مستوى وعي المعلّمين في مدارس التعليم العام بدولة الكويت بالأمن السيبراني من وجهة نظرهم

تمَّ دعم وتمويل هذا العمل من قبل جامعة الكويت، مشروع بحث رقم (TT04/23)

إعداد

أ.د. عمار حسن صفر

أستاذ تكنولوجيا التعليم: الحاسوب التربوي + التعلّم عن بُعد (التعلّم الإلكتروني)
قسم المناهج وطرق التدريس، كلية التربية، جامعة الكويت
البريد الإلكتروني: dr.ammar@ku.edu.kw

مستوى وعي المعلّمين في مدارس التعليم العام بدولة الكويت بالأمن السيبراني من وجهة نظرهم

المُلخّص

هدفت الدراسة إلى قياس مستوى وعي المعلّمين في مدارس التعليم العام بدولة الكويت بالأمن السيبراني، إضافةً إلى الكشف عن أثر متغيّرات الجنس/النوع، ونوع التخصُّص، والمؤهّل العلميّ، ومؤهّل الـ ICT، ودورات الأمن السيبراني، ومستوى الـ ICT، وسنوات الخبرة المهنية في آرائهم وتصوّراتهم إزاء مستوى وعيهم هذا. وتبنّت الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ باعتبارها المنهجيَّة البحثيَّة العلميَّة المعهود بها إتمام مقاصد الدراسة البحثيَّة الاستقصائيَّة، واستخدمت أداة الاستبانة لجمع البيانات، وَتكوَّن المقياس – بعد التأكُّد من صدقه وثباته – من ٤٧ عبارة/فقرة. أمّا بالنسبة لعيّنتها الطبقيَّة القصديَّة فتألّفت من ١,٦٦٤ معلّمًا ومعلّمةً، جرى اختيارهم بالطريقة العشوائيَّة البسيطة، وبصورة آليَّة/إلكترونيَّة خلال الفَصْلَيْن الدراسِيَّيْن الأول والثاني من العام الدراسيّ ٢٠٢٣/٢٠٢٤م. وقد كشفت نتائج الدراسة أنّ مستوى الوعي بالأمن السيبراني لدى المعلّمين جاء عمومًا بدرجة "مرتفعة جدًّا" (م = 4.21، ن.م = 0.58، RII = 0.84)؛ إذْ بيّنت النتائج أنّ مستوى وعيهم كان على درجة "مرتفعة جدًّا" في الغالبيّة العظمى من عبارات المقياس (٤٠ عبارة)، في حين تدنّت/انخفضت درجة الوعي لديهم إلى تقدير "مرتفعٍ" في الفقرات السبع الأخرى للمقياس. وأشارت النتائج كذلك إلى عدم وجود فروق ذات دلالة إحصائيَّة عند مستوى الدلالة 0.05 ($\alpha \geq 0.05$) بين متوسّطات استجابات أعضاء الهيئة التعليميَّة بشأن آرائهم وتصوّراتهم (اتّجاهاتهم) فيما يتعلّق بمستوى وعيهم بالأمن السيبراني تُعزى لمتغيّرات الجنس/النوع (ذكر، أنثى)، ونوع التخصُّص (أدبي، علمي)، ومؤهّل الـ ICT (حاصل على شهادة دوليَّة، ليس لديه أيّ شهادة دوليَّة)، ودورات الأمن السيبراني (التحق بدورات، لم يلتحق بأيّ دورات)، وسنوات الخبرة المهنية (من ٠ إلى أقل من ١٠ سنوات، من ١٠ إلى أقل من ٢٠ سنة، من ٢٠ سنة فأكثر)، وذلك في الأداة عامّةً. أمّا بالنسبة لمتغيّرَيْ المؤهّل العلميّ (شهادة البكالوريوس، شهادة الماجستير/الدكتوراه)، ومستوى الـ ICT (مبتدئ، ملم/متوسّط، محترف/متقدّم)، فقد بيّنت النتائج وجود اختلافات دالَّة إحصائيًّا بين متوسّطات استجابات المشاركين، وذلك في المقياس عامّةً، لصالح المعلّمين والمعلّمات حاملي شهادة الإجازة الجامعية (البكالوريوس) وذوي مستوى الـ ICT الأعلى. وخَلُصَتْ الدراسة بتقديم بعض التوصيات.

الكلمات المفتاحيّة: الأمن السيبراني، مستوى/ درجة الوعي، المعلّمين والمعلّمات، مدارس التعليم العام، دولة الكويت.

Teachers' Cybersecurity Awareness Level in General Education Schools in the State of Kuwait From Their Perspective

Abstract

The study aimed to measure the cybersecurity awareness level of teachers in the general education schools in the State of Kuwait. Additionally, it sought to explore the impact of some independent variables such as gender, specialization, qualification, ICT international certificate, cybersecurity training courses, ICT proficiency, and years of professional experience on their perceptions and awareness level. The study employed a descriptive analytical quantitative research 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 1,664 teachers during the first and second semesters of 2023/2024 school year. The study revealed that the awareness level of teachers regarding cybersecurity was generally categorized as "very high" (M = 4.21, SD = 0.58, RII = 0.84). The results indicated that their awareness level was "very high" for the majority of the scale items (40 statements), while the remaining scale items (7 statements) also achieved a "high" level. Furthermore, the findings showed no statistically significant differences at the 0.05 significance level ($\alpha \leq 0.05$) among the means of the inservice teachers' responses attributed to the variables of gender (male, female), specialization (literary, scientific), ICT international certificate (have, does not have), participation in cybersecurity training courses (attended, did not attend), and years of professional experience (from 0 to less than 10 years, from 10 to less than 20 years, 20 years and above), within the entire instrument/scale. As for the variables of qualification (bachelor, master/doctorate) and ICT proficiency (beginner, intermediate/competent, advanced/proficient), the results demonstrated statistically significant differences in the means responses of participants in favor of teachers who have bachelor degrees and higher ICT proficiency. The study concluded with some recommendations.

Keywords: Cybersecurity, Awareness Level/Degree, Teachers, General Education Schools, State of Kuwait.

المُقدِّمة

الأمن السيبراني هو مجال مهم وحيوي في العصر الحديث، حيث تتزايد التقنيات الرقمية والاتّصالات الإلكترونية بمعدّل مذهل. يُشير مصطلح الأمن السيبراني إلى مجموعة من الإجراءات والتدابير التي تُتّخذ لحماية الأنظمة الإلكترونية والشبكات والبيانات من التهديدات والهجمات الإلكترونية. تهدف الجهود المبذولة في مجال الأمن السيبراني إلى الحفاظ على سلامة وسرية البيانات والمعلومات وضمان استمرارية العمليات الرقمية (خليفة، ٢٠١٧) (International Telecommunication Union [ITU], 2022).

يُعد الأمن السيبراني أمرًا حيويًّا للمؤسّسات والشركات والحكومات وحتّى الأفراد، حيث أصبحت الهجمات السيبرانية تهديدًا حقيقيًّا يُمكن أنْ يتسبّب في خسائر مادية وفقدان للبيانات والمعلومات السرية والحسّاسة والتعرّض لانتهاكات خصوصية كبيرة. تتضمّن التهديدات السيبرانية الشائعة الفيروسات وبرامج التجسّس والاختراقات والهجمات الاحتيالية والقرصنة الإلكترونية والهجمات المُنسّقة والتصيّد الاحتيالي، وغيرها الكثير. وتُشير التقديرات إلى أنّ تكلفة الجرائم السيبرانية من المُرجّح أنْ تتجاوز ستة تريليونات دولار في عام ٢٠٢١م، ممّا يجعل هذه المسألة ذات أهمية بالغة وتستدعي الاهتمام الشديد (فرج، ٢٠٢٢). يتطلّب الأمن السيبراني استراتيجيّات شاملة ومتعدّدة المستويات للوقاية والاستجابة والاستعادة، وذلك للتصدّي لهذه التهديدات المُتنامية. يجب أنْ تعتمد هذه الاستراتيجيّات على تحليل المخاطر وتقييم الثغرات وتنفيذ إجراءات الحماية وتعزيز الوعي الأمني وتدريب الكوادر وتطوير تقنيات الكشف المُبكّر والاستجابة السريعة. بالإضافة إلى ذلك، يلعب التشريعات والسياسات الحكومية دورًا هامًّا في تعزيز الأمن السيبراني وتطوير التعاون الدولي في مكافحة الجرائم السيبرانية (العقلاء وعلي، ٢٠٢٢؛ اللصاصمة والمجالي، ٢٠٢٢؛ المنتشري وحريري، ٢٠٢٠؛ بانقا، ٢٠١٩؛ خليفة، ٢٠١٧) (European Union Agency for Cybersecurity [ENISA], 2021, 2022; ITU, 2022; Schneier, 2015).

يتطلّب الأمن السيبراني أيضًا التحديث المستمر والتكنولوجيا المتقدّمة، حيث يتطوّر المهاجمون باستمرار ويبتكرون طرقًا جديدة للاختراق والاعتداء. لذلك، يتعيّن على الحكومات والمؤسّسات والمنظمات الاستثمار في أنظمة الحماية وتطوير الأدوات والتقنيات المُبتكرة للكشف عن

التهديدات والتصدّي لها. علاوةً على ذلك، يلعب الجانب البشري دورًا حاسمًا في الأمن السيبراني. يجب تعزيز الوعي الأمني بين الموظفين والأفراد وتعليمهم المُمارسات الأمنية الجيّدة، مثل استخدام كلمات مرور قويّة وعدم مشاركة بيانات ومعلومات حسّاسة عبر البريد الإلكتروني غير المُشفّر والابتعاد عن روابط ومرفقات البريد الإلكتروني المشبوهة (الشهري، ٢٠٢١؛ الظويفري، ٢٠٢١) (Organization for Security and Co-operation in Europe [OSCE], 2023; Singer & Friedman, 2014).

في نهاية المطاف، يتعيّن أنْ يكون الأمن السيبراني جزءًا أساسيًّا من استراتيجيّات المنظمات والمؤسّسات والشركات والدول في العصر الرقمي. يجب الاعتراف بأنّ الأمن السيبراني ليس مسؤولية فقط لفرق الأمن وتكنولوجيا المعلومات، بل يجب أنْ يشمل جميع أفراد المؤسّسة أيضًا. إنّ الاستثمار في الأمن السيبراني يُعد استثمارًا حيويًّا للحفاظ على سلامة البيانات والمعلومات والحفاظ على الثقة في البيئة الرقمية المتطوّرة التي نعيش فيها.

مشكلة الدراسة

أظهرت الدراسات البحثيَّة العلميّة الأكاديميّة التربوية في مجال الأمن السيبراني والتعليم نقصًا في وعي المعلّمين بهذا المجال. وجدت الدراسات أنّ الكثير من المعلّمين يفتقرون إلى معرفة كافية بالتهديدات السيبرانية وطرق الاحتيال الإلكتروني المُستخدمة حاليًّا. كما أشارت الدراسات إلى نقص في القدرات والمعارف والمهارات والكفايات والخبرات الأساسيَّة المطلوبة للتعامل مع الأمن السيبراني، مثل إدارة كلمات المرور والتعرّف على رسائل البريد الإلكتروني المشبوهة والروابط الخبيثة. وتَوصّلت الدراسات أيضًا إلى أنّ الوعي بالأمن السيبراني يُعتبر مهمًّا بشكل خاص في بيئات التعليم والتعلّم الرقميّ (الإلكترونيّ الشبكيّ المتنقّل)، سواءٌ الوجاهيّ (التقليدي) أو الافتراضي (عن بُعد)، حيث يتم استخدام التكنولوجيا بشكل واسع في هذه البيئات (الشهري، ٢٠٢١؛ الصحفي وعسكول، ٢٠١٩؛ العقلاء وعلي، ٢٠٢٢؛ المنتشري وحريري، ٢٠٢٠؛ صفر، ٢٠٢٤) (Jazeel, 2018; Moyo et al., 2022).

استنادًا إلى ذلك، يُعدُّ فهم معلّمينا لمستوى الوعي السيبراني وجاهزيّتهم لمواجهة التهديدات في بيئة التعليم والتعلّم الرقميّ تحدّيًّا مهمًّا في العصر الحالي. إنّ تحسين وعيهم بالأمن السيبراني ضروري لضمان سلامة البيانات والمتعلّمين. ينبغي للمؤسّسات التعليميَّة والجهات ذات العلاقة

اتّخاذ إجراءات فعّالة، مثل توفير التدريب المستمر والدعم، لتعزيز معرفة ومهارات وكفايات وقدرات المعلّمين في مجال الأمن السيبراني والتصدّي للتهديدات المُحتملة (المنتشري، ٢٠٢٠؛ المنتشري وحريري، ٢٠٢٠).

إنَّ البحث في مجال الوعي بالأمن السيبراني يُسهم في تعزيز المعرفة والمُمارسات الأمنية. يعمل الباحثون والخبراء على تحديد وفهم التهديدات الأمنية، وتطوير الحلول الفعّالة لمواجهتها، واتّخاذ التدابير الوقائيَّة لردعها (الصحفي وعسكول، ٢٠١٩). وهنا ظهرت الحاجة الماسّة إلى إجراء هذه الدراسة البحثيَّة، وبناءً عليه قام الباحث بإعداد الدراسة الحالية بُغية فهم مستوى وعي المعلّمين والمعلّمات – أثناء الخدمة – في مدارس التعليم العام بدولة الكويت بالأمن السيبراني، والتعرّف على مدى تهيّؤهم للتعامل مع التهديدات والمخاطر الأمنية السيبرانية في بيئة التعليم والتعلّم الرقميّ من وجهة نظرهم بوصفهم مُكوّنًا من المُكوّنات الأساسيّة الفاعلة والفعّالة العاملة في الحقل التربوي، وبهدف خدمة أغراض البحث العلميّ والتطوير المهنيّ في هذا المجال الجوهريّ.

أسئلة الدراسة

حاولت هذه الدراسة البحثيَّة الإجابة عن الأسئلة الآتية:

١. ما مستوى وعي المعلّمين في مدارس التعليم العام بدولة الكويت بالأمن السيبراني؟

٢. هل توجد فروق ذات دلالة إحصائيَّة عند مستوى الدلالة ($\alpha \leq 0.05$) في آراء معلّمي مدارس التعليم العام بدولة الكويت وتصوّراتهم تجاه مستوى وعيهم بالأمن السيبراني يُمكنْ عزوها لمتغيّرات الجنس/النوع، ونوع التخصُّص، والمؤهّل العلميّ، ومؤهّل الـ ICT، ودورات الأمن السيبراني، ومستوى الـ ICT، وسنوات الخبرة المهنية؟

أهداف الدراسة

أرادت الدراسة الراهنة تحقيق الأهداف التالية:

١. بيان مدى وعي المعلّمين في مدارس التعليم العام بدولة الكويت بالأمن السيبراني، وقياس قدراتهم ومعارفهم ومهاراتهم وكفاياتهم وخبراتهم واستعدادهم لمواجهة التهديدات والهجمات والاختراقات السيبرانية في بيئة التعليم والتعلّم الرقمي.

٢. الكشف عن أثر متغيّرات الجنس/النوع، ونوع التخصُّص، والمؤهّل العلميّ، ومؤهّل الـ ICT، ودورات الأمن السيبراني، ومستوى الـ ICT، وسنوات الخبرة المهنية في/على اتّجاهات معلّمي مدارس التعليم العام بدولة الكويت وآرائهم نحو درجة وعيهم بالأمن السيبراني.

أهمية الدراسة

تتلخّص أهمية الدراسة الحالية في النقاط الآتية:

١. تُساعد الدراسة صُنّاع القرار التربوي على تبيان الواقع الفعلي لمستوى الوعي بالأمن السيبراني لدى المعلّمين والمعلّمات في مدارس التعليم العام بدولة الكويت، وقياس قدراتهم ومعارفهم ومهاراتهم وكفاياتهم وخبراتهم، وتقييم استعدادهم لمواجهة التهديدات والهجمات والاختراقات السيبرانية في سياق التعليم والتعلّم الرقمي الذي انتشر بشكل واسع في الفترة القصيرة الماضية بسبب جائحة كورونا؛ حيث أصبحت الاستخدامات التربوية لوسائل – الأدوات، والمنصّات، والبرمجيّات، والشبكات، والخدمات، وغيرها – تكنولوجيا المعلومات والاتّصالات في بيئة التعليم والتعلّم العصرية أمرًا حاسمًا وحتميًّا – لا نستطيع تجاهله – يُمكن أنْ يُحدث تغييرًا ثوريًّا في العملية التعليميَّة والتعلّمية.

٢. تُسهم هذه الدراسة في تطوير وزيادة مستوى الوعي والإلمام والمعرفة بمفاهيم الأمن السيبراني وتطبيقاته ومخاطر الانتهاكات السيبرانية لدى المعلّمين والمعلّمات في مدارس التعليم العام بدولة الكويت، وتُعزّز بذلك من المُمارسات الأمنية السلوكية لديهم – في أماكن عملهم وفي حياتهم الشخصية – بشكل فعّال عبر استخدام الأساليب والاستراتيجيّات الفاعلة في الحماية والردع من مخاطر وتهديدات وهجمات الفضاء السيبراني، فيُساعدوا بذلك على خلق بيئة عمل ودراسة وحياة أكثر أمنًا وأمانًا.

٣. تُسلّط الدراسة الضوء على أهمية دور المعلّمين والمعلّمات في مجال الأمن السيبراني، إذْ يحملون أدوارًا حيويّةً ومؤثّرة لا يُمكن تجاهلها في تعزيز وتنمية الوعي بالأمن السيبراني في الميدان التربوي بشكل خاص وفي المجتمع بشكل عام.

٤. تُساعد هذه الدراسة في توجيه اهتمام المسؤولين التربويّين عن برامج إعداد وتأهيل المعلّمين في معاهد وكليات التربية إلى ضرورة إعادة النظر بتطويرها، وأهمية تضمين مبحث الأمن

السيبراني بمفاهيمه وتطبيقاته وموضوعاته المختلفة ضمن هذه البرامج لتتلاءم مع طبيعة العصر المعرفيّ الرقميّ والتقدّم الهائل والسريع في التكنولوجيا.

٥. تجلب الدراسة الحالية انتباه القياديّين في وزارة التربية ووزارة التعليم العالي والبحث العلمي بدولة الكويت نحو أهميّة تنظيم دورات تدريبية توعويَّة مستمرّة للمعلّمين والمتعلّمين والإداريّين وبقية العاملين في القطاع التربوي في مجال الأمن السيبراني. إضافةً إلى تضمين مبحث الأمن السيبراني بمفاهيمه وتطبيقاته ومخاطره وموضوعاته المختلفة ضمن المناهج الدراسية في المدارس والمعاهد والكليات والجامعات.

٦. يُساير موضوع الدراسة الحالية الاتّجاهات والمتغيّرات والقضايا التربوية العالمية العصرية في مجال تكنولوجيا المعلومات والاتّصالات التربوية – و/أو تكنولوجيا التعليم/التربية – بشكل عام، وفي مبحث تعزيز ورفع الوعي بالأمن السيبراني لدى المعلّمين والمعلّمات – والمتعلّمين والإداريّين وكل العاملين في الميدان التربوي – بشكل خاص؛ ممّا يُسهم في بناء مجتمع تربوي واعي بأهمية الأمن السيبراني، وكذلك يُؤمّن بيئة تربوية تعليمية وتعلّمية آمنة ومُستدامة عبر تنبيه المؤسّسات التربوية بدور الأمن السيبراني في الحفاظ على سرية البيانات والمعلومات عند التعامل مع التِّقَانَة، وأيضًا يُساعد على الارتقاء بثقافة المعلّمين والمتعلّمين والإداريّين وبقية المكوّنات العاملة في القطاع التربوي حول الأمن السيبراني.

٧. تأتي هذه الدراسة كاستجابة لجهود حكومة دولة الكويت في نشر الوعي بالأمن السيبراني، وتدريب المتعلّمين والمعلّمين والإداريّين والعاملين بالقطاع التربوي، وبقية الموظّفين في جميع قطاعات الدولة، على تطبيق الأمن السيبراني في مختلف مجالات الحياة.

٨. من المُمكن أنْ تُقدّم نتائج الدراسة الحالية مقترحات وتوصيات توجيهيّة إرشاديّة لواضعي السياسات التربوية التعليميَّة والتعلّمية، ممّا يستلزم إعادة النظر في أدوار ومهام المعلّم في هذا العصر المعرفيّ الرقميّ، وضرورة تجهيز وتأهيل المعلّم لمواجهة التحوّلات الحديثة في عالم المعرفة والرقمنة.

٩. تُعدُّ هذه الدراسة من إحدى الدراسات العربية التطبيقية القليلة – في حدود معرفة الباحث – في مجال الأمن السيبراني، والتي تتناول موضوع قياس درجة الوعي والإلمام والمعرفة بالأمن السيبراني لدى المعلّمين والمعلّمات. ولذا، رُبّما تكون الدراسة الحالية نواة (نقطة

الانطلاق) لأبحاث ودراسات تربوية علمية مستقبلية في هذا المجال الحيويّ، الذي لم ينل الاهتمام الكافي من قبل، بالرُغم من أهميّته البالغة في عصرنا المعرفيّ الرقميّ الراهن.

١٠. تُثري الدراسة الحالية الأدبيات الدراسية البحثيَّة التربوية العلمية – المحلية والخليجية والعربية والإقليمية والدولية – حول موضوع الدراسة الجوهريّ، وتفتح الأفق إلى التعمّق والتوسّع أكثر فيه فكريًّا، وأدبيًّا، ومعرفيًّا، وذلك بإجراء دراسات أكاديمية علمية بحثيَّة جديدة حوله ولمتغيّرات أخرى.

حدود الدراسة

صُنّفت حدود هذه الدراسة البحثيَّة إلى الآتي:

١. الحدود الموضوعيَّة: تمثّلت في قياس مستوى الوعي بالأمن السيبراني.

٢. الحدود البشريَّة: تمثّلت في وجهة نظر أعضاء الهيئة التدريسيَّة (المعلّمين والمعلّمات أثناء الخدمة).

٣. الحدود المكانيّة: اقتصرت على مدارس التعليم العام – الحكومية والخاصة – بدولة الكويت.

٤. الحدود الزمانيّة: طُبّقت في الفَصْلَيْن الدراسِيَّيْن الأول والثاني من العام الدراسي ٢٠٢٣/٢٠٢٤م.

٥. الحدود العلمية: تتمثّل في ندرة أو قلّة الأدبيات الدراسية التي تُغطي هذا المبحث الحيوي قيد الدراسة في حيّزنا الجغرافي.

مصطلحات الدراسة

نعرض فيما يلي بعض المفاهيم والمصطلحات الواردة في هذه الدراسة بالتعريف والتوضيح المُفصّل، ومن أبرزها:

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 (صفر، ٢٠٢٤؛ فرج،

٢٠٢٢؛ فوزي، ٢٠١٩) (Cisco, 2023a; ENISA, 2021, 2022; Hibberd, 2022; ITU, 2022).

٢. الوعي بالأمن السيبراني (Awareness of Cybersecurity): الوعي هو الإدراك العقلي للحقيقة ومضامينها (أو سياقاتها) الجامعة، والوعي الكلي هو مجموع ما يدركه الإنسان من حقائق (الحبيّب، ٢٠٢٢). ويُعرّف الوعي أيضًا بأنّه إدراك الإنسان لذاته ولما يحيط به مباشرةً، ويُشكّلُ أساسًا أساسيًّا لكلّ معرفة. يُشير الوعي أيضًا إلى الفهم والإدراك الصحيح، حيث يُعنى بفهم الإنسان لنفسه وللبيئة المحيطة به. ويتضمّن هذا الفهم أيضًا تفهّم الإنسان لذاته وللآخرين خلال تفاعله معهم، متطلّعًا لتلبية حاجاته الشخصية وتحقيق مصالحه. كما يعكس الوعي الاستدراك للعلاقات بين الفرد والآخرين والبيئة في سياق المواقف المتنوّعة. ويتم تعريف الوعي بالأمن السيبراني إجرائيًّا على أنّه الإدراك الذي يكتسبه المعلّم بشأن الجرائم الإلكترونية واختراقات البيانات والحسابات الشخصية. يهدف ذلك إلى تحقيق الأمان المعلوماتي أو الرقميّ، واتّخاذ جميع الإجراءات الاحترازية والتدابير اللازمة للوقاية من اختراق الأجهزة والبيانات والشبكات وكل ما يتعلّق بالتكنولوجيا. كما يُقاس هذا الوعي بالدرجة التي يحصل عليها المعلّم في المقاييس المُعدّة لهذا الغرض (ابن إبراهيم، ٢٠٢١، الحبيّب، ٢٠٢٢؛ اللصاصمة والمجالي، ٢٠٢٢؛ صفر، ٢٠٢٤).

الدراسات السابقة

(١) دراسة Jazeel (٢٠١٨): أُجريت لقياس مدى الوعي بالأمن السيبراني لدى المعلّمين والمعلّمات الجدد قبل الخدمة في كلية المعلّمين الحكومية في Addalaichenai بسريلانكا، وقد اعتمدت الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ، واستخدمت الاستبانة كأداة لجمع البيانات، والتي احتوتْ في صورتها النهائية – بعد التأكّد من صدقها وثباتها – على ١٥ عبارة. شملت عيّنة الدراسة الطبقيَّة العمديَّة ٢٠٠ معلم ومعلمة جدد قبل الخدمة، تمّ اختيارهم بشكل عشوائي، وتمّ تطبيق الدراسة عليهم في الفصل الأول من العام الأكاديمي ٢٠١٨/٢٠١٧م. وأشارت نتائج الدراسة إلى أنّ مستوى وعي المعلّمين والمعلّمات الجدد قبل الخدمة بالأمن السيبراني كان "منخفضًا" بشكلٍ عام؛ وتفصيليًّا، كان لدى ٦٠٪ من المشاركين مستوى وعي "منخفض"، في حين كان لدى ٢٩٪ مستوى "متوسط"، وحقق ١١٪ مستوى "عالي"

من الوعي. وكذلك أظهرت النتائج وجود فروق دالَّة إحصائيًّا بين استجابات المشاركين بناءً على عدّة متغيّرات، منها: الجنس/النوع – حيث كان الوعي أكبر بين الذكور، والمنطقة الجغرافية – حيث كان الوعي أعلى في المناطق الحضرية، ومستوى المعرفة بالحاسوب – حيث كان الوعي أكبر بين الذين ليس لديهم أيّ معرفة، ومُلكيّة جهاز الحاسوب – حيث كان الوعي أعلى بين الذين ليس لديهم جهاز حاسوب.

(٢) دراسة الصحفي وعسكول (٢٠١٩): ابتغت التحرّي عن مستوى الوعي بالأمن السيبراني لدى معلّمات الحاسب الآلي بالمرحلة الثانوية في مدارس التعليم العام الحكومي بمدينة جدة في المملكة العربية السعودية. اعتمدت الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ، واستخدمت الاستبانة كأداة رئيسية لجمع البيانات. تضمّن مقياس الوعي بالأمن السيبراني في صورته النهائية – بعد التحقّق من صدقه وثباته – ٢٥ فقرة موزّعة على مجالين هما: الوعي بماهية الأمن السيبراني (سبع عبارات)، والوعي بطرق المحافظة على نظام الأمن السيبراني (١٨ عبارة). وبخصوص عيّنة الدراسة الطبقيَّة القصديَّة المشاركة والتي تمّ اختيارها بالطريقة العشوائيَّة البسيطة فتشكّلت من ١٠٦ معلّمةً، وقد تمّ تطبيق الدراسة عليهنّ خلال الفصل الدراسي الثاني من العام الدراسي ٢٠١٩/٢٠٢٠م. وأشارت نتائج الدراسة إلى أنّ مستوى الوعي والإلمام والمعرفة بالأمن السيبراني لدى معلّمات الحاسب الآلي بوجهٍ عام جاء بدرجة "متوسّطة"؛ إذْ بيّنت النتائج التفصيليَّة أنّ المعلّمات كُنّ على مستوى "متوسّط" من الوعي والإلمام في مِحْوَرَيْ الدراسة بشكلٍ منفصلٍ، ممّا يدل على وجود ضعف وقصور في الوعي لديهنّ. كما كشفت النتائج أيضًا عن عدم وجود فروق ذات دلالة إحصائيَّة بين متوسّطات استجابات المعلّمات المشاركات في درجة وعيهنّ بالأمن السيبراني تُعزى لمتغيّرات الدراسة: المؤهّل العلميّ، وسنوات الخبرة المهنية، والدورات التدريبية. وخلُصت الدراسة بتقديم عدّة توصيات أبرزها تقديم دورات تدريبية وتثقيفية متخصّصة في مجال الأمن السيبراني لأعضاء الهيئة التعليميَّة.

(٣) دراسة المنتشري وحريري (٢٠٢٠): تركّزت على تقييم مستوى الوعي بالأمن السيبراني لدى معلّمات المرحلة المتوسّطة في مدارس التعليم العام بمدينة جدة في المملكة العربية السعودية. تبنّتْ الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ، واستعانت بالاستبانة كأداة لجمع البيانات المطلوبة، وضمّتْ في شكلها النهائي – بعد التحقّق من صدقها وثباتها – ٢١ عبارة

تُغطّي ثلاثة محاور رئيسية حول الأمن السيبراني: المفاهيم، المخاطر، والانتهاكات. تضمّنتْ عيّنة الدراسة الطبقيَّة العمديَّة ٣٦٢ معلّمةً تمّ اختيارهنّ بالطريقة العشوائية البسيطة، وتمّ تنفيذ الدراسة عليهنّ خلال الفصل الدراسي الأول من العام الدراسي ٢٠١٩/٢٠٢٠م. كشفتْ نتائج الدراسة أنّ مستوى وعي المعلّمات بالأمن السيبراني بشكلٍ عام كان "متوسّطًا"؛ حيثُ أظهرتْ النتائج التفصيليَّة أنّ المعلّمات كُنّ على مستوى "متوسّط" من الوعي في كُلٍّ من محاور الدراسة الثلاثة على حدة. وعلاوة على ذلك، لم تُظهر النتائج فروقًا ذات دلالة إحصائية بين استجابات المعلّمات تتعلّق بمتغيّري المؤهّل العلميّ وسنوات الخبرة المهنية. ومع ذلك، وُجِدَتْ هناك اختلافات ذات دلالة إحصائية بين تقديرات المعلّمات اللّاتي حصلنَ على دورات في الأمن السيبراني وتلك اللّاتي لم تحصلنَ عليها، وكانت لصالح من حصلنَ على دورات في الأمن السيبراني.

(٤) دراسة الصانع وآخرون (٢٠٢٠): استهدفت قياس درجة وعي المعلّمين والمعلّمات في المرحلتين الابتدائية والمتوسّطة في مدارس الطائف (الحكوميَّة والخاصَّة) بالمملكة العربية السعودية إزاء الأمن السيبراني، واعتمدت منهج البحث الكميّ الوصفيّ التحليليّ الارتباطيّ المسحيّ لتحقيق أهدافها، واستعانت بالاستبانة أداةً لجمع البيانات المطلوبة، وتكوَّنت في شكلها النهائي – بعد التحقّق من صدقها وثباتها – من ٢١ عبارة. أمّا بخصوص عيّنة الدراسة الطبقيَّة القصديَّة فتألّفت من ١٠٤ معلّمًا ومعلّمةً، وقد تمّ اختيارهم بالطريقة العشوائيَّة البسيطة، وطُبّقت عليهم 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 أَوْضَحَتْ النتائج التفصيليَّة أنّهم لديهم وعيٍ "مرتفعٍ جدًّا" في مجال حماية بياناتهم وأجهزتهم من أخطار الاختراق الإلكترونيّ والهجمات السيبرانية وذلك في ١١ عبارة من مقياس الوعي، في حين تدنّت درجة الوعي لديهم إلى تقدير "مرتفعٍ" في العبارات العشر الأخرى، كما تبيَّنَ كذلك بأنّهم يستخدمون أساليب وطرق تدريس وأنشطة ومشروعات تربوية فعّالة تُعزّز الوعي بأمن الإنترنت لدى المتعلّمين لحمايتهم من أخطارها، وتُنمّي القيم والهُويَّة الوطنيَّة لديهم. وأظهرت نتائج الدراسة أيضًا وجود علاقة ارتباطيَّة إيجابيَّة متوسّطة بين وعي المعلّمين والمعلّمات بالأمن السيبراني واستخدامهم لأساليب وطرق وإستراتيجيَّات لحماية طلابهم من أخطار الإنترنت وتعزيز القيم والهُويَّة الوطنيَّة لديهم، ولمْ تُظْهِرْ نتائج التحليلات الإحصائيَّة وجود أيّ فروق دالَّة

إحصائيًّا بين استجابات أو تقديرات المشاركين تُعزى للمتغيّرات التالية: نوع المدرسة، الجنس، التخصُّص، المؤهّل العلميّ، وسنوات الخبرة.

(٥) دراسة المنتشري (٢٠٢٠): سَعَتْ إلى استكشاف دور القيادة المدرسية في تعزيز الأمن السيبراني في مدارس البنات الحكومية بمدينة جدة في المملكة العربية السعودية، وذلك من خلال وجهة نظر المعلّمات، مع تقديم تصوّر مقترح حول كيفية تعزيز دور القيادة المدرسية في هذا السياق. اتّبعتْ الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ، واستخدمت الاستبانة كأداة لجمع البيانات، وتضمّنتْ في صورتها النهائية – بعد التأكّد من صدقها وثباتها – على ١٩ عبارة مُوزّعة على مِحْوَرَيْن رئيسيّين: الأول يُركّز على دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلّمات (١٠ عبارات)، بينما الثاني يُناقش دورها في تعزيز الأمن السيبراني لدى الطالبات (٩ عبارات). وبالنسبة لعيّنة الدراسة الطبقيَّة القصديَّة، والتي اختيرتْ بالطريقة العشوائيَّة البسيطة، فتكوّنت من ٤٢٠ معلّمةً، وقد تمّ تطبيق الدراسة عليهنّ خلال الفصل الدراسي الثاني من العام الدراسي ٢٠١٩/٢٠٢٠م. وكشفتْ نتائج الدراسة أنّ دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلّمات والطالبات بوجهٍ عام حصل على درجة موافقة "قليلة" من وجهة نظر المعلّمات؛ إذْ بيّنت النتائج التفصيلية حصول كِلا المِحْوَرَيْن على درجة موافقة "قليلة" كلٍّ على حدة. وفي ضوء هذه النتائج، تقدّمت الدراسة بمقترح يُركّز على دور القيادة المدرسية في تحسين الأمن السيبراني للمعلّمات والطالبات. وقد شمل هذا المقترح آليّات تطبيقية يُمكن تنفيذها بالتنسيق مع الجهات ذات الصلة في المملكة العربية السعودية المُختصّة بالأمن السيبراني. تضمنت هذه الآليّات خططًا خاصة للمعلّمات وأخرى للطالبات، بالإضافة إلى خطط مشتركة تشمل كِلا الطرفين. كما تضمّن المقترح آليّات لحماية البيئة المادية لشبكة الإنترنت.

(٦) دراسة سراج الدين وآخرون (٢٠٢١): كانت غايتها قياس درجة الوعي بالأمن السيبراني لدى المعلّمين والمعلّمات في المدارس الخاصة بإمارة عجمان في الإمارات العربية المتحدة، وتبنّت الدراسة المنهج البحثيّ الكميّ الوصفيّ التحليليّ المسحيّ، واستعانت بالاستبانة أداةً لجمع البيانات، واحتوَتْ في نسختها النهائية – بعد التأكّد من صدقها وثباتها – على ٢١ عبارةً حول الأمن السيبراني. أمّا بخصوص عيّنة الدراسة الطبقيَّة القصديَّة العشوائيَّة فتألّفت من ١٤٥ معلّمًا ومعلّمةً، وطُبّقت عليهم الدراسة في الفصل الثاني من العام الدراسي ٢٠١٩/٢٠٢٠م. لقد

أظهرت نتائج الدراسة أنّ مستوى الوعي بالأمن السيبراني لدى أعضاء الهيئة التعليميَّة بوجهٍ عام جاء بدرجة "مرتفعة"؛ إذْ أَوْضَحَتْ النتائج التفصيليَّة أنّ المشاركين كانوا على درجة "مرتفعة" من الوعي في ١٣ فقرة من مقياس الوعي المُستخدم، بينما انخفض مستوى درجة الوعي لديهم في ثماني عبارات. كما كشفت النتائج عن عدم وجود فروق ذات دلالة إحصائيَّة بين استجابات أو تقديرات المعلّمين والمعلّمات تُعزى لمتغيّرات النوع (الجنس)، والعمر، والخبرة، في حين وُجِدَتْ هذه الفروق ذات الدلالة الإحصائيَّة بينهم بالنسبة لمتغيّر التخصُّص.

(٧) دراسة الشهري (٢٠٢١): هدفت إلى قياس مستوى الوعي بالأمن السيبراني عند طلبة كلية التربية في جامعة الإمام محمد بن سعود الإسلاميَّة في المملكة العربية السعودية، هذا بالإضافة إلى التعرّف على دور الإدارة الجامعية في تعزيز الوعي بالأمن السيبراني لديهم. اعتمدت الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ، واستخدمت الاستبانة أداةً لجمع البيانات المطلوبة، واحتوَتْ في صيغتها النهائية – بعد التأكّد من صدقها وثباتها – على ٣٢ عبارة موزّعة على محورين. أمّا بالنسبة لعيّنة الدراسة الطبقيَّة القصديَّة العشوائيَّة فتكوّنت من ١٨٨ مشاركًا، وقد طُبِّقت عليهم الدراسة في الفصل الدراسي الأول من العام الأكاديمي ٢٠٢٠/٢٠٢١م. لقد كشفت نتائج الدراسة أنّ مستوى وعي طلبة كلية التربية ومعرفتهم بالأمن السيبراني جاء بوجهٍ عام بدرجة "متوسّطة"، وأنّ ممارسة الإدارة الجامعية لدورها المنوط بها في نشر الوعي بالأمن السيبراني وتعزيزه لدى هؤلاء الطلبة جاءت بوجهٍ عام بدرجة "متوسّطة" أيضًا، كما أظهرت النتائج عدم وجود اختلافات ذات دلالة إحصائيَّة بين متوسّطات تقديرات أفراد عيّنة الدراسة حول مستوى وعيهم بالأمن السيبراني تُعزى لمتغيّر الجنس/النوع، في حين وُجِدَتْ هذه الفروق الدالة إحصائيًّا بين متوسّطات استجاباتهم بالنسبة لمتغيّر المؤهّل العلميّ، ولصالح فئة حاملي شهادات الدراسات العُليا.

(٨) دراسة الظويفري (٢٠٢١): ابتغت قياس واقع الأمن السيبراني في مدارس التعليم العام بالمدينة المنوَّرة في المملكة العربية السعودية، وتحدّيات تفعيله، وإستراتيجيّات زيادة فاعليّته، حسب وجهة نظر القيادة المدرسية (القادة والقائدات والمعلّمين والمعلّمات). انتهجت الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ، واستعانت بالاستبانة أداةً لجمع البيانات، وتألّفت في صورتها النهائية – بعد التأكّد من صدقها وثباتها – من ٤٦ فقرة أو عبارة موزّعة على ثلاثة مجالات. أمّا بخصوص عيّنة الدراسة الطبقيَّة القصديَّة العشوائيَّة فتألّفت من ٤١٨ مشاركًا، وقد

طُبّقت عليهم الدراسة في الفصل الثاني من العام الدراسي ٢٠٢٠/٢٠٢١م. وأشارت نتائج الدراسة أنّ واقع الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنوَّرة جاء بوجهٍ عام بدرجة "عالية"، وأنّ التحدّيات والمعوّقات التي تواجه تفعيله في المدارس جاءت بوجهٍ عام بدرجة "عالية" كذلك. وقدّمت الدراسة أيضًا ضمن نتائجها مُقترحًا يَضُمُّ عدّة استراتيجيّات لزيادة فاعليّة الأمن السيبراني في المدارس منها: (أ) نشر ثقافة الوعي بالأمن السيبراني لدى أعضاء الهيئتين الإداريَّة والتدريسية، (ب) تعزيز وعي المتعلّمين بالأمن السيبراني ومخاطره، و(ج) توفير دليل تربويّ تفاعليّ عن أخلاقيّات الأمن السيبراني. كما أظهرت النتائج أيضًا عدم وجود فروق دالَّة إحصائيًّا بين متوسّطات استجابات المشاركين تُعزى للمتغيّرات التالية: الجنس/النوع، والوظيفة، والمؤهّل العلميّ، وعدد سنوات الخبرة المهنية، وعدد الدورات التدريبيَّة في مجال تكنولوجيا المعلومات والاتّصالات.

(٩) دراسة ابن إبراهيم (٢٠٢١): هدفت إلى قياس مستوى وعي معلّمات العلوم بالمرحلة الابتدائية في مدارس التعليم العام بالمملكة العربية السعودية بجوانب الأمن السيبراني في التعليم والتعلّم عن بُعد. بالإضافة إلى الكشف عن مدى فاعليّة برنامج تدريبي مُقترح استخدم لتنمية وعيهم بالأمن السيبراني. واعتمدت الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ التجريبيّ ذا التصميم شبه التجريبيّ ذي المجموعة الواحدة لتحقيق أهدافها، واستخدمت الاستبانة أداةً لجمع البيانات، وتَكوَّن مقياس الوعي بجوانب الأمن السيبراني في صيغته النهائية – بعد التأكّد من صدقه وثباته – من ٤٤ فقرة موزّعة على ثمانية مجالات أو أبعاد حول الأمن السيبراني في التعليم والتعلّم عن بُعد اللازم تنميتها لدى المعلّمات، وهي: جوانب الأمن السيبراني في التعليم والتعلّم عن بُعد، وتحصين بيئة المعلومات وسدّ ثغراتها الأمنية، والإجراءات الوقائية لتحصين الحاسوب، وإرشادات أمنية لتقديم الدروس الافتراضية، والمنصّة التعليميَّة في ظل أهم الجوانب الأمنية، والحفاظ على سريّة رقم السجل المدني، وعلامات الخطر التي تدل على أنّ الجهاز مُخترق، وخدمات مهمّة في نظام التعليم والتعلّم عن بُعد. هذا بالإضافة إلى استخدام برنامج تدريبي مُقترح – قائم على ١٠ جلسات، كل جلسة تستغرق ساعتين، بمجموع خمسة أسابيع اعتمادًا على برنامج زوم – يتضمّن مجموعة من المعارف والمهارات والكفايات والخبرات والأنشطة التدريبية لتنمية وزيادة الوعي بجوانب الأمن السيبراني في التعليم والتعلّم عن بُعد لدى المعلّمات، وذلك باستخدام أساليب تدريسية/تدريبية متنوّعة تسعى إلى توفير بيئة

إلكترونية/رقمية تعليمية وتعلّمية سليمة آمنة من أهم ركائزها المشاركة الفعّالة. أمّا بالنسبة لعيّنة الدراسة الطبقيَّة العمديَّة – والتي اختيرت بطريقة عشوائيَّة بسيطة – فتكوّنت من ٣٠ معلّمة علوم، المعلمات لمْ يحصلنَ على أيّ دورة سابقة في مجال الأمن السيبراني، وقد طُبّقت عليهنّ الدراسة في الفصل الدراسي الأول من العام الدراسي ٢٠٢٠/٢٠٢١م. وأشارت نتائج الدراسة إلى وجود فروق دالَّة إحصائيًّا بين متوسّطات درجات المعلّمات في التطبيق القبلي والبعدي لمقياس الوعي بجوانب الأمن السيبراني لصالح التطبيق البعدي، ممّا يدل على فاعليّة وأثر البرنامج التدريبي المُقترح ونجاحه في تنمية وزيادة مستوى الوعي لدى المعلّمات بجوانب الأمن السيبراني؛ إذْ بيّنت النتائج التفصيليَّة أنّ حجم تأثير البرنامج التدريبي المُقترح في جوانب الوعي بالأمن السيبراني في التعليم والتعلّم عن بُعد لدى معلّمات العلوم كان "كبير جدًّا"، حيث تشير قيمة مربع إيتا إلى أنّ نسبة التباين المُفسّر الذي تُحدثه المعالجة التجريبية (البرنامج التدريبي) في التباين المنظّم للمُتغيّر التابع (الوعي بالأمن السيبراني) لدى عيّنة الدراسة يُقدّر بـ ٩٥٪. وترجع هذه النِّسب من التباين الكلي للفروق بين المتوسّطات؛ لصالح التطبيق البعدي. كما جاءت قيمة d مساوية 8.72 (>١)؛ ممّا يُشير إلى فاعليّة "كبيرة" للمعالجة التجريبية. وبناءً عليه، تُشير النتائج التي توصّلت إليها الدراسة بأنّ مستوى وعي معلّمات العلوم بالمرحلة الابتدائية في مدارس التعليم العام بالسعودية بجوانب الأمن السيبراني في التعليم والتعلّم عن بُعد بوجهٍ عام جاء بدرجة "منخفضة"، وإنّ البرنامج التدريبي المُقترح ساهم برفعه إلى مستوى وعي "كبير إلى كبير جدًّا". وخلُصت الدراسة ببعض التوصيات، أهمّها: توفير برامج تدريبية وتوعويَّة تثقيفية للمعلّمات في مجال الأمن السيبراني بشكل مستمر، وإضافة موضوعات الأمن السيبراني بالمناهج المدرسية المختلفة، ودمجها بالبرامج التربوية وبرامج إعداد المعلّم.

(١٠) دراسة العقلاء وعلي (٢٠٢٢): هدفت إلى تقييم درجة التوعية بالأمن السيبراني عند معلّمي ومعلّمات الحاسب الآلي في المرحلتين المتوسّطة والثانوية بمدينة حائل في المملكة العربية السعودية، وتبنّت الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ لتحقيق أهدافها، واستخدمت الاستبانة كأداة رئيسة لجمع البيانات، وتضمّنت في صورتها الأخيرة – بعد التيقّن من صدقها وثباتها – من ٢٨ فقرة تمّ توزيعها على مجالين يتعلّقان بالأمن السيبراني، وهما: مفهوم وماهيَّة الأمن السيبراني، وطرق المحافظة على نظام الأمن السيبراني. وبخصوص عيّنة الدراسة الطبقيَّة القصديَّة فتكوّنت من ١٨٤ معلّمًا ومعلّمةً، وقد تمّ اختيارهم بالطريقة

العشوائيَّة البسيطة، وطُبّقت عليهم الدراسة في الفصل الدراسي الثاني من العام الدراسي ٢٠٢٠/٢٠٢١م. وأشارت نتائج الدراسة إلى أنّ مستوى الوعي بالأمن السيبراني لدى المعلّمين والمعلّمات بوجهٍ عام جاء بدرجة "متوسّطة"؛ إذْ كشفت النتائج التفصيليَّة أنّ المشاركين كانوا على درجة "متوسّطة" من التوعية في محوريْ الدراسة كلٍّ على حدة، كما أظهرت النتائج عدم وجود اختلافات دالَّة إحصائيًّا بين استجابات المشاركين تُعزى لمتغيّرَيْ المؤهّل العلميّ وسنوات الخبرة المهنية، بينما وُجِدَتْ هذه الفروق ذات الدلالة الإحصائيَّة بين المعلّمين والمعلّمات بالنسبة لمتغيّر الجنس لصالح المعلّمات، وأيضًا بالنسبة لمتغيّر الدورات التدريبيَّة في الأمن السيبراني لصالح من لم يتلقّوا أيَّ دورة تدريبيَّة، وكذلك بالنسبة لمتغيّر المرحلة التعليميَّة لصالح المرحلة المتوسّطة.

(١١) دراسة زقوت وآخرون (٢٠٢٢): استهدفت تقييم مستوى وعي أعضاء هيئة التدريس في جامعة الزاوية بليبيا تجاه التحوّل الرقميّ الذي طرأ جرّاء جائحة كورونا. اعتمدت الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ، واستخدمت الاستبانة كأداة رئيسية لجمع البيانات. تضمّن مقياس الوعي بالأمن السيبراني – بعد التحقّق من صدقه وثباته – ٣١ فقرة موزّعة على محاور مختلفة. وبالنسبة للعيّنة الطبقيَّة القصديَّة المشاركة في الدراسة والتي تمّ اختيارها بالطريقة العشوائيَّة البسيطة فتشكّلت من ٧٨ عضوًا من أعضاء هيئة التدريس، وتمّ تطبيق الدراسة عليهم خلال العام الجامعي ٢٠٢١/٢٠٢٢م. أظهرت نتائج الدراسة أنّ مستوى وعي أعضاء هيئة التدريس بالأمن السيبراني كان عمومًا على مستوى "كبير"؛ إذْ كشفت النتائج التفصيليَّة أنّ المشاركين كانوا على مستوى "متوسّط إلى كبير" في كل فقرة من فقرات المقياس بشكلٍ منفصلٍ.

(١٢) دراسة Moyo وآخرون (٢٠٢٢): استهدفت التحقّق من درجة التوعية بالأمن السيبراني لدى معلّمي قبل الخدمة – معلّمي مرحلة التدريس العام الجدد – في جامعة كيب تاون في جنوب إفريقيا، وخاصة بعد استخدامهم للتقنيّات الرقمية بعامة واعتمادهم بشكل كبير على منصّات التعليم والتعلّم عن بُعد (الإلكترونيّ الشبكيّ المتنقّل الافتراضيّ) بخاصة لدعم عمليّتي التعليم والتعلّم خلال جائحة كورونا (COVID-19). وقد اعتمدت الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ، واستخدمت الاستبانة أداةً لجمع البيانات، وقد تمّ توزيعها على عيّنة الدراسة الطبقيَّة القصديَّة العشوائيَّة وتكوّنت من ٣٠٠ معلّمًا ومعلّمةً قبل الخدمة. وأظهرت نتائج

الدراسة أنّ معلّمي ومعلّمات قبل الخدمة كانوا محدودين في مستوى وعيهم نحو الأمن السيبراني والتهديدات والمخاطر التي قد تؤثّر على استخدامهم للتقنيّات الرقمية المختلفة في التعليم والتعلّم عن بُعد؛ إذْ كشفت النتائج التفصيليَّة أنّ مستوى وعيهم بوجهٍ عام جاء بدرجة "منخفضة". علاوةً على ذلك، بيّنت النتائج أنّ المعلّمين والمعلّمات الجدد نفّذوا استراتيجيّات أساسية للتخفيف من تهديدات ومخاطر الأمان السيبراني، ولكن تبيّن بأنّها ليست كافية لمواجهة الهجمات المتقدّمة. اختتمت الدراسة بأنّ نقص التوعية بالأمان السيبراني السليم والمعرفة بين معلّمي ومعلّمات قبل الخدمة – الجدد – يُعرّضهم لصعوبات في مواجهة هجمات التهديد المرتبطة بمنع الخدمة (DoS)، وسرقة أو اصطياد البيانات والمعلومات عند استخدام أجهزة الحاسوب الشخصية الرقمية الخاصة بهم.

(١٣) دراسة الحبيّب (٢٠٢٢): كانت غايتها التعرّف على مستوى الوعي بمفاهيم وتطبيقات الأمن السيبراني لدى طلاب وطالبات الدراسات العُليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية في المملكة العربية السعودية وسبل تعزيزه من وجهة نظرهم. اعتمدت الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ، واستخدمت الاستبانة أداةً لجمع البيانات، وتألّفت في صيغتها النهائية – بعد التأكّد من صدقها وثباتها – من ٣٢ عبارة موزّعة على ثلاثة مجالات حول الوعي بالأمن السيبراني هي: الوعي بمفاهيم الأمن السيبراني (١٠ عبارات)، الوعي بتطبيقات الأمن السيبراني (١٢ عبارة)، وأبرز سبل تعزيز الوعي بالأمن السيبراني (١٠ عبارات). أمّا بالنسبة لعيّنة الدراسة الطبقيَّة القصديَّة العشوائيَّة فتكوَّنت من ٢٦٩ طالبًا وطالبةً، وقد طُبّقت عليهم الدراسة في العام الجامعي ٢٠٢٢/٢٠٢١م. وأظهرت نتائج الدراسة أنّ مستوى الوعي بالأمن السيبراني لدى الطلاب والطالبات المعلّمين بوجهٍ عام جاء بدرجة "عالية"؛ إذْ بيّنت النتائج التفصيليَّة أنّهم يملكون درجة "عالية" من الوعي بمفاهيم الأمن السيبراني، وكذلك بتطبيقات الأمن السيبراني. أمّا بخصوص درجة موافقة أفراد العيّنة حول أبرز السبل لتعزيز الأمن السيبراني لدى الطلاب والطالبات فجاءت بدرجة "موافق". وخلُصت الدراسة بتقديم عدّة توصيات أبرزها تنظيم كلية التربية لدورات تدريبية وتثقيفية متخصّصة في مجال الأمن السيبراني في كل فصل دراسي، وإعداد ونشر أو توزيع الملصقات والكتيّبات والنشرات التوعويَّة في أروقة مبنى الكلية.

(١٤) دراسة فرج (٢٠٢٢): سَعَتْ إلى تبيان وتحديد الدواعي الخاصة بتعزيز ثقافة الأمن السيبراني في ظل التحوّل الرقميّ بجامعة الأمير سطام بن عبد العزيز في المملكة العربية السعودية من وجهة نظر أعضاء هيئة التدريس، هذا بالإضافة إلى الكشف عمّا إذا كانت هناك فروق ذات دلالة إحصائية في آراء وتصوّرات أفراد العيّنة وفقًا لمتغيرات: الكلية، الرُتبة العلمية، وسنوات الخبرة. وقد اعتمدت الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ باعتبارها المنهجيّة البحثيَّة العلميَّة المنوط بها تحقيق أهدافها، واستعانت بأداة الاستبانة لجمع البيانات، وَتكوَّن المقياس – بعد التأكُّد من صدقه وثباته – من ٢٦ عبارة موزّعة على ثلاثة مجالات حول دواعي تعزيز الأمن السيبراني هي: الدواعي المعرفية (٩ فقرات)، الدواعي التقنية/الفنية (٩ عبارات)، والدواعي المجتمعية/الوطنية (٨ فقرات). أمّا بالنسبة لعيّنتها الطبقيَّة العمديَّة فتكوّنت من ١٢٥ عضوًا من أعضاء هيئة التدريس، جرى اختيارهم بالطريقة العشوائيَّة البسيطة، وطُبّقت عليهم الدراسة خلال الفصل الدراسي الأول من العام الأكاديميّ ٢٠٢٢/٢٠٢٣م. وأشارت نتائج الدراسة إلى أنّ درجة موافقة المشاركين نحو دواعي تعزيز ثقافة الأمن السيبراني في ظل التحوّل الرقميّ بالجامعة بوجهٍ عام جاءت بدرجة "متوسّطة" (م = 3.55)؛ إذْ بيّنت النتائج التفصيليَّة حصول محور الدواعي المجتمعية/الوطنية على درجة موافقة "مرتفعة/كبيرة" (م = 3.70)، أمّا محور الدواعي المعرفية فحصلت على درجة موافقة "متوسّطة" (م = 3.51)، وكذلك هو الحال بالنسبة لمحور الدواعي التقنية/الفنية فقد حصلت على درجة موافقة "متوسّطة" (م = 3.46) أيضًا. كما توصّلت النتائج إلى غياب وجود اختلافات دالَّة إحصائيًّا تبعًا لمتغيّرَيْ الكلية والرُتبة العلمية، بينما وُجدت هذه الفروق وفقًا لمتغيّر سنوات الخبرة المهنية وجاءت لصالح فئة "أقل من ٥ سنوات"، لأنّهم يملكون من الكفاءة والمستوى في المعرفة والمهارات والكفايات والخبرات التكنولوجية الرقمية المتقدّمة ما يساعدهم على ويُمكّنهم من تعزيز الأمن السيبراني خلال فترة التحوّل الرقمي. وخلُصت الدراسة بتقديم عدّة توصيات من أبرزها ضرورة رفع مستوى الوعي بالأمن السيبراني بين الطلاب والطالبات، وفهم فوائد البرمجيّات المُتاحة لمكافحة المخاطر والهجمات السيبرانية، وتصميم حملات توعية حول هذه المخاطر والتهديدات.

(١٥) دراسة صفر (٢٠٢٤): استهدفت قياس مستوى وعي طالبات كلية التربية بجامعة الكويت – معلّمات قبل الخدمة – بالأمن السيبراني، هذا بالإضافة إلى الكشف عن أثر متغيّرات نوع التخصُّص، ودورات الأمن السيبراني، ومستوى الـ ICT في آرائهنّ وتصوّراتهنّ حيال مستوى

وعيهنّ هذا. تبنّتْ الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ لتحقيق أهدافها، واستخدمت الاستبانة أداةً لجمع البيانات، وضَمّتْ في صيغتها الأخيرة – بعد التأكُّد من صدقها وثباتها – ٤٧ عبارة، وبخصوص عيّنتها الطبقيَّة القصديَّة فتألّفتْ من ٤٦٤ معلّمةً قبل الخدمة، جرى اختيارهنّ بالطريقة العشوائيَّة البسيطة خلال الفصل الدراسي الأول والثاني من العام الجامعيّ ٢٠٢٢/٢٠٢٣م. وأشارت نتائج الدراسة إلى أنّ مستوى وعي معلّمات قبل الخدمة في كلية التربية بجامعة الكويت نحو الأمن السيبراني بوجهٍ عام جاء بدرجة "مرتفعة جدًّا"؛ حيث كشفتْ النتائج التفصيليَّة أنّ مستوى وعي معظم المعلّمات كان "مرتفعًا جدًّا" في الغالبية العظمى من العبارات في المقياس (٣٩ عبارة)، بينما كان مستوى وعيهنّ في الباقي من العبارات في المقياس (٨ عبارات) "مرتفعًا". وأكّدت النتائج كذلك عدم وجود فروق دالَّة إحصائيًّا بين متوسّطات استجابات المشاركات بشأن آرائهنّ وتصوّراتهنّ (اتّجاهاتهنّ) فيما يتعلّق بمستوى وعيهنّ بالأمن السيبراني يُمكن عزوها لمتغيّرَيْ نوع التخصُّص (أدبي، علمي)، ومستوى الـ ICT (مبتدئة، ملمّة/متوسّطة، محترفة/متقدّمة)، وذلك في الأداة بوجهٍ عام. بينما وُجِدَتْ هذه الاختلافات ذات الدلالة الإحصائية بين متوسّطات استجابات معلّمات قبل الخدمة في المقياس بشكلٍ عام، بما يخص متغيّر دورات الأمن السيبراني (التحقت، لم تلتحق)؛ وكانت هذه الفروق لصالح معلّمات قبل الخدمة اللّواتي الْتَحَقْنَ بدورات سابقة في مجال الأمن السيبراني. وخلُصت الدراسة بتقديم مجموعة من التوصيات أبرزها لزوم توفير التدريب والتوعية المستمرّة لأعضاء الهيئة التعليميَّة بشأن الأمن السيبراني وتهديداته وأخطاره، وضرورة تضمين مبحث الأمن السيبراني ومواضيعه المتعدّدة كجزء من المناهج الدراسية في المدارس والجامعات.

التعقيب على الدراسات السابقة:

تماثلت الدراسة الحالية مع الدراسات السابقة في موضوعها البحثي، إذْ تناولتْ قياس أو تقييم مستوى وعي المعلّمين والمعلّمات – قبل الخدمة وأثناء الخدمة – في المؤسّسات التربوية التعليميَّة بالأمن السيبراني. إضافةً إلى وجود تطابق بين الدراسة الراهنة وجموع الدراسات السابقة في المنهجيَّة البحثيَّة العلميَّة المُستخدمة – منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ؛ وأيضًا في أداة الدراسة المُعتمدة – الاستبانة – بقصد استطلاع رأي المشاركين وجمع البيانات المُرتبطة بموضوع البحث. وعلاوةً على التوافق في العيّنة الطبقيَّة التي تمَّ اختيارها بطريقة

عشوائيَّة بسيطة – معلّمي ومعلّمات قبل الخدمة وأعضاء الهيئة التعليمية في المدارس والجامعات. إنّ هذه الدراسة البحثيَّة تُضاف إلى جموع البحوث السابقة في هذا المجال، وتُسهم في توسيع المعرفة إزاء هذا المبحث الحيويّ في هذا العصر المعرفيّ الرقميّ.

وتفرّدت الدراسة الحالية عن سابقاتها بأنّها طُبِّقَتْ بعد مرور فترة زمنية كافية على جائحة فيروس كورونا (COVID-19) التي تسبّبت في إحداث نقلة نوعيَّة في النظام التربوي، واقتضت دمج وتوظيف وسائل وأدوات وتطبيقات ومنصّات وشبكات وخدمات تكنولوجيا المعلومات والاتّصالات في التعليم والتعلّم للوصول إلى التحوّل الرقميّ. هذا بالإضافة إلى أنّها تميّزت بكونها دراسة طوليَّة (Longitudinal Study)؛ إذْ تمَّ جمع بياناتها بكل حرص ودقّة على مدى فَصْلَيْن دراسِيَّيْن مُتَتالِيَيْن (الأول، والثاني) من العام الأكاديمي ٢٠٢٣/٢٠٢٤م؛ وفي الدراسة الطوليَّة، يقوم الباحث بفحص وتقصّي أفراد العيّنة أنفسهم بشكل مُتكرّر بُغية اكتشاف أيّ تغيّرات قد تحدث خلال حقبة من الزمن. وكذلك تميّزت الدراسة الحالية عن الدراسات المُماثلة السابقة بأنَّ أداتها المُستخدمة لجمع البيانات – الاستبانة – كانت أكثر عُمْقًا وشُمولِيَّةً؛ إذْ احتوتْ في صورتها النهائية على ٤٧ فقرة أو عبارة مُرْتَبِطَةً ارتباطًا وثيقًا بموضوع البحث.

أدبيّات الدراسة

مفهوم الأمن السيبراني وماهيّته

الأمن السيبراني يُشير إلى مجموعة الإجراءات والتدابير التي تتّخذها الأفراد والشركات والحكومات والمؤسّسات لحماية الأنظمة الحاسوبية والشبكات والبرامج والبيانات من التهديدات السيبرانية والهجمات الإلكترونية. يهدف الأمن السيبراني إلى ضمان سلامة وسريّة البيانات والمعلومات، وحماية الأنظمة من الاختراق والتلف، وضمان استمرارية الخدمات الرقمية والعمليات الحيوية. يتضمّن مفهوم الأمن السيبراني العديد من الجوانب والمبادئ، بما في ذلك (ابن إبراهيم، ٢٠٢١؛ التيماني، ٢٠٢١؛ الحبيّب، ٢٠٢٢؛ الداغر، ٢٠٢١؛ الزبيدي وآخرون، ٢٠٢١؛ السواط وآخرون، ٢٠٢٠؛ الشهري، ٢٠٢١؛ الصانع وآخرون، ٢٠٢٠؛ الصحفي وعسكول، ٢٠١٩؛ الظويفري، ٢٠٢١؛ القحطاني، ٢٠١٩؛ المنتشري، ٢٠٢٠؛ المنتشري وحريري، ٢٠٢٠؛ الهيئة الوطنية للأمن السيبراني، ٢٠١٨؛ زقوت وآخرون، ٢٠٢٢؛ صائغ، ٢٠١٨؛ فرج، ٢٠٢٢؛ فوزي، ٢٠١٩؛ قطب وحلبي، ٢٠٢١) (Bamford, 2009;

Canongia & Mandarino, 2014; ENISA, 2021, 2022; National Institute of Standards and Technology [NIST], 2020; Schneier, 2015; Singer & Friedman, 2014):

(١) الحماية من الاختراق: يتعلّق بتأمين الأنظمة الحاسوبية والشبكات والبرمجيّات من الاختراق والوصول غير المصرّح به. يتضمّن ذلك تطبيق تقنيات التشفير ونظم المصادقة وإدارة الوصول للحد من فرص الاختراق واستغلال الثغرات الأمنية.

(٢) الكشف والاستجابة: يتعلّق بالقدرة على اكتشاف الهجمات السيبرانية والتهديدات المُحتملة واستجابة فعّالة لها. يتضمّن ذلك استخدام أنظمة الكشف عن التسلّل (Intrusion Detection Systems) والتحليل الأمني وتقنيات الرصد المستمر لتحديد الأنشطة غير المشروعة والتعامل معها بشكل سريع وفعّال.

(٣) إدارة المخاطر: يتعلّق بتحليل وتقييم المخاطر السيبرانية المُحتملة وتطبيق استراتيجيّات للتعامل معها. يشمل ذلك وضع سياسات وإجراءات أمنية قويّة، وتطبيق مُمارسات أمنية متقدّمة، وتدريب الموظفين على التعرّف على التهديدات والتصرّف بشكل مناسب.

(٤) التوعية والتدريب: يتعلّق برفع الوعي بأهميّة الأمن السيبراني وتوعية الأفراد والموظفين بالمخاطر السيبرانية وكيفية الحماية منها. يشمل ذلك توفير التدريب والتعليم المستمر، وإشراك الجمهور في حملات توعية وتثقيف حول مُمارسات الأمان السيبراني.

(٥) التعاون الدولي وتبادل الخبرات والمعرفة: يُعتبر التعاون الدولي وتبادل الخبرات والمعرفة أمرًا حاسمًا في مجال الأمن السيبراني. يتطلّب التصدّي للتهديدات السيبرانية التعاون بين الدول والمؤسّسات لتبادل البيانات والمعلومات والآراء والخبرات والتجارب وتطوير القدرات الأمنية المشتركة.

باختصار، يهدف الأمن السيبراني إلى حماية الأنظمة والبيانات الرقمية من التهديدات السيبرانية والحفاظ على سلامة وخصوصيّة البيانات والمعلومات. يُعتبر جزءًا أساسيًّا من التكنولوجيا الحديثة ويُسهم في ضمان استقرار العالم الرقمي وتعزيز الثقة والأمان في استخدام التقنيات الرقمية.

أهميّة الأمن السيبراني

الأمن السيبراني أصبح أمرًا حاسمًا بالغ الأهمِّيَّة في عالمنا الرقمي المتطوّر. يتعلّق الأمر بحماية الأنظمة الإلكترونية والشبكات من التهديدات والهجمات السيبرانية. يُعد الأمن السيبراني ضروريًّا للحفاظ على الخصوصية والسلامة والأمان الإلكتروني للأفراد والشركات والمؤسّسات والحكومات. إليكم أهميّة الأمن السيبراني (ابن إبراهيم، ٢٠٢١؛ الصحفي وعسكول، ٢٠١٩؛ المنتشري وحريري، ٢٠٢٠؛ حمدان، ٢٠٢١؛ زقوت وآخرون، ٢٠٢٢) (Anderson, 2020; Calder, 2020; Furnell, 2003; Furnell & Dowling, 2019; Furnell & Moore, 2014; Hibberd, 2022; Lewis, 2020; Schneier, 2015; Singer & Friedman, 2014):

(١) حماية البيانات الحسّاسة: يلعب الأمن السيبراني دورًا حاسمًا في حماية البيانات الحسّاسة والمعلومات السرية في عالم يتزايد فيه التبادل الرقمي للبيانات والمعلومات. فقد تؤدّي فقدان أو سرقة هذه البيانات إلى تبعات خطيرة، بما في ذلك الاستغلال الاحتيالي والتجسّس الصناعي والتأثير على الحياة الشخصية والمالية للأفراد والشركات والحكومات.

(٢) حماية البُنية التحتية الحيوية: تشمل البُنية التحتية الحيوية الأنظمة المهمّة مثل الشبكات الكهربائية والماء والطاقة والنقل والاتّصالات والتعليم. يحمي الأمن السيبراني هذه البُنية التحتية من الاختراق والتعطيل، ممّا يُسهم في ضمان استمرارية الخدمات الأساسية وحماية الحياة العامة والاقتصاد.

(٣) الدفاع عن الأمن القومي: يتعلّق الأمن السيبراني بالأمن القومي والدفاع عن الدولة. تُشكّل الهجمات السيبرانية تهديدًا جديًّا للأمن القومي، حيث يُمكن للمهاجمين تعطيل الخدمات الحكومية الحيوية وسرقة البيانات والمعلومات الحسّاسة والتأثير سلبًا على البُنية التحتية الحيوية الخدماتية والاقتصادية والعسكرية للدولة.

(٤) حماية المؤسّسات والشركات: تعتمد الشركات والمؤسّسات بشكل كبير على الأنظمة الإلكترونية والشبكات الحاسوبية لتنفيذ عمليّاتها اليومية وتبادل البيانات والمعلومات. يحمي الأمن السيبراني هذه المؤسّسات والشركات من فقدان البيانات والمعلومات والتلاعب بها وتعطيل الخدمات بسبب التهديدات السيبرانية المستمرّة، ممّا يُساعد في الحفاظ على سمعتها وثقة العملاء.

(٥) تعزيز الثقة الرقمية: يُساهم الأمن السيبراني في بناء الثقة الرقمية بين المستخدمين والمؤسّسات والحكومات. عندما يكون هناك ثقة في أمان الأنظمة الإلكترونية، يُمكن للأفراد والمؤسّسات والحكومات اتّخاذ خطوات مُبتكرة في العالم الرقمي والاستفادة الكاملة من فوائده؛ ممّا يُسهم في دعم التطوّر المُستدام للاقتصاد الرقمي.

بشكل عام، يُساهم الأمن السيبراني في الحفاظ على استقرار العالم الرقمي وحماية المستخدمين والمؤسّسات من التهديدات السيبرانية المتزايدة. إنّه جزء أساسي من التكنولوجيا الحديثة ويُعزّز الثقة والأمان في استخدام الأنظمة الرقمية.

أهداف الأمن السيبراني

الأمن السيبراني يُشير إلى مجموعة من التدابير والإجراءات المُتّخذة لحماية أنظمة البيانات والمعلومات والشبكات الإلكترونية من التهديدات السيبرانية. وتتمَحْوَر أهداف الأمن السيبراني حول حماية البيانات والمعلومات الحسّاسة وضمان استمراريّة الأعمال في وجه التهديدات الإلكترونية. فيما يلي نظرة شاملة عن أهم أهداف الأمن السيبراني (الحبيّب، ٢٠٢٢؛ الشهري، ٢٠٢١؛ العقلاء وعلي، ٢٠٢٢؛ المنتشري، ٢٠٢٠؛ المنتشري وحريري، ٢٠٢٠؛ زقوت وآخرون، ٢٠٢٢؛ صائغ، ٢٠١٨) (Anderson, 2020; Cisco, 2022, 2023a, 2023b; ENISA, 2021, 2022; European Commission, & High Representative of the Union for Foreign Affairs and Security Policy, 2020; Furnell & Moore, 2014; Hibberd, 2022; International Organization for Standardization [ISO], 2022, 2023; NIST, 2020; OSCE, 2107, 2023; Schneier, 2015; Singer & Friedman, 2014; U.S. Department of Homeland Security [U.S. DHS], 2013; World Bank Group, 2019):

(١) حماية البيانات والمعلومات: أحد أهم أهداف الأمن السيبراني هو حماية البيانات والمعلومات الحسّاسة. تُعتبر البيانات الحسّاسة مثل المعلومات الشخصية والمالية والتجارية والحكومية هدفًا للقراصنة والهاكرز والمجرمين الإلكترونيّين. يجب توفير الحماية اللازمة لهذه البيانات والمعلومات لمنع الوصول غير المُصرّح به والاستخدام غير القانوني. تشمل الإجراءات المهمّة لحماية البيانات والمعلومات التشفير، وتقييد الوصول بواسطة طبقات من الحماية ونظم المصادقة الثنائيَّة، وتطبيق السياسات الأمنية المناسبة.

(٢) ضمان سلامة الأنظمة والشبكات: تُعد سلامة الأنظمة والشبكات الإلكترونية أحد الأهداف الرئيسية للأمن السيبراني. يهدف الأمن السيبراني إلى حماية الأنظمة والشبكات من الهجمات والاختراقات الإلكترونية التي يُمكن أنْ تتسبّب في تعطيل الخدمات أو سرقة البيانات والمعلومات الحسّاسة. يجب اتّخاذ إجراءات مثل تطبيق الجدران النارية، وتحديث البرامج الأمنية بانتظام، واستخدام أنظمة الكشف عن التسلّل للحفاظ على سلامة الأنظمة والشبكات.

(٣) حماية البُنية التحتيّة الحيوية: تستهدف استراتيجيّات الأمن السيبراني حماية البُنية التحتيّة الحيوية التي تشمل محطات الطاقة والشبكات الكهربائية والمرافق الحيوية الأخرى. يُمكن لهجمات القرصنة الموجّهة لهذه البُنية التحتيّة أنْ تؤدّي إلى انقطاع التيار الكهربائي أو تعطيل الخدمات الحيوية الأخرى. يجب تطبيق الحماية السيبرانية المتقدّمة على هذه البُنى التحتيّة لمنع واستدامة أي هجمات مُحتملة.

(٤) التصدّي للتهديدات النشطة: تهدف جهود الأمن السيبراني إلى التصدّي للتهديدات النشطة مثل هجمات القرصنة والبرمجيّات الخبيثة والاحتيال الإلكتروني. القراصنة والمجرمون الإلكترونيّون والدول الأعداء والمنافسون يُشكّلون تهديدًا مُحتملًا للأنظمة السيبرانية. يجب توفير أنظمة الكشف المُبكّر والاستجابة السريعة وتحديثات الأمان المستمرّة للحد من هذه التهديدات وتقليل الأضرار المُحتملة.

(٥) تعزيز الوعي والتثقيف السيبراني: تهدف جهود الأمن السيبراني أيضًا إلى تعزيز الوعي والتثقيف السيبراني لدى المستخدمين. يُعتبر التوعية بمفاهيم الأمان السيبراني ومُمارساته الجيّدة مهّمًا للغاية في الحد من المخاطر والهجمات. يجب توفير التدريب والتثقيف المستمر للمستخدمين للتعرّف على التهديدات الحديثة وكيفيّة التعامل معها بشكل آمن.

باختصار، تهدف استراتيجيات الأمن السيبراني إلى حماية الأنظمة الرقمية والبيانات والمعلومات الحسّاسة وضمان سلامة العمليّات الحاسوبية. من خلال تحقيق هذه الأهداف، يُمكن للحكومات والمؤسّسات والشركات والأفراد الاستمرار في الاعتماد على التقنية الرقمية بثقة وتجنّب الأضرار المُحتملة الناجمة عن التهديدات السيبرانية.

الجرائم الإلكترونية في الفضاء السيبراني (الجرائم السيبرانية)

في عصرنا الحالي، يُشكّل العالم الرقمي جزءًا حيويًّا من حياة الناس وعملهم. مع التقدّم التكنولوجي واعتمادنا في الكثير من جوانب حياتنا على الاتّصال والتفاعل الرقمي باستخدام

وسائل تكنولوجيا المعلومات والاتّصالات، ظهرتْ جرائم ومخاطر سيبرانية جديدة ومُعقّدة ولا حدود لها تُشكّل تحدّيًا كبيرًا في عصر التكنولوجيا الحديثة، وتُهدّد الأفراد والمجتمعات والشركات والمؤسّسات الحكومية على حد سواء في جميع أنحاء العالم. تُشير الجرائم والمخاطر السيبرانية إلى الأنشطة الضارة (مثل التهديدات، والاختراقات) التي يقوم بها المهاجمون الإلكترونيّون ويستهدفون بها الأنظمة الرقمية والشبكات والبيانات للاستيلاء على البيانات والمعلومات الحسّاسة والسرية أو التلاعب بها أو تعطيل الأنظمة والشبكات الإلكترونية. يُمكن لمُرتكبي هذه الجرائم وضحاياهم أنْ يتواجدوا في مناطق مختلفة، ممّا يُبْرز الحاجة الماسَّة إلى وضع استجابة عاجلة وديناميكيَّة ودوليَّة بشأنها (العنزي، ٢٠٢١؛ اللصاصمة والمجالي، ٢٠٢٢) (United Nations Office on Drugs and Crime, 2024).

سمات المجرم السيبراني

إنّ مرتكبي الجرائم السيبرانية لهم من الصفات والدوافع ما يُميّزهم عن غيرهم من الجُناة. لقد تنوّعت الدراسات الأدبية التي تُحدّد خصائص وسمات المجرم السيبراني وشخصيّته ومدى جسامة جُرمه كأساس تبرير وتقدير العقوبة؛ وفيما يلي نستعرض لكم بعض أبرز هذه السمات (العنزي، ٢٠٢١؛ حمدان، ٢٠٢١) (Schneier, 2015; Singer & Friedman, 2014):

(١) مجرم ذو مهارات تقنية عالية: يتّصف المجرم السيبراني بأنّه ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في تشغيل الحاسوب، وباللغة المستخدمة في تخزين البيانات والمعلومات وكيفية استدعائها، وقادر على استخدام هذا التكتيك لاختراق الرمز (الكود) السرّي والمساس بالبيانات والمعلومات المخزّنة أو زرع الفيروس أو محو أو إدخال بيانات ومعلومات تؤدّي إلى إتلاف ما هو موجود.

(٢) مجرم ذكي: فالمجرم السيبراني يتمتّع بذكاء غير عادي ذلك نظرًا لقدراته العالية على ارتكاب الجريمة ضد نظام/أنظمة البيانات والمعلومات وإتلاف الحاسوب/الحواسيب أو الدعائم المُمغنطة عن طريق استخدام تقنيات التدمير الناعمة. ولذا، فإنّه من الصعب مُلاحقته وتتبّع أفعاله الإجرامية.

(٣) مجرم متخصّص: فالمجرم السيبراني يتمتّع بمهارات تقنية استثنائية، إذْ يستخدم مداركه ومهاراته وقدراته التقنية العالية لاختراق الشبكات وكسر الشفرات وكلمات المرور، بهدف الحصول على البيانات والمعلومات الثمينة المُخزّنة على أجهزة الحواسيب عبر الشبكات.

(٤) مجرم محترف: يستغل المجرم السيبراني خبراته وقدراته الاحترافية ومهاراته التقنية المتقّدمة في الاختراق وانتهاك حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال، ويُشكّل تهديدًا مباشرًا للأنشطة والمصالح عبر شبكة الإنترنت.

(٥) مجرم متميّز: فالمجرم السيبراني يظل مستمرًّا في ارتكاب أعماله الإجرامية بشكل دائم.

دوافع ارتكاب الجرائم السيبرانية

أشارت الدراسات البحثيَّة السيكولوجية إلى أنّ معظم المجرمين السيبرانيّين ينتمون إلى فئات اجتماعية مثقّفة ومتعلّمة، ورُغم أنّ الدوافع التي تحرّكهم لارتكاب الجرائم السيبرانية لا تتأثّر بالهدف أو الغاية التي تقف وراء الجريمة، فهؤلاء الأشخاص يتحرّكون بدوافع مختلفة ومتعدّدة لارتكاب هذه الأفعال أو الأعمال الإجرامية في الفضاء السيبراني؛ نسرد فيما يلي بعضًا منها (العنزي، ٢٠٢١؛ اللصاصمة والمجالي، ٢٠٢٢؛ حمدان، ٢٠٢١؛ قطب وحلبي، ٢٠٢١) (Schneier, 2015; Singer & Friedman, 2014):

(١) من أجل التسلية والمزاح مع الآخرين دون أنْ يكون لديهم قصد أو نيّة فعلية بإلحاق الأذى أو الضرر أو الخسائر بأي شخص، ومن الأمثلة على ذلك فئة صغار المجرمين السيبرانيّين، ويُطلق عليهم اسم "المهاجمون العابرون" (Script Kiddies)، ويُمكن أنْ يكونوا غير متخصّصين تقنيًّا، ويعتمدون على أدوات وبرمجيّات مُطوّرة من قبل مجرمين محترفين لتنفيذ هجمات بسيطة دون فهم كامل للتأثيرات الحقيقية لأفعالهم.

(٢) رغبة في إثبات القدرة على اختراق الأنظمة والشبكات تنبع من فضول الشخص وتَوْقِهِ في اكتساب المعرفة والخبرة وتطوير مهاراته الشخصية (إثبات الذات).

(٣) تسبّب الضرر للأفراد دون الاستفادة المالية هو هدف لعدد كبير من مُبتكري فيروسات الحاسوب والمُسوّقين أو الموزّعين لها عبر الإنترنت.

(٤) السعي للربح وتكبيد خسائر كبيرة للضحية، حيث يكون الغرض من ذلك حل مشاكل مالية تواجه الشخص الذي يقوم بالجريمة.

(٥) التهديد والانتقام: استخدام التهديد والابتزاز لإجبار شخص على فعل أمر معيّن أو منعه من القيام به، وقد يشمل هذا الانتقام الأفراد العاملين في المؤسّسات والشركات التجارية أو حتى أصحاب العمل، ويُمكن أنْ يتسبّب في إلحاق الضرر بهم من قبل العاملين داخل تلك المنشآت.

(٦) الدوافع السياسية: تُعتبر الدوافع السياسية أحد أبرز الأسباب وراء محاولات اختراق الشبكات الحكومية في عدّة دول حول العالم، حيث يُمكن للأفراد أيضًا أنْ يتسلّلوا إلى الأجهزة الأمنية التابعة للحكومة. تحمل شبكة الإنترنت أخبارًا وبيانات ومعلومات ذات أهميّة قُصوى لأمن الدولة، إلى جانب وجود حالات سب، قذف، طعن، استهزاء، وانتقاد لرموز دوليَّة والنظام الحاكم، ممّا يُمثّل تحدّيات أمنية كبيرة.

(٧) الدوافع الإرهابية: نعم، الإرهاب السيبراني أصبح تهديدًا خطيرًا يواجه العالم اليوم. فالجماعات الإرهابية استغلت شبكة الإنترنت وخدماته المختلفة التي توفّرها كوسيلة لتوجيه التحريض ونشر الأفكار الإرهابية، بالإضافة إلى تبادل البيانات والمعلومات حول صناعة الأسلحة والتكتيكات الإرهابية. يقومون أيضاً بشن هجمات إلكترونية تستهدف البُنية التحتية الحيويّة والبيانات والمعلومات الحسّاسة والسرية، ممّا يزيد من تأثيراتهم الخطيرة على الأمن العام والسلام العالمي.

خصائص الجرائم السيبرانية

تتميّز الجرائم السيبرانية بعدّة خصائص أو سمات، ومنها أنّها (العنزي، ٢٠٢١؛ حمدان، ٢٠٢١؛ صائغ، ٢٠١٨، ص ص. ٤٠-٤٣):

(١) جرائم بالغة الخطورة: لأنّ حجم الخسائر والأضرار التي تنشئها/تخلقها كبير وجسيم غير قابلة للقياس؛ فهي تمسُّ وتُؤثّرُ على أفكار الأفراد وحياتهم الشخصية، وتُهدّد المؤسّسات والشركات والأفراد في اقتصادها، كما أنّها توعد أمن البلاد على الصُعد القومية والسياسية والاقتصادية والاجتماعية والثقافية.

(٢) جرائم عالمية عابرة الحدود (عن بُعد): كونها جرائمًا لا تتقيّد بحدود زمانية (توقيت زمني) أو مكانية، فإنّها لم تعد مقتصرة على إقليم محدّد، بل هي عالمية وعابرة للحدود (تمتاز بالتباعد الجغرافي). يُمكن الآن ارتكاب الجرائم في دول مختلفة أو أنْ يُنفّذ الجاني جريمته وهو متواجدًا في بلد والضحية مقيمًا في بلد آخر. ولذا، تحتاج القوانين إلى أنْ تأخذ طابعًا عالميًّا نظرًا للضرورة المُلِحّة لتكييفها مع التحدّيات العابرة للحدود والقضايا التي تتجاوز السيادة الوطنية.

(٣) جرائم تُرتكب بواسطة الأجهزة الإلكترونية: لأنّها تُنفّذ من خلال استخدام الحواسيب والأجهزة اللوحية والهواتف الخلوية الذكية، إذْ تُعتبر هذه الأدوات وسائل تُمكّن المجرم السيبراني من الولوج إلى شبكة الإنترنت لتنفيذ جريمته/جرائمه.

(٤) جرائم ناعمة: كونها تختلف عن الجرائم التقليدية بعدم استخدام الأدوات والعنف والقوة والبطش والقتل والعمليات الإرهابية والسطو المسلّح وغيرها؛ أو أنّها ذات عنف وجهد أقل من الجرائم التقليدية.

(٥) جرائم سريعة التنفيذ: لأنّ تنفيذها سريع ولا يتطلّب الوقت الكثير، بل يستغرق ارتكابها دقائق وأحيانًا ثواني معدودة بكبسة زر واحدة على لوحة المفاتيح، كما أنّها قد لا تتطلّب أو تحتاج التخطيط المُسبق أو الإعداد قبل التنفيذ أو استخدام معدّات وبرمجيّات معيّنة.

(٦) جرائم خفيّة: لأنّه ليس بالأمر السهل اكتشافها نظرًا لضعف القدرات التقنية/الفنية للضحية مقارنةً بالمجرم، وأحيانًا بسبب المهارات التقنية/الفنية والعلمية الاحترافية والمتقدّمة التي يتمتّع بها الجاني لإخفاء الجريمة، أو ربّما يكون الضحية خائفًا من الإبلاغ عن الجريمة خوفًا من تشويه سمعته. وهذه الجرائم تكون جاذبة لأنّها لا تترك آثارًا واضحة، ممّا يجعل من الصعب التنبّؤ بحدوثها، وباستطاعة الجُناة اختراق الشبكات، وتغيير مسارها، والتلاعب بها، وسرقة بياناتها.

(٧) جرائم غامضة وصعبة التتبّع والإثبات: نظرًا لأنّها تتطلّب الاستعانة بخبرات ومهارات تقنية/فنية احترافية متقدّمة (عالية المستوى)، وتكون صعبة التتبّع والإثبات، ويختلف عملية التحقيق فيها تمامًا عن التحقيق في الجرائم التقليدية. هذا بالإضافة إلى أنّ مرتكبو هذه الجرائم يتمتّعون بذكاء عالي، فهم لا يتركون أثرًا واضحًا، ممّا يجعل من الصعب تتبّعهم وتعقّبهم والقبض عليهم بسبب التنوّع في المواقع بين دول مختلفة، واختلاف التوقيتات بين هذه الدول أيضًا، وكذلك بسبب سهولة إخفاء آثار الجريمة/الجرائم والأدِلّة التي تُشير إلى الجاني بفضل التشفير والترميز الذي يُطبّق على البيانات والمعلومات المُخزّنة، ممّا يجعل من الصعب كشف مرتكب الجريمة إلا باستخدام أساليب أمنية وتقنية ذات جودة عالية.

(٨) جرائم سهلة: يُمكن أنْ تُرتكب أو تُنفّذ بسهولة، وتتطلّب موارد قليلة فيما يتعلّق بالأضرار أو الخسائر الجسيمة التي يُمكن أنْ تُسبّبها، ويكون من السهولة أنْ تقع الضحية في هذه الجرائم، وقد لا يتم اكتشافها إلا بعد مرور فترة زمنية طويلة.

أنواع الجرائم السيبرانية

فيما يلي سنستكشف بعض أبرز أنواع الجرائم والمخاطر السيبرانية الشائعة التي قد تواجهنا وتأثيرها على المجتمعات الحديثة، ونذكر منها الآتي (الحبيّب، ٢٠٢٢؛ الصحفي وعسكول، ٢٠١٩؛ العنزي، ٢٠٢١؛ اللصاصمة والمجالي، ٢٠٢٢؛ المنتشري، ٢٠٢٠؛ المنتشري وحريري، ٢٠٢٠؛ بانقا، ٢٠١٩؛ حمدان، ٢٠٢١؛ زقوت وآخرون، ٢٠٢٢؛ صائغ، ٢٠١٨) (Bamford, 2009; Hadnagy & Fincher, 2015; Jakobsson & Myers, 2007; Li et al., 2018; Mitnick & Simon, 2012; OpenAI, 2024; Peltier, 2014; Russinovich, 2012; Schneier, 2015; Singer & Friedman, 2014; Vasani et al., 2023):

(١) الاختراقات السيبرانية (Hacking): يتعرّض الأنظمة الإلكترونية والشبكات الرقمية والتطبيقات لخطر الاختراقات الهجومية من قبل قراصنة الإنترنت والمهاجمين الذين يستخدمون تقنيات وأدوات مختلفة للوصول إلى البيانات والمعلومات الحسّاسة والسرية أو التلاعب بها أو سرقتها أو تعطيل الخدمات. يعتمد المهاجمون على الثغرات الأمنية في البرامج والنظم للدخول بشكل غير مصرّح به. يُمكن للهجمات الاستغلالية أنْ تتسبّب في تسريب البيانات والمعلومات الشخصية أو الأسرار التجارية أو البيانات الحكومية.

(٢) البرمجيّات الخبيثة (Malware): تُعد البرمجيّات الخبيثة (مثل الفيروسات، وأحصنة طروادة، وبرامج التجسّس) تهديدًا خطيرًا، فهي برامج تهدف إلى التسبّب في ضرر للأنظمة الإلكترونية والشبكات والبيانات. يتمْ تطوير البرمجيّات الخبيثة لأغراض مختلفة مثل سرقة البيانات والمعلومات الشخصية أو تعطيل النظام/الأنظمة أو طلب فدية من المستخدمين أو الجهات المعنيّة. قدْ تأتي البرمجيّات الخبيثة على شكل برامج تجسّس أو برامج العروض الترويجية أو برامج ضارة أخرى. تنتشر هذه البرمجيّات عادةً من خلال ملفّات مصابة أو رسائل البريد الإلكتروني الاحتيالية، وتستهدف تلك البرامج الضعف في الأنظمة والشبكات وتتسبّب في تلف البيانات والمعلومات والتطبيقات والأجهزة أو اختراق الخصوصية.

(٣) الاحتيال الإلكتروني (Phishing): الاحتيال أو التصيّد أو الخداع الإلكتروني يشمل الأنشطة التي يقوم بها المهاجمون للتلاعب بالبيانات والمعلومات الحسّاسة والسرية والحصول على مكاسب غير مشروعة. يشمل ذلك احتيال الهويّة، والتصيّد الاحتيالي (Phishing)،

والتلاعب بالمدفوعات الإلكترونية. يتمّ استخدام التقنيات الاجتماعية لخداع الأفراد والشركات والمؤسّسات الحكومية وإقناعهم بتقديم البيانات والمعلومات الشخصية أو المالية.

(٤) هجمات الحرمان من الخدمة (Distributed Denial-of-Service – DDoS): تُعتبر هجمات الحرمان من الخدمة تهديدًا شائعًا، حيث يقوم المهاجمون بتعطيل موقع أو خدمة عبر تحميل الخوادم بكمية كبيرة من الطلبات، ممّا يجعلها غير قادرة على التعامل مع الحمولة الزائدة وبالتالي تعطيلها عن المستخدمين الشرعيّين. هذا يُمكن أنْ يسبّب خسائر مالية كبيرة وتأثير سلبي على سمعة الشركات والمؤسّسات والحكومات المُستهدفة.

(٥) التجسّس السيبراني (Cyber Espionage): يتعلّق التجسّس/التنصّت السيبراني أو الإلكتروني باختراق الهدف واستخراج البيانات والمعلومات السرية أو الحسّاسة من الأنظمة الحاسوبية. يهدف المهاجمون إلى الوصول إلى البيانات والمعلومات التجارية أو البحثيَّة أو السياسية أو العسكرية للاستفادة الشخصية أو بيعها للأطراف الثالثة. يُمكن للتجسّس السيبراني أنْ يتسبّب في خسائر مالية هائلة وفقدان الثقة بين الدول والشركات.

(٦) الهجمات على البُنية التحتيّة الحاسوبية الحيويّة (Attacks on Critical Computing Infrastructure): تهدف هجمات البُنية التحتيّة الحاسوبية الحيويّة إلى التلاعب بالأنظمة التحتيّة الحيويّة مثل الشبكات الكهربائية والطاقة والاقتصاد والأنظمة الصحية والنقل والتعليم. قد تتسبّب هذه الهجمات في تعطيل الخدمات العامة وتهديد الأمن العام. على سبيل المثال، يُمكن للهجمات الإلكترومغناطيسية توجيه نبضات كهرومغناطيسية قويّة نحو البُنية التحتيّة الحاسوبية، ممّا يُؤدّي إلى تعطّل الشبكات الكهربائية وانقطاع التيّار الكهربائي للمناطق الواسعة.

(٧) هجمات الفدية (Ransomware): هي هجمات إلكترونية يستخدم فيها القراصنة برمجيّات تهديد الفدية لاختراق أنظمة المعلومات وتشفير الملفّات والبيانات على الأنظمة المُستهدفة، ممّا يجعلها غير قابلة للوصول. بعد التشفير، يُطالب القراصنة ضحاياهم بدفع مبالغ مالية – فدية – (عادة بعملة رقمية مثل البيتكوين Bitcoin) مقابل مفتاح فك التشفير الضروري لاستعادة الملفات والبيانات. هذا النوع من الهجمات شهد انتشارًا متزايدًا في السنوات الأخيرة وأثّر بشكل كبير على الأفراد والشركات والحكومات. تستهدف هذه الهجمات مؤسّسات حكومية وشركات وأفراد على حد سواء، بهدف الحصول على أموال سريعة من خلال ابتزاز الضحايا. إذا تمّ دفع الفدية، يُمكن أنْ يتم تقديم مفتاح فك التشفير، ولكن لا يُمكن ضمان تلبية المهاجمين للمطالب.

التعامل مع هجمات الفدية يتطلّب استراتيجية أمان سيبراني قويّة وعدم دفع الفدية، مع التشجيع على الإبلاغ عن الهجوم للجهات الأمنية المختصّة واستكشاف وسائل أخرى لاستعادة الملفّات والبيانات بدون دفع فدية.

(٨) انتهاك الخصوصيّة (Privacy Violation): يتضمّن انتهاك الخصوصيّة الوصول أو النفاذ غير المصرّح به إلى البيانات والمعلومات الشخصيّة للأفراد، ويُمكن أنْ يؤدّي إلى سرقة الهُويّة، والابتزاز، والاحتيال، والسرقة من الحسابات الإلكترونية، واستخدام البطاقات الائتمانية المملوكة للآخرين، والتنمّر الإلكترونيّ.

(٩) انتهاك المُلكية الفكرية (Intellectual Property Violation): يشمل انتهاك المُلكية الفكرية استخدام أو نسخ الأفكار أو الابتكارات أو الإبداعات التي يمتلكها فرد أو مؤسّسة دون إذن؛ ويتضمّن ذلك العديد من الأصناف مثل القرصنة الإلكترونية، وتعني تزوير وتقليد الأعمال الفنية أو توزيع الملفات المحميّة بحقوق الطبع والنشر بشكل غير مشروع/قانوني، وسرقة الأفكار المحميّة ببراءة اختراع، واستخدام العلامات التجارية دون إذن، واستخدام معلومات وأسرار الشركات التجارية بطرق غير مشروعة/قانونية، وغيرها. هذه المُمارسات تضر بحقوق المُبتكرين وتُقلّل من حوافز الابتكار والإبداع، وتُؤثّر سلبًا على الاقتصاد والتطوّر الثقافي والتكنولوجي.

(١٠) التنمّر الإلكتروني (Cyber Bullying): التنمّر أو الاعتداء الإلكتروني هو استخدام التكنولوجيا الرقمية مثل الإنترنت ووسائل التواصل الاجتماعي للقيام بأعمال تنمّر أو اعتداءات على الآخرين. يشمل ذلك إرسال الرسائل السلبية أو التهديدات أو نشر البيانات والمعلومات الخاصة أو الكذب عن شخص ما دون إذنه، وكذلك التشهير أو استخدام الصور أو الفيديوهات بطريقة مهينة أو مسيئة. يُمكن أنْ يكون التنمّر الإلكتروني عبر الرسائل النصية، وسائل التواصل الاجتماعي، البريد الإلكتروني، وحتى في الألعاب عبر الإنترنت. يُمكن أنْ يكون له تأثيرات نفسية وعاطفية خطيرة على الأفراد المعنيّين، ويُمكن أنْ يؤدّي إلى مشاكل صحية نفسية مثل القلق والاكتئاب وحتى الانعزال الاجتماعي. التنمّر الإلكتروني هو مشكلة عالمية وتتطلّب جهودًا كبيرة للتوعية وتعزيز السلوكيات الإيجابية على الإنترنت ووسائل التواصل الاجتماعي.

(١١) الهندسة الاجتماعية (Social Engineering): وتُعرف بعلم أو فن اختراق العقول، وقد انتشرت بشكل كبير مع زيادة استخدام شبكات التواصل الاجتماعي. تُشير هذه الممارسات إلى مجموعة من الطرق التي يستخدمها المجرمون لاستحصال بيانات ومعلومات حسّاسة وسريّة أو

إقناع الأشخاص باتّخاذ خطوات تؤدّي إلى اختراق أنظمتهم وإتلافها. الهندسة الاجتماعية تُعَدُّ واحدة من أخطر التهديدات السيبرانية، حيث لا تقتصر على الاتّصالات عبر الإنترنت فقط، بل قد تحدث في سياقات الحياة اليومية. يستغل المهاجمون سذاجة الأفراد للحصول على بيانات ومعلومات شخصية، وزادت حالات الهندسة الاجتماعية بشكل كبير مع انتشار واستخدام مواقع التواصل الاجتماعي والبريد الإلكتروني. هؤلاء المهاجمون يستفيدون من البيانات والمعلومات التي ينشرونها مستخدمو هذه المواقع للتلاعب بهم ولإلحاق الضرر بهم بطرق مختلفة.

(١٢) تشويه السمعة (Denigration/Dissing): هذا المفهوم يُعرف بـ "التشهير السيبراني/الإلكتروني (Defamation)"، ويُشير إلى تشويه سمعة الضحية في الفضاء السيبراني، وهو نوع من أنواع الاعتداءات السيبرانية التي تهدف إلى تشويه صورة الشخص أو الجهة المستهدفة عبر نشر بيانات ومعلومات زائفة أو مضلّلة عبر الإنترنت. يتضمّن ذلك نشر الصور المعدّلة بواسطة برامج التعديل الرقمي على منصّات التواصل الاجتماعي أو عبر البريد الإلكتروني بهدف الإضرار بسمعة الشخص المعني وخدمة مصالح المهاجم.

(١٣) الإرجاف الإلكتروني (Destabilization): ويهدف إلى نشر الأخبار المحبطة والمسيئة والشائعات لتحقيق مقاصد معيّنة. يُستخدم هذا النوع من الإرجاف لخلق الفوضى والارتباك وزعزعة الاستقرار والثقة لدى الناس. يُعدُّ بث الأخبار الكاذبة والشائعات وسيلة خطيرة لتشويش الرأي العام، ويُستخدم غالبًا لتدمير مصادر الأخبار الحقيقية، وفي بعض الأحيان يُرَوَّج خبر كاذب للحصول على الأخبار الصحيحة.

(١٤) الاستمالة أو التغرير والاستدراج (Grooming): هو نوع من الجرائم السيبرانية التي تتمثّل في محاولة شخص بالغ استغلال الأطفال جنسيًّا من خلال بناء علاقة ودّية مع طفل دون سن الثامنة عشر. يبدأ الشخص الذي يقوم بالاستمالة بالتظاهر بالاهتمام والمشاركة في نفس اهتمامات الطفل أو المراهق، ومن ثمّ يبني الثقة معهم. يتم استخدام هذه الثقة المُكتسبة لطلب إرسال صور جنسية أو تبادل رسائل ذات محتوى جنسي. قد يتطوّر الأمر لمواجهة مباشرة بين الشخصين أو استخدام الصور لنشرها عبر الإنترنت.

(١٥) الإرهاب السيبراني (Cyberterrorism): يستهدف استخدام الإنترنت وتكنولوجيا المعلومات والاتّصالات للتخويف والتأثير الفكري والتحريض ضد الأفكار المختلفة. يتضمّن هذا النوع من الإرهاب استخدام الوسائط الرقمية ووسائل التواصل الاجتماعي لترويج الأفكار

المُتطرّفة أو المُعادية لأجندات معيّنة. يرتبط الإرهاب السيبراني بشكل كبير بتقدّم تقنيات المعلومات والاتّصالات، ويُعتبر جزءًا ممّا يُعرف بحروب الجيل السادس. يُمكن لهذا النوع من الإرهاب أنْ يُؤدّي إلى قطع شبكات الاتّصال، والتأثير على أنظمة الدفاع والأمن والحماية وتعطيلها، ووقف الخدمات، وغير ذلك.

(١٦) الحروب السيبرانية (Cyber Warfare): تعتمد الحروب السيبرانية على فِرَق مُتخصّصة في استخدام التكنولوجيا للتصدّي للتحدّيات، حيث يُخطّط ويُدير مُشغّلو هذه الحروب للعمليّات الهجوميّة والدفاعيّة عبر البيئة الرقمية.

بناءً على المعلومات السابقة، يظهر أنّ جرائم الأمن السيبراني تشمل جميع الأنشطة التقنية الخبيثة التي يُنفّذها أفراد أو مجموعات بهدف جنائي داخل الفضاء السيبراني. تستهدف هذه الأنشطة ثلاث فئات رئيسية: الأفراد، والمؤسسات التجارية وغير التجارية، وكذلك الجهات الحكومية.

التأثيرات السلبية للجرائم السيبرانية

تُؤثّر الجرائم السيبرانية بشكل كبير على الأفراد والمؤسّسات والمجتمعات بطرق عديدة، بما في ذلك (بانقا، ٢٠١٩؛ حمدان، ٢٠٢١) (Hibberd, 2022; Schneier, 2015; Singer & Friedman, 2014):

(١) فقدان البيانات والمعلومات الحسّاسة: يُمكن للاختراقات والبرمجيّات الخبيثة أنْ تتسبّب في سرقة البيانات والمعلومات السرية والحسّاسة مثل المعلومات الشخصية وتفاصيل الحسابات المالية. يُمكن استغلال هذه البيانات والمعلومات في الاحتيال أو الابتزاز أو التلاعب بالهويّة.

(٢) تعطيل الأنظمة والخدمات: يُمكن لهجمات الحرمان من الخدمة والاختراقات الهجومية أنْ تتسبّب في تعطيل الأنظمة والخدمات الحيويّة. هذا يُؤدّي إلى توَقّف عمليّات الأعمال وفقدان الإنتاجية وله تأثير سلبي على الاقتصاد.

(٣) الخسائر المالية: تترتّب على الهجمات السيبرانية تكاليف مالية هائلة على الأفراد والشركات والحكومات. يتضمّن ذلك تكاليف استعادة الأنظمة والشبكات والتعويضات للأضرار الناجمة عن الهجوم وفقدان العملاء والإيرادات المُتَوَقّفة.

(٤) الأثر على السلامة العامة: قد تتسبّب الهجمات على البُنية التحتيّة الحاسوبية الشبكية الحيويّة في تأثير سلبي على السلامة العامة. على سبيل المثال، يُمكن للتلاعب بأنظمة النقل أنْ يُؤدّي إلى حوادث مرورية خطيرة، أو يُمكن لتعطيل الشبكات الكهربائية أنْ يُؤدّي إلى انقطاع التيّار الكهربائي في المستشفيات أو المناطق السكنية.

التدابير الوقائيّة والحماية

للتصدّي للجرائم السيبرانية، هناك حاجة ماسة إلى اتّخاذ تدابير وقائية قويّة وتعزيز الحماية السيبرانية. بعض التدابير الفعّالة تشمل (حمدان، ٢٠٢١؛ صائغ، ٢٠١٨، ص ص. ٤٦-٥٢) (Hibberd, 2022; Schneier, 2015; Singer & Friedman, 2014):

(١) التوعية والتدريب: يجب توعية الأفراد والمستخدمين بالجرائم أو المخاطر السيبرانية وتعريفهم بأفضل المُمارسات للأمان السيبراني. يجب تقديم التدريب المُنتظم للموظفين والأفراد للتعرّف على التهديدات الحديثة وكيفيّة التصدّي لها.

(٢) تحديث البرامج والأنظمة: يجب تحديث البرمجيّات والأنظمة بانتظام لسد الثغرات الأمنية المعروفة وتطبيق التصحيحات الأمنية الضرورية.

(٣) تشفير البيانات والمعلومات: يجب تشفير البيانات والمعلومات السرية والحسّاسة والمهمّة للحماية من الوصول غير المصرّح به. يتمْ استخدام تقنيات التشفير لتحويل البيانات والمعلومات إلى شكل غير قابل للقراءة دون المفتاح الصحيح.

(٤) استخدام جدران الحماية النارية وأنظمة اكتشاف التسلّل: يجب تنصيب جدران الحماية النارية وأنظمة اكتشاف التسلّل لمنع الوصول غير المصرّح به واكتشاف الهجمات المُحتملة.

(٥) إجراءات النسخ الاحتياطي: يجب إجراء نسخ احتياطيّة مُنتظمة للبيانات والمعلومات الحسّاسة والسرية وتخزينها في مواقع آمنة ومُنفصلة. هذا يُساعد في استعادة البيانات والمعلومات في حالة حدوث هجوم سيبراني أو فقدان للبيانات.

(٦) تقييم الأمان السيبراني: يجب إجراء تقييم دوري للأمان السيبراني لتحديد الثغرات والضعف في الأنظمة والشبكات والتطبيقات واتّخاذ التدابير اللازمة لتعزيز الحماية.

(٧) التعاون والتبادل للبيانات والمعلومات والخبرات: يجب تعزيز التعاون والتبادل للبيانات والمعلومات والخبرات بين الجهات المعنيّة للكشف عن التهديدات السيبرانية والاستجابة الفعّالة لها.

باختصار، تتزايد الجرائم والمخاطر السيبرانية مع التطوّر التكنولوجي، ولذلك فإنّ الحماية السيبرانية أصبحت أمرًا حيويًّا للأفراد والمنظمات والشركات والحكومات على حد سواء. من خلال التوعية والتدريب وتبنّي تدابير الأمان السيبراني الفعّالة، يُمكننا تقليل التهديدات السيبرانية وحماية البيانات والمعلومات والأنظمة والشبكات الحيويّة. يجب أنْ نعمل معًا كجماعة عالمية لمكافحة التهديدات السيبرانية وبناء بيئة رقمية أكثر أمانًا وموثوقيّة في المستقبل.

أهميّة توعية المعلّمين بالأمن السيبراني

توعية المعلّمين بالأمن السيبراني أمر ضروري وحيوي في زمننا الحالي، حيث أصبحت التكنولوجيا جزءًا لا يتجزّأ من عمليات التعليم والتعلّم. إنّ توجيه الانتباه نحو الأمان السيبراني للمعلّمين يُعدُّ أمرًا أساسيًّا للحفاظ على سلامة البيانات والمعلومات، وللتصدّي للتحدّيات السيبرانية المتزايدة. وفيما يلي نلقي نظرة على الأسباب التي تستدعي الاهتمام بتوعية المعلمين بالأمن السيبراني (السواط وآخرون، ٢٠٢٠؛ الصحفي وعسكول، ٢٠١٩؛ المنتشري، ٢٠٢٠؛ المنتشري وحريري، ٢٠٢٠):

(١) تكامل التكنولوجيا في التعليم والتعلّم: مع تزايد استخدام التكنولوجيا في الفصول الدراسية، يصبح الوعي بالأمن السيبراني أمرًا أساسيًّا للتأكيد على أمان وسلامة بيانات المتعلّمين والمعلّمين.

(٢) حماية البيانات والمعلومات الشخصيَّة للمتعلّمين: تأتي حماية البيانات والمعلومات الشخصية للمتعلّمين في مقدّمة الأولويّات في بيئة التعليم والتعلّم الرقمية. يُعتبر وجود بيانات ومعلومات شخصية للمتعلّمين، مثل الأسماء والعناوين وتفاصيل الحسابات، أمرًا حيويًّا، ويتطلب من المعلّمين أنْ يكونوا على دراية بأفضل الممارسات لضمان حمايتها والتعامل معها بشكل آمن.

(٣) تعزيز الوعي السيبراني للمتعلّمين: يُمكن للمعلّمين أنْ يكونوا قدوةً ومثلًا حسنًا للمتعلّمين في سياق السلوك السيبراني الآمن، من خلال رفع مستوى الوعي الأمني وتوجيه الانتباه إلى مفاهيم الأمان السيبراني. يتضمّن ذلك توجيه المعلّمين حول أمن الإنترنت، وتعريفهم بالتهديدات السيبرانية وأفضل الممارسات لتجنّبها. علاوة على ذلك، يمكن للمعلّمين نقل هذه المعرفة إلى المتعلّمين، وتعزيز الوعي السيبراني لديهم، ممّا يُساهم في تحضيرهم للتفاعل بشكل آمن وواعٍ في العالم الرقمي المتقدّم.

(٤) الحفاظ على سلامة الشبكة المدرسيَّة: تعتمد الكثير من المدارس على شبكات الحواسيب والإنترنت لتوفير التعليم والتعلّم والموارد التعليميَّة والتعلّمية الرقمية. لذلك، يجب على المعلّمين أنْ يكونوا على دراية بأفضل الممارسات لتأمين الشبكة المدرسية وحمايتها من الهجمات السيبرانية. يأتي ذلك بهدف ضمان استمرارية عملية التعليم والتعلّم، وحماية البيانات والمعلومات الحسّاسة.

(٥) التصدّي للتحرُّش السيبراني والتنمُّر: يُعدُّ التحرُّش السيبراني والتنمُّر عبر الإنترنت من المشكلات الشائعة في البيئة المدرسية الرقمية. يُمكن للمعلّمين أنْ يلعبوا دورًا فعّالًا في التوعية بأخطار التحرُّش السيبراني والتنمُّر، وفي تعليم المتعلّمين كيفية التصدّي لهذه التحدّيات والإبلاغ عنها.

(٦) حماية الأنظمة والتطبيقات التعليميَّة والتعلّميّة: تعتمد العديد من المدارس على التطبيقات التعليميَّة والتعلّمية والأنظمة الإلكترونية لتقديم المحتوى التعليمي وتنظيم العملية التعليميَّة والتعلّمية. لذا، يجب على المعلّمين أنْ يكونوا على دراية بأمان هذه الأنظمة والتطبيقات، وأنْ يعملوا على توعية المتعلّمين بأهميّة استخدامها بشكل آمن، وتحفيزهم على الابتعاد عن المُمارسات الضارة.

(٧) التصدّي للتهديدات السيبرانية: توعية المعلّمين بالأمن السيبراني تُعتبر ركيزة أساسية في التصدّي للتهديدات السيبرانية. من خلال فهم المعلّمين للتهديدات الحالية وأساليب الهجمات السيبرانية، يصبح بإمكانهم اتّخاذ الإجراءات الوقائيَّة المناسبة والاستجابة الفعّالة في حالة وجود هجوم سيبراني.

(٨) المُساهمة في بناء جيل آمن سيبرانيًّا: توعية المعلّمين بالأمن السيبراني تُشكّل جزءًا أساسيًّا من بناء جيل قادر على التعامل مع التحدّيات السيبرانية وحماية أنفسهم ومجتمعهم في العالم الرقمي. يتم ذلك من خلال تعليم المعلّمين وتوجيههم لنقل هذه المعرفة للمتعلّمين، مساهمين في بناء ثقافة أمان سيبراني تتماشى مع التطوّرات التكنولوجية.

وتأسيسًا على ما سبق، إنّ توعية المعلّمين بالأمن السيبراني ضرورية لحفظ سلامة المتعلّمين والبيانات والمعلومات والأنظمة التعليميَّة والتعلّمية. يُمكن للمعلّمين اللعب دورًا فعّالًا في تعزيز الوعي السيبراني لدى المتعلّمين ومواجهة التحدّيات السيبرانية من خلال تعليمهم أفضل المُمارسات وتوفير بيئة تعليمية وتعلّمية آمنة ومحميّة.

زيادة فاعليّة الأمن السيبراني في المؤسّسات التعليميَّة

زيادة فاعليّة الأمن السيبراني في المؤسّسات التربوية التعليميَّة أمر حيوي في هذا العصر المعرفي الرقمي المُتقدّم. يعتمد العديد من المدارس والجامعات والكليات والمعاهد على التكنولوجيا والشبكات لتوفير التعليم والتعلّم وتسهيل العملية التعليميَّة والتعلّمية، وهو ما يجعلها عرضة للعديد من التهديدات السيبرانية والاختراقات والهجمات الإلكترونية. لذلك، يُعَد توفير الأمن السيبراني أمرًا حيويًّا لحماية البيانات والمعلومات وضمان استمرارية العملية التعليميَّة والتعلّمية بشكل آمن. في هذا السياق، سنستعرض بعض الإجراءات والتدابير الهامّة التي يُمكن أنْ تُساهم في زيادة فاعليّة الأمن السيبراني في المؤسّسات التربوية التعليميَّة (السواط وآخرون، ٢٠٢٠؛ الصانع وآخرون، ٢٠٢٠؛ العقلاء وعلي، ٢٠٢٢؛ المنتشري، ٢٠٢٠؛ المنتشري وحريري، ٢٠٢٠) (Kritzinger et al., 2017; Tiwari et al., 2016):

(١) التوعية والتدريب: توفير التوعية والتدريب المستمر للمعلّمين والمتعلّمين والإداريّين والموظفين حول مفاهيم الأمن السيبراني وأفضل المُمارسات الأمنية. يُمكن تنظيم دورات وورش عمل تدريبية وجلسات ومحاضرات تثقيفية للتعريف بالتهديدات السيبرانية الشائعة وكيفية التعامل معها.

(٢) تطوير سياسات الأمن السيبراني: يجب وضع سياسات وإجراءات واضحة للأمن السيبراني في المؤسّسة التربوية، تُحدّد مسؤوليّات الموظفين والمتعلّمين والإجراءات والتدابير الوقائيَّة التي يجب اتّباعها للحفاظ على الأمان السيبراني.

(٣) حماية البيانات والشبكات والأنظمة الإلكترونية: ضمان حماية البيانات والمعلومات السرية والحسّاسة والشخصيَّة للمتعلّمين والمعلّمين والموظفين، وكذلك حماية الشبكات والأنظمة الإلكترونية المُستخدمة في المؤسّسة التربوية التعليميَّة عبر تحديث البرمجيّات بانتظام وتطبيق التحديثات الأمنية اللازمة لتجنب الثغرات الأمنية، وأيضًا من خلال تشفير البيانات والمعلومات الهامة (الحسّاسة والسرية) أو إتلافها بشكل آمن، وتطبيق سياسات الوصول الصارمة، والتحديث المستمر لكلمات المرور، واستخدام كلمات مرور قوية من شأنها أنْ تُقلّل بشكل كبير من فرص التخمين والوصول غير المصرّح به للبيانات والمعلومات، خاصة تلك ذات الأهمِّيَّة العالية.

(٤) استخدام البرامج الأمنية: تثبيت برمجيّات مكافحة الفيروسات وجدران الحماية النارية وبرامج اكتشاف التسلّل والحماية من البرمجيّات الخبيثة للحماية من الهجمات والتهديدات والاختراقات السيبرانية.

(٥) إدارة صلاحيّات الوصول: تحديد صلاحيّات الوصول للمستخدمين والموظفين بدقّة، ومراقبة الوصول إلى البيانات والمعلومات السرية والحسّاسة.

(٦) تفعيل التحقّق الثنائي: تشجيع استخدام التحقّق الثنائي للدخول إلى الحسابات الهامّة للحماية من الاختراقات وسرقة الحسابات.

(٧) التحقّق من البريد الإلكتروني: فحص البريد الإلكتروني لاكتشاف الرسائل الاحتيالية والرسائل الإلكترونية الضارة وتجنّب الوقوع في فخ الاحتيال الإلكتروني.

(٨) تنفيذ النسخ الاحتياطي: عمل نسخ احتياطية من البيانات بشكل منتظم وتخزينها بشكل آمن لضمان استعادة البيانات في حالة وقوع هجمات أو فقدان البيانات.

(٩) مراقبة وكشف التهديدات: استخدام أنظمة مراقبة الأمان وكشف التهديدات المُتطوّرة والاستجابة لها بشكل فوري وفعّال.

(١٠) التقييم الدوري وتحسين الأمان: إجراء تقييمات دورية للأمان السيبراني وتحديث سياسات الأمان بناءً على التهديدات المُستجدّة والتطوّرات التكنولوجية.

(١١) التعاون مع مؤسّسات أمن البيانات والمعلومات: يجب على المؤسّسات التعليميَّة والتعلّمية أنْ تتعاون مع مؤسّسات أمن البيانات والمعلومات المتخصّصة، والاستفادة من خبراتها وتجاربها، بهدف تعزيز أمان المؤسسة.

دولة الكويت والأمن السيبراني

حفاظًا على الأمن المجتمعيّ في دولة الكويت في هذا العصر الرقميّ، وضمانًا لحرّيّات الأفراد وكرامتهم وسمعتهم، وللحيلولة دون العدوان على الأموال والمُمتلكات والأصول المعلوماتيَّة العامّة والخاصّة، سواء كانت تقليديَّة أو رقميَّة، وتماشيًا مع التوجّهات العالميَّة لمكافحة الجرائم السيبرانية، وتنفيذًا لأحكام الاتفاقيّات الدوليَّة والإقليميَّة والمحليَّة المُتعلّقة بمكافحة هذه الجرائم؛ فقد بذلت دولة الكويت جهودًا مكثّفة خلال العقد الماضي لمواجهة هذه التحدّيات وتعزيز الأمن السيبراني في المجتمع الكويتي (صفر، ٢٠١٧)، ونذكر منها الآتي:

(١) في عام ٢٠١٤م، تأسّست "الهيئة العامة للاتّصالات وتقنية المعلومات"، وتَوَلّتْ مسؤولية الإشراف على قطاع الاتّصالات في دولة الكويت ورقابته، وحماية مصالح المستخدمين ومزوّدي الخدمات، وتنظيم خدمات جميع شبكات الاتّصالات في الدولة بكفاءة عالية لضمان الأداء الأمثل للقطاع.

(٢) في السابع من يوليو ٢٠١٥م، أقرّت دولة الكويت "قانون مكافحة جرائم تقنية المعلومات" بمرسوم أميري، وبدأ سريانه اعتبارًا من الثاني عشر من يناير ٢٠١٦م.

(٣) في يناير عام ٢٠١٨م، أعلنت دولة الكويت عن "الاستراتيجيَّة الوطنيَّة للأمن السيبراني"، والتي جاءت نتيجة جهود عمل مُكثّفة استمرت على مدى عامين، بالتعاون بين "الهيئة العامة للاتّصالات وتقنية المعلومات" والقطاعين العام والخاص في الكويت. تُعَدُّ هذه الاستراتيجية أحد العناصر الأساسيَّة في تطوير القدرات وتكثيف الجهود لتعزيز الأمن السيبراني وتجاوز التحدّيات والمصاعب التي تواجه دولة الكويت في هذا المجال. تهدف الاستراتيجية إلى وضع رؤية للأمن السيبراني على المدى البعيد، وتحديد الأسس والقواعد والإجراءات اللازمة لتحقيق ذلك، واستغلال الإمكانيَّات الكاملة للعلم وتكنولوجيا المعلومات والاتّصالات الحديثة، وتطوير مهارات وقدرات الكوادر البشرية، وتعزيز القدرة على التعامل مع القضايا الأخلاقية والقانونية المُتعلّقة بالأمن السيبراني. كما تسعى الاستراتيجية أيضًا إلى جمع المعلومات والبيانات من قبل المؤسّسات ووضع اللوائح والسياسات لحماية منظوماتها الأمنيَّة بفعاليَّة (وكالة الأنباء الكويتية، ٢٠١٨).

(٤) في الخامس من فبراير عام ٢٠٢٢م، أصدر أمير دولة الكويت مرسومًا أميريًّا يَنُصُّ على إنشاء "المركز الوطنيّ للأمن السيبراني" في الكويت. يُعَدُّ هذا المركز جهازًا حكوميًّا مُكلّفًا بتحقيق الإدارة الاستباقيَّة الفعّالة لتهديدات وأخطار الفضاء السيبراني. يسعى المركز إلى تطوير وتعزيز وسائل الدفاع الاستباقيَّة الملائمة، والمراقبة المستمرّة لإعداد آليَّات الاستجابة للقطاعات والمؤسّسات الحيويَّة، وكذلك الإبلاغ عن هجمات واختراقات القرصنة والجرائم السيبرانية. ويَتَوَلّى المركز مهام متعدّدة تشمل توعية الجمهور وبناء قدرات بشريَّة وطنيَّة قادرة على التعامل مع قضايا الأمن السيبراني، بالإضافة إلى تأمين مؤسّسات الدولة بما يتوافق مع السياسات واللوائح والإجراءات والمعايير الفنيَّة. يشمل نطاق عمل المركز الجهات الحكوميَّة والمدنيَّة والعسكريَّة والأمنيَّة، ومؤسّسات القطاع الخاص ذات الصلة بمهام المركز، وكذلك الجهات الأخرى التي

يُحدّدها رئيس المركز. وتتضمّن مسؤوليَّات المركز وضع الاستراتيجية الوطنيَّة لقطاع الأمن السيبراني والإشراف عليه، وتأمين وحماية الشبكات المعلوماتية والاتّصالات وأنظمة المعلومات وقواعد البيانات، بالإضافة إلى إدارة عمليَّات جمع المعلومات والبيانات وتبادلها بواسطة وسائل إلكترونية (قاسم، ٢٠٢٢).

منهج الدراسة وإجراءاتها

منهج الدراسة

تبنّتْ هذه الدراسة منهج البحث الكميّ الوصفيّ التحليليّ المسحيّ باعتباره المنهجيَّة البحثيَّة المُخوّل بها تحقيق أهدافها البحثيَّة الاستقصائيَّة لقياس درجة وعي المعلّمين والمعلّمات في مدارس التعليم العام بدولة الكويت حول الأمن السيبراني، إضافةً إلى تحديد أثر بعض المتغيّرات المستقلة في/على اتّجاهات المشاركين وآرائهم نحو مستوى وعيهم بالأمن السيبراني. ويُعتبرُ هذا المنهج البحثيّ من أكثر طرق، ومناهج، وأساليب البحث العلميّ ملاءمةً لطبيعة هذا النوع من الدراسات البحثيَّة العلميَّة من وجهة نظر عدد كبير من الباحثين والمُختصّين؛ إذْ إنّه يُعنى بوصف المشكلات أو الظواهر المجتمعيّة كما هي على أرض الواقع من خلال المسح الشامل لفئة معيّنة من أفراد المجتمع، ويستخدمه الباحثون بكثرة في الآونة الأخيرة (أبو علام، ٢٠١٨؛ العسّاف، ٢٠١٢) (Creswell & Creswell, 2018; Fraenkel et al., 2019; Johnson & Christensen, 2020).

مجتمع الدراسة وعيّنتها

تكوّن مجتمع الدراسة من جميع أعضاء الهيئة التعليميَّة – المعلّمين والمعلّمات – في مدارس التعليم العام بدولة الكويت المُقيّدين في الفصل الدراسي الأول والثاني من العام الدراسي ٢٠٢٣/٢٠٢٤م، والبالغ عددهم حسب إحصائيّات وزارة التربية للعام الدراسي ٢٠٢٢/٢٠٢٣م حوالي ٨٨,٩٨٥ عضوًا (٢١,٩٠٨ ذكرًا و٦٧,٠٧٧ أنثى)؛ بواقع ٦٥,٥٤٢ كويتيًّا، وما يقارب ٢٣,٤٤٣ غير كويتي (الإدارة المركزية للإحصاء، ٢٠٢٣). أمّا عيّنة الدراسة فتكوّنت من ١,٦٦٤ معلّمًا ومعلّمةً (أي بنسبة تُقدّر بحوالي 1.9% من مجتمع الدراسة)، إذْ تمّ اختيارهم

بالطريقة الطبقية العشوائية وبصورة آلية/إلكترونية، وعُوّل عليها في معالجة البيانات وتحليل النتائج.

أداة الدراسة

بعد الاطّلاع على الأدبيّات والدراسات البحثيَّة السابقة ذات الصلة بموضوع البحث الحالي أُعِدَّتْ أداة الدراسة البحثيَّة الاستقصائيّة الرئيسيّة (الاستبانة) بكل دقّة وموضوعيّة، وقد احتوتْ على قسمين رئيسين: (١) البيانات الديموغرافيّة (الشخصية والمهنية)، و(٢) مقياس الوعي بالأمن السيبراني. اشتمل القسم الأول على اثنتي عشر سؤالًا تُزوّدنا ببيانات عامة تضمّ معلومات تكشف عن طبيعة أفراد العيّنة المشاركة، أمّا القسم الثاني فقد ضمّ مقياس الوعي بالأمن السيبراني، واحتوى على ٤٧ عبارة أو فقرة تقيس وتُقيّم مستوى وعي المعلّمين والمعلّمات في مدارس التعليم العام بدولة الكويت إزاء 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 ثَمَّ 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 قَدْرَ الإمكان في كل مرّة تُستخدَم فيها الأداة) عمد الباحث إلى تجربتها على عيّنة استطلاعيَّة عددها ٥٠ مشاركًا، ومن ثَمَّ 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 0.972 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

وُزِّعَتْ الاستبانة خلال الفَصْلَيْن الدراسِيَّيْن الأول والثاني من العام الدراسي ٢٠٢٣/٢٠٢٤م بطريقةٍ آليّةٍ إلكترونيةٍ (بالاستعانة بوسائط تكنولوجيا المعلومات والاتّصالات المختلفة) على العيّنة الطبقيَّة العشوائيَّة المُختارة من معلّمي ومعلّمات مدارس التعليم العام بدولة الكويت، وجرى التأكيد للمشارِكين في الدراسة أنَّ مشاركتهم اختياريَّة، وأنَّ 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 ٢٩ – لمُعالجتها إحصائيًا، ومن ثمّ استخراج البيانات الإحصائيَّة والتحليلات، والمقارنات اللازمة (نتائج الدراسة). وتحديدًا، تطلّبت هذه الدراسة البحثيَّة العلميّة استخدام الأساليب الإحصائيَّة التالية:

(١) التحليل الوصفيّ الاستكشافيّ (Exploratory Descriptive Analysis): كمعاملات الاتّساق الداخليّ (معاملات الثبات) كرونباخ ألفا، والتكرارات، والنسب المئويَّة، والمتوسّطات الحسابيَّة، والانحرافات المعياريّة، ومؤشّرات الأهمّيَّة 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 الأهمّيَّة النسبيَّة (الأوزان النسبيَّة)

مدى مؤشّرات الأهمّيَّة النسبيَّة	مدى الأوزان النسبيَّة	درجة الوعي

مرتفعة جدًّا	100.0 – 80.0	1.00 – 0.80
مرتفعة	79.0 – 60.0	0.79 – 0.60
متوسّطة	59.0 – 40.0	0.59 – 0.40
ضئيلة	39.0 – 20.0	0.39 – 0.20
ضئيلة جدًّا	19.0 – 0.0	0.19 – 0.00

(٢) الاختبارات المعلميَّة/البارامتريَّة (Parametric Tests): كاختبارات الفروق بين المجموعات، وهي بالتحديد اختبار ت للعيّنات المستقلّة (Independent–Samples t–test)، وتحليل التباين الأُحادي (One–way Analysis of Variance – ANOVA)، واختبار ليفين لتجانس التباين (Levene's Test of Equality of Error Variances)، والمقارنات البعدية (Post Hoc Comparisons) باستخدام اختبار دونت سي (Dunnett's C Test) حينما تختلف الفروق (Variances) بدلالة إحصائيَّة واختبار شيفيه (Scheffé's Test) عندما لا تَختلف الفروق (Variances) بدلالة إحصائيَّة. والجدير بالذكر، أنَّ هذه الاختبارات الإحصائيَّة طُبِّقت للأغراض الاستدلاليَّة بُغية الإجابة عن بعض أسئلة الدراسة، وعند تطبيقها تمَّ اختيار قيمة ألفا (α) لتكون ٠.٠٥ (α≤0.05).

نتائج الدراسة ومناقشتها

أوّلًا: وصفٌ عامٌّ للعيّنة والبيانات الديموغرافيَّة

يُبَيِّنُ الجدول ٢ توزيعَ أفرادِ عيِّنة الدراسة (المشاركين) بحسبِ المتغيِّرات الديموغرافيَّةِ (المستقلّة).

جدول ٢

توزيع أفراد عيّنة الدراسة حسب متغيّرات الدراسة المستقلّة

المتغيّر	الصنف	العدد	النسبة
الجنس/النوع	ذكر	664	39.9
	أنثى	1,000	60.1
الجنسية	كويتي (مواطن)	1,080	64.9
	غير كويتي (مقيم)	584	35.1
نوع	التخصُّصات الأدبيّة	928	55.8

التخصُّص	التخصُّصات العلميّة	736	44.2
المؤهّل العلميّ	شهادة الإجازة الجامعية (البكالوريوس)	1,460	87.7
	شهادة الدراسات العُليا (الماجستير/الدكتوراه)	204	12.3
العمر	من ٢٠ إلى أقل من ٣٠ سنة	484	29.1
	من ٣٠ إلى أقل من ٤٠ سنة	456	27.4
	من ٤٠ إلى أقل من ٥٠ سنة	436	26.2
	من ٥٠ سنة فأكثر	288	17.3
سنوات الخبرة المهنية	من ٠ إلى أقل من ١٠ سنوات	732	44.0
	من ١٠ إلى أقل من ٢٠ سنة	536	32.2
	من ٢٠ سنة فأكثر	396	23.8
نوع المدرسة	مدارس التعليم العام الحكومية	1,512	90.9
	مدارس التعليم العام الخاصة	152	9.1
المنطقة التعليميَّة	الأحمدي	252	15.1
	الجهراء	284	17.1
	حولي	596	35.8
	العاصمة	148	8.9
	الفروانية	132	7.9
	مبارك الكبير	252	15.1
المرحلة التعليميَّة	رياض الأطفال	92	5.5
	المرحلة الابتدائية	576	34.6
	المرحلة المتوسّطة	380	22.8
	المرحلة الثانوية	616	37.0
مستوى الـ ICT	مبتدئ	356	21.4
	ملم/متوسّط	1,084	65.1
	محترف/متقدّم	224	13.5
مؤهّل الـ ICT	حاصل على شهادة دوليَّة	720	43.3
	ليس لديه أيّ شهادة دوليَّة	944	56.7
دورات الأمن السيبراني	التحق بدورات في الأمن السيبراني	104	6.3
	لم يلتحق بأيّ دورات في الأمن السيبراني	1,560	93.8

ثانيًا: نتائج أسئلة الدراسة ومناقشتها

نتائج سؤال الدراسة الأوّل. نصّ سؤال الدراسة الأول على: ما مستوى وعي المعلّمين في مدارس التعليم العام بدولة الكويت بالأمن السيبراني؟ للإجابة عن هذا السؤال، أُستخدِم الإحصاءُ الوصفيُّ (Descriptive Statistics). ويُظهر الجدول ٣ تفصيليًّا: التحليل الإحصائيّ الوصفيّ – المتوسّطات الحسابيّة، والانحرافات المعياريّة، ومؤشّرات الأهمِّيَّة النسبيَّة، ودرجات الوعي، والرُتب – للعبارات الخاصة بسؤال الدراسة الأول.

جدول ٣

المتوسّطات الحسابيّة، والانحرافات المعياريّة، ومؤشّرات الأهمِّيَّة النسبيَّة، ودرجات الوعي، والرُّتب لعبارات سؤال الدراسة الأول – "مستوى وعي المعلّمين في مدارس التعليم العام بدولة الكويت بالأمن السيبراني"

م	العبارة	المتوسّط الحسابيّ	الانحراف المعياريّ	مؤشّر الأهمِّيَّة النسبيَّة	درجة الوعي	الرُتبة
1	أتواصلُ مع الجهات الأمنيّة المختصّة عند تعرُّضي لأيّ شكلٍ من أشكال الجرائم السيبرانيَّة.	4.20	0.88	0.84	مرتفعة جدًّا	27
2	أتجنَّبُ الاتّصال بالشبكات اللّاسلكيّة (WiFi) العامّة، وأَحذَرُ كثيرًا عند الاتّصال بها وقت الضرورة.	3.95	1.03	0.79	مرتفعة	41
3	أحرصُ على استخدام متصفّحٍ آمنٍ عند استخدام شبكة الإنترنت.	4.45	0.75	0.89	مرتفعة جدًّا	6
4	أتجنّبُ استخدامَ التطبيقات الإلكترونيّة، أو تصفُّحَ المواقع الإلكترونية، أو استقبالَ المكالمات الهاتفيّة المجهولة التي تقدِّم خدماتٍ مجانيّةً للمستخدمين.	4.34	0.90	0.87	مرتفعة جدًّا	16
5	أحتفظُ 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.	4.26	0.90	0.85	مرتفعة جدًّا	25
6	أتأكَّدُ من مصدر المعلومة المتداولة في مواقع التواصل الاجتماعي قبل نشرها وإرسالها للآخرين.	4.46	0.73	0.89	مرتفعة جدًّا	4
7	أستخدمُ المحتوى المرخّص من قبل الناشرِ أو المؤلِّف.	4.27	0.84	0.85	مرتفعة جدًّا	٢٢
8	أحرصُ على إبلاغ الجهات القانونيَّة المختصَّة عن التطبيقات، أو المواقع الإلكترونيّة، أو المكالمات الهاتفيّة المشكوك فيها.	3.94	0.99	0.79	مرتفعة	٤٢
9	أُلغي اشتراكاتي في التطبيقات، أو المواقع الإلكترونيّة، أو الخدمات	4.21	0.91	0.84	مرتفعة جدًّا	26

	الهاتفيّة التي تتضمَّن إعلاناتٍ مستهدفةٍ، لحماية بياناتي الشخصيّة والماليّة.					
10	أحترمُ آراءَ الآخرين وأفكارَهم ومشاعرَهم عند مناقشة موضوعٍ ما في التخصُّص عبر شبكة الإنترنت.	4.45	0.71	0.89	مرتفعة جدًّا	5
11	أتجنَّب التواصلَ مع أشخاصٍ مجهولي الهويَّة عبر التطبيقات، والمواقع الإلكترونيّة، والمكالمات الهاتفيَّة.	4.52	0.77	0.90	مرتفعة جدًّا	1
12	أستخدمُ التشفيرَ (بتعيين كلمة مرورٍ) لملفّاتي المهمَّة التي أُرسلها عبر شبكة الإنترنت.	4.28	0.88	0.86	مرتفعة جدًّا	20
13	أعرف أبرزَ العلامات والمؤشّرات الخطرة التي تدلُّ على أنّ أجهزتي قد تعرَّضَتْ للاختراق.	4.00	0.95	0.80	مرتفعة جدًّا	38
14	أُراعي الضوابطَ الاحترازيَّةَ والإجراءات الوقائيَّة لتحصين أجهزتي من الاختراق.	4.27	0.79	0.85	مرتفعة جدًّا	21
15	استخدم كلمات مرورٍ قويَّةٍ ومعقَّدة (تتكون من حروفٍ وأرقامٍ ورموزٍ) لحساباتي الشخصيَّة، وأتجنَّب تكرارها.	4.27	0.86	0.85	مرتفعة جدًّا	23
16	أهتمُّ بتحديثِ كلماتِ المرور الخاصَّة بحساباتي أو تغييرها بين الحين والآخر.	3.85	1.11	0.77	مرتفعة	45
17	أحرصُ على عدم الإفصاح عن كلمات المرور الخاصَّة بحساباتي لأيّ أحد.	4.48	0.75	0.90	مرتفعة جدًّا	3
18	أقرأ النشرات التعريفيَّة التوعويَّة الخاصَّة بمفاهيم الأمن السيبرانيّ وأخلاقيّاته ومخاطره.	3.94	1.02	0.79	مرتفعة	43
19	أستخدمُ تقنيةَ التحقُّق الثنائيّ (كلمة المرور – البصمة أو غيرها) لتحصينِ أجهزتي من الاختراق.	4.32	0.85	0.86	مرتفعة جدًّا	18
20	أَحترمُ القوانينَ والسياساتِ واللوائحَ التي تُشرِّعها الدولةُ وتفرضها في التعامل مع شبكة الإنترنت واستخدامها.	4.43	0.79	0.89	مرتفعة جدًّا	9
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 المُمكنْ أنْ تضرَّ بأجهزتي وبياناتي.	4.06	0.92	0.81	مرتفعة جدًّا	34
22	أُحدِّثُ برمجيّات الحماية الموجودة على أجهزتي باستمرار.	4.19	0.88	0.84	مرتفعة جدًّا	28
23	أعدِّلُ سياساتِ الخصوصيَّة للأجهزة والتطبيقات من خلال الإعدادات بما يضمن تطبيق مستوى عالٍ من الخصوصيَّة.	4.15	0.86	0.83	مرتفعة جدًّا	31
24	أستخدمُ الروابطَ الرسميَّةَ التي تنشرُها وزارة التربية في موقعها الإلكترونيّ الرسميّ، وفي حساباتها الرسميّة عبر شبكات التواصل الاجتماعيّ.	4.38	0.77	0.88	مرتفعة جدًّا	15

25	أحترمُ سياساتِ التطبيقاتِ والمواقعِ الإلكترونيّة التي أستخدمُها.	4.39	0.74	0.88	مرتفعة جدًّا	14
26	أتجاهلُ العروضَ الإعلانيَّةَ، والتطبيقاتِ، والمواقعَ الإلكترونيَّةَ، والمكالمات الهاتفية، إذا كانت مجهولة المصدر أو مشبوهة.	4.45	0.75	0.89	مرتفعة جدًّا	7
27	أستخدم أدوات الإبلاغ عن الإساءات التي يتعرَّض لها المستخدمون عبر شبكة الإنترنت.	4.04	0.95	0.81	مرتفعة جدًّا	35
28	أحرصُ على عدم فتح الرسائل الإلكترونيّة (مثل: الرسائل النصيّة أو البريد الإلكترونيّ) أو استقبال المكالمات الهاتفيّة مجهولة المصدر أو المشبوهة.	4.44	0.78	0.89	مرتفعة جدًّا	8
29	أحظرُ (Block) الرسائلَ النصيَّةَ أو البريد الإلكترونيّ أو المكالمات الهاتفية مجهولة المصدر أو المشبوهة، وأبلّغ (Report) عنها.	4.42	0.78	0.88	مرتفعة جدًّا	12
30	أتجنّب فتح أي الروابط والمرفقات التي تتضمنها الرسائل الإلكترونيّة التي تصلني من شخصٍ مجهولٍ أو مصدرٍ غير معروفٍ لديّ.	4.50	0.70	0.90	مرتفعة جدًّا	2
31	أفحصُ الروابطَ والمرفقات التي تصلني عبر الرسائل النصية أو البريد الإلكتروني التي يبدو لي أنها ضارة.	4.14	0.91	0.83	مرتفعة جدًّا	32
32	أحرصُ على تعطيل خدمات الوصول لموقعي في التطبيقات المُحمَّلة على أجهزتي.	4.17	0.85	0.83	مرتفعة جدًّا	29
33	أُفَعِّلُ خدمات الوصول لموقعي تفعيلًا مؤقَّتًا أثناء استخدام بعض التطبيقات والمواقع الإلكترونية التي تتطلّب ذلك.	4.17	0.85	0.83	مرتفعة جدًّا	30
34	أُغيِّر إعدادات أجهزتي باستمرار لحمايتها وتحصينها من القرصنة أو اختراق الاتّصال بالشبكة اللاسلكية (WiFi).	4.01	0.98	0.80	مرتفعة جدًّا	37
35	أنشرُ الوعيَ الرقميَ بالأمن السيبرانيّ عند التعرُّض للمواقف السلبية في شبكة الإنترنت.	3.99	0.94	0.80	مرتفعة جدًّا	٣٩
36	أراعي النزاهةَ والشفافيَّةَ والأصالةَ في هويَّتي الرقمية حين أستخدم مواقع شبكات التواصل الاجتماعي وتطبيقاتها.	4.26	0.82	0.85	مرتفعة جدًّا	24
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.	4.42	0.76	0.88	مرتفعة جدًّا	11
38	أتوخّى الحذر عند مشاركة الآخرين ببياناتٍ حسّاسةٍ، وذلك باستخدام إعداداتِ الخصوصيَّة للخدمات الإلكترونية.	4.40	0.75	0.88	مرتفعة جدًّا	13
39	أحرصُ باستمرار على تحميل البرامج الآمنة (الموثوقة والمعتمدة) واستخدامها.	4.33	0.81	0.87	مرتفعة جدًّا	17

40	أحرصُ دومًا على تثبيت آخر التحديثاتِ للبرمجيَّات أو التطبيقات المُحمَّلة على أجهزتي.	4.31	0.82	0.86	مرتفعة جدًّا	19
41	أتجنَّب استخدامَ البريد الإلكترونيّ الرسميّ في التسجيلِ أو الاشتراك في مواقع شبكات التواصل الاجتماعيّ وتطبيقاتها.	3.94	1.02	0.79	مرتفعة	44
42	أتجنَّب استخدامَ هاتفي الشخصيّ الرسميّ في تفعيل التسجيل والاشتراك في مواقع شبكات التواصل الاجتماعيّ وتطبيقاتها.	3.77	1.07	0.75	مرتفعة	46
43	أحرصُ على غلق أجهزتي أو تسجيل الخروج من التطبيقات والمواقع الإلكترونية بطريقةٍ صحيحةٍ لتجنُّب فقدان البيانات.	4.10	0.94	0.82	مرتفعة جدًّا	33
44	أتجنَّب 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).	4.43	0.80	0.89	مرتفعة جدًّا	10
45	أقرأُ دليلَ السياسات والإجراءات الخاصَّة بحفظ الأمن السيبرانيّ في المدرسة، وأحرصُ على الالتزام بتطبيقها.	3.98	0.98	0.80	مرتفعة جدًّا	40
46	أُشاركُ في الدورات التدريبيّة والندوات التوعويَّة والتخصُّصيّة في مجال الأمن السيبراني.	3.72	1.07	0.74	مرتفعة	47
47	أهتمُّ بالاطّلاع على الجهود الحكوميّة الهادفة إلى تعزيز الأمن السيبرانيّ وزيادة فاعليّته.	4.04	0.98	0.81	مرتفعة جدًّا	36
	المتوسِّط المرجّح	4.21	0.58	0.84	مرتفعة جدًّا	

يتبيّن من الجدول ٣ أنّ مستوى وعي المعلّمين في مدارس التعليم العام بدولة الكويت حيال الأمن السيبراني جاء بوجهٍ عام بدرجة "مرتفعة جدًّا" (م = 4.21، ن.م = 0.58، RII = 0.84)؛ إذْ بيّنت النتائج أنّ مستوى وعيهم كان على درجة "مرتفعة جدًّا" في الأغلبية العظمى من عبارات المقياس (٤٠ عبارة)، بينما حصلت بقية فقرات المقياس (٧ فقرات) على درجة "مرتفعة". وتتّفق هذه النتيجة نوعًا ما في فحواها مع نتائج دراسات بحثيَّة أخرى، كدراسة صفر (٢٠٢٤) التي أشارت إلى أنّ مستوى الوعي بالأمن السيبراني لدى معلّمات قبل الخدمة في كلية التربية بجامعة الكويت بوجهٍ عام جاء بدرجة "مرتفعة جدًّا". وكذلك مع دراسة الصانع وآخرون (٢٠٢٠)، ودراسة سراج الدين وآخرون (٢٠٢١)؛ إذْ جاءت درجة الوعي بالأمن السيبراني لدى المعلّمين والمعلّمات فيهما بشكلٍ 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". وبالمثل دراسة الحبيّب (٢٠٢٢) التي أظهرت أنّ مستوى الوعي بالأمن السيبراني لدى طلاب وطالبات الدراسات العُليا المعلّمين بوجهٍ عام جاء بدرجة "عالية". وأيضًا دراسة الظويفري (٢٠٢١) التي أَوْضَحَتْ أنّ واقع الأمن السيبراني في مدارس التعليم العام بمنطقة المدينة المنوَّرة جاء بوجهٍ عام بدرجة "عالية" حسب وجهة نظر القيادة المدرسية (القادة والقائدات والمعلّمين والمعلّمات). ولكنّها في الوقت ذاته تختلف عن نتائج دراسات علميَّة أخرى، كدراسة الصحفي وعسكول (٢٠١٩) التي أشارت إلى أنّ مستوى الوعي والإلمام والمعرفة بالأمن السيبراني لدى معلّمات الحاسب الآلي بالمرحلة الثانوية في مدارس التعليم العام الحكومي بمدينة جدة بوجهٍ عام جاء بدرجة "متوسّطة". وبالمثل دراسة المنتشري وحريري (٢٠٢٠)، ودراسة العقلاء وعلي (٢٠٢٢) اللتين أظهرتا أنّ مستوى وعي المعلّمين والمعلّمات بالأمن السيبراني بوجهٍ عام جاء بدرجة "متوسّطة". وأيضًا دراسة فرج (٢٠٢٢) التي بيّنت أنّ درجة موافقة أعضاء هيئة التدريس بجامعة الأمير سطام بن عبد العزيز نحو دواعي تعزيز ثقافة الأمن السيبراني في ظل التحوّل الرقميّ بالجامعة بوجهٍ عام جاءت بدرجة "متوسّطة". إضافةً إلى دراسة Jazeel (٢٠١٨) التي كشفت أنّ درجة وعي معلّمي ومعلّمات قبل الخدمة بكلية المعلّمين الحكوميَّة في سريلانكا بالأمن السيبراني كانت بوجهٍ عام "منخفضة". وبالمثل دراسة Moyo وآخرون (٢٠٢٢) التي أكّدت أنّ مستوى وعي معلّمي ومعلّمات قبل الخدمة بجامعة كيب تاون في جنوب إفريقيا بخصوص الأمن السيبراني كان بوجهٍ عام "منخفضًا". هذا بالإضافة إلى دراسة ابن إبراهيم (٢٠٢١) التي أظهرت أنّ مستوى وعي معلّمات العلوم بالمرحلة الابتدائية في مدارس التعليم العام بالسعودية بجوانب الأمن السيبراني في التعليم والتعلّم عن بُعد بوجهٍ عام جاء بدرجة "منخفضة"، وإنّ البرنامج التدريبي المُقترح ساهم برفعه إلى مستوى وعي "كبير إلى كبير جدًّا". وكذلك دراسة المنتشري (٢٠٢٠) التي أشارت إلى أنّ دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلّمات والمتعلّمات في مدارس البنات الحكومية بمدينة جدة بوجهٍ عام حصل على درجة موافقة "قليلة" من وجهة نظر المعلّمات.

نتائج سؤال الدراسة الثاني. نصّ سؤال الدراسة الثاني على: هل توجد فروق ذات دلالة إحصائيَّة عند مستوى الدلالة ($0.05\geq\alpha$) في آراء معلّمي مدارس التعليم العام بدولة الكويت وتصوّراتهم تجاه مستوى وعيهم بالأمن السيبراني يُمكنْ عزوها لمتغيّرات الجنس/النوع، ونوع

التخصُّص، والمؤهّل العلميّ، ومؤهّل الـ ICT، ودورات الأمن السيبراني، ومستوى الـ ICT، وسنوات الخبرة المهنية؟ للإجابة عن هذا السؤال، أُستخدِم الإحصاء الاستدلاليّ (Inferential Statistics)، إذْ طُبِّقَ 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 المستقلّة لمقياس الدراسة تبعًا للمتغيّرات الآتية: الجنس/النوع، ونوع التخصُّص، والمؤهّل العلميّ، ومؤهّل الـ ICT، ودورات الأمن السيبراني

م	المتغيّر المستقل	الصنف	التكرار	المتوسّط الحسابيّ	الانحراف المعياريّ	قيمة ت	درجة الحريّة	الدلالة الإحصائيَّة	مستوى الدلالة
١	الجنس/النوع	ذكر	664	4.19	0.55	−1.177	1,662	0.239	غير دالَّة
		أنثى	1,000	4.23	0.59				
٢	نوع التخصُّص	التخصُّصات الأدبيّة	928	4.21	0.61	−0.232	1,662	0.816	غير دالَّة
		التخصُّصات العلميّة	736	4.22	0.54				
٣	المؤهّل العلميّ	شهادة البكالوريوس	1,460	4.24	0.54	4.489	1,662	0.000*	دالَّة
		شهادة الماجستير/الدكتوراه	204	4.05	0.76				
٤	مؤهّل الـ ICT	حاصل على شهادة دوليَّة	720	4.18	0.59	−1.976	1,662	0.053	غير دالَّة
		ليس لديه أيّ شهادة دوليَّة	944	4.24	0.57				
٥	دورات الأمن السيبراني	التحق بدورات	104	4.30	0.83	1.566	1,662	0.118	غير دالَّة
		لم يلتحق بأيّ دورات	1,560	4.21	0.56				

*ملاحظة. * دالٌّ إحصائيًّا عند مستوى دلالة 0.01 (α≥0.01).*

يتّضح من الجدول 4 أنّ اختبارات الفروق بين المجموعات المشاركة أظهرت عدم وجود فروق ذات دلالة إحصائيَّة عند مستوى الدلالة 0.05 بين متوسّطات استجابات المعلّمين في مدارس التعليم العام بدولة الكويت بشأن آرائهم وتصوّراتهم (اتّجاهاتهم) حول مستوى وعيهم بالأمن السيبراني تُعزى لمتغيّر الجنس/النوع (ذكر، أنثى)، وذلك في الأداة عامّةً. ويُمكن تفسير هذه النتيجة بأنّ الأمن السيبراني موضوع جوهريّ يهمُّ جميع الأفراد في المجتمع بغض النظر عن

نمط جنسهم. وبناءً عليه، نجد أنّ الوعي والإلمام والمعرفة بهذا المبحث يُعدُّ من الاهتمامات والأولويّات للجميع بمختلف أجناسهم، ولَعَلَّ يكون ذلك هو الباعث في ظهور توافق وانسجام تام في آراء وتصوّرات (اتّجاهات) المعلّمين والمعلّمات. وتتّفق هذه النتيجة في فحواها مع نتائج دراسات أخرى، كدراسة الصانع وآخرون (٢٠٢٠)، ودراسة سراج الدين وآخرون (٢٠٢١)، ودراسة الشهري (٢٠٢١)، ودراسة الظويفري (٢٠٢١)، التي أشارت إلى عدم وجود أيّ اختلافات دالَّة إحصائيًّا بين متوسّطات استجابات المجموعات المشاركة من أعضاء الهيئة التعليميَّة حول مستوى وعيهم بالأمن السيبراني يُمكن عزوها لمتغيّر الجنس (النوع). ولكنّها في المقابل تعارضت مع النتيجة التي توصّلت إليها دراسة Jazeel (٢٠١٨) والتي أظهرت وجود فروق دالَّة إحصائيًّا بين متوسّطات استجابات معلّمي ومعلّمات قبل الخدمة نحو مستوى وعيهم بالأمن السيبراني يُمكن عزوها لمتغيّر الجنس (النوع)، وكانت لصالح فئة الذكور، حيث كان مستوى الوعي لديهم أكبر. وأيضًا اختلفت مع نتيجة دراسة العقلاء وعلي (٢٠٢٢) التي كشفت عن وجود هذه الفروق ذات الدلالة الإحصائيَّة بين متوسّطات تقديرات المعلّمين والمعلّمات نحو استجاباتهم لمستوى وعيهم بالأمن السيبراني تُعزى لمتغيّر الجنس (النوع)، وكانت لصالح المعلّمات.

وكذلك يتبيّن من الجدول 4 أنّ اختبارات الفروق بين المجموعات المشاركة أظهرت عدم وجود فروق ذات دلالة إحصائيَّة عند مستوى الدلالة 0.05 بين متوسّطات استجابات المعلّمين في مدارس التعليم العام بدولة الكويت بشأن آرائهم وتصوّراتهم (اتّجاهاتهم) حول مستوى وعيهم بالأمن السيبراني تُعزى لمتغيّر نوع التخصُّص (أدبي، علمي)، وذلك في الأداة عامّةً. ويُمكن تعليل هذه النتيجة بأنّ الأمن السيبراني مبحث حيويّ يهمُّ جميع الأفراد بغض النظر عن نمط تخصّصاتهم العلميَّة. ولذا، نجد بأنّ 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 مضمونها مع نتائج دراسة بحثيَّة أخرى، كدراسة الصانع وآخرون (٢٠٢٠)، ودراسة صفر (٢٠٢٤)، اللَّتان أشارتا إلى عدم وجود أيّ فروق دالَّة إحصائيًّا بين متوسّطات استجابات المجموعات المشاركة من أعضاء الهيئة التعليميَّة حول مستوى وعيهم بالأمن السيبراني يُمكن عزوها لمتغيّر نوع التخصُّص. 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 التخصُّص.

كما يتّضح من الجدول 4 أنّ اختبارات الفروق بين المجموعات المشاركة أبانت عن وجود فروق ذات دلالة إحصائيَّة عند مستوى الدلالة 0.01 بين متوسّطات استجابات أعضاء الهيئة التعليميَّة في مدارس التعليم العام بدولة الكويت بشأن آرائهم وتصوّراتهم (اتّجاهاتهم) حول مستوى وعيهم بالأمن السيبراني تُعزى لمتغيّر المؤهّل العلميّ (شهادة البكالوريوس، شهادة الماجستير/الدكتوراه)، وذلك في الأداة عامّةً، وجاءت لصالح المشاركين حاملي شهادة الإجازة الجامعية (البكالوريوس). ويُمْكِنْ أنْ نُفَسِّرَ تلك النتيجة حسب السياق الإحصائيّ ونُرْجِعُها إلى كبر حجم أفراد العيّنة المشاركة من أعضاء الهيئة التعليميَّة الحاصلين على شهادة الإجازة الجامعية (البكالوريوس) البالغ عددهم ١,٤٦٠ معلّمًا ومعلّمةً (حوالي 87.7%) مقارنةً بعدد المشاركين من فئة أعضاء الهيئة التعليميَّة الحاصلين على شهادة الدراسات العُليا (الماجستير/الدكتوراه) الذي بلغ ٢٠٤ معلّمًا ومعلّمةً (حوالي 12.3%). فربّما يكون هذا هو السبب في ظهور الاختلافات ذات الدلالة الإحصائية بين متوسّطات استجابات المشاركين من المعلّمين والمعلّمات وفقًا لمتغيّر المؤهّل العلميّ. وتتطابق نتيجة الدراسة الحالية نوعًا ما مع نتيجة دراسة الشهري (٢٠٢١) التي أكّدت على وجود فروق دالَّة إحصائيًّا بين متوسّطات استجابات المشاركين – معلّمي ومعلّمات قبل الخدمة – بالنسبة لمتغيّر المؤهّل العلميّ، وجاءت لصالح فئة حاملي شهادات الدراسات العُليا. وفي المقابل، تختلف هذه النتيجة للدراسة الراهنة مع النتائج التي ظهرت في بحوث أخرى، كدراسة الصحفي وعسكول (٢٠١٩)، ودراسة المنتشري وحريري (٢٠٢٠)، ودراسة الصانع وآخرون (٢٠٢٠)، إضافةً إلى دراسة الظويفري (٢٠٢١)، ودراسة العقلاء وعلي (٢٠٢٢)، التي لم تُشير إلى وجود أيّ فروق ذات دلالة إحصائيَّة بين متوسّطات استجابات المشاركين – أعضاء الهيئة التعليميَّة – في درجة وعيهم بالأمن السيبراني تُعزى لمتغيّر المؤهّل العلميّ.

وأيضًا يتبيّن من الجدول 4 أنّ اختبارات الفروق بين المجموعات المشاركة أظهرت عدم وجود اختلافات ذات دلالة إحصائيَّة عند مستوى الدلالة 0.05 بين متوسّطات تقديرات المعلّمين في مدارس التعليم العام بدولة الكويت بشأن آرائهم وتصوّراتهم (اتّجاهاتهم) حول مستوى وعيهم

بالأمن السيبراني تُعزى لمتغيّر مؤهّل الـ ICT (حاصل على شهادة دوليَّة، ، ليس لديه أيّ شهادة دوليَّة)، وذلك في الأداة عامّةً. ويُمكن أنْ نُفَسِّرَ هذه النتيجة بأنّ الأمن السيبراني قضية أساسيَّة تَهُمُّ وتَمِسُّ جميع أعضاء الهيئة التعليميَّة بغض النظر عمّا إذا كانوا قد حصلوا على أيّ شهادة دوليَّة في مجال الـ ICT من عدمه. وبناءً عليه، نجد بأنّ الوعي والإلمام والمعرفة بهذا الموضوع يُعَدُّ من الاهتمامات والأولويّات للجميع، ورُبّما يكون ذلك هو الباعث في ظهور توافق وانسجام تام في آراء وتصوّرات (اتّجاهات) الفئتين.

وكذلك يتّضح من الجدول 4 عدم وجود فروق ذات دلالة إحصائيَّة عند مستوى الدلالة 0.05 بين متوسّطات استجابات المعلّمين في مدارس التعليم العام بدولة الكويت بشأن آرائهم وتصوّراتهم (اتّجاهاتهم) حول مستوى وعيهم بالأمن السيبراني تُعزى لمتغيّر دورات الأمن السيبراني (التحق، لم يلتحق)، وذلك في المقياس عامّةً. ويُمكن تفسير هذه النتيجة حسب السياق المنطقي بأنّ الأمن السيبراني مسألة حيويَّة تَهُمُّ وتَمِسُّ كل المعلّمين بغض النظر عمّا إذا كانوا قد انضمّوا إلى دورات مُسبقة في مجال الأمن السيبراني من عدمه. وبناءً عليه، نجد بأنّ الوعي والمعرفة والإدراك بهذا الموضوع يُعَدُّ من الاهتمامات والأولويّات للجميع، ورُبّما يكون ذلك هو المُتسبّب في ظهور توافق وانسجام تام في آراء وتصوّرات (اتّجاهات) الفئتين. وتتطابق هذه النتيجة للدراسة الحالية في مضمونها مع نتيجة دراسة الصحفي وعسكول (٢٠١٩) التي أظهرت عدم وجود فروق دالَّة إحصائيًّا بين متوسّطات تقديرات معلّمات الحاسب الآلي بالمرحلة الثانوية في مدينة جدة نحو درجة وعيهنّ بالأمن السيبراني تبعًا لمتغيّر الدورات التدريبية، وبالمثل اتَّفقت 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 التدريبيَّة في مجال تكنولوجيا المعلومات والاتّصالات. بينما تتباين هذه النتيجة للدراسة الراهنة في فحواها 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 تدريبيَّة، وبالمثل اختلفت مع نتيجة دراسة صفر (٢٠٢٤) التي كشفت عن وجود اختلافات دالَّة إحصائيًّا بين متوسّطات استجابات

معلّمات قبل الخدمة بكلية التربية في جامعة الكويت بشأن مستوى وعيهنّ بالأمن السيبراني تُعزى لمتغيّر الدورات التدريبيَّة في مجال الأمن السيبراني لصالح من الْتَحَقْنَ بدورات تدريبيَّة مُسبقة في هذا المجال. وكذلك تغايرت مع نتيجة دراسة العقلاء وعلي (٢٠٢٢) التي كشفت عن وجود فروق دالَّة 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 تدريبيَّة.

جدول ٥

نتائج الإحصاء الاستدلاليّ لاختبار تحليل التباين الأحاديّ (ANOVA) لمقياس الدراسة تبعًا لمتغيّرَيْ مستوى الـ ICT وسنوات الخبرة المهنية

م	المتغيّر المستقل	مصدر التباين	مجموع المربعات	درجة الحرية	متوسّط المربعات	قيمة ف	الدلالة الإحصائيَّة	مستوى الدلالة
١	مستوى الـ ICT	بين المجموعات	24.290	2	12.145	38.047	0.000*	دالَّة
		داخل المجموعات	530.215	1,661	0.319			
		الكُلّي	554.505	1,663				
٢	سنوات الخبرة المهنية	بين المجموعات	1.108	2	0.554	1.663	0.190	غير دالَّة
		داخل المجموعات	553.396	1,661	0.333			
		الكُلّي	554.505	1,663				

*ملاحظة. * دالٌّ إحصائيًّا عند مستوى دلالة 0.01 (α≤0.01).*

يتّضح من الجدول ٥ وجود فروق دالَّة إحصائيًّا عند مستوى الدلالة 0.01 بين متوسّطات استجابات أفراد العيّنة المُشاركة – أعضاء الهيئة التعليميَّة في مدارس التعليم العام بدولة الكويت – بشأن آرائهم وتصوّراتهم (اتّجاهاتهم) نحو مستوى وعيهم بالأمن السيبراني تُعزى لمتغيّر مستوى الـ ICT (مبتدئ، ملم/متوسّط، محترف/متقدّم)، وذلك في الأداة عامّةً استنادًا إلى قيمة (ف) المحسوبة. وبالتحديد، فقد كشفت نتائج المقارنات البعدية إلى أنّ الفروق وُجِدَتْ بين المجموعات الزوجيَّة الثلاث: (مبتدئ، ملم/متوسّط)، و(مبتدئ، محترف/متقدّم)، و(ملم/متوسّط، محترف/متقدّم)؛ وهي دومًا لصالح فئة المشاركين ذات مستوى الـ ICT الأعلى. ويُمكن تعليل هذه النتيجة حسب السياق المنطقي إلى أنّ أفراد العيّنة المشاركة من فئة مستوى الـ ICT الأعلى هم الأكثر وعيًا، ودرايةً، ومعرفةً، واهتمامًا، ودافعيَّةً، ودعمًا لموضوع تبنّي استخدام وسائل،

وأدوات، وخدمات تكنولوجيا المعلومات والاتّصالات؛ ممّا يُؤثّر بالإيجاب أكثر على درجة أو مستوى وعيهم ومعرفتهم وإدراكهم بالأمن السيبراني، مقارنةً بالفئة ذات مستوى الـ ICT الأقل. وتتّفق هذه النتيجة في فحواها مع نتائج بحوث علميَّة أخرى، كدراسة Safar (٢٠٢٠) التي كشفت عن وجود فروق ذات دلالة إحصائيَّة بين متوسّطات استجابات أفراد عيّنة الدراسة في جميع العناصر السبعة المُكوّنة لنموذج قبول تكنولوجيا المعلومات والاتّصالات (ICT Acceptance Model – ICTAM) تُعزى لمتغيّر مستوى الـ ICT، وهذه الفروق هي دائمًا لصالح الأفراد ذوي الفئة الأعلى مستوى في الـ ICT. هذا بالإضافة إلى دراسة Amornkitpinyo وPiriyasurawong (٢٠١٥) التي أكّدت على وجود علاقة ارتباطيَّة إيجابيَّة (موجبة) وثيقة بين قبول التكنولوجيا ومستوى الـ ICT عند الأفراد؛ فكُلّما ارتفع مستوى الـ ICT عند الأفراد، زادت نسبة أو درجة قبول التكنولوجيا عندهم. وعلى النقيض، نجد بأنّ نتيجة الدراسة الراهنة قد تباينت نوعًا ما مع نتائج دراسات 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 أيّ معرفة (الأقل مستوى في الـ ICT). وكذلك اختلفت كُلِّيًا مع نتيجة دراسة صفر (٢٠٢٤) التي أشارت إلى عدم وجود فروق دالَّة 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.

كما يتبيّن من الجدول ٥ أيضًا عدم وجود فروق ذات دلالة إحصائيَّة عند مستوى الدلالة 0.05 بين متوسّطات تقديرات المشاركين – معلّمي ومعلّمات مدارس التعليم العام بدولة الكويت – بشأن آرائهم وتصوّراتهم (اتّجاهاتهم) نحو مستوى وعيهم ومعرفتهم ودرايتهم بالأمن السيبراني تُعزى لمتغيّر سنوات الخبرة المهنية (من ٠ إلى أقل من ١٠ سنوات، من ١٠ إلى أقل من ٢٠ سنة، من ٢٠ سنة فأكثر)، وذلك في الأداة عامّةً استنادًا إلى قيمة (ف) المحسوبة. ويُمكن تعليل هذه النتيجة بأنّ الأمن السيبراني هو الموضوع الجوهريّ الذي يَهُمُّ ويَمِسُّ الأشخاص في كل شرائح المجتمع بالعالم في الوقت الحاليّ – بما فيهم أعضاء الهيئة التعليميَّة – لأنّهم يعتمدون بشكل رئيس على وسائل التقانة الرقميَّة وأدواتها وتطبيقاتها في حياتهم اليومية –

الشخصية والمهنية – بغض النظر عن مستوى معارفهم ومهاراتهم وكفاياتهم وقدراتهم وخبراتهم في مجال تكنولوجيا المعلومات والاتّصالات. وبناءً عليه، نجد أنّ الوعي والإلمام بهذا المبحث يُعَدُّ من الاهتمامات والأولويّات لجميع الفئات العمرية من أعضاء الهيئة التعليميَّة وبمختلف عدد سنوات خبرتهم المهنية، ورُبّما يكون ذلك هو السبب في ظهور توافق وانسجام تام في آراء وتصوّرات (اتّجاهات) الفئات الثلاث. وتتّفق نتيجة الدراسة الحالية مع نتائج دراسات بحثيَّة أخرى، كدراسة الصحفي وعسكول (٢٠١٩)، ودراسة المنتشري وحريري (٢٠٢٠)، وكذلك دراسة الصانع وآخرون (٢٠٢٠)، ودراسة سراج الدين وآخرون (٢٠٢١)، وأيضًا دراسة الظويفري (٢٠٢١)، ودراسة العقلاء وعلي (٢٠٢٢)، التي لم تكشف عن وجود أيّ فروق ذات دلالة إحصائيَّة بين متوسّطات استجابات المشاركين – أعضاء الهيئة التعليميَّة – في درجة وعيهم ومعرفتهم ودرايتهم بالأمن السيبراني تُعزى لمتغيّر عدد سنوات الخبرة المهنية. بينما نجد بأنّ نتيجة الدراسة الراهنة قد اختلفت في فحواها مع نتائج دراسات أخرى، كنتيجة دراسة فرج (٢٠٢٢) التي أكّدت على وجود اختلافات دالَّة إحصائيًّا بين تقديرات المشاركين – أعضاء هيئة التدريس – نحو دواعي تعزيز ثقافة الأمن السيبراني في ظل التحوّل الرقميّ بجامعة الأمير سطام بن عبدالعزيز في السعودية تُعزى لمتغيّر سنوات الخبرة المهنية، وجاءت لصالح فئة "أقل من ٥ سنوات".

الخلاصة والتوصيات

في عصر التكنولوجيا الرقمية المُتقدّمة، أصبح الأمن السيبراني قضية حاسمة تشغل اهتمامنا جميعًا. يُشير مصطلح الأمن السيبراني إلى حماية أنظمتنا الإلكترونية وشبكاتنا وبياناتنا من التهديدات والهجمات الإلكترونية التي قد تُعرّضها للخطر. تُعد التقنيات الحديثة والتواصل الرقمي جزءًا لا يتجزأ من حياتنا اليومية، حيث ينعكس ذلك في استخدامنا للأجهزة المحمولة والشبكات الاجتماعية والتجارة الإلكترونية والخدمات الحكومية عبر الإنترنت. ومع زيادة هذا الاعتماد على التكنولوجيا الرقمية، تنمو أيضًا التهديدات والهجمات التي تستهدف أنظمتنا وبياناتنا السرية والحسّاسة. تتنوّع التهديدات السيبرانية وتصبح أكثر تطوّرًا وانتشارًا يومًا بعد يوم. فمن اختراقات القرصنة المباشرة إلى البرمجيّات الضارة والهجمات القائمة على الهندسة الاجتماعية، يُمكن أنْ تتسبّب هذه التهديدات في تعطيل الشركات والحكومات، وسرقة البيانات

والمعلومات السرية والحسّاسة، وانتهاك الخصوصيّة الشخصية، وتأثيرات سلبية أخرى على الأفراد والمجتمعات. تتطلب حماية الأنظمة والشبكات الإلكترونية إجراءات أمنية قويّة ومتنوّعة. يشمل ذلك تأمين البيانات والمعلومات، ومراقبة النشاطات غير المشروعة، وتطوير سياسات الأمن والتشفير، وتعزيز الوعي الأمني للمستخدمين وتدريبهم المُستمر على المُمارسات المُثلى في التعامل مع التهديدات والهجمات والاختراقات السيبرانية بشتّي أنواعها للتصدّي لها وردعها (الشهري، ٢٠٢١؛ الظويفري، ٢٠٢١؛ العقلاء وعلي، ٢٠٢٢؛ المنتشري وحريري، ٢٠٢٠) (ISO, 2023; ITU, 2022).

وفي ضوء النتائج التي توصّلت إليها الدراسة يُمكن أن نوصي بما يلي:

١. التركيز على نشر ثقافة الأمن السيبراني والاستخدام الفعّال للتكنولوجيا، لضمان الوقاية والحماية من التهديدات في العالم الرقمي. هذا من شأنه أنْ يُسهم في تعزيز الوعي بين أعضاء الهيئة التعليميَّة، وبناء جيل مثقّف في هذا الصدد.

٢. توفير التدريب والتوعية المستمرّة للمعلّمين والمعلّمات حول الأمن السيبراني ومخاطره – سواء السابقة، الحالية أو المستقبلية. يُمكن ذلك عبر استضافة خبراء متخصّصين لتقديم دورات وورش عمل تدريبية، جلسات نقاش ومحاضرات توعويَّة. كما يُمكن استخدام ملصقات، كتيّبات، نشرات توعويَّة، وتفعيل مواقع التواصل الاجتماعي لزيادة الوعي بهذه القضايا.

٣. إنشاء دليل إرشاديّ تربويّ تفاعليّ رقميّ حول الأمن السيبراني يُمكن أنْ يكون خطوة مهمّة. يُمكن استخدام تقنيات التفاعليّة مثل الفيديوهات التفاعليّة، والأسئلة العملية، والأمثلة الواقعية لتوضيح المفاهيم. كما يُمكن أنْ يتضمّن دليل الأمن السيبراني نصائح وإرشادات وتوجيهات عملية للمعلّمين والمتعلّمين والإداريّين حول السلوك الآمن عبر الإنترنت وحماية المعلومات والبيانات الشخصية. ويُمكن أنْ يشمل أيضًا أمثلة واقعية لحالات انتهاكات الأمان السيبراني وكيفية التعامل معها بشكل فعّال.

٤. تطوير السياسات والإجراءات والتدابير الوقائيَّة الأمنيّة في المؤسّسات التربوية التعليميَّة يُعدُّ أمرًا حيويًّا بالغ الأهمِّيَّة لحماية البيانات والمعلومات الشخصيَّة، وتعزيز الأمن السيبراني بشكلٍ عام، وفقًا للضوابط والمعايير الأساسيّة المحدّدة من قبل الهيئات والمؤسّسات والمنظّمات والجهات المعنيّة المختصّة في مجال الأمن السيبراني. هذا يشمل وضع

إجراءات واضحة للوقاية من الهجمات السيبرانية وتقديم التدريب المناسب للمعلّمين والمتعلّمين والإداريّين وبقيّة الموظّفين، بالإضافة إلى تطبيق إجراءات لحماية البيانات والمعلومات وتأمين الأنظمة ضد التهديدات الرقمية.

٥. تضمين المناهج التربوية في المدارس والمعاهد والكليات والجامعات بمبحث الأمن السيبراني وموضوعاته المتنوّعة، وذلك لتعزيز فهم المتعلّمين لمخاطر الإنترنت وطرق حماية البيانات والمعلومات الشخصية والأمان الرقميّ، وتوفير المعرفة والمهارات والكفايات والخبرات الضرورية للتعامل مع التحدّيات السيبرانية المتزايدة في عصرنا الحديث.

٦. دمج مبحث الأمن السيبراني وتضمينه في البرامج التربوية وبرامج إعداد المعلّم.

٧. إصدار تقارير ودلائل وموارد ومعايير الأمان السيبراني لتوجيه المؤسّسات والحكومات والأفراد في تعزيز الأمن السيبراني وتفعليه وزيادة فاعليّته.

٨. تعزيز التنسيق والتعاون والشراكة – محليًّا وخليجيًّا وعربيًّا وإقليميًّا ودوليًّا – بين المؤسّسات التربوية والهيئات والمنظمات المتخصّصة في مجال الأمن السيبراني يُسهم في زيادة الوعي وتعزيز الفهم العميق لمفاهيم الأمان السيبراني، وذلك من خلال تبادل المعرفة والخبرات وتقديم الموارد والدروس العملية التي تُسهم في تعزيز السلوكيّات الأمنية السليمة.

٩. إجراء المزيد من الدراسات البحثيَّة المشابهة باستخدام عيّنات ومتغيّرات ومنهجيّات مختلفة، وذلك على مجتمعات ذات سياقات مغايرة، لتعزيز الشمولية والتنوّع في النتائج والاستنتاجات. هذا النهج يُسهم في فهم أعمق للتحدّيات والحلول المتعلّقة بالأمن السيبراني في سياقات متنوّعة ويُساعد في تطوير قرارات وسياسات واستراتيجيات أكثر فاعليّة وملائمة لاحتياجات كل مجتمع.

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. (٢٠٢٣). *النشرة السنوية لإحصاءات التعليم ٢٠٢٢/٢٠٢٣* . الإدارة المركزية للإحصاء، دولة الكويت. https://www.csb.gov.kw/Pages/Statistics?ID=58&ParentCatID=70

التيماني، مداخل زيد عبدالرحيم. (٢٠٢١). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني. *مجلة الخدمة الاجتماعية*، (٦٧-ج)، ١-٢٣.

الحبيّب، 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.

الداغر، مجدي. (٢٠٢١). اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبراني في مصر: دراسة ميدانية. *المجلة العربية لبحوث الإعلام والاتصال*، (٣٣)، ٤-١١٠. https://doi.org/10.21608/JKOM.2021.195915

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. (٢٠١٢). *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

العنزي، ناهس. (٢٠٢١). *جرائم تقنية المعلومات ومنصّات التواصل الاجتماعي: دراسة تحليلية لمنصّات التواصل الاجتماعي وفقًا لقانون جرائم مكافحة تقنية المعلومات الكويتي قانون رقم ٦٣ لسنة ٢٠١٥ بإنشاء هيئة تنظيم الاتّصالات وتقنية المعلومات والتعديلات المتعلّقة بهما معلّقًا عليها بآراء الفقه مع أحدث الأحكام والمبادئ القانونية*. الموسوعة للمحاماة والاستشارات القانونية.

القحطاني، نورة بنت ناصر. (٢٠١٩). مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. *شؤون اجتماعية*، ٣٦ (١٤٤)، ٨٥-١٢٠. https://doi.org/10.35217/0048-036-144-004

اللصاصمة، عبدالكريم سلمان، والمجالي، فايز عبدالقادر. (٢٠٢٢). الأدوار الأكاديمية والتوعوية للجامعات الأردنية الرسمية نحو أمن المعلومات الإلكترونية من وجهة نظر أعضاء هيئة التدريس فيها. *حوليات آداب عين شمس*، ٥٠(٣)، ٨٢-٩٦. https://doi.org/10.21608/AAFU.2022.235517

المنتشري، فاطمة يوسف. (٢٠٢٠). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلّمات. *المجلة العربية للعلوم التربوية والنفسية*، ٤ (١٧)، ٤٥٧-٤٨٤. https://doi.org/10.33850/JASEP.2020.100703

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

الهيئة الوطنية للأمن السيبراني. (٢٠١٨). *تقرير الضوابط الأساسية للأمن السيبراني*. الهيئة الوطنية للأمن السيبراني، المملكة العربية السعودية. https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

بانقا، علم الدين. (٢٠١٩). مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي. *دراسات تنموية*، (٦٣)، ١-٦٥.

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.

خليفة، إيهاب. (٢٠١٧). *القوة الإلكترونية: كيف يُمكن أن تدير الدول شؤونها في عصر الإنترنت؟ "الولايات المتحدة الأمريكية نموذجًا"*. العَربيّ للنشر والتوزيع.

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

صفر، عمار حسن. (٢٠٢٤). مستوى وعي معلّمات قبل الخدمة في كلية التربية بجامعة الكويت بالأمن السيبراني. *المجلة التربوية – جامعة سوهاج*، (١١٨-١)، ٢٣٧-٢٧٨. https://doi.org/10.21608/EDUSOHAG.2024.245756.1362

فرج، علياء عمر كامل. (٢٠٢٢). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي: جامعة الأمير سطام بن عبدالعزيز نموذجاً. *المجلة التربوية – جامعة سوهاج*، (٩٤-١)، ٥٠٩-٥٣٧. https://doi.org/10.21608/EDUSOHAG.2022.212365

فوزي، إسلام. (٢٠١٩). الأمن السيبراني: الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي. *المجلة الاجتماعية القومية*، ٥٦(٢)، ٩٩-١٣٩. https://doi.org/10.21608/JNS.2019.205220

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

قطب، بشائر حامد عبدالقادر، وحلبي، آمال سعد الدين. (٢٠٢١). دور الصحف السعودية في تنمية الوعي بالأمن السيبراني: دراسة على القائم بالاتصال. *المجلة العربية للإعلام والاتصال*، (٢٥)، ٢٩٥-٣٣٥.

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.

Amornkitpinyo, T., & Piriyasurawong, P. (2015). Causal Relationship Model of the information and communication technology skill affect the Technology Acceptance Process in the 21st century for undergraduate students. *International Journal of Emerging Technologies in Learning, 10*(1), 68-71. https://doi.org/10.3991/ijet.v10i1.4185

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

Bamford, J. (2009). *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America*. Anchor.

Calder, A. (2020). *The cyber security handbook: Prepare for, respond to and recover from cyber attacks with the IT Governance Cyber Resilience Framework (CRF)*. IT Governance Publishing.

Canongia, C., & Mandarino, R. (2014). Cybersecurity: The new challenge of the information society. In I. Management Association (Ed.), *Crisis management: Concepts, methodologies, tools, and applications* (pp. 60-80). IGI Global. https://doi.org/10.4018/978-1-4666-4707-7.ch003

Cisco. (2022). *Security outcomes report, volume 3: Achieving security resilience*. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/security-outcomes-vol-3-report.pdf

Cisco. (2023a). *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

Cisco. (2023b). *Privacy's growing importance and impact: Cisco 2023 data privacy benchmark study*. Cisco. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-

2023.pdf?CCID=cc000160&DTID=odicdc000016&OID=rptsc030828

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

European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2020). *The EU's Cybersecurity Strategy for the digital decade*. European Commission, and High Representative of the Union for Foreign Affairs and Security Policy. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

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

European Union Agency for Cybersecurity. (2022). *ENISA threat landscape 2022: July 2021 to July 2022*. European Union Agency for Cybersecurity (ENISA). https://doi.org/10.2824/764318

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

Furnell, S. (2003). Cybercrime: Vandalizing the information society. In J. M. C. Lovelle, B. M. G. Rodríguez, J. E. L. Gayo, M. del Puerto Paule Ruiz, & L. J. Aguilar (Eds.), *Lecture notes in computer science: Vol. 2722. Web engineering: ICWE 2003* (pp. 8-16). Springer. https://doi.org/10.1007/3-540-45068-8_2

Furnell, S., & Dowling, S. (2019). Cyber crime: A portrait of the landscape. *Journal of Criminological Research, Policy and Practice, 5*(1), 13-26. https://doi.org/10.1108/JCRPP-07-2018-0021

Furnell, S., & Moore, L. (2014, May). Security literacy: The missing link in today's online society? *Computer Fraud & Security, 2014*(5), 12-18. https://doi.org/10.1016/S1361-3723(14)70491-9

Hadnagy, C., & Fincher, M. (2015). *Phishing dark waters: The offensive and defensive sides of malicious emails*. Wiley.

Hibberd, G. (2022). *The art of cyber security: A practical guide to winning the war on cyber crime*. IT Governance Publishing.

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 (ITU). https://www.itu.int/hub/publication/d-ind-global-01-2022/

Jakobsson, M., & Myers, S. (2007). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. Wiley-Interscience.

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.

Kritzinger, E., Bada, M., & Nurse, J. R. C. (2017). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In M. Bishop, L. Futcher, N. Miloslavskaya, & M. Theocharidou (Eds.), *Information security education for a global digital society, Proceedings of the 10th IFIP world conference on information security education (WISE) 2017. IFIP Advances in Information and Communication Technology: Vol. 503*, (pp. 110-120). Springer. https://doi.org/10.1007/978-3-319-58553-6_10

Lewis, T. G. (2020). *Critical infrastructure protection in homeland security: Defending a networked nation* (3rd ed.). Wiley.

Li, P., Yang, X., Xiong, Q., Wen, J., & Tang, Y. Y. (2018). Defending against the advanced persistent threat: An optimal control approach. *Security and Communication Networks, 2018*, Article 2975376. https://doi.org/10.1155/2018/2975376

Mitnick, K., & Simon, W. L. (2012). *Ghost in the wires: My adventures as the world's most wanted hacker*. Hachette Book Group.

Moyo, M., Sadeck, O., Tunjera, N., & Chigona, A. (2022). Investigating cyber security awareness among preservice teachers during the COVID-19 pandemic. In M. Themistocleous, & M. Papadaki (Eds.), *Lecture notes in business information processing: Vol. 437. Information systems: EMCIS 2021* (pp. 527-550). Springer. https://doi.org/10.1007/978-3-030-95947-0_38

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. (2024). *ChatGPT* (Jan 8 version) [Large language model]. https://chat.openai.com/chat

Organization for Security and Co-operation in Europe. (2017). *European Union's cybersecurity report*. Organization for Security and Co-operation in Europe (OSCE).

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

Peltier, T. R. (2014). *Information security fundamentals* (2nd ed.). Routledge.

Russinovich, M. (2012). *Zero day*. Thomas Dunne Books.

Safar, A. H. (٢٠٢٠). Kuwait University students' awareness, usage, perceptions, and satisfaction pertaining to e-books. *Annals of the Arts and Social Sciences, 40*(549), 5-100. https://doi.org/10.34120/0757-040-549-001

Schneier, B. (2015). *Data and goliath: The hidden battles to collect your data and control your world*. W. W. Norton & Company.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Tiwari, S., Bhalla, A., & Rawat, R. (2016). Cyber-crime and security. *International Journal of Advanced Research in Computer Science and Software Engineering, 6*(4), 46-52.

United Nations Office on Drugs and Crime. (2024). *Cybercrime*. United Nations. https://www.unodc.org/romena/en/cybercrime.html

U.S. Department of Homeland Security. (2013). *The National Infrastructure Protection Plan (NIPP) 2013: Partnering for critical infrastructure security resilience*. U.S. Department of Homeland Security (U.S. DHS). https://fedvte.usalearning.gov/publiccourses/critical101/0110.htm

Vasani, V., Bairwa, A. K., Joshi, S., Pljonkin, A., Kaur, M., & Amoon, M. (2023). Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion. *Electronics, 12*(20), Article 4299. https://doi.org/10.3390/electronics12204299

World Bank Group. (2019). *ID4D practitioner's guide*. World Bank Group. https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf