراء ومختصين في الأمن السيبراني؛ لفحص الأجهزة والبرمجيات بصفة دورية في المدارس.
- توفير دليل تفاعلي عن أخلاقيات الأمن السيبراني، ومفاهيمه لمستخدمي منصة تيمز.
- تضمين مفاهيم الأمن السيبراني بمقرر تكنولوجيا التعليم ببرامج إعداد المعلمين والمعلمات.
- عقد دورات تدريبية بإشراف معلمي الحاسب الآلي لتوعية منسوبي المدرسة بالأمن السيبراني.
- تعزيز وعي الطلاب بمخاطر الروابط الضارة عند تصفح الإنترنت.
- رفع الوعي بمفاهيم ومخاطر وانتهاكات الأمن السيبراني من خلال عرض فيديوهات تعريفية موجزة على منصة مدرستي.
- توفير برامج توعوية للتعريف ب الأمن السيبراني، وآليات تعزيزه في المدارس.
- اتباع الضوابط الأساسية في الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني
- تخصيص ميزانية مخصصة للأمن السيبراني تتناسب مع ما يتم صرفه على التقنية والخدمات الإلكترونية وتضمن استدامة أنشطة الأمن السيبراني.
- رفع وعي الطلاب بأهمية التحقّق من المصادر الموثوق بها؛ لحصولهم على معلومات تتعلق بدراستهم.
- وضع إجراءات، وسياسات لحفظ الأمن السيبراني داخل المدرسة، وفقا للضوابط الأساسية الصادرة من الهيئة الوطنية للأمن السيبراني.
- إرسال رسائل نصية توعوية بمفاهيم ومخاطر وانتهاكات الأمن السيبراني.

رابعاً: مناقشة نتائج السؤال الرابع: هل توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة (0.05) بين الوعي بالأمن السيبراني والأمن النفسي عند المعلمات بدولة الكويت؟

أظهرت النتائج الإحصائية أن معامل الارتباط بين الوعي بالأمن السيبراني والأمن النفسي هو ارتباط موجب قوي، بمعنى أنه عند زيادة الوعي السيبراني لأفراد العينة يزيد الأمن النفسي عند نفس الأفراد.

2.6. توصيات البحث:

- التأكيد على ضرورة اهتمام (مركز الأمن الوطني السيبراني NCSC)، وزارتي التربية والتعليم العالي بتطبيق الاستراتيجية الوطنية للأمن السيبراني والعمل بها.
- حماية أنظمة المعلومات الإداريـــة بالجامعات والمؤسسات التعليمية.
- إدراج مجال الفضاء السيبراني ضمن مناهج التعليم في دولة الكويت.
- تشجيع بحوث ودراسات الأمن السيبراني في أطروحات الماجستير والدكتوراه
- تشجيع مجالات البحث العلمي والابتكار في مجال الأمن السيبراني.

- توعية العاملين بكافة مؤسسات الدولة وتنمية المعايير المهنية الاحترافية لديهم وإرســـاء بنية تحتية للدخول إلى مجال صناعة البرمجيات العالمية والقدرة على منافسة المنتج المستورد.

- عقد دورات تدريبية وورش لتوعية الطلبة والمعلمات والعاملين في مجال التعليم بمفهوم الأمن السيبراني.

- تعزيز تمويل الأبحاث العلمية في مجال الأمن السيبراني، والتركيز بشكل خاص على توسيع مشاركة الشركات الصغيرة والمتوسطة في هذه الأبحاث العلمية.

7. المراجع والمصادر

1.7. المصادر العربية:

ابريعم سامية خالد (2019). **سيكولوجية الأمن النفسي**. دار التعليم الجامعي.

الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت (2017-2020). **الهيئة العامة للاتصالات وتقنية المعلومات**، الإصدار الأول، الكويت.

أماني حمدي عبد الباسط أحمد، علي كمال معبد، أسامة عربي محمد (2021). برنامج قائم على معايير الأمن النفسي في تنمية الأداءات المهنية لمعلمي علم النفس بالمرحلة الثانوية. **المجلة العلمية**، كلية التربية، جامعة أسيوط، 37(7)، 412-446.

الأمن السيبراني. **الموسوعة السياسية** https://political-encyclopedia.org/dictionary

إيمان الحياري (2019). **ما هو الأمن السيبراني، وما هي معاييره، وما أهميته؟** منشور https://www.mah6at.net/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A/

بدر سعود عناد مهنا خلف الخالدي. (2022) الأمن النفسي لدى الأطفال، **المجلة العلمية لكلية التربية للطفولة المبكرة**، 8(4)، جامعة المنصورة - كلية التربية للطفولة المبكرة، 1-23.

بلال جمال القرالة (2016). **الأمن النفسي وعلاقته بقلق المستقبل لدى طلبة المرحلة الثانوية في تربية قصبة الكرك**. رسالة ماجيستير، كلية الدراسات العليا، جامعة مؤته: الأردن.

حنين جميل أبو حسين (2021). **الإطار القانوني لخدمات الأمن السيبراني: دراسة مقارنة.** رسالة ماجيستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن.

ضاري عادل الحويل (2022). **واقع الأمن السيبراني وأمن المعلومات في الكويت. منشور** https://www.alqabas.com/article/5885103

عبد العزيز البكر (2018). **الأمن السيبراني - مفهومه – أهدافه. منشور** https://www.al-jazirah.com/2018/20180926/ar6.htm

عبد العزيز بن رشيد الغامدي (2016). الأمن النفسي لدى طلاب وطالبات المرحلة الثانوية بمدينة الدمام. **مجلة كلية التربية**، جامعة بنها، 27(107)، ج2، 411- 446.

علي محمد الرابغي (2020). **الأمن السيبراني والثورة الصناعية الرابعة. منشور** https://www.okaz.com.sa/articles/authors/2010045

فاطمة علي إبراهيم أحمد (2022). الأمن السيبراني والنظافة الرقمية. **المجلة المصرية لعلوم المعلومات**، كلية الآداب، جامعة بني سويف، 9(2)، 390- 422.

فاطمة يوسف المنتشري (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.

لطيفة بن عبد الرحمن العمير (2019). **الأمن السيبراني في التعليم. اتجاهات معاصرة في التربية**. كلية التربية، جامعة الإمام محمد بن سعود الإسلامية، السعودية.

مبادرة العطاء الرقمي (2019). https://attaa.sa/arabic_content/view/20

مشاعل بنت شبيب بن مطيران الظويفري (2021). واقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية. **المجلة الدولية للدراسات التربوية والنفسية، 10(3)**، 635-655.

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

نورة الصانع (2020). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. **مجلة كلية التربية**، جامعة أسيوط، 36(6): 41 - 90.

همت مختار مصطفى (2016). استخدام موقع التواصل الاجتماعي الفيس بوك وعلاقته بالثقة بالنفس وتقدير الذات والأمن النفسي لدى عينة من طلاب المؤسسات الإيوائية. **مجلة كلية التربية**، جامعة الأزهر، (167)، ج2، 279- 350.

ورشة عمل نظمتها السفارة الأميركية لدى الكويت بالتعاون مع كلية الكويت للعلوم والتكنولوجيا حول الأمن السيبراني لطلبة الكلية وموظفي الدولة (2023).

الهيئة الوطنية للأمن السيبراني (2018). **الضوابط الأساسية للأمن السيبراني** Retrieved from https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

الموسوعة السياسية (2020). **الأمن السيبراني- Cyber Security**. تم الاسترداد من الموسوعة السياسية: https://cutt.ly/CBTCUh6

الهيئة المنظمة للاتصالات (2008). **لمحة عامة حول الأمن السيبراني** Retrieved from http://www.tra.gov.lb/Cybersecurity-in-few-words-AR

2.7. المراجع الأجنبية:

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

Corrigan, L., Robertson, L. (2015). Inside the digital wild west: how school leaders both access and avoid social media. A paper presented at proceedings of 12th International Conference on Cognition and Exploratory Learning in Digital Age (CELDA 2015).

Fenniman, A. (2010). Understanding each other at work: An examination of the effects of perceived empathetic listening on psychological safety in the supervisor -subordinate relationship. (Order No. 3389636). Available from ProQuest Dissertations & Theses Global; Publicly Available Content Database. (305202979).

Holly, K., Sterling, L., Alexandra, H. & Michael, O. (2018). School leaders and technology: results from a national survey. Bethesda: Education week researcher center.

3.7. مواقع النت:

https://alseyassah.com

https://aws.amazon.com/ar/what-is/cybersecurity/

https://bakkah.com/ar/knowledge-center/how-to-perform-a-cyber-risk-assessment

https://citra.gov.kw/sites/ar/LegalReferences/Cyber%20Security.pdf

https://maed.journals.ekb.eg/article_140786_92feaa0b360fd79ceb4b6c5d7a95be72.pdf

https://www.aljarida.com/article/40760

https://www.alqabas.com/article/

https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html#~types-of-threats

https://www.e3melbusiness.com/blog/cyber-security

Doi: doi.org/10.52133/ijrsp.v5.59.2