جامعة سوهاج
كلية التربية
المجلة التربوية

مستوى وعي معلّمات قبل الخدمة في كلية التربية بجامعة الكويت بالأمن السيبراني

إعداد

أ.د. عمار حسن صفر
أستاذ بقسم المناهج وطرق التدريس، كلية التربية
جامعة الكويت، دولة الكويت

تاريخ استلام البحث : ٣١ أكتوبر ٢٠٢٣م – تاريخ قبول النشر: ١٢ نوفمبر ٢٠٢٣م

DOI: 10.12816/EDUSOHAG.2024.

المُلخَّص

هدفت الدراسة إلى قياس مستوى وعي طالبات كلية التربية بجامعة الكويت – معلّمات قبل الخدمة – بالأمن السيبراني، إضافةً إلى الكشف عن أثر متغيّرات نوع التخصُّص، ودورات الأمن السيبراني، ومستوى الـ ICT في آرائهنّ وتصوّراتهنّ إزاء مستوى وعيهنّ هذا. وقد اعتمدت الدراسة منهج البحث الوصفيّ باعتباره المنهجيّة البحثيَّة العلميَّة المنوط بها إتمام مقاصد الدراسة البحثيّة الاستقصائيَّة، واستعانت بأداة الاستبانة لجمع البيانات، وَتكوَّنت الاستبانة – بعد التأكُّد من صدقها وثباتها – من ٤٧ عبارة، أمّا بالنسبة لعيّنتها الطبقيّة فتكوّنت من ٤٦٤ معلّمةً قبل الخدمة، جرى اختيارهنّ بالطريقة العشوائيّة البسيطة، وبصورة آليّة / إلكترونيّة خلال الفصلين الدراسيّين الأول والثاني من العام الأكاديميّ ٢٠٢٢/٢٠٢٣م. وقد كشفت نتائج الدراسة أنّ مستوى وعي معلّمات قبل الخدمة في كلية التربية بجامعة الكويت تجاه الأمن السيبراني جاء عمومًا بدرجة "مرتفعة جدًّا" (م = 4.26، ن.م = 0.50، RII = 0.85)؛ إذْ بيّنت النتائج أنّ مستوى وعيهنَّ كان على درجة "مرتفعة جدًّا" في الغالبيّة العظمى من عبارات المقياس (٣٩ عبارة)، بينما حصلت بقية فقرات المقياس (٨ فقرات) على درجة "مرتفعة"، وأشارت النتائج كذلك إلى عدم وجود فروق ذات دلالة إحصائيَّة عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات استجابات معلّمات قبل الخدمة بشأن آرائهنّ وتصوّراتهنّ (اتّجاهاتهنّ) فيما يتعلّق بمستوى وعيهنّ بالأمن السيبراني تُعزى لمتغيّري نوع التخصُّص (أدبي، علمي)، ومستوى الـ ICT (مبتدئة، ملمّة/متوسّطة، محترفة/متقدّمة)، وذلك في الأداة عامّةً. أمّا بالنسبة لمتغيّر دورات الأمن السيبراني (التحقت، لم تلتحق)، فقد بيّنت النتائج وجود اختلافات دالة إحصائيًّا بين متوسّطات استجابات المشاركات، وذلك في الأداة عامّةً، لصالح معلّمات قبل الخدمة اللّاتي التحقنَ بدورات مسبقة في مجال الأمن السيبراني. وخلُصت الدراسة إلى بعض التوصيات أبرزها: (١) ضرورة توفير التدريب والتوعية المستمرّة للمعلّمين والمعلّمات بشأن الأمن السيبراني وتهديداته وأخطاره؛ (٢) توفير دليل إرشاديّ تربويّ تفاعليّ رقميّ عن الأمن السيبراني؛ (٣) إدراج مبحث الأمن السيبراني بموضوعاته المختلفة ضمن المناهج التربويّة في المدارس والجامعات؛ و(٤) تعزيز التنسيق والتعاون والشراكة بين المؤسّسات التربويّة والهيئات والمنظمات المختصّة بالأمن السيبراني لتعزيز وزيادة الوعي في مجال الأمن السيبراني.

الكلمات المفتاحيّة: الأمن السيبراني، مستوى/ درجة الوعي، معلّمات قبل الخدمة، طلبة كلية التربية بجامعة الكويت، التعليم العالي، دولة الكويت.

Pre-service Female Teachers' Cybersecurity Awareness Level in the College of Education at Kuwait University

Abstract

The study aimed to measure the cybersecurity awareness level of pre-service female teachers in the College of Education at Kuwait University. Additionally, it sought to explore the impact of some independent variables such as specialization, cybersecurity training courses, and ICT proficiency on their perceptions and awareness level. The study employed a descriptive methodology as its scientific research approach, which was suitable for achieving its research objectives. Data were collected using an online questionnaire, consisting of 47 items after it was validated and tested for reliability, distributed electronically to a purposive stratified sample of 464 pre-service female teachers during the first and second semesters of 2022/2023 academic year. The study revealed that the awareness level of pre-service female teachers at the College of Education, Kuwait University, regarding cybersecurity was generally categorized as "very high" (M = 4.26, SD = 0.50, RII = 0.85). The results indicated that their awareness level was "very high" for the majority of the scale items (39 statements), while the remaining scale items (8 statements) also achieved a "high" level. Furthermore, the findings showed no statistically significant differences at the significance level ($\alpha \leq 0.05$) among the means of the pre-service female teachers' responses attributed to the variables of specialization (literary, scientific), and ICT proficiency (beginner, intermediate/competent, advanced/proficient), within the entire instrument/scale. As for the variable of participation in cybersecurity courses (attended, did not attend), the results demonstrated statistically significant differences in the means responses of participants in favor of pre-service female teachers who had attended prior cybersecurity courses. The study concluded with some recommendations, including: (1) The necessity of providing continuous training and awareness for teachers about cybersecurity, its threats, and dangers; (2) Providing an interactive digital educational cybersecurity guide; (3) Incorporating cybersecurity topics into various educational curricula in schools and universities; and (4) Enhancing coordination, collaboration, and partnerships between educational institutions and cybersecurity authorities and organizations to promote and increase awareness in the field of cybersecurity.

Keywords: Cybersecurity, Awareness Level/Degree, Pre-service Teachers, Students of the College of Education at Kuwait University, Higher Education, State of Kuwait.

المُقدِّمة

في عصر الابتكار التكنولوجيّ السريع والتواصل الرقميّ واسع النطاق، أصبح الأمن السيبراني أحد أبرز التحدّيات التي نواجهها، فمع تزايد استخدام التكنولوجيا الرقميَّة في جميع جوانب حياتنا أصبحت الأجهزة والشبكات والأنظمة الإلكترونيَّة والبرامج هدفًا للهجمات السيبرانيَّة المتطوّرة والمُتنامية، وتهدف هذه الهجمات إلى الوصول غير المشروع إلى المعلومات أو البيانات الحسّاسة وتعطيل الأجهزة والشبكات والأنظمة والبرامج، والتسبّب بخسائر كبيرة للأفراد والمنظّمات والحكومات (International Telecommunication Union [ITU], 2022). ويتعدّد نطاق الهجمات السيبرانيَّة وتنوُّعها، حيث تشمل الاختراقات الإلكترونية، والبرمجيّات الخبيثة، والتصيّد الاحتياليّ، والهجمات الرامية لتعطيل الخدمات المهمّة، وسرقة البيانات الحسّاسة. وليس الهدف الوحيد من هذه الهجمات سرقة المعلومات أو التسبّب في الضرر، بل يهدف بعضها أيضًا إلى ترويع الأفراد والمجتمعات وتخويفهم وتعطيل العمليّات الحيويَّة، وتمزيق الوحدة الوطنيَّة. ويُعدُّ الأمن السيبراني عنصرًا أساسيًّا في البنية التحتيّة الرقميَّة والتكنولوجيَّة للدول والمؤسّسات والمجتمعات، فمن دون أمن سيبراني قوي ومتين يتعرّض كلُّ جانب من جوانب الحياة الحديثة للخطر، سواء أكان ذلك في مجال الاقتصاد والصناعة أم القطاع الحكومي أم الخدمات الحيويّة مثل الرعاية الصحيّة، والتعليم، والإسكان، والنقل، والطاقة. ولذلك أصبحت الحكومات والمؤسّسات والأفراد يولون اهتمامًا كبيرًا للحفاظ على الأمان السيبراني وتعزيزه (العقلاء وعلي، ٢٠٢٢؛ المنتشري وحريري، ٢٠٢٠) (OpenAI, 2023).

تتسبّب التهديدات السيبرانية بخسائر كبيرة بالنسبة للأفراد والشركات والحكومات على المستوى العالمي، فمن خلال سرقة البيانات الحسّاسة يُمكن للمجرمين السيبرانيّين الوصول إلى المعلومات الشخصيَّة والماليَّة للأفراد واستغلالها في أنشطة احتياليَّة، وفي القطاع الاقتصادي يُمكن للهجمات السيبرانية أنْ تُسبّب خسائر ماليَّة هائلة للشركات وتُهدّد استقرارها وسمعتها، وفي المستوى الحكومي تهدّد الهجمات السيبرانية الأمن القوميّ والمعلومات الإستراتيجيَّة وتتسبّب في تعطيل الخدمات الحكوميّة الحيويَّة. ويتعدّى تأثير الأمن السيبراني حدود الدولة الواحدة، حيث تتسرّب التهديدات السيبرانية بسرعة عبر الحدود الإلكترونية، ولذلك أصبح التعاون الدوليّ في مجال الأمن السيبراني ضرورة مُلحّة، حيث يجب على الدول

تبادل المعلومات والخبرات والتعاون في مجال مكافحة الجرائم السيبرانية وتطوير القوانين والمعايير الدوليّة، وينبغي أنْ تتعاون الحكومات مع القطاع الخاص والمؤسّسات الأكاديميَّة والمنظمات الدوليَّة لتعزيز قدرات الأمن السيبراني وتعزيز التعاون المشترك (الشهري، ٢٠٢١؛ الظويفري، ٢٠٢١) (OpenAI, 2023).

ولتعزيز الأمن السيبراني يجب أنْ تتبنّى الدول سياسات وإطارات تنظيميَّة قويَّة تُعزِّز الحماية والاستجابة والاستعادة، كما يجب أنْ تضمن السياسات والتشريعات القويّة معايير الأمان السيبراني وتلتزم بتطوير القدرات السيبرانية، وتُشجّع الشركات والمؤسّسات على اعتماد مُمارسات الأمان الأفضل، ويجب أنْ تُشجّع الدول على إجراء تقييمات دوريّة للثغرات الأمنيّة وتعزيز التدابير الوقائيَّة وتعزيز الوعي الأمني لدى الموظفين والجمهور، وبالإضافة إلى السياسات والتشريعات يجب على الدول تعزيز القدرات التقنيّة في مجال الأمن السيبراني، إذ يتعيّن تطوير التقنيات والأدوات الأمنية المتطوّرة للكشف المُبكّر عن التهديدات والاستجابة السريعة والاستعادة من الهجمات، وينبغي أنْ تُركّز الجهود على تطوير تقنيات التحليل الاستباقي والاستخبارات الاصطناعيَّة وتقنيات التعرُّف على السلوك غير العادي والتشفير القوي والحوسبة السحابيَّة الآمنة (European Union Agency for Cybersecurity [ENISA], 2021; ITU, 2022; OpenAI, 2023).

ومن الجوانب الهامّة للأمن السيبراني: تعزيز الوعي الأمنيّ لدى الموظفين والجمهور، فيجب توفير التدريب والتثقيف المستمر للأفراد بشأن التهديدات السيبرانية وكيفيّة الوقاية منها، كما ينبغي أنْ يتعلّم الأفراد كيفيَّة التعرّف على رسائل البريد الإلكترونيّ المشبوهة والروابط الخبيثة، وكيفيّة استخدام كلمات مرور قويّة وتحديث البرامج بانتظام، وينبغي أنْ تُقدّم الحكومات والمؤسّسات الدروس والمحاضرات والدورات وَوُرش العمل التدريبيَّة وحملات التوعية لتعزيز الوعي الأمنيّ وتعزيز الثقافة السيبرانية الصحيَّة (Organization for Security and Co-operation in Europe [OSCE], 2023).

ولا بدَّ من أنْ يشمل التعاون الدوليّ في مجال الأمن السيبراني تبادُل المعلومات والتجارب والخبرات بين الدول، وأنْ تُعزّز المنظمات الدولية التعاون وتوفّر المنصّات للتواصل والتعاون في مجال الأمن السيبراني، كذلك يجب أنْ تتعاون الدول معًا لتطوير قوانين دوليّة لمكافحة الجرائم السيبرانية وتوحيد المعايير وتوجيهات الأمان السيبراني.

يُعدُّ الأمن السيبراني تحدّيًا شاملًا وعالميًّا يتطلّب التعاون والتنسيق والجهود المشتركة، فعلينا أنْ نعترف بأهمّية الأمن السيبراني ونضعه على رأس أولويّاتنا، ولا بدّ من أنْ تتبنّى الدول إستراتيجيات وسياسات شاملة للأمن السيبراني، وتُعزّز القدرات التقنية والتعاون الدولي، فمن خلال تعزيز الوعي الأمني وتنفيذ التدابير الوقائيّة والاستجابة الفعّالة يُمكننا بناء بيئة رقميّة آمنة وموثوقة للأجيال الحاليّة والمستقبليّة

مشكلة الدراسة

أظهرت نتائج العديد من الدراسات البحثيّة العلميّة الأكاديميّة التربويّة في مجال الأمن السيبراني والتعليم أنّ هناك نقصًا في مستوى وعي المعلّمين بالأمن السيبراني؛ فقد أبدى العديد من المعلّمين قلّة معرفتهم بالتهديدات السيبرانية الحاليّة وأساليب الاحتيال الإلكتروني المُستخدمة، كما أشارت هذه الدراسات البحثية بأنّ هناك نقصًا في القدرات والمعارف والمهارات والكفايات والخبرات الأساسيَّة المطلوبة للتعامل مع الأمان السيبراني، مثل إدارة كلمات المرور والتعرُّف على البريد الإلكتروني المشبوه والروابط الخبيثة، واستنتجت الدراسات السابقة أيضًا أنّ الوعي بالأمن السيبراني يحظى باهتمامٍ أكبر في بيئات التعليم والتعلّم الرقميّ (الإلكترونيّ الشبكيّ المتنقّل) – سواءٌ التقليدي (الوجاهيّ) أم عن بُعد (الافتراضي) – حيث تُستخدم التكنولوجيا على نطاق واسع (الشهري، ٢٠٢١؛ العقلاء وعلي، ٢٠٢٢؛ المنتشري وحريري، ٢٠٢٠) (Jazeel, 2018).

وبناءً عليه، فإنّ فهم مستوى وعي المعلّمين بالأمن السيبراني، ومعرفة مدى استعدادهم للتعامل مع التهديدات السيبرانية في بيئة التعليم والتعلّم الرقميّ أصبح أحد التحدّيات الهامّة في عصرنا الحالي؛ حيث يُعدُّ تحسين وعي المعلّمين بالأمن السيبراني أمرًا حاسمًا لضمان سلامة المتعلّمين والبيانات في بيئة التعليم والتعلّم الرقمي. ومنْ المهم أنْ تتخذ المؤسّسات التعليميّة والجهات المعنيّة إجراءات فعّالة لتوفير التدريب والدعم المُستمر للمعلّمين لتعزيز قدراتهم ومعارفهم ومهاراتهم وكفاياتهم وخبراتهم في مجال الأمن السيبراني والحدّ من التهديدات السيبرانية المُحتملة (United Nations Educational, Scientific and Cultural Organization [UNESCO], 2022).

إنَّ البحث في مجال الوعي بالأمن السيبراني يُسهم في تطوير المعرفة وتعزيز المُمارسات الأمنية، حيث يسعى الباحثون والخبراء إلى تحديد التهديدات الأمنيّة المختلفة

وفهمها، وتطوير الحلول الفعّالة لمواجهتها، والتدابير الوقائية لردعها. وهنا ظهرت الحاجة الماسّة إلى إجراء هذه الدراسة، وبناءً عليه قام الباحث بإعداد الدراسة الحاليّة بقصد فهم مستوى وعي طالبات كلية التربية بجامعة الكويت – معلّمات قبل الخدمة – بالأمن السيبراني، ومعرفة مدى استعدادهنّ للتعامل مع التهديدات السيبرانية في بيئة التعليم والتعلّم الرقمي من وجهة نظرهنّ بوصفهنَّ مُكوّنًا من المُكوّنات الأساسيّة الفاعلة والفعّالة العاملة في الميدان التربوي، وبقصد خدمة أغراض البحث العلميّ والتطوير المهنيّ في هذا المجال الحيويّ.

أسئلة الدراسة

حاولت هذه الدراسة البحثيّة الإجابة عن الأسئلة الآتية:

١. ما مستوى وعي معلّمات قبل الخدمة في كلية التربية بجامعة الكويت بالأمن السيبراني؟
٢. هل توجد فروق ذات دلالة إحصائيَّة عند مستوى الدلالة ($\alpha \leq 0.05$) في آراء معلّمات قبل الخدمة في كلية التربية بجامعة الكويت وتصوّراتهنّ تجاه مستوى وعيهنّ بالأمن السيبراني يُمكنْ عزوها لمتغيّرات نوع التخصّص، ودورات الأمن السيبراني، ومستوى المعرفة/الخبرة أو المهارات في استخدام وسائل وأدوات وخدمات تكنولوجيا المعلومات والاتّصالات (ICT)؟

أهداف الدراسة

أرادت الدراسة الراهنة تحقيق الأهداف التالية:

١. بيان مدى وعي معلّمات قبل الخدمة في كلية التربية بجامعة الكويت بالأمن السيبراني، وقياس قدراتهنّ ومعارفهنّ ومهاراتهنّ وكفاياتهنّ وخبراتهنّ واستعدادهنّ لمواجهة التهديدات والهجمات والاختراقات السيبرانية في بيئة التعليم والتعلّم الرقمي.
٢. الكشف عن أثر متغيّرات نوع التخصّص، ودورات الأمن السيبراني، ومستوى الـ ICT على اتّجاهات معلّمات قبل الخدمة في كلية التربية بجامعة الكويت وآرائهنّ نحو درجة وعيهنّ بالأمن السيبراني.

حدود الدراسة

صُنّفت حدود هذه الدراسة البحثيّة إلى الآتي:

١. حدود الموضوع: تمثّلت في قياس مستوى وعي أعضاء الهيئة التعليميَّة بالأمن السيبراني.
٢. الحدود البشريَّة: تمثّلت في وجهة نظر طالبات كلية التربية – معلّمات قبل الخدمة – بجامعة الكويت.
٣. الحدود المكانيّة: اقتصرت على كلية التربية بجامعة الكويت.
٤. الحدود الزمانيّة: طُبّقت في الفصلين الدراسيّين الأول والثاني من العام الأكاديمي ٢٠٢٢/٢٠٢٣م.

مصطلحات الدراسة

١. الأمن السيبراني (Cybersecurity): يُشير إلى مجموعة الإجراءات والتدابير التي تتّخذها الشركات والحكومات والمؤسّسات والأفراد لحماية الأنظمة الحاسوبيّة والشبكات والبرامج والبيانات من التهديدات السيبرانية والهجمات الإلكترونيّة. ويهدف الأمن السيبراني إلى ضمان سلامة البيانات والمعلومات الحسّاسة وسريّتها، وحمايتها من الوصول غير المشروع أو تغييرها أو تدميرها، وحماية الأنظمة والشبكات والبرامج من الاختراق والتلف، وضمان استمراريّة الخدمات الرقميَّة وعمليّات الأعمال العاديّة الحيويّة (Cisco, 2023; ENISA, 2021; ITU, 2022).
٢. الوعي بالأمن السيبراني (Awareness of Cybersecurity): الوعي هو إدراك الإنسان المباشر لذاته ومحيطه، ويُعدُّ ركيزةً أساسيَّةً لكلّ معرفة. إلى جانب ذلك، يُعبّر الوعي عن الفهم وسلامة الإدراك، ويشمل هذا الإدراك تفهُّمَ الإنسان لنفسه وللبيئة المحيطة به، ويعني ذلك فهم الإنسان لذاته وللآخرين خلال تفاعله معهم، وهذا يأتي في إطار سعيه لتلبية احتياجاته وتحقيق مصالحه، وتفهُّمه للعلاقات بينه وبين الآخرين والبيئة في مختلف السياقات. ويُعرّف الوعي بالأمن السيبراني بأنّه الاستدراك الفعّال للأخطار المتعلّقة بجرائم الإنترنت واختراقات البيانات والحسابات الشخصيّة. ويهدف ذلك إلى تحقيق الأمان الرقميّ من خلال اتّخاذ جميع الإجراءات والتدابير الوقائيَّة الضروريَّة للوقاية من اختراق الأنظمة والبيانات والشبكات، وضمان بيئة عمل وتعليم وتعلُّم آمنة

للأفراد. ويُمكن قياس مدى وعي المعنيّين بهذا المجال من خلال الدرجة التي يحصلون عليها في المقاييس المُعترف بها والمُعدّة لذلك (ابن إبراهيم، ٢٠٢١).

الدراسات السابقة

(١) دراسة Jazeel (٢٠١٨): كانت غايتها قياس مستوى وعي معلّمي ومعلّمات قبل الخدمة في كلية المعلّمين الحكوميَّة بمدينة Addalaichenai في سريلانكا بالأمن السيبراني، وقد اعتمدت الدراسة منهج البحث الوصفيّ، واستخدمت الاستبانة أداةً لجمع البيانات، وتَكوَّن مقياس الوعي بالأمن السيبراني في صيغته النهائية – بعد التأكّد من صدقه وثباته – من ١٥ فقرة، أمّا بالنسبة لعيّنة الدراسة الطبقيَّة العشوائيَّة فتكوّنت من ٢٠٠ معلّمًا ومعلّمةً قبل الخدمة، وقد طُبّقت عليهم الدراسة في الفصل الأول من العام الأكاديمي ٢٠١٨/٢٠١٧م. وأظهرت نتائج الدراسة أنّ مستوى وعي معلّمي ومعلّمات قبل الخدمة بالأمن السيبراني بوجهٍ عام جاء بدرجة "منخفضة"؛ إذْ بيّنت النتائج التفصيلية أنّ ٦٠% من المشاركين كانت درجة الوعي لديهم "منخفضة"، وأنّ ٢٩% منهم جاءت درجة وعيهم "متوسّطة"، في حين حصل ١١% منهم على درجة وعي "عالية". كما أشارت النتائج أيضًا إلى وجود فروق ذات دلالة إحصائيَّة بين استجابات أفراد عيّنة الدراسة تُعزى للمتغيّرات التالية: الجنس/النوع لصالح الذكور، والمنطقة الجغرافيَّة لصالح المناطق الحضرية، ومستوى المعرفة بالحاسوب لصالح من ليس لديه أيّ معرفة، ومُلكيّة جهاز الحاسوب لصالح من ليس لديه أيُّ جهاز.

(٢) دراسة المنتشري وحريري (٢٠٢٠): استهدفت معرفة درجة الوعي بالأمن السيبراني لدى معلّمات المرحلة المتوسّطة في مدارس التعليم العام بمدينة جدة في المملكة العربية السعودية، واعتمدت الدراسة منهج البحث الوصفيّ، واستخدمت الاستبانة أداةً لجمع البيانات، وتكوَّنت في صورتها النهائية – بعد التأكّد من صدقها وثباتها – من ٢١ عبارة موزّعة على ثلاثة مجالات حول الأمن السيبراني هي: المفاهيم، المخاطر، والانتهاكات. أمّا بالنسبة لعيّنة الدراسة الطبقيَّة العشوائيَّة فتألّفت من ٣٦٢ معلّمةً، وقد طُبّقت عليهنَّ الدراسة في الفصل الأول من العام الدراسي ٢٠٢٠/٢٠١٩م. وأشارت نتائج الدراسة إلى أنّ مستوى وعي المعلّمات بالأمن السيبراني بوجهٍ عام جاء بدرجة "متوسّطة"؛ إذْ بيّنت النتائج أنّهنَّ كنَّ على درجة "متوسّطة" من الوعي في محاور الدراسة الثلاثة كلٍّ على حدة، كما أظهرت النتائج

عدم وجود فروق دالة إحصائيًا بين استجابات المعلّمات تُعزى لمتغيّري المؤهّل العلميّ وسنوات الخبرة، في حين وُجدتْ هذه الاختلافات ذات الدلالة الإحصائية بينهنَّ بالنسبة لمتغيّر الدورات التدريبية في الأمن السيبراني لصالح من حصلنَ على دورات في الأمن السيبراني.

(٣) دراسة الصانع وآخرون (٢٠٢٠): هدفت إلى قياس مستوى وعي المعلّمين والمعلّمات في المرحلتين الابتدائية والمتوسّطة في مدارس مدينة الطائف (الحكوميَّة والأهليَّة) بالمملكة العربية السعودية حول الأمن السيبراني، واعتمدت الدراسة منهج البحث الوصفيّ، واستخدمت الاستبانة أداةً لجمع البيانات، وتكوَّن المقياس في صيغته النهائية – بعد التأكّد من صدقه وثباته – من ٢١ عبارة، أمّا بالنسبة لعيّنة الدراسة الطبقيَّة العشوائيَّة فتكوَّنت من ١٠٤ معلّمًا ومعلّمةً، وقد طُبّقت عليهم الدراسة في الفصل الدراسي الثاني من العام الدراسي ٢٠١٩/٢٠٢٠م. وأظهرت نتائج الدراسة أنّ مستوى وعي المعلّمين والمعلّمات بالأمن السيبراني بوجهٍ عام جاء بدرجة "عالية"؛ إذْ بيّنت النتائج التفصيليّة أنّهم يتمتّعون بوعيٍ "عالٍ جدًّا" في مجال حماية بياناتهم وأجهزتهم من أخطار الاختراق الإلكترونيّ والهجمات السيبرانية وذلك في ١١ فقرة من المقياس، بينما انخفضت درجة الوعي لديهم إلى تقدير "عالٍ" في الفقرات العشر الأخرى، كما تبيَّنَ أنّهم يستخدمون أساليب وطرق تدريس وأنشطة ومشروعات فعّالة تُعزّز الوعي بأمن الإنترنت لدى الطلبة لحمايتهم من مخاطرها، وتُنمّي القيم والهُويَّة الوطنيَّة لديهم. وقد توصّلت الدراسة أيضًا إلى وجود علاقة ارتباطيَّة إيجابيَّة متوسّطة بين وعي أعضاء الهيئة التعليميَّة بالأمن السيبراني واستخدامهم لأساليب وإستراتيجيَّات لحماية طلابهم من أخطار الإنترنت وتعزيز القيم والهُويَّة الوطنيَّة لديهم، ولم يتبيَّنْ من نتائج التحليلات الإحصائيَّة وجود فروق ذات دلالة إحصائيَّة بين استجابات المشاركين تُعزى للمتغيّرات التالية: نوع المدرسة، والجنس/النوع، والتخصُّص، والمؤهّل العلميّ، وسنوات الخبرة المهنيَّة.

(٤) دراسة سراج الدين وآخرون (٢٠٢١): سعت إلى قياس مستوى وعي معلّمي ومعلّمات المدارس الخاصة بإمارة عجمان في الإمارات العربية المتحدة بالأمن السيبراني لحماية الطلبة، واعتمدت الدراسة منهج البحث الوصفيّ، واستخدمت الاستبانة أداةً لجمع البيانات، وتكوّنت في صورتها النهائية – بعد التأكّد من صدقها وثباتها – من ٢١ فقرةً حول الأمن السيبراني، أمّا بالنسبة لعيّنة الدراسة الطبقيَّة العشوائيَّة فتكوَّنت من ١٤٥ معلّمًا

ومعلّمةً، وقد طُبّقت عليهنَّ الدراسة في الفصل الثاني من العام الدراسي ٢٠١٩/٢٠٢٠م. وكشفت نتائج الدراسة أنّ مستوى وعي المعلّمين والمعلّمات بالأمن السيبراني بوجهٍ عام جاء بدرجة "مرتفعة"؛ إذْ بيّنت النتائج التفصيليَّة أنّ المشاركين كانوا على درجة "مرتفعة" من الوعي في ١٣ عبارة من المقياس، بينما انخفض مستوى الوعي لديهم في ثماني فقرات. كما أشارت النتائج إلى عدم وجود فروق دالة إحصائيًّا بين استجابات المشاركين تُعزى لمتغيّرات النوع، والعمر، والخبرة، في حين وُجدتْ هذه الاختلافات ذات الدلالة الإحصائيَّة بينهم بالنسبة لمتغيّر التخصُّص.

(٥) دراسة الشهري (٢٠٢١): كانت غايتها قياس مستوى وعي طلبة كلية التربية في جامعة الإمام محمد بن سعود الإسلاميَّة في المملكة العربية السعودية بالأمن السيبراني، إضافةً إلى التعرّف على دور إدارة الجامعة في تعزيز الوعي بالأمن السيبراني لديهم، وقد انتهجت الدراسة منهج البحث الوصفيّ، واستعملت الاستبانة أداةً لجمع البيانات، وتضمّنت في صورتها النهائية – بعد التأكّد من صدقها وثباتها – على ٣٢ فقرة موزّعة على مجالين، أمّا بالنسبة لعيّنة الدراسة الطبقيَّة العشوائيَّة فتألّفت من ١٨٨ مشاركًا، وقد طُبّقت عليهم الدراسة في الفصل الدراسي الأول من العام الأكاديمي ٢٠٢٠/٢٠٢١م. وأظهرت نتائج الدراسة أنّ مستوى وعي طلبة كلية التربية ومعرفتهم بالأمن السيبراني جاء بوجهٍ عام بدرجة "متوسّطة"، وأنّ ممارسة إدارة الجامعة لدورها في نشر الوعي بالأمن السيبراني وتعزيزه لدى هؤلاء الطلبة جاءت بوجهٍ عام بدرجة "متوسّطة" أيضًا، كما أشارت النتائج إلى عدم وجود فروق ذات دلالة إحصائيَّة بين متوسّطات استجابات أفراد عيّنة الدراسة تُعزى لمتغيّر الجنس/النوع، بينما وُجدتْ هذه الفروق ذات الدلالة الإحصائيَّة بين متوسّطات تقديرات المشاركين حول الوعي بالأمن السيبراني بالنسبة لمتغيّر المؤهّل العلمي لصالح حملة شهادات الدراسات العُليا.

(٦) دراسة الظويفري (٢٠٢١): استهدفت قياس واقع الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنوَّرة في المملكة العربية السعودية وتحدّيات تفعيله وإستراتيجيّات زيادة فاعليّته من وجهة نظر القيادة المدرسية (القادة والقائدات والمعلّمين والمعلّمات)، واعتمدت الدراسة منهج البحث الوصفيّ، واستخدمت الاستبانة أداةً لجمع البيانات، وتكوَّنت في شكلها النهائي – بعد التأكّد من صدقها وثباتها – من ٤٦ عبارة موزّعة

على ثلاثة مجالات، أمّا بالنسبة لعيّنة الدراسة الطبقيَّة العشوائيَّة فتألّفت من ٤١٨ مشاركًا، وقد طُبّقت عليهم الدراسة في الفصل الدراسي الثاني من العام الدراسي ٢٠٢٠/٢٠٢١م. وكشفت نتائج الدراسة أنّ واقع الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنوَّرة جاء بوجهٍ عام بدرجة "عالية"، وأنّ التحدّيات التي تواجه تفعيله في المدارس جاءت بوجهٍ عام بدرجة "عالية" أيضًا. وقد اقترحت الدراسة كذلك عدّة آليّات لزيادة فاعليّة الأمن السيبراني في المدارس منها: (أ) نشر ثقافة الوعي بالأمن السيبراني لدى أعضاء الهيئتين الإداريَّة والتعليميَّة، (ب) تعزيز وعي الطلبة بالأمن السيبراني وأخطاره، (ج) توفير دليل تربويّ تفاعليّ عن أخلاقيّات الأمن السيبراني. كما أشارت النتائج أيضًا إلى عدم وجود فروق ذات دلالة إحصائيَّة بين متوسّطات استجابات أفراد العيّنة تُعزى للمتغيّرات التالية: الجنس/النوع، والوظيفة، والمؤهّل العلمي، وعدد سنوات الخبرة، وعدد الدورات التدريبيَّة في مجال تكنولوجيا المعلومات والاتّصالات.

(٧) دراسة العقلاء وعلي (٢٠٢٢): ابتغت قياس درجة الوعي بالأمن السيبراني لدي معلّمي ومعلّمات الحاسب الآلي في المرحلتين المتوسّطة والثانوية بمدينة حائل في المملكة العربية السعودية، واعتمدت الدراسة منهج البحث الوصفيّ، وتبنّت الاستبانة أداةً رئيسة لجمع البيانات، وتكوَّنت في صيغتها النهائية – بعد التأكّد من صدقها وثباتها – من ٢٨ عبارة موزّعة على مجالين حول الأمن السيبراني هما: ماهيَّة الأمن السيبراني، وطرق المحافظة على نظام الأمن السيبراني. أمّا بالنسبة لعيّنة الدراسة الطبقيَّة العشوائيَّة فتألّفت من ١٨٤ معلّمًا ومعلّمةً، وقد طُبّقت عليهم الدراسة في الفصل الثاني من العام الدراسي ٢٠٢٠/٢٠٢١م. وأظهرت نتائج الدراسة أنّ مستوى وعي المعلّمين والمعلّمات بالأمن السيبراني بوجهٍ عام جاء بدرجة "متوسّطة"؛ إذْ بيّنت النتائج التفصيلية أنّ المشاركين كانوا على درجة "متوسّطة" من الوعي في محوريْ الدراسة كلٍّ على حدة، كما أشارت النتائج إلى عدم وجود فروق ذات دلالة إحصائيَّة بين استجابات المعلّمين والمعلّمات تُعزى لمتغيّري المؤهّل العلميّ وسنوات الخبرة، في حين وُجدتْ هذه الاختلافات ذات الدلالة الإحصائيَّة بين المشاركين بالنسبة لمتغيّر الجنس لصالح المعلّمات، وكذلك بالنسبة لمتغيّر الدورات التدريبيَّة في الأمن السيبراني لصالح من لم يتلقّوا أيَّ دورة تدريبيَّة، وأيضًا بالنسبة لمتغيّر المرحلة التعليميَّة لصالح المرحلة المتوسّطة.

(٨) دراسة زقوت وآخرون (٢٠٢٢): استهدفت معرفة مستوى وعي أعضاء هيئة التدريس بجامعة الزاوية في ليبيا في ظلِّ التحوّل الرقميّ الذي صاحب جائحة كورونا، واعتمدت الدراسة منهج البحث الوصفيّ، واستخدمت الاستبانة أداةً أساسيّة لجمع البيانات، واشتمل مقياس الوعي بالأمن السيبراني في شكله النهائي – بعد التأكّد من صدقه وثباته – على ٣١ فقرة موزّعة على محورين، أمّا بالنسبة لعيّنة الدراسة الطبقيَّة العشوائيَّة فتألّفت من ٧٨ عضوَ هيئةِ تدريس، وقد طُبّقت عليهم الدراسة في العام الدراسي ٢٠٢٢/٢٠٢١م. وكشفت نتائج الدراسة أنّ مستوى وعي أعضاء هيئة التدريس بالأمن السيبراني بوجهٍ عام جاء بدرجة "كبيرة"؛ إذْ بيّنت النتائج التفصيليَّة أنّ المشاركين كانوا على درجة "متوسّطة إلى كبيرة" من الوعي في عبارات المقياس كلٍّ على حدة.

التعقيب على الدراسات السابقة:

تطابقت الدراسة الحالية مع الدراسات السابقة في موضوعها البحثي، إذْ تناولتْ قياس أو تقييم مستوى وعي المعلّمين والمعلّمات – قبل الخدمة وأثناء الخدمة – في المؤسّسات التربوية التعليمية بالأمن السيبراني. هذا وبالإضافة إلى وجود تطابق بين الدراسة الحالية وجموع الدراسات السابقة في المنهجية العلمية البحثية المستخدمة – منهج البحث الوصفيّ؛ وكذلك في أداة الدراسة المُعتمدة – الاستبانة – بقصد استطلاع رأي المشاركين وجمع البيانات المرتبطة بموضوع البحث. وعلاوةً على التوافق في العيّنة الطبقيَّة التي تمّ اختيارها بطريقة عشوائيَّة بسيطة – معلّمي ومعلّمات قبل الخدمة وأعضاء الهيئة التعليمية في المدارس. إنّ هذه الدراسة البحثية تُضاف إلى جموع البحوث السابقة في هذا المجال، وتُساهم في توسيع المعرفة حيال هذا المبحث الحيوي في هذا العصر المعرفي الرقمي.

وتفرّدت الدراسة الحالية عن سابقاتها بأنّها طُبّقت بعد مرور فترة زمنية كافية على جائحة كورونا التي تسبّبت في إحداث نقلة نوعية في النظام التربوي، واقتضت دمج وتوظيف وسائل وأدوات وتطبيقات ومنصّات وشبكات وخدمات تكنولوجيا المعلومات والاتّصالات في التعليم والتعلّم للوصول إلى التحوّل الرقميّ. إضافةً إلى أنّها تميّزت بكونها دراسة طولية (Longitudinal Study)؛ إذْ تمّ جمع بياناتها بكل حرص ودقّة على مدى فصلين دراسيّين متتاليّين (الأول، والثاني) من العام الأكاديمي ٢٠٢٣/٢٠٢٢م؛ وفي الدراسة الطولية، يقوم الباحث بفحص وتقصّي أفراد العيّنة أنفسهم بشكل مُتكرّر بُغية اكتشاف أي تغيّرات قد تحدث

خلال حقبة من الزمن. وكذلك تميّزت الدراسة الحالية عن الدراسات المُماثلة السابقة بأنّ أداتها المستخدمة لجمع البيانات – الاستبانة – كانت أكثر عُمقًا وشموليّةً؛ إذْ احتوتْ في صيغتها النهائية على ٤٧ فقرة أو عبارة مرتبطةً ارتباطًا وثيقًا بموضوع البحث.

أدبيَّات الدراسة

مفهوم الأمن السيبراني

الأمن السيبراني هو مجالٌ يتعامل مع حماية أنظمة المعلومات والشبكات والبيانات من التهديدات الإلكترونيَّة والهجمات السيبرانية. ويشمل الأمن السيبراني الإجراءات والتقنيّات والمُمارسات التي تهدف إلى تأمين البيئة الرقميَّة والحفاظ على سرّيَّة البيانات وسلامتها وحمايتها من الوصول غير المُصرّح به والتلاعُب أو التلف أو الاختراق. وتشمل التهديدات السيبرانية المشتركة الهجمات الإلكترونيَّة مثل: الفيروسات، وبرامج التجسّس، والبرمجيّات الخبيثة، وهجمات القرصنة والاختراق، والهجمات المُنسّقة، والهجمات الموجّهة، والاحتيال الإلكترونيّ، والتصيّد الاحتياليّ (Phishing). وبالإضافة إلى ذلك يشمل الأمن السيبراني أيضًا مجالات أخرى مثل حماية البيانات الشخصيَّة والتحقّق من الهُويَّة والحفاظ على الخصوصيَّة وتأمين التجارة الإلكترونيَّة وحماية الأنظمة الحيويَّة المُتّصلة بالإنترنت مثل البنية التحتيَّة للطاقة والماء والنقل والصحّة والتعليم وغيرها (الحبيب، ٢٠٢٢؛ الشهري، ٢٠٢١؛ الصانع وآخرون، ٢٠٢٠؛ الصحفي وعسكول، ٢٠١٩؛ الظويفري، ٢٠٢١؛ زقوت وآخرون، ٢٠٢٢؛ صائغ، ٢٠١٨) (Cisco, 2023; OpenAI, 2023).

ولتحقيق الأمن السيبراني، تُتّخذُ مجموعة مُتنوَّعة من الإجراءات التقنيّة والتنظيميَّة والتعليميَّة، بما في ذلك تطوير سياسات وإجراءات الأمان، وتنفيذ تقنيات التشفير والمصادقة والتحقّق، وإدارة الوصول والتحكّم بالحسابات، ورصد الأنشطة غير المشروعة والاستجابة للحوادث، وتوعية المستخدمين وتدريبهم على المُمارسات الأمنيَّة الجيّدة. ويُعدُّ الأمن السيبراني مهمًّا ـ لا سيّما ـ في عصرنا الرقميّ، حيث أصبحت البيانات الحسّاسة والمعلومات الشخصيَّة والأنظمة المُتّصلة عُرضةً للهجمات المستمرّة، ويُعدُّ تأمين الأنظمة السيبرانية ضرورة حتميَّة للشركات والحكومات والمؤسّسات والأفراد لحماية مصالحهم والحفاظ على الثقة والاستقرار في العالَم الرقميّ (الزبيدي وآخرون، ٢٠٢١؛ الظويفري، ٢٠٢١؛ المنتشري وحريري، ٢٠٢٠) (UNESCO, 2022; OpenAI, 2023).

أهميّة الأمن السيبراني

للأمن السيبراني أهميَّة حاسمة في عصرنا الرقميّ المُتّصل، ويُمكن تحديد جوانب أهميّته في النقاط التالية (الصحفي وعسكول، ٢٠١٩؛ المنتشري وحريري، ٢٠٢٠؛ حمدان، ٢٠٢١؛ زقوت وآخرون، ٢٠٢٢) (OpenAI, 2023):

(١) حماية البيانات الحسّاسة: يُساعد الأمن السيبراني في حماية البيانات الحسّاسة مثل المعلومات الشخصيَّة والماليَّة والتجاريَّة، إذ تُعد هذه البيانات هدفًا مُغريًا للقراصنة والمجرمين السيبرانيّين الذين يسعون لاستغلالها في أنشطة غير قانونية، مثل الاحتيال الماليّ وسرقة الهُويَّة. وتأمين هذه البيانات يحمي الأفراد والشركات والمؤسّسات من التبعات السلبيّة المُحتملة.

(٢) الحفاظ على الأنظمة والبُنية التحتيّة: تتطوّر التهديدات السيبرانية بشكل مستمرّ، وتستهدف الأنظمة الحاسوبيَّة والشبكات والبُنية التحتيَّة المهمّة مثل البُنية التحتيّة للطاقة والنقل والماء والتعليم والصحّة، وإذا تعرّضت هذه الأنظمة للهجمات أو التلف فإنّ ذلك يُمكن أنْ يتسبّب في تعطّل الخدمات الحيويّة وتنجم عنه تأثيرات اقتصاديّة واجتماعيّة خطيرة. والأمن السيبراني يعمل على حماية هذه الأنظمة وضمان استمراريّة العمليّات والخدمات الحيويّة.

(٣) حماية الثقة والسُمعة: تعتمد الثقة والسُمعة على الثقة في النظم السيبرانية، سواء أكان ذلك في العمل أم التجارة أم الحكومة، وفي حال اختراق النظام أو حدوث انتهاك سيبراني فإنّ ذلك يتسبّب بفقدان الثقة والتشكيك في الأنظمة والخدمات. والأمن السيبراني يحمي سُمعة الشركات والحكومات والمؤسّسات ويُعزّز الثقة في النظم السيبرانية.

(٤) الحماية من الهجمات المُستهدفة: يستهدف القراصنة والمجرمون السيبرانيّون بعض الأهداف المحدّدة، مثل الشركات الكبرى أو المؤسّسات الحكوميّة، وتُعرف هذه الهجمات بأنّها هجمات مُستهدفة تهدف إلى سرقة البيانات الحسّاسة أو التلاعُب بالأنظمة أو إلحاق الضرر. والأمن السيبراني يُساعد في كشف هذه الهجمات ومنعها وتقليل التأثير السلبيّ الناجم عنها.

(٥) تأمين الاقتصاد الرقميّ: يعتمد الاقتصاد العالميّ بصورةٍ متزايدة على العمليات الرقميّة والتجارة الإلكترونيّة، والأمن السيبراني يُسهم في حماية الاقتصاد الرقميّ وتأمين

المعاملات الماليّة والتجاريّة عبر الإنترنت، فهو يحمي البنوك والشركات والمتاجر الإلكترونيّة والعملاء من الاحتيال وسرقة المعلومات الماليّة.

بوجهٍ عام، يُعدُّ الأمن السيبراني ضرورةً حتميَّة لضمان استمراريَّة العمليات والحفاظ على الثقة والأمان في العالم الرقميّ، إذ يُساعد في الحماية من التهديدات السيبرانيّة والاحتفاظ بالبيانات الحسّاسة وضمان سلامة الأنظمة والخدمات والعمليات الحيويّة.

أهداف الأمن السيبراني

أهداف الأمن السيبراني تتعلّق بحماية الأنظمة والشبكات الإلكترونيَّة والبيانات الحسّاسة من التهديدات السيبرانية، ويُعدُّ الأمن السيبراني أمرًا حيويًّا في عصرنا الحالي، حيث يتزايد التبادل الإلكترونيّ للبيانات والاعتماد على الشبكات والتقنيات الرقميَّة في العديد من جوانب الحياة اليوميّة والأعمال التجاريّة، وتتمثّل الأهداف الرئيسة للأمن السيبراني في حماية الأنظمة الرقميّة وضمان سلامة البيانات والحفاظ على استقرار العمليّات الحاسوبيّة. وفيما يلي نُقدّم نظرة شاملة على أهمّ أهداف الأمن السيبراني (العقلاء وعلي، ٢٠٢٢؛ المنتشري وحريري، ٢٠٢٠؛ زقوت وآخرون، ٢٠٢٢؛ صائغ، ٢٠١٨) (ENISA, 2021; International Organization for Standardization [ISO], 2022, 2023; National Institute of Standards and Technology [NIST], 2020; OpenAI, 2023; OSCE, 2023):

(١) حماية البيانات والمعلومات: من أهمّ أهداف الأمن السيبراني حماية البيانات والمعلومات الحسّاسة من الوصول غير المصرّح به والاستخدام غير القانونيّ، وتُعدُّ البيانات الحسّاسة مثل المعلومات الشخصيّة والماليّة والسرّيّة التجاريّة والمعلومات الحكوميَّة مُهدَّدة من قبل القراصنة والهاكرز والمجرمين الإلكترونيّين، ويجب تطبيق تدابير الأمان المناسبة مثل التشفير والوصول المحدود وتطبيق السياسات الأمنيّة للحفاظ على سرّيّة البيانات وسلامتها.

(٢) ضمان سلامة الأنظمة والشبكات: تشمل أهداف الأمن السيبراني ضمان سلامة الأنظمة والشبكات الإلكترونيَّة من الهجمات والاختراقات الإلكترونيّة، وتُعدُّ استمراريّة الأعمال وعدم توقّف الخدمات الرقميَّة أمرًا حاسمًا في عصر الاعتماد الكبير على التقنية الرقميّة، فلا بدَّ من اتّخاذ إجراءات مثل الجدران النارية، وأنظمة الكشف عن التسلّل، وتحديثات البرامج الأمنيّة لضمان استقرار الأنظمة وحمايتها من الهجمات.

(٣) حماية البُنية التحتيَّة الحيويَّة: تستهدف إستراتيجيّات الأمن السيبراني حماية البُنية التحتيّة الحيويَّة مثل محطات الطاقة، والشبكات الكهربائيَّة، والمرافق الحيويَّة الأخرى، حيث يُمكن أنْ تكون لهجمات القرصنة المُوجّهة للبُنية التحتيّة الحيويَّة عواقبُ كارثيَّة، فقد تؤدّي إلى انقطاع التيار الكهربائيّ، أو تعطيل الخدمات الحيويَّة الأخرى، لذا يجب تطبيق الحماية السيبرانية المُتقدّمة على هذه البُنى التحتيَّة لمنع أيّ هجمات مُحتملة أو منع استدامتها.

(٤) التصدّي للتهديدات النشطة: تسعى جهود الأمن السيبراني إلى التصدّي للتهديدات النشطة مثل هجمات القرصنة والبرمجيّات الخبيثة، والاحتيال الإلكتروني، ويُمثّل القراصنة والمجرمون الإلكترونيّون والدولُ المعادية والمنافسون تهديداتٍ مُحتملة للأنظمة السيبرانية، لذا يجب توفير أنظمة الكشف المُبكّر والاستجابة السريعة وتحديثات الأمان المستمرة للحدّ من هذه التهديدات وتقليل الأضرار المُحتملة.

(٥) تعزيز الوعي والتثقيف السيبراني: تهدف جهود الأمن السيبراني أيضًا إلى تعزيز الوعي والتثقيف السيبراني لدى المستخدمين وتعزيز قدراتهم ومعارفهم ومهاراتهم وكفاياتهم في التعامل مع التهديدات السيبرانية، وتُعدُّ التوعية بمفاهيم الأمن السيبراني ومُمارساته الجيّدة مهمّةً للغاية في الحدِّ من المخاطر والهجمات، لذا يجب توفير التدريب والتثقيف المستمرّ للمستخدمين للتعرُّف على التهديدات الحديثة وكيفيّة التعامل معها بصورةٍ آمنة.

باختصار، يهدف الأمن السيبراني إلى حماية الأنظمة الرقميَّة والبيانات الحسّاسة وضمان سلامة العمليّات الحاسوبيَّة، ومن خلال تحقيق هذه الأهداف يُمكن للحكومات والمؤسّسات والأفراد الاستمرار في الاعتماد على التقنية الرقميَّة بثقة وتجنُّب الأضرار المُحتملة الناجمة عن التهديدات السيبرانية.

مخاطر الأمن السيبراني

المخاطر السيبرانية هي تهديدات تواجهنا في عصر التكنولوجيا الحديثة؛ حيث يعتمد المجتمع الرقميّ على نظم المعلومات والاتّصالات اعتمادًا كبيرًا. وتشمل الأخطار السيبرانية الأنشطة الضارّة التي يقوم بها المهاجمون الإلكترونيّون بهدف الوصول غير المصرّح به إلى البيانات والمعلومات أو التلاعُب بها أو تعطيل الأنظمة الإلكترونيَّة. وفيما يلي نستعرض بعض أهمّ المخاطر السيبرانية (الحبيب، ٢٠٢٢؛ الصحفي وعسكول، ٢٠١٩؛ المنتشري وحريري، ٢٠٢٠؛ زقوت وآخرون، ٢٠٢٢؛ صائغ، ٢٠١٨) (OpenAI, 2023):

(١) هجمات الاختراق (Hacking): يشمل الاختراق الهجوميّ اختراق الأنظمة الإلكترونيَّة والتطبيقات بغرض الوصول غير المصرّح به إلى البيانات والمعلومات الحسّاسة أو التلاعُب بها، ويستغل المهاجمون الثغرات الأمنية في البرامج والأنظمة للدخول إلى النظام بطرق غير قانونيَّة، ويُمكن أنْ تُؤدّي هذه الهجمات إلى تسريب البيانات والمعلومات الشخصيَّة أو السرقة التجاريَّة أو تعطيل الأنظمة.

(٢) البرمجيّات الخبيثة والفيروسات (Malware): تشمل البرمجيّات الخبيثة والفيروسات جميع أنواع البرامج التي تهدف إلى إلحاق الضرر بالأنظمة الإلكترونيّة والبيانات، حيث يجري تطوير هذه البرامج لأغراض مختلفة مثل التجسّس، وتعطيل النظام، وتحقيق مكاسب غير قانونيَّة، ويُمكن أنْ تنتشر البرمجيّات الخبيثة عبر البريد الإلكترونيّ المشبوه أو الروابط الضارّة أو الأجهزة القابلة للتوصيل بالشبكة.

(٣) الاحتيال الإلكترونيّ (Phishing): يشمل الاحتيال الإلكترونيّ العديدَ من الأنشطة غير القانونيَّة التي تستهدف الأفراد والشركات، والتي يقوم بها المهاجمون بهدف الحصول على مكاسب غير قانونيّة، ويتضمّن ذلك احتيال الهُويّة، والتصيُّد الاحتيالي (Phishing)، والتلاعُب بالمدفوعات الإلكترونيَّة، ويعتمد الاحتيال الإلكترونيّ على تقنيات التلاعُب الاجتماعيّ لخداع الأفراد والشركات وإقناعهم بتقديم بيانات ومعلومات حسّاسة مثل بيانات الحسابات المصرفيّة.

(٤) هجمات الحرمان من الخدمة (Distributed Denial–of–Service – DDoS): تُعدُّ هجمات الحرمان من الخدمة أو هجوم حجب الخدمة تهديدًا شائعًا، حيث يقوم المهاجمون بتعطيل موقع أو خدمة عن طريق تحميل الخوادم بكميّات كبيرة من الطلبات، ممّا

يجعلها غير قادرة على التعامل مع الحمولة الزائدة وبالتالي تعطيلها عن المستخدمين الشرعيّين. ويَستخدِمُ المهاجمون شبكات الحاسوب المُكوّنة من الأجهزة المُخترَقة لتوجيه هجمات الحرمان من الخدمة.

(٥) التجسّس السيبراني (Cyber Espionage): يُشير التجسّس السيبراني أو الإلكترونيّ إلى اختراق الهدف واستخراج البيانات والمعلومات السرّيّة أو الحسّاسة من الأنظمة الحاسوبيَّة المُتاحة عبر الشبكة وذلك باستخدام برمجيّات التجسّس (Spyware) المختلفة، ويسعى المهاجمون للوصول إلى البيانات والمعلومات التجاريَّة أو البحثيَّة أو العسكريّة من أجل الاستفادة الشخصيَّة منها أو بيعها لطرفٍ ثالث، إذ يُمكن استخدام هذه البيانات والمعلومات في السرقة التجاريَّة أو الابتزاز أو لأغراض أخرى غير قانونيَّة، ويُعدُّ التجسّس السيبراني تهديدًا خطيرًا للأمن الوطنيّ والتجاريّ.

(٦) انتهاك الخصوصيّة (Privacy Violation): يشمل انتهاك الخصوصيّة الوصول غير المصرّح به إلى البيانات والمعلومات الشخصيّة للأفراد، ويُمكن أنْ يتسبّب انتهاك الخصوصيّة في سرقة الهُويّة، والابتزاز، والتنمّر الإلكترونيّ.

باختصار، تُمثّل الأخطار السيبرانية تحدّيًا كبيرًا في عالم مُتّصل رقميًّا، ويجب على الأفراد والمنظمات والشركات والمؤسّسات والحكومات اتّخاذ التدابير اللازمة لحماية أنفسهم وأنظمتهم من هذه الأخطار، ومن بين هذه التدابير تعزيز الوعي السيبراني للأفراد، وتحديث البرامج والأنظمة بانتظام، واستخدام برامج مُضادة للفيروسات والبرامج الخبيثة، وتنفيذ التشفير القوي للبيانات والمعلومات الحسّاسة والسرّيّة، وتوفير نظام جدران حماية النار، وإجراء نسخ احتياطيَّة مُنتظمة للبيانات، ومن المهمّ أيضًا التعاون وتبادل البيانات والمعلومات والخبرات بين الجهات المعنيّة، بما في ذلك القطاعين العام والخاص والمجتمع الدولي، للكشف عن التهديدات الجديدة وتطوير إستراتيجيّات وأدوات فعّالة لمكافحة الأخطار أو الجرائم السيبرانية.

في النهاية، يجب أنْ نُدرك أنّ التكنولوجيا الحديثة لها جوانب إيجابيّة كبيرة، وتُحقّق تقدّمًا هائلًا في حياتنا وأعمالنا، ولكنّها تواجه تحدّياتٍ سيبرانية، ومن خلال تبنّي إجراءات الأمان السيبراني الملائمة، يُمكننا الاستمتاع بالفوائد الكاملة للتكنولوجيا مع الحفاظ على سلامتنا وأماننا الرقميّ.

أهميّة توعية المعلّمين بالأمن السيبراني

توعية المعلّمين بالأمن السيبراني يُعد أمرًا ضروريًّا ومهمًّا في عصرنا الحالي، حيث أصبحت التكنولوجيا جزءًا حيويًّا من التعليم والتعلّم، وتُعدُّ التوعية بالأمن السيبراني للمعلّمين أمرًا أساسيًّا للحفاظ على سلامة البيانات والمعلومات والحماية من التهديدات السيبرانية. وفيما يلي نستعرض دواعي الاهتمام بتوعية المعلّمين بالأمن السيبراني (السواط وآخرون، ٢٠٢٠؛ الصحفي وعسكول، ٢٠١٩؛ المنتشري وحريري، ٢٠٢٠) (OpenAI, 2023):

(١) حماية البيانات والمعلومات الشخصيَّة للمتعلّمين: تُعدُّ حماية البيانات والمعلومات الشخصيّة للمتعلّمين أمرًا حيويًّا في بيئة التعليم والتعلم الرقمية، ذلك أنّ وجود البيانات والمعلومات الشخصيّة للمتعلّمين: مثل الأسماء والعناوين وتفاصيل الحسابات يستدعي أنْ يكون المعلّمون على دراية بأفضل المُمارسات لحماية هذه البيانات والمعلومات والتعامُل معها بصورةٍ آمنة.

(٢) تعزيز الوعي السيبراني للمتعلّمين: يُمكن للمعلّمين أنْ يكونوا القدوة والمثل الحسن للمتعلّمين فيما يتعلق بالسلوك السيبراني الآمن، وذلك عن طريق توعية المعلّمين بالأمن السيبراني وتعريفهم بالتهديدات السيبرانية وأفضل المُمارسات، ويُمكنهم تمرير هذه المعرفة إلى المتعلّمين وتعزيز الوعي السيبراني لديهم.

(٣) الحفاظ على سلامة الشبكة المدرسيَّة: تعتمد العديد من المدارس على شبكات الحواسيب والإنترنت لتوفير التعليم والتعلّم والموارد التعليميَّة والتعلُّميّة الرقميّة، فيجب على المعلّمين أنْ يكونوا على دراية بأفضل المُمارسات لتأمين الشبكة المدرسيَّة وحمايتها من الهجمات السيبرانية، وذلك من أجل ضمان استمراريَّة عمليّة التعليم والتعلُّم وحماية البيانات والمعلومات المهمّة.

(٤) التصدّي للتحرُّش السيبراني والتنمُّر: يُعدُّ التحرُّش السيبراني والتنمّر عبر الإنترنت من المشكلات الشائعة في البيئة المدرسية الرقميَّة، ويُمكن للمعلّمين القيام بدور فعّال في التوعية بأضرار التحرُّش السيبراني والتنمّر، وتعليم المتعلّمين كيفيّة التصدّي لهذه التحدّيات والإبلاغ عنها.

(٥) حماية الأنظمة والتطبيقات التعليميَّة والتعلّميّة: تعتمد العديد من المدارس على التطبيقات التعليميَّة والتعلّميّة والأنظمة الإلكترونيَّة لتقديم المحتوى التعليميّ والتعلّمي وتنظيم

العمليّة التعليميّة والتعلّمية، فينبغي أنْ يكون المعلّمون على دراية بأمن هذه الأنظمة والتطبيقات، وأن يعملوا على توعية المتعلّمين بأهميّة استخدامها على نحوٍ آمن، والابتعاد عن المُمارسات الضارة.

(٦) التصدّي للتهديدات السيبرانية: تُعدُّ التوعية بالأمن السيبراني للمعلّمين ركيزةً أساسيَّةً في عمليّة التصدّي للتهديدات السيبرانية، فبمعرفة المعلّمين بالتهديدات الحالية وأساليب الهجمات السيبرانية يُمكنهم اتّخاذ الإجراءات الوقائيّة المناسبة والاستجابة السريعة في حالة وجود هجوم سيبراني.

(٧) المُساهمة في بناء جيل آمن سيبرانيًّا: تُعد توعية المعلّمين بالأمن السيبراني جزءًا من بناء جيل قادر على التعامل مع التحدّيات السيبرانية وحماية أنفسهم ومجتمعهم الرقمي، وذلك عن طريق تعليم المعلّمين وتوجيههم لتعليم المتعلّمين حول الأمن السيبراني، ليسهموا في بناء ثقافة أمن سيبراني تواكب التطوُّر التكنولوجيّ.

باختصار، تُعدُّ توعية المعلّمين بالأمن السيبراني أمرًا ضروريًّا للحفاظ على سلامة المتعلّمين والبيانات والمعلومات والأنظمة التعليميَّة والتعلّميّة، ويُمكن للمعلّمين القيام بدور فعّال في تعزيز الوعي السيبراني لدى المتعلّمين والتصدّي للتهديدات السيبرانية من خلال تعليمهم أفضل المُمارسات وتوفير بيئة تعليميّة وتعلّمية آمنة ومحميَّة.

زيادة فاعليّة الأمن السيبراني في المؤسّسات التعليميَّة

زيادة فاعليّة الأمن السيبراني في المؤسّسات التربويَّة (التعليميَّة والتعلّميَّة) أصبحت أمرًا حيويًّا في العصر الرقمي الحديث، حيث تعتمد هذه المؤسّسات على التكنولوجيا والشبكات لتقديم التعليم والتعلُّم وتسهيل العمليّة التعليميّة والتعلّميّة، حيث تواجه المؤسّسات التعليمية العديد من التحدّيات والتهديدات السيبرانية، مثل اختراقات الهجمات الإلكترونيَّة، والبرمجيّات الخبيثة، والتلاعُب بالبيانات والمعلومات، ولذلك يجب أنْ يكون الأمان السيبراني على رأس أولويّاتها.

وفيما يلي بعض الخطوات والإجراءات التي يُمكن للمؤسّسات التعليميّة اتّخاذها لزيادة فاعليّة الأمن السيبراني (الصانع وآخرون، ٢٠٢٠؛ العقلاء وعلي، ٢٠٢٢؛ المنتشري وحريري، ٢٠٢٠) (OpenAI, 2023):

(١) التوعية والتدريب: يجب على المؤسّسات التعليميَّة توفير التوعية والتدريب المناسبيْن للموظفين والمعلّمين والمتعلّمين حول أهمّيّة الأمان السيبراني والأخطار المُحتملة، وذلك من خلال تنظيم دورات وورش عمل تدريبية، ومحاضرات وجلسات توعويّة لتعزيز وعي الجميع بأفضل المُمارسات الأمنية والوقاية من الهجمات الإلكترونيّة.

(٢) تحديث البرمجيّات والأجهزة: لا بدَّ من تحديث البرمجيّات والأجهزة المستخدَمة في المؤسّسة بشكل مُنتظم، وتطبيق التحديثات الأمنية اللازمة للحفاظ على ثغرات الأمان.

(٣) تطوير سياسات وإجراءات الأمان: يجب أنْ تكون هناك سياسات وإجراءات واضحة للأمان السيبراني تُحدّد السلوكيّات المقبولة وغير المقبولة، وتُحدّد الإجراءات الواجب اتّباعها في حالة حدوث اختراقٍ أمنيّ.

(٤) الحماية من البرمجيّات الخبيثة: يجب استخدام برامج مكافحة الفيروسات والحماية من البرمجيّات الخبيثة للحماية من التهديدات الإلكترونيَّة.

(٥) التحقُّق الثنائي: ينبغي تفعيل التحقُّق الثنائي للحسابات الهامّة للمؤسّسة، ممّا يضمن طبقة إضافية من الأمان، ويحول دون اختراق الحسابات بسهولة.

(٦) حماية البيانات: يجب حماية البيانات والمعلومات السرّيَّة والحسّاسة والشخصيَّة للمتعلّمين والمعلّمين والموظفين عبر تشفير البيانات وتطبيق سياسات الوصول الصارمة.

(٧) إدارة التهديدات: يجب تنفيذ أدوات وأنظمة لمراقبة التهديدات السيبرانية المُحتملة وكشفها والاستجابة لها استجابةً سريعة وفعّالة.

(٨) الاحتياطات الفنّية/التقنيّة: يجب تنفيذ نُسَخ احتياطيّة للبيانات بصورةٍ مُنتظمة وتخزينها بطريقةٍ آمنة، لضمان استعادة البيانات في حال وقوع هجمات أو فقدان البيانات.

(٩) التقييم الدوريّ والاختبارات الأمنيّة: يجب إجراء تقييم دوريّ للأمان السيبراني وإجراء اختبارات أمنية للتحقُّق من فاعليّة التدابير والإجراءات المُتّخذة، والبحث عن نقاط الضعف وتحسينها.

(١٠) التعاون مع مؤسّسات أمن البيانات والمعلومات: ينبغي للمؤسّسات التعليميَّة التعاون مع مؤسّسات أمن البيانات والمعلومات المُتخصّصة والاستفادة من خبراتها وتجاربها لتعزيز أمان المؤسّسة،

باعتبارها حاملة لبيانات ومعلومات حسّاسة وسرّيّة وهامّة، فإنّ زيادة فاعليّة الأمن السيبراني في المؤسّسات التربويّة التعليميّة يُسهم في حماية البيانات والمعلومات وضمان استمراريَّة عمليّة التعليم والتعلّم بطرق آمنة ومأمونة.

دولة الكويت والأمن السيبراني

حفاظًا على الأمن المجتمعيّ في دولة الكويت في هذا العصر الرقميّ، وحمايةً لحرّيّات الأشخاص وشرفهم وسمعتهم، ودرءًا للعدوان على الأموال والمُمتلكات والأصول المعلوماتيَّة العامّة والخاصة، سواءً التقليديّة منها أم الرقميَّة، وسعيًا منها في سياق دعم التوجّهات العالميَّة الخاصة بمكافحة الجرائم السيبرانية، والتزامًا منها بأحكام الاتفاقيّات الخاصة بمكافحة الجرائم السيبرانية التي صادقت عليها في المؤسّسات الدوليَّة والإقليميّة والمحليّة؛ فقد بذلت دولة الكويت جهودًا مكثّفة خلال العقد الماضي في التصدّي لهذه الجرائم السيبرانية، لإرساء الأمن السيبراني في المجتمع الكويتيّ وتعزيزه (صفر، ٢٠١٧)، ومنها الآتي:

(١) أنشأتْ في العام ٢٠١٤م "الهيئة العامة للاتّصالات وتقنية المعلومات"، ومسؤوليّتها الإشراف على قطاع الاتّصالات ورقابته، وحماية مصالح المستخدمين ومزوّدي الخدمات، وتنظيم خدمات جميع شبكات الاتّصالات في الدولة بكفاءة عالية بما يُحقّق الأداء الأمثل للقطاع.

(٢) قامتْ في تاريخ ٧ يوليو، ٢٠١٥م، بِسَن "قانون مكافحة جرائم تقنية المعلومات"، وعُمل به ابتداءً من تاريخ ١٢ يناير، ٢٠١٦م.

(٣) أطلقتْ في يناير عام ٢٠١٨م "الإستراتيجيَّة الوطنيَّة للأمن السيبراني" – نتاج عمل مكثّف بين الهيئة والقطاعين العامّ والخاص على مدى عامين – تلك الإستراتيجيّة التي تلعب دورًا مهمًّا وحيويًّا في تطوير قدراتنا وتكثيف جهودنا في سبيل تعزيز الأمن السيبراني وتخطّي العقبات والتغلّب على التحدّيات بكلِّ أشكالها لدولة الكويت، والتي جاءت نتيجة استشعار الحكومة الكويتية وإدراكها لخطورة التحدّيات والنوازل والتهديدات والمخاطر السيبرانية التي تواجهها الدولة. وتهدف هذه الخطة الإستراتيجيّة لوضع تصوّرٍ للأمن السيبراني الوطني للسنوات الآتية، إذْ تعمل على تحديد الأُسس والقواعد والإجراءات الضروريّة الواجب اتّخاذها واتّباعها، وتوظيف الإمكانات الكاملة للعلم وتكنولوجيا المعلومات والاتّصالات

الحديثة، وتدريب الموارد البشرية وتأهيلها وتنميتها، وتجويد القدرة على التعامل مع القضايا الأخلاقيَّة والقانونيَّة في مجال الأمن السيبراني، كما تسعى أيضًا إلى جمع المعلومات والبيانات من قبل المؤسّسات ووضع اللوائح لكلّ جهة بهدف حماية منظومتها الأمنيَّة (وكالة الأنباء الكويتية، ٢٠١٨).

(٤) أصدرتْ في تاريخ ٥ فبراير، ٢٠٢٢م، مرسومًا أميريًّا يقضي بإنشاء "المركز الوطنيّ للأمن السيبراني"، وهو جهازٌ حكوميٌّ يسعى جاهدًا إلى تحقيق الإدارة الاستباقيّة الفعّالة لتهديدات وأخطار الفضاء السيبراني، إذْ يجري العمل من خلاله على تطوير وسائل الدفاعات الاستباقية المناسبة وتعزيزها، والمراقبة المستمرة لإعداد آليّة الاستجابة الملائمة للقطاعات والمؤسّسات الحيويّة، وكذلك آليّة الإبلاغ عن هجمات واختراقات القرصنة والجرائم السيبرانية، فضلًا عن نشر التوعية الوطنيَّة وبناء كوادر بشريّة وطنيّة قادرة على التعامل مع قضايا الأمن السيبراني، هذا بالإضافة إلى تأمين مؤسّسات الدولة في إطار أمنيّ شامل ومتكامل من السياسات واللوائح والاجراءات والمعايير والضوابط الفنيّة. ويختص المركز بوضع الإستراتيجيّة الوطنيّة لقطاع الأمن السيبراني والإشراف عليه، ويعمل على تأمين وحماية الشبكات المعلوماتيّة وشبكة الاتّصالات وأنظمة المعلومات وقواعد البيانات، وكذلك يشرف على عمليّات جمع المعلومات والبيانات وتبادلها باستخدام أيّ وسيلة إلكترونيّة. ويشمل نطاق عمل المركز الجهات الحكوميَّة والمدنيَّة والعسكريَّة والأمنيَّة، بالإضافة إلى مؤسّسات القطاع الخاص داخل دولة الكويت التي تتعلّق باختصاصات المركز، وأيضًا الجهات الأخرى التي يجري تحديدها من قبل رئيس المركز (قاسم، ٢٠٢٢).

منهج الدراسة وإجراءاتها

منهج الدراسة

اعتمدتْ هذه الدراسة على منهج البحث الوصفيّ باعتباره المنهجيَّة البحثيَّة المنوط بها إتمام أهدافها البحثيّة الاستقصائيَّة لقياس مستوى وعي معلّمات قبل الخدمة في كلية التربية بجامعة الكويت بالأمن السيبراني، هذا بالإضافة إلى تحديد أثر بعض المتغيّرات المستقلة على اتّجاهات المشاركاتِ وآرائهنّ نحو درجة وعيهنّ بالأمن السيبراني. ويُعدُّ هذا المنهج البحثيّ من أكثر طرق، ومناهج، وأساليب البحث العلميّ مناسَبةً ومطابَقةً لطبيعة هذا النوع من الدراسات البحثيّة العلميَّة من وجهة نظر عدد كبير من الباحثين؛ إذْ إنّه يُعنى

بوصف المشكلات أو الظواهر المجتمعيّة كما هي على أرض الواقع من خلال المسح الشامل لفئة معيّنة من أفراد المجتمع، ويستعين به الباحثون بكثرة في الفترة الأخيرة (أبو علام، ٢٠١٨؛ العسّاف، ٢٠١٠) (Creswell & Creswell, 2018; Fraenkel et al., 2019; Johnson & Christensen, 2020).

مجتمع الدراسة وعيّنتها

تكوَّنَ مجتمع الدراسة من جميع طلبة كلية التربية بجامعة الكويت المُقيّدين في الفصل الدراسي الأول والثاني من العام الأكاديمي ٢٠٢٢/٢٠٢٣م، والبالغ عددهم حسب إحصائيّات جامعة الكويت للعام الأكاديمي ٢٠٢١/٢٠٢٢م حوالي ٧,٨٧٥ طالبًا وطالبةً (٩٧٣ من الذكور و٦,٩٠٢ من الإناث) (الإدارة المركزية للإحصاء، ٢٠٢٢، ص. ٦٨–٦٩). أمّا عيّنة الدراسة فتكوّنت من ٤٦٤ مشاركِةً أو معلّمةً قبل الخدمة (أي بنسبة تُقدّر بنحو 5.9% من مجتمع الدراسة)، جرى اختيارهنّ بالطريقة الطبقيَّة العشوائيَّة وبصورةٍ آليّةٍ إلكترونيّةٍ، وعُوّل عليها في معالجة البيانات وتحليل النتائج.

أداة الدراسة

بعد الاطّلاع على الأدبيّات والدراسات البحثية السابقة المُرتبطة بموضوع البحث أُعدّت أداة الدراسة البحثيّة الاستقصائيّة الأساسيّة (الاستبانة)، وقد احتوتْ على قسمين رئيسين: (١) البيانات الديموغرافيّة، (٢) مقياس الوعي بالأمن السيبراني، واشتمل الجزء الأول على ستة أسئلة تُزوّدنا ببيانات عامة تضمّ معلومات تكشف عن طبيعة أفراد العيّنة المشاركة، أمّا القسم الثاني فقد تضمّن مقياس الوعي بالأمن السيبراني، واحتوى على ٤٧ عبارة أو فقرة تقيس وتُقيّم مستوى وعي معلّمات قبل الخدمة في كلية التربية بجامعة الكويت نحو الأمن السيبراني، ويُقابل الأسئلة خمس استجابات تُحدّد درجة الموافقة (الوعي) الخاصة بها وذلك وفقًا لمقياس ليكرت (Likert) الخماسيّ، وهي على النحو التالي: معارض بشدّة = ١، معارض = ٢، محايد = ٣، موافق = ٤، وموافق بشدّة = ٥.

صدق الأداة.

للتحقُّق من صدق أداة الدراسة (إلى أيّ مدى تبدو مناسبة لقياس ما يُراد قياسه) عمد الباحث إلى عرضها على مجموعة من المُحكّمين من ذوي الخبرة والاختصاص بُغيةَ الاستفادة من خبراتهم، وآرائهم، ومقترحاتهم، وتوصياتهم، وراعى الباحث جميع الملاحظات

الواردة منهم، ومن ثَمّ جرى اعتماد أداة الدراسة (الاستبانة) وتصميمها وإخراجها بصورتها النهائيَّة.

ثبات الأداة.

للتحقّق من ثبات أداة الدراسة (إلى أيّ مدى تُعطي النتائج ذاتها، أو قراءات قريبة منها قدْرَ الإمكان في كل مرّة تُستخدَم فيها الأداة) عمد الباحث إلى تجربتها على عيّنة استطلاعيَّة عددها ٤٠ مشاركًا، ومن ثَمّ جرى حساب مُعامِل ثبات الأداة عن طريق قياس مُعامِل الاتّساق الداخليّ، أو مُعامِل الثبات الكُلّي كرونباخ ألفا (Cronbach's alpha) لجميع عبارات مقياس الوعي (الاستبانة) الخاص بالدراسة، وقد بلغت قيمة درجة الثبات 0.951 وهي قيمة مرتفعة جدًّا، ما يدل على أنّ الأداة على درجة كبيرة جدًّا من الاتّساق الداخليّ بين عباراتها، ممّا يجعلها مقبولة لأغراض الدراسة والبحث العلميّ، وتُعطي الثقة التامة في استخدام الأداة. والجدير بالذكر أنّ بيانات العيّنة الاستطلاعيّة أُستبعدَت من المعالجة الإحصائيَّة والتحليل، ولم تكنْ ضمن عيّنة الدراسة الفعليّة.

تطبيق الأداة.

وُزّعَتْ الاستبانة خلال الفصلين الدراسيّين الأول والثاني من العام الأكاديمي ٢٠٢٢/٢٠٢٣م بطريقةٍ آليّةٍ إلكترونيةٍ (بالاستعانة بوسائط تكنولوجيا المعلومات والاتّصالات المختلفة) على العيّنة الطبقيَّة العشوائيَّة المختارة من معلّمات قبل الخدمة في كلية التربية بجامعة الكويت، وجرى التأكيد للمشارِكات في الدراسة أنَّ مشاركتهنّ اختياريَّة، وأنّ جميع البيانات أو الاستجابات الواردة تُعدُّ سرّيَّة، ولنْ تُستخدَم إلّا لخدمة أغراض البحث العلميّ والتطوير.

المعالجة الإحصائيَّة

بعد تطبيق الدراسة وإتمام عمليّة جمع البيانات، فُرِّغت البيانات الكميّة إلى جهاز الحاسوب في برنامج جداول البيانات مايكروسوفت إكسل (Microsoft Excel)، ثُمّ أُدخلت بعد ذلك في برنامج الحزمة الإحصائيَّة للعلوم الاجتماعيَّة (IBM SPSS Statistics) – النسخة ٢٨ – لمُعالجتها إحصائيًا، ومن ثمّ استخراج البيانات الإحصائيَّة والتحليلات، والمقارنات اللازمة (نتائج الدراسة). وتحديدًا، تطلّبت هذه الدراسة البحثيّة العلميّة استخدام الأساليب الإحصائيَّة التالية:

١. التحليل الوصفيّ الاستكشافيّ (Descriptive Analysis Exploratory) كمعاملات الاتّساق الداخليّ (معاملات الثبات) كرونباخ ألفا، والتكرارات، والنسب المئويَّة، والمتوسّطات الحسابيَّة، والانحرافات المعياريّة، ومؤشّرات الأهمِّيَّة النسبيّة (Relative Importance Indexes – RII) (الأوزان النسبية) للبيانات، وذلك للأغراض الوصفيّة. وقد أُستخدِم المعيار الإحصائيّ المُوضّح في الجدول ١ لتفسير تقديرات أفراد العيّنة (صفر، ٢٠٢٠) (Akadiri, 2011).

جدول 1

المعيارُ الإحصائيّ لتفسير تقديرات أفراد العيّنة وفقًا لمدى مؤشّرات الأهمِّيَّة النسبيَّة (الأوزان النسبيَّة)

مدى مؤشّرات الأهمِّيَّة النسبيَّة	مدى الأوزان النسبيَّة	درجة الوعي
1.00 – 0.80	100.0 – 80.0	مرتفعة جدًا
0.79 – 0.60	79.0 – 60.0	مرتفعة
0.59 – 0.40	59.0 – 40.0	متوسّطة
0.39 – 0.20	39.0 – 20.0	ضئيلة
0.19 – 0.00	19.0 – 0.0	ضئيلة جدًا

٢. الاختبارات المعلميّة / البارامترية (Parametric Tests) كاختبارات الفروق بين المجموعات، وهي بالتحديد اختبار (ت للعيّنات المستقلّة) (Independent–Samples t–test)، وتحليل التباين الأُحادي (ANOVA). والجدير بالذكر، أنّ هذه الاختبارات الإحصائيّة طُبّقت للأغراض الاستدلاليَّة بُغية الإجابة عن بعض أسئلة الدراسة، وعند تطبيقها تمّ اختيار قيمة ألفا (α) لتكون ٠.٠٥ ($\alpha \leq 0.05$).

نتائج الدراسة ومناقشتها

أوّلًا: وصفٌ عامٌّ للعيِّنة والبيانات الديموغرافيَّة.

يُبَيِّنُ الجدول ٢ توزيعَ أفرادِ عيّنة الدراسة (المشاركين) بحسبِ المتغيّرات الديموغرافيَّةِ (المستقلّة).

جدول ٢
توزيع أفراد عيّنة الدراسة حسب متغيّرات الدراسة المستقلّة

المتغيّر	الصنف	النسبة
نوع التخصّص	التخصّصات الأدبيّة	72.0
	التخصّصات العلميّة	28.0
مستوى الـ ICT	مبتدئة	38.4
	ملمّة/متوسّطة	56.9
	محترفة/متقدّمة	4.7
مؤهّل الـ ICT	حاصلة على شهادة دوليّة	1.3
	ليس لديها أيّ شهادة دوليّة	98.7
دورات الأمن السيبراني	التحقت بدورات في الأمن السيبراني	5.2
	لم تلتحق بأيّ دورات في الأمن السيبراني	94.8

ثانيًا: نتائج أسئلة الدراسة ومناقشتها.

نتائج سؤال الدراسة الأوّل.

نصّ سؤال الدراسة الأول على: ما مستوى وعي معلّمات قبل الخدمة في كلية التربية بجامعة الكويت بالأمن السيبراني؟ للإجابة عن هذا السؤال، أُستخدِم الإحصاءُ الوصفيُّ (Descriptive Statistics). وهذا ما يوضّحه الجدول التالي.

جدول ٣

المتوسّطات الحسابيّة، والانحرافات المعياريّة، ومؤشّرات الأهمّيَّة النسبيَّة، ودرجات الوعي، والرُّتب لعبارات سؤال الدراسة الأول - "مستوى وعي معلّمات قبل الخدمة بالأمن السيبراني"

م	العبارة	المتوسّط الحسابيّ	الانحراف المعياريّ	مؤشّر الأهمّيَّة النسبيَّة	درجة الوعي	الرتبة
1	أتواصلُ مع الجهات الأمنيّة المختصّة عند تعرُّضي لأيّ شكلٍ من أشكال الجرائم السيبرانيَّة.	4.38	0.77	0.88	مرتفعة جدًّا	19
2	أتجنّبُ الاتّصال بالشبكات اللّاسلكيّة (WiFi) العامّة، وأحذَرُ كثيرًا عند الاتّصال بها وقت الضرورة.	3.78	1.16	0.76	مرتفعة	٤٤
3	أحرصُ على استخدام متصفّحٍ آمنٍ عند استخدام شبكة الإنترنت.	4.50	0.86	0.90	مرتفعة جدًّا	9
4	أتجنّبُ استخدامَ التطبيقات الإلكترونيّة، أو تصفُّحَ المواقع الإلكترونية، أو استقبالَ المكالمات الهاتفيّة المجهولة التي تقدّم خدماتٍ مجانيّة للمستخدمين.	4.13	1.08	0.83	مرتفعة جدًّا	٣٦
5	أحتفظ بنسخةٍ أو بنسخٍ احتياطيَّةٍ من ملفّاتي أو بياناتي المخزّنة على أجهزتي بأكثر من وسيلة (مثل: ذاكرة أو وحدة تخزين خارجية، خدمة التخزين السحابية، ...إلخ)، لتفادي السرقة أو التلف.	4.31	0.87	0.86	مرتفعة جدًّا	٢٣
6	أتأكّدُ من مصدر المعلومة المتداولة في مواقع التواصل الاجتماعي قبل نشرها وإرسالها للآخرين.	4.51	0.71	0.90	مرتفعة جدًّا	6
7	أستخدمُ المحتوى المرخّص من قبل الناشرِ أو المؤلّف.	4.31	0.80	0.86	مرتفعة جدًّا	٢٢
8	أحرصُ على إبلاغ الجهات القانونيَّة المختصّة عن التطبيقات، أو المواقع الإلكترونيّة، أو المكالمات الهاتفيّة المشكوك فيها.	3.91	1.02	0.78	مرتفعة	٤٢
9	ألغي اشتراكاتي في التطبيقات، أو المواقع الإلكترونيّة، أو الخدمات الهاتفيّة التي تتضمَّن إعلاناتٍ مستهدفةٍ، لحماية بياناتي الشخصيّة والماليّة.	4.29	0.87	0.86	مرتفعة جدًّا	٢٤

10	أحترمُ آراءَ الآخرين وأفكارَهم ومشاعرَهم عند مناقشة موضوعٍ ما في التخصّص عبر شبكة الإنترنت.	4.51	0.78	0.90	مرتفعة جدًّا	7
11	أتجنّب التواصلَ مع أشخاصٍ مجهولي الهويَّة عبر التطبيقات، والمواقع الإلكترونيّة، والمكالمات الهاتفيَّة.	4.44	0.84	0.89	مرتفعة جدًّا	16
12	أستخدمُ التشفيرَ (بتعيين كلمة مرورٍ) لملفّاتي المهمَّة التي أُرسلُها عبر شبكة الإنترنت.	4.40	0.92	0.88	مرتفعة جدًّا	18
13	أعرف أبرزَ العلامات والمؤشّرات الخطرة التي تدلُّ على أنّ أجهزتي قد تعرَّضَتْ للاختراق.	4.19	0.90	0.84	مرتفعة جدًّا	٣٢
14	أراعي الضوابطَ الاحترازيَّة والإجراءات الوقائيَّة لتحصين أجهزتي من الاختراق.	4.41	0.76	0.88	مرتفعة جدًّا	17
15	استخدم كلمات مرورٍ قويَّةٍ ومعقَّدة (تتكون من حروفٍ وأرقامٍ ورموزٍ) لحساباتي الشخصيَّة، وأتجنّب تكرارها.	4.29	0.96	0.86	مرتفعة جدًّا	٢٥
16	أهتمُّ بتحديثِ كلماتِ المرور الخاصَّة بحساباتي أو تغييرها بين الحين والآخر.	3.69	1.21	0.74	مرتفعة	٤٦
17	أحرصُ على عدم الإفصاح عن كلمات المرور الخاصَّة بحساباتي لأيّ أحد.	4.59	0.73	0.92	مرتفعة جدًّا	3
18	أقرأ النشرات التعريفيَّة التوعويَّة الخاصَّة بمفاهيم الأمن السيبرانيّ وأخلاقيّاته ومخاطره.	3.93	1.04	0.79	مرتفعة	٤١
19	أستخدمُ تقنية التحقّق الثنائيّ (كلمة المرور – البصمة أو غيرها) لتحصينِ أجهزتي من الاختراق.	4.48	0.79	0.90	مرتفعة جدًّا	12
20	أحترمُ القوانينَ والسياساتِ واللوائحَ التي تُشرّعها الدولةُ وتفرضها في التعامل مع شبكة الإنترنت واستخدامها.	4.53	0.68	0.91	مرتفعة جدًّا	4
21	أستخدمُ برمجيّات حمايةٍ خاصَّةٍ لمساعدتي في حماية أجهزتي، وتحصينها، ورفع كفاءة مقاومتها للفيروسات والاختراقات وعمليات التجسّس (الملفّات والمواقع والبرمجيّات الخبيثة أو الضارة) التي من	4.10	0.97	0.82	مرتفعة جدًّا	٣٧

	المُمكنْ أنْ تضرَّ بأجهزتي وبياناتي.					
22	أحدِّثَ برمجيّات الحماية الموجودة على أجهزتي باستمرار.	4.17	0.93	0.83	مرتفعة جدًّا	٣٣
23	أعدِّلُ سياساتِ الخصوصيَّة للأجهزة والتطبيقات من خلال الإعدادات بما يضمن تطبيق مستوى عالٍ من الخصوصيَّة.	4.21	0.90	0.84	مرتفعة جدًّا	٣٠
24	أستخدمُ الروابطَ الرسميَّة التي تنشرُها وزارة التربية في موقعها الإلكترونيّ الرسميّ، وفي حساباتها الرسميّة عبر شبكات التواصل الاجتماعيّ.	4.50	0.74	0.90	مرتفعة جدًّا	8
25	أحترمُ سياساتِ التطبيقاتِ والمواقعِ الإلكترونيّة التي أستخدمُهَا.	4.46	0.71	0.89	مرتفعة جدًّا	14
26	أتجاهلُ العروضَ الإعلانيَّة، والتطبيقاتِ، والمواقعَ الإلكترونيَّةَ، والمكالمات الهاتفية، إذا كانت مجهولة المصدر أو مشبوهة.	4.45	0.78	0.89	مرتفعة جدًّا	15
27	أستخدم أدوات الإبلاغ عن الإساءات التي يتعرَّض لها المستخدمون عبر شبكة الإنترنت.	4.25	0.82	0.85	مرتفعة جدًّا	٢٦
28	أحرصُ على عدم فتح الرسائل الإلكترونيّة (مثل: الرسائل النصيّة أو البريد الإلكترونيّ) أو استقبال المكالمات الهاتفيّة مجهولة المصدر أو المشبوهة.	4.34	0.91	0.87	مرتفعة جدًّا	٢١
29	أحظرُ (Block) الرسائلَ النصيَّة أو البريد الإلكترونيّ أو المكالمات الهاتفية مجهولة المصدر أو المشبوهة، وأبلّغ (Report) عنها.	4.48	0.79	0.90	مرتفعة جدًّا	11
30	أتجنّب فتح أي الروابط والمرفقات التي تتضمنها الرسائل الإلكترونيّة التي تصلني من شخصٍ مجهولٍ أو مصدرٍ غير معروفٍ لديّ.	4.59	0.68	0.92	مرتفعة جدًّا	2
31	أفحصُ الروابطَ والمرفقات التي تصلني عبر الرسائل النصية أو البريد الإلكتروني التي يبدو لي أنها ضارة.	4.25	0.97	0.85	مرتفعة جدًّا	٢٧

32	أحرصُ على تعطيل خدمات الوصول لموقعي في التطبيقات المحمَّلة على أجهزتي.	4.24	0.91	0.85	مرتفعة جدًّا	٢٨
33	أفعِّلُ خدمات الوصول لموقعي تفعيلًا مؤقَّتًا أثناء استخدام بعض التطبيقات والمواقع الإلكترونية التي تتطلّب ذلك.	4.20	0.91	0.84	مرتفعة جدًّا	٣١
34	أغيّر إعدادات أجهزتي باستمرار لحمايتها وتحصينها من القرصنة أو اختراق الاتّصال بالشبكة اللاسلكية (WiFi).	3.97	0.98	0.79	مرتفعة	٤٠
35	أنشرُ الوعيَ الرقميَ بالأمن السيبرانيّ عند التعرُّض للمواقف السلبية في شبكة الإنترنت.	4.03	0.96	0.81	مرتفعة جدًّا	٣٩
36	أراعي النزاهة والشفافيَّة والأصالةَ في هويَّتي الرقمية حين أستخدم مواقع شبكات التواصل الاجتماعي وتطبيقاتها.	4.21	0.89	0.84	مرتفعة جدًّا	٢٩
37	أتجنّب الكشف عن بياناتي الشخصيّة والعائليّة أو إرسالها أو مشاركتها مع الغرباء في الفضاء السيبراني (مثل: عبر الرسائل النصيّة في مواقع التواصل الاجتماعي وتطبيقاتها، أو البريد الإلكتروني، أو عند تصفُّحي مواقع شبكة الإنترنت)، وفي أثناء المكالمات الهاتفيّة مع أشخاص مجهولين أو غير موثوقين.	4.52	0.73	0.90	مرتفعة جدًّا	5
38	أتوخّى الحذر عند مشاركة الآخرين ببياناتٍ حسّاسةٍ، وذلك باستخدام إعداداتِ الخصوصيَّة للخدمات الإلكترونية.	4.48	0.72	0.90	مرتفعة جدًّا	10
39	أحرصُ باستمرار على تحميل البرامج الآمنة (الموثوقة والمعتمدة) واستخدامها.	4.47	0.74	0.89	مرتفعة جدًّا	13
40	أحرصُ دومًا على تثبيت آخر التحديثاتِ للبرمجيَّات أو التطبيقات المُحمَّلة على أجهزتي.	4.38	0.80	0.88	مرتفعة جدًّا	20
41	أتجنّب استخدامَ البريد الإلكترونيّ الرسميّ في التسجيلِ أو الاشتراك في مواقع شبكات التواصل الاجتماعيّ وتطبيقاتها.	3.84	1.14	0.77	مرتفعة	٤٣
42	أتجنّب استخدامَ هاتفي الشخصيّ الرسميّ في تفعيل التسجيل	3.64	1.22	0.73	مرتفعة	٤٧

	والاشتراك في مواقع شبكات التواصل الاجتماعيّ وتطبيقاتها.					
43	أحرصُ على غلق أجهزتي أو تسجيل الخروج من التطبيقات والمواقع الإلكترونية بطريقةٍ صحيحةٍ لتجنّب فقدان البيانات.	4.17	0.97	0.83	مرتفعة جدًّا	٣٤
44	أتجنّب المواقع والتطبيقات ذات المحتوى المخالف للدين والعقيدة والأخلاق (مثل: المواقع الإباحيَّة، ومواقع نشر الأفكار الإلحادية أو اللادينيّة، والأفكار التعصّبية المذهبية أو العرقية، والأفكار المتطرّفة العنيفة).	4.60	0.70	0.92	مرتفعة جدًّا	1
45	أقرأ دليلَ السياسات والإجراءات الخاصَّة بحفظ الأمن السيبرانيّ في المدرسة، وأحرصُ على الالتزام بتطبيقها.	4.09	0.97	0.82	مرتفعة جدًّا	٣٨
46	أشاركُ في الدورات التدريبيّة والندوات التوعويّة والتخصّصيّة في مجال الأمن السيبراني.	3.77	1.10	0.75	مرتفعة	٤٥
47	أهتمُّ بالاطّلاع على الجهود الحكوميّة الهادفة إلى تعزيز الأمن السيبرانيّ وزيادة فاعليّته.	4.14	0.94	0.83	مرتفعة جدًّا	٣٥
	المتوسّط المرجّح	4.26	0.50	0.85	مرتفعة جدًّا	

يتبيّن من الجدول ٣ أنّ مستوى وعي معلّمات قبل الخدمة في كلية التربية بجامعة الكويت حيال الأمن السيبراني جاء بوجهٍ عام بدرجة "مرتفعة جدًّا" (م = 4.26، ن.م = 0.50، RII = 0.85)؛ إذْ بيّنت النتائج أنّ مستوى وعيهنَّ كان على درجة "مرتفعة جدًّا" في الأغلبية العظمى من عبارات المقياس (٣٩ عبارة)، بينما حصلت بقية فقرات المقياس (٨ فقرات) على درجة "مرتفعة". وتتّفق هذه النتيجة نوعًا ما في فحواها مع نتائج دراسات بحثية أخرى، كدراسة الصانع وآخرون (٢٠٢٠)، ودراسة سراج الدين وآخرون (٢٠٢١)؛ إذْ جاءت درجة وعي المعلّمين والمعلّمات بالأمن السيبراني فيهما بشكل عام بدرجة "عالية/مرتفعة". هذا بالإضافة إلى دراسة زقوت وآخرون (٢٠٢٢) التي أشارت إلى أنّ مستوى وعي أعضاء هيئة التدريس في الجامعة بالأمن السيبراني بوجهٍ عام كان بدرجة "كبيرة". وكذلك دراسة الظويفري (٢٠٢١) التي بيّنت أنّ واقع الأمن السيبراني ومستوى الوعي به في مدارس التعليم العام بمنطقة المدينة المنوَّرة جاء بوجهٍ عام بدرجة "عالية". ولكنّها في الوقت ذاته تختلف عن نتائج دراسات علميَّة أخرى، كدراسة المنتشري وحريري (٢٠٢٠)، ودراسة العقلاء وعلي

(٢٠٢٢) اللتين أظهرتا أنّ مستوى وعي المعلّمين والمعلّمات بالأمن السيبراني بوجهٍ عام جاء بدرجة "متوسّطة". إضافةً إلى دراسة Jazeel (٢٠١٨) التي بيّنت أنّ درجة وعي معلّمي ومعلّمات قبل الخدمة بكلية المعلّمين الحكوميَّة في سريلانكا كانت بوجهٍ عام "منخفضة". وبالمثل دراسة الصحفي وعسكول (٢٠١٩) التي أكّدت أنّ مستوى وعي معلّمات الحاسب الآلي بالمرحلة الثانوية في مدينة جدة بخصوص الأمن السيبراني كان بوجهٍ عام "ضعيفًا".

نتائج سؤال الدراسة الثاني.

نصّ سؤال الدراسة الثاني على: هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05\geq\alpha$) في آراء معلّمات قبل الخدمة في كلية التربية بجامعة الكويت وتصوّراتهنّ تجاه مستوى وعيهنّ بالأمن السيبراني يُمكنْ عزوها لمتغيّرات نوع التخصّص، ودورات الأمن السيبراني، ومستوى المعرفة/الخبرة أو المهارات في استخدام وسائل وأدوات وخدمات تكنولوجيا المعلومات والاتّصالات (ICT)؟ للإجابة عن هذا السؤال، أُستخدِم الإحصاء الاستدلاليّ (Inferential Statistics)، إذْ طُبِّق اختبار (ت للعيّنات المستقلّة)، وتحليل التباين الأحادي، للكشف عن الفروق ذات الدلالة الإحصائيَّة. ويُبيّن الجدولان (٤ . ٥) نتائج هذا التحليل.

جدول ٤

نتائج الإحصاء الاستدلاليّ لاختبار ت (t-test) للعيّنات المستقلَّة لمقياس الدراسة تبعًا لمتغيّري نوع التخصّص ودورات الأمن السيبراني

م	المتغيّر المستقل	الصنف	التكرار	المتوسّط الحسابيّ	الانحراف المعياريّ	قيمة ت	درجة الحريّة	الدلالة الإحصائيّة	مستوى الدلالة
١	نوع التخصص	التخصّصات الأدبية	334	4.26	0.53	-0.196	462	0.845	غير دالّة
		التخصّصات العلمية	130	4.27	0.39				
٢	دورات الأمن السيبراني	التحقت بدورات	24	4.46	0.41	2.103	462	0.036*	دالّة
		لم تلتحق بأيّ دورات	440	4.25	0.50				

*ملاحظة. * دالّ إحصائيًا عند مستوى دلالة 0.05 ($0.05\geq\alpha$).*

يتّضح من الجدول 4 أنّ اختبارات الفروق بين المجموعات المشاركة أظهرت عدم وجود اختلافات دالّة إحصائيًّا عند مستوى الدلالة 0.05 بين متوسّطات استجابات معلّمات قبل الخدمة في كلية التربية بجامعة الكويت بشأن آرائهنّ وتصوّراتهنّ (اتّجاهاتهنّ) حول مستوى وعيهنّ بالأمن السيبراني تُعزى لمتغيّر نوع التخصّص (أدبي، علمي)، وذلك في الأداة عامّةً. ويُمكن تعليل هذه النتيجة بأنّ الأمن السيبراني مبحث حيويّ يهمُّ جميع الأفراد بغض النظر عن نمط تخصّصاتهم العلميَّة. وبناءً عليه، نجد أنّ الوعي والمعرفة بهذا الموضوع يُعدُّ من الاهتمامات والأولويّات للجميع، ورُبّما يكون ذلك هو السبب في ظهور توافق وانسجام تام في آراء وتصوّرات (اتّجاهات) الفئتين. وتتّفق هذه النتيجة في فحواها مع نتيجة دراسة الصانع وآخرون (٢٠٢٠) التي أشارت إلى عدم وجود أيّ فروق دالّة إحصائيًّا بين متوسّطات استجابات المجموعات المشاركة من أعضاء الهيئة التعليميَّة في مدارس مدينة الطائف حول مستوى وعيهم بالأمن السيبراني يُمكن عزوها لمتغيّر نوع التخصّص، ولكنّها في الوقت ذاته تعارضت مع النتيجة التي توصّلت إليها دراسة سراج الدين وآخرون (٢٠٢١) التي أظهرت وجود فروق ذات دلالة إحصائيَّة بين متوسّطات تقديرات أفراد عيّنة الدراسة من معلّمي ومعلّمات المدارس الخاصة بإمارة عجمان نحو استجاباتهم لمستوى وعيهم بالأمن السيبراني تُعزى لمتغيّر نمط التخصّص.

وكذلك يتبيّن من الجدول 4 وجود فروق ذات دلالة إحصائيَّة عند مستوى الدلالة 0.05 بين متوسّطات تقديرات معلّمات قبل الخدمة في كلية التربية بجامعة الكويت بشأن آرائهنّ وتصوّراتهنّ (اتّجاهاتهنّ) حول مستوى وعيهنّ بالأمن السيبراني تُعزى لمتغيّر دورات الأمن السيبراني (التحقت، لم تلتحق)، وذلك في المقياس عامّةً، لصالح المعلّمات اللّاتي انضممنَ إلى دورات مسبقة في مجال الأمن السيبراني. ويُمكن تفسير هذه النتيجة حسب السياق المنطقي بأنّ المشارِكات اللّاتي انخرطنَ في دورات سابقة مختصّة بالأمن السيبراني كُنَّ على درجة عالية من الوعي والمعرفة والدراية بهذا المبحث الجوهريّ مقارنةً بأقرانهنّ اللّاتي لم يلتحقنَ بأيّ دورة، كما يُمكنْ أنْ نُفسّر النتيجة السابقة حسب السياق الإحصائيّ ونُرجعها إلى صِغر حجم أفراد العيّنة المشاركة من معلّمات قبل الخدمة اللّاتي حصلنَ على دورات آنفة في الأمن السيبراني البالغ عددهنّ ٢٤ معلّمةً (حوالي 5.2%) مقارنةً بعدد المشارِكات من فئة معلّمات قبل الخدمة اللّاتي لم ينخرطنَ بأيّ دورة في مجال الأمن

السيبراني الذي بلغ ٤٤٠ معلّمةً (حوالي 94.8%)، فربّما يكون هذا هو السبب في ظهور الاختلافات ذات الدلالة الإحصائيّة بين متوسّطات استجابات المشارِكات وفقًا لمتغيّر دورات الأمن السيبراني.

وتتطابق هذه النتيجة للدراسة الحالية في مضمونها مع نتيجة دراسة المنتشري وحريري (٢٠٢٠) التي أكّدت وجود فروق ذات دلالة إحصائيَّة بين متوسّطات استجابات معلّمات المرحلة المتوسّطة في مدارس التعليم العام بمدينة جدة حول مستوى وعيهنّ بالأمن السيبراني تُعزى لمتغيّر الدورات التدريبيّة في مجال الأمن السيبراني لصالح من حصلنَ على دورات تدريبية، وكذلك اتّفقت مع نتيجة دراسة العقلاء وعلي (٢٠٢٢) التي كشفت عن وجود اختلافات دالة إحصائيًّا بين متوسّطات استجابات معلّمي ومعلّمات الحاسب الآلي بالمرحلتين المتوسّطة والثانوية بمدينة حائل إزاء درجة وعيهم بالأمن السيبراني تُعزى لمتغيّر الدورات التدريبية في مجال الأمن السيبراني لصالح من لم يتلقّوا أيّ دورة تدريبيّة، بينما تباينت نتيجة الدراسة الراهنة مع نتيجة دراسة الصحفي وعسكول (٢٠١٩) التي أظهرت عدم وجود فروق دالة إحصائيًّا بين متوسّطات تقديرات معلّمات الحاسب الآلي بالمرحلة الثانوية في مدينة جدة نحو درجة وعيهنّ بالأمن السيبراني تبعًا لمتغيّر الدورات التدريبية، وبالمثل اختلفت مع نتيجة دراسة الظويفري (٢٠٢١) التي دلّلت على عدم وجود أيّ فروق ذات دلالة إحصائيّة بين متوسّطات استجابات القيادة المدرسيّة (القادة والقائدات والمعلّمين والمعلّمات) تجاه واقع الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنوَّرة تُعزى لمتغيّر عدد الدورات التدريبيّة في مجال الـ ICT.

جدول ٥

نتائج الإحصاء الاستدلاليّ لاختبار تحليل التباين الأحاديّ (ANOVA) لمقياس الدراسة تبعًا لمتغيّر مستوى الـ ICT

م	المتغيّر المستقل	مصدر التباين	مجموع المربعات	درجة الحرية	متوسّط المربعات	قيمة ف	الدلالة الإحصائيّة	مستوى الدلالة
١	مستوى الـ ICT	بين المجموعات	1.451	2	0.725	2.971	0.052	غير دالّة
		داخل المجموعات	112.558	461	0.244			
		الكُلّي	114.009	463				

يتّضح من الجدول ٥ عدم وجود فروق دالة إحصائيًّا عند مستوى الدلالة 0.05 بين متوسّطات استجابات معلّمات قبل الخدمة في كلية التربية بجامعة الكويت بشأن آرائهنّ وتصوّراتهنّ (اتّجاهاتهنّ) نحو مستوى وعيهنّ بالأمن السيبراني تُعزى لمتغيّر مستوى الـ ICT (مبتدئة، ملمّة/متوسّطة، محترفة/متقدّمة)، وذلك في الأداة عامّةً. ويُمكن تعليل هذه النتيجة بأنّ الأمن السيبراني هو الموضوع الجوهريّ الذي يهمُّ ويمسُّ الأشخاص في كل شرائح المجتمع بالعالم لأنّهم يعتمدون بشكل رئيس على وسائل التقانة الرقميّة وأدواتها وتطبيقاتها في حياتهم اليومية بغض النظر عن مستوى معارفهم ومهاراتهم وكفاياتهم وقدراتهم وخبراتهم في مجال تكنولوجيا المعلومات والاتّصالات. وبناءً عليه، نجد أنّ الوعي والإلمام بهذا المبحث يُعدُّ من الاهتمامات والأولويّات للجميع، ورُبّما يكون ذلك هو السبب في ظهور توافق وانسجام تام في آراء وتصوّرات (اتّجاهات) الفئات الثلاث. وتتباين هذه النتيجة في فحواها مع نتائج بحوث علميّة أخرى، كدراسة Jazeel (٢٠١٨) التي شدّدت على وجود فروق ذات دلالة إحصائيَّة بين استجابات معلّمي ومعلّمات قبل الخدمة في كلية المعلّمين الحكوميَّة في سريلانكا حيال درجة وعيهم بالأمن السيبراني تُعزى لمتغيّر مستوى المعرفة بالحاسوب لصالح من ليس لديه أي معرفة.

الخلاصة والتوصيات

في عصر التكنولوجيا الحديثة والتواصل الرقميّ أصبح الأمن السيبراني أحد أهم التحدّيات التي تواجهها المجتمعات العالميّة، ويُشير مصطلح الأمن السيبراني إلى حماية الأنظمة الإلكترونيّة والشبكات والبيانات من التهديدات والهجمات الإلكترونيَّة، وذلك بهدف ضمان السلامة والسرّيَّة والموثوقيَّة في عالم يعتمد اعتمادًا كبيرًا على التقنية والمعلومات. وتتنوّع التهديدات السيبرانية التي تواجهنا، فتشمل القرصنة الإلكترونيّة، والاختراقات السيبرانيّة، والبرمجيّات الخبيثة، والاحتيال الإلكترونيّ، والتجسّس، وغيرها الكثير. هذه التهديدات قادرة على التسبّب في خسائر ماديّة وتعطيل الأنظمة الحيويّة، بالإضافة إلى التأثير السلبيّ على الخصوصيَّة الشخصيَّة والثقة في استخدام التكنولوجيا، وتزداد أهمّيَّة الأمن السيبراني مع تطوّر التكنولوجيا وازدياد التواصل الإلكترونيّ، حيث تصبح الشبكات والأنظمة الرقميَّة أكثر تعقيدًا وتنوّعًا، ولذلك تتطلّب حماية الأنظمة السيبرانية تنفيذ إستراتيجيّات وسياسات فعّالة، بالإضافة إلى استخدام التقنيات المُتقدّمة وتحسين الوعي

السيبراني لدى المستخدمين، ولا يقتصر الأمر على الحكومات والمؤسّسات والشركات فحسب، بل يجب أنْ يشعر الأفراد والمجتمعات بالمسؤوليّة الشخصيّة تجاه الأمن السيبراني، ويجب علينا أنْ نتبنّى سُلوكيّات ومُمارسات آمنة في استخدامنا للتكنولوجيا والإنترنت، وأنْ نكون على دراية بالتهديدات والخطوات والتدابير الوقائيّة اللازمة لردعها (الشهري، ٢٠٢١؛ الظويفري، ٢٠٢١؛ العقلاء وعلي، ٢٠٢٢؛ المنتشري وحريري، ٢٠٢٠) (ISO, 2023; ITU, 2022; OpenAI, 2023).

وفي ضوء النتائج التي توصّلت إليها الدراسة يمكن أن نوصي بما يلي: (١) وجوب الاهتمام بنشر ثقافة الأمن السيبراني والاستخدام الأمثل للتكنولوجيا – بما يكفل الوقاية والحماية من التهديدات والمخاطر في العالم الرقمي – بين أعضاء الهيئة التعليميّة ممّا ينشئ جيلًا مثقفًا واعيًا. (٢) ضرورة توفير التدريب والتوعية المستمرّة للمعلّمين والمعلّمات بشأن الأمن السيبراني وتهديداته وأخطاره – السابقة والحاليّة والمستقبليّة – من خلال استضافة المتخصّصين البارزين لعقد الدورات ووُرَش العمل التدريبيّة، وحلقات النقاش والمحاضرات التوعويّة، وكذلك وضع ملصقات، أو توزيع كتيّبات، أو نشرات للتوعية، أو عبر مواقع التواصل الاجتماعي. (٣) توفير دليل إرشاديّ تربويّ تفاعليّ رقميّ عن الأمن السيبراني. (٤) إدراج مبحث الأمن السيبراني بموضوعاته المختلفة ضمن المناهج التربويّة في المدارس والجامعات. (٥) أهميّة تطوير السياسات والإجراءات الأمنيّة في المؤسّسات التعليميّة لحماية البيانات والمعلومات الشخصيَّة وتعزيز الأمن السيبراني بوجهٍ عام وفق الضوابط الأساسيّة الصادرة من الهيئات والمؤسّسات والمنظّمات المختصة بالأمن السيبراني. (٦) تعزيز التنسيق والتعاون والشراكة بين المؤسّسات التربويّة والهيئات والمنظمات المختصّة بالأمن السيبراني لتعزيز وزيادة الوعي في مجال الأمن السيبراني. (٧) إجراء المزيد من الدراسات البحثيّة المشابهة باستخدام عيّنات ومتغيّرات ومنهجيّات أخرى، وعلى مجتمعات مغايرة.

المراجع

المراجع العربية

ابن إبراهيم، منال حسن محمد. (٢٠٢١). الوعي بجوانب الأمن السيبراني في التعليم عن بُعد. *المجلة العلمية لجامعة الملك فيصل: العلوم الإنسانية والإدارية*، ٢٢ (٢)، ٢٩٩–٣٠٧. https://doi.org/10.37575/h/edu/0089

أبو علام، رجاء محمود. (٢٠١٨). *مناهج البحث الكمي والنوعي والمختلط* (الطبعة الثانية). دار المسيرة.

الإدارة المركزية للإحصاء. (٢٠٢٢). *النشرة السنوية لإحصاءات التعليم ٢٠٢١/٢٠٢٢*. الإدارة المركزية للإحصاء، دولة الكويت. https://www.csb.gov.kw/Pages/Statistics?ID=58&ParentCatID=70

الحبيب، ماجد بن عبد الله. (٢٠٢٢). درجة الوعي بالأمن السيبراني لدى طلاب وطالبات الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية وسُبل تعزيزه من وجهة نظرهم. *مجلة العلوم التربوية*، (٣٠–١)، ٢٦٩–٣٢٦.

الزبيدي، محمد بن علي، عسيري، محمد بن جابر، البقمي، سعود بن سعد، والمناخرة، الحسن بن يحيى. (٢٠٢١). العلاقة بين الوعي بالأمن السيبراني وقيم الانتماء الوطني لدى طلبة المرحلة الثانوية بمنطقة مكة المكرمة. *مجلة جامعة الملك عبد العزيز: الآداب والعلوم الإنسانية*، ٢٩ (٨)، ٦١–٩٢. https://doi.org/10.4197/Art.29-8.3

السواط، حمد بن حمود، الصانع، نورة عمر، أبو عيشة، زاهدة جميل، سليمان، إيناس محمد، وعسران، عواطف سعد الدين. (٢٠٢٠). العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف. *مجلة البحث العلمي في التربية*، *21*(4)، ٢٧٨–٣٠٦. https://doi.org/10.21608/JSRE.2020.92657

الشهري، مريم بنت محمد فضل. (٢٠٢١). دَورُ إدارة الجامعة في تعزيزِ الوعيِ بالأمنِ السيبرانيّ لدى طلبةِ كليةِ التربيةِ بجَامِعَة الإمَام محمد بن سعود الإسلامية. *مجلة العلوم الإنسانية والإدارية*، (٢٥)، ٨٣–١٠٤.

الصانع، نورة عمر، السواط، حمد بن حمود، أبو عيشة، زاهدة جميل، سليمان، إيناس محمد، وعسران، عواطف سعد الدين. (٢٠٢٠). وعي المعلّمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهويّة الوطنية لديهم. *مجلة كلية التربية – جامعة أسيوط*، ٣٦ (٦)، ٤١–٩٠. https://doi.org/10.21608/mfes.2020.114629

الصحفي، مصباح أحمد حامد، وعسكول، سناء صالح. (٢٠١٩). مستوى الوعي بالأمن السيبراني لدى معلّمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. *مجلة البحث العلمي في التربية*، (٢٠-١٠)، ٤٩٣-٥٣٤. https://doi.org/10.21608/JSRE.2019.56490

الظويفري، مشاعل بنت شبيب بن مطيران. (٢٠٢١). واقع الأمن السيبراني وزيادة فاعليّته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية. *المجلة الدولية للدراسات التربوية والنفسية*، ١٠ (٣)، ٦٣٥-٦٥٥. https://doi.org/10.31559/EPS2021.10.3.7

العسّاف، صالح بن حمد. (٢٠١٠). *المدخل إلى البحث في العلوم السلوكية*. دار الزهراء.

العقلاء، رؤى أحمد صالح، وعلي، نور الدين عيسى آدم. (٢٠٢٢). درجة الوعي بمفاهيم الأمن السيبراني لدى معلّمي ومعلّمات الحاسب الآلي بمدينة حائل. *دراسات عربية في التربية وعلم النفس*، (١٤٤-٢)، ٢٧٧-٣٠٠. https://doi.org/10.21608/SAEP.2022.263396

المنتشري، فاطمة يوسف، وحريري، رندة. (٢٠٢٠). درجة وعي معلّمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلّمات. *المجلة العربية للتربية النوعية*، ٤ (١٤)، ٩٥-١٤٠. https://doi.org/10.33850/ejev.2020.101830

حمدان، سماح محمد سامي. (٢٠٢١). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته بالإجراءات الاحترازية للحماية من الهجمات الإلكترونية في ظل جائحة كورونا. *المجلة العربية للعلوم الاجتماعية*، (١٩-١)، ١٨-٦٩.

زقوت، نشوه إسماعيل، السائح، سناء أحمد، والعطاب، الصديق عبد القادر. (٢٠٢٢). مدى وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحوّل الرقمي: دراسة تطبيقية بجامعة الزاوية. *المجلة الدولية للعلوم والتقنية*، (٢٩)، ١-٢٢.

سراج الدين، عثمان، ناصف، سعيد، الرواشدة، علاء، والطاهر، محمد. (٢٠٢١). مستوى وعي معلّمي المدارس بالأمن الإلكتروني للطلبة وعلاقته ببعض المتغيّرات. *دراسات: العلوم الإنسانية والاجتماعية*، ٤٨ (٤)، ٢٣٩-٢٥٣.

صائغ، وفاء حسن. (٢٠١٨). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية. *المجلة العربية للعلوم الاجتماعية*، (١٤-٣)، ١٨-٧٠.

صفر، عمار حسن. (٢٠١٧). اتّجاهات التربويّين نحو قانون مكافحة جرائم تقنية المعلومات في دولة الكويت. *دراسات تربوية واجتماعية*، ٢٣ (١-١)، ٣٤٩-٤١٨.

صفر، عمار حسن. (٢٠٢٠). معوّقات التعليم والتعلّم عن بُعد في التعليم الحكومي بدولة الكويت أثناء تفشّي جائحة فيروس كورونا المستجد (كوفيد–١٩) من وجهة نظر أعضاء هيئة التدريس بجامعة الكويت: دراسة استطلاعية تحليلية. *المجلة التربوية – جامعة سوهاج*، (٧٩–٤)، ٢٠٥٧–٢١٠٤. https://doi.org/10.12816/EDUSOHAG.2020.116653

قاسم، علي. (٢٠٢٢، فبراير ٥). مرسوم أميري بإنشاء المركز الوطني للأمن السيبراني. *الراي*. https://www.alraimedia.com/article/1575027

وكالة الأنباء الكويتية. (٢٠١٨، يناير ١٧). (هيئة الاتّصالات) الكويتية: استراتيجية الأمن السيبراني تعزّز أمن المعلومات. *وكالة الأنباء الكويتية (كونا)*. https://www.kuna.net.kw/ArticleDetails.aspx?id=2684437&amplanguage=ar

المراجع الأجنبية

Akadiri, O. P. (2011). *Development of a multi-criteria approach for the selection of sustainable materials for building projects* (Publication No. U568440) [Doctoral dissertation, University of Wolverhampton]. ProQuest Dissertations Publishing.

Cisco. (2023). *Cisco cybersecurity readiness index: Resilience in a hybrid world*. Cisco. https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-index-report.pdf

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

European Union Agency for Cybersecurity. (2021). *Raising awareness of cybersecurity: A key element of national cybersecurity strategies*. European Union Agency for Cybersecurity (ENISA). https://doi.org/10.2824/363629

Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2019). *How to design and evaluate research in education* (10th ed.). McGraw-Hill Education.

International Organization for Standardization. (2022). *ISO/IEC 27001: Information security management systems - requirements*. International Organization for Standardization (ISO). https://www.iso.org/standard/27001

International Organization for Standardization. (2023). *ISO/IEC 27032: Cybersecurity - guidelines for Internet security*. International Organization for Standardization (ISO). https://www.iso.org/standard/76070.html

International Telecommunication Union. (2022). *Global connectivity report 2022*. International Telecommunication Union. https://www.itu.int/hub/publication/d-ind-global-01-2022/

Jazeel, A. M. (2018). A study on awareness of cybercrime among teacher trainees in Addalaichenai Government Teachers' College. *Journal of Social Welfare and Management, 10*(1), 31-34.

Johnson, R. B., & Christensen, L. (2020). *Educational research: Quantitative, qualitative, and mixed approaches* (7th ed.). SAGE Publications.

National Institute of Standards and Technology. (2020). *NIST special publication 800-53, rev. 5: Security and privacy controls for information systems and organizations*. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

OpenAI. (2023). *ChatGPT* (Sep 25 version) [Large language model]. https://chat.openai.com/chat

Organization for Security and Co-operation in Europe. (2023). *Emerging practices in cybersecurity-related public-private partnerships and collaboration in OSCE participating states*. Organization for Security and Co-operation in Europe (OSCE). https://www.osce.org/files/f/documents/2/7/539108_0.pdf

United Nations Educational, Scientific and Cultural Organization. (202٢). *Minding the data: Protecting learners' privacy and security*. United Nations Educational, Scientific and Cultural Organization (UNESCO). https://unesdoc.unesco.org/ark:/48223/pf0000381494