المجلة العلمية لجامعة الملك فيصل
The Scientific Journal of King Faisal University
العلوم الإنسانية والإدارية
Humanities and Management Sciences

The Awareness of Cyber Security in Distance Learning

الوعي بجوانب الأمن السيبراني في التعليم عن بعد

Manal Hassan Muhammad Bin Ibrahim
Department of Curricula and Teaching, College of Education, University of Jeddah, Jeddah, Saudi Arabia

منال حسن محمد بن إبراهيم
قسم المناهج والتدريس، كلية التربية، جامعة جدة، جدة، المملكة العربية السعودية

LINK الرابط	RECEIVED الاستقبال	ACCEPTED القبول	PUBLISHED ONLINE النشر الإلكتروني	ASSIGNED TO AN ISSUE الإحالة لعدد
https://doi.org/10.37575/h/edu/0089	01/11/2020	05/03/2021	05/03/2021	01/09/2021

NO. OF WORDS عدد الكلمات	NO. OF PAGES عدد الصفحات	YEAR سنة العدد	VOLUME رقم المجلد	ISSUE رقم العدد
7983	9	2021	22	2

ABSTRACT

The present paper aims to investigate the effectiveness of a training program in improving the awareness of cyber security in distance learning among female primary school science teachers in the Kingdom of Saudi Arabia. To achieve the study objectives, the researcher used the quasi-experimental approach based on the one-group experimental design; the study tool was the cyber security awareness scale. The sample consisted of 30 teachers. The pre-application of the cyber security awareness scale was performed, then teachers were trained on the proposed program during the first semester of 2020–2021. At the end of the experiment, the post-scale was conducted. The results show that there are statistically significant differences between the mean scores of the teachers in the pre- and post-application phases of testing of the cyber security awareness scale for the sake of the post application. These differences indicate the degree of effectiveness of the suggested training program. A number of recommendations are suggested in light of the obtained results.

الملخص

استهدف البحث الكشف عن فاعلية برنامج تدريبي مُقترح لتنمية الوعي بجوانب الأمن السيبراني في التعليم عن بُعد لدى معلمات العلوم بالمرحلة الابتدائية في المملكة العربية السعودية، واستخدم المنهج التجريبي ذو التصميم شبه التجريبي ذي المجموعة الواحدة، وتمثَّلت أداة الدراسة في مقياس الوعي بجوانب الأمن السيبراني في التعليم عن بُعد، وشمل مجتمع الدراسة معلمات العلوم بالمرحلة الابتدائية، وتكوَّنت عينة الدراسة من (30) معلمة، وطُبّق مقياس الوعي بجوانب الأمن السيبراني في التعليم عن بُعد قبليًّا، وبعد تدريب المعلمات على البرنامج المُقترح خلال الفصل الدراسي الأول لعام 1442/1441هـ، بواقع (10) جلسات تدريبية، ثم طُبّق المقياس بعديًّا. وأسفرت نتائج البحث عن وجود فرق ذي دلالة إحصائية عند مستوى ($\alpha \leq 0,05$)، بين متوسطي درجات المعلمات في التطبيقين القبلي والبعدي لمقياس الوعي؛ لصالح التطبيق البعدي؛ ويدلّ هذا على فاعلية البرنامج التدريبي المُقترح، وقد انتهى البحث إلى صياغة عدد من التوصيات في ضوء نتائج البحث.

KEYWORDS
الكلمات المفتاحية
Training, cybercrimes, e-learning, coronavirus, Arab society, and educational technology
التدريب، الجرائم الإلكترونية، التعليم الإلكتروني، الكورونا، المجتمع العربي، تقنيات التعليم

CITATION
الإحالة
Bin Ibrahim, M.H.M. (2021). Alwaey bijawanib al'amn alsiybranii fi altaelim ean baed 'The awareness of cyber security in distance learning'. *The Scientific Journal of King Faisal University: Humanities and Management Sciences*, **22**(2), 299–307. DOI: 10.37575/h/edu/0089

إبراهيم، منال حسن محمد. (2021). فعالية برنامج تدريبي مقترح لتنمية الوعي بجوانب الأمن السيبراني في التعليم عن بُعد لدى معلمات العلوم. *المجلة العلمية لجامعة الملك فيصل: العلوم الإنسانية والإدارية*، **22**(2)، 299-307.

1. مقدمة

شهدت الآونة الأخيرة تغيرًا جذريًّا في تكنولوجيا المعلومات والاتصالات، وأصبح العالم بأكمله في حالة من التواصل والتكامل، وأصبحت تكنولوجيا المعلومات هي المهيمن والمسيطر؛ حتى إنها صارت المحرك الأساسي الذي يقود عملية النمو والتقدم، حيث سيطرت على حياتنا اليومية ودخلت في تفاصيلها، سواء الحياة العلمية أو العملية. وأصبحت أمور حياتنا متعلّقة باستخدام الإنترنت والتكنولوجيا، ورغم كل الإيجابيات والراحة التي توفّرها التكنولوجيا؛ لكن ظهرت مشكلات من أهمها سلبيات الجرائم السيبرانية التي تهدد الأمن الشخصي والدولي بكافة أنواعه.

وقد أصبح الأمن السيبراني (Cyber Security) موضوعًا للاهتمام العام والجهود البحثية بشكل متزايد؛ إذ ازداد عدد الدراسات التي تبحث في أدوار المعلمين والمعلمات بشكل خاص، كوضع قواعد في المنهج والصف تساعد على فهم الأمن السيبراني بشكل واضح، وتمكين الطالبات من مهارات حل المشكلات، وتقديم مشورة الأقران، وتوعية الأهل بالأمن السيبراني من خلال اجتماعات أولياء الأمور، ومن خلال النشرات الإخبارية (الصحفي والعسكول، 2019: 495).

وتزداد أهمية الأمن السيبراني بوصفه يشمل جميع الجوانب: التعليمية، والاجتماعية، والاقتصادية، والإنسانية، وبوصفه مثالًا لقدرة الدولة على حماية مصالحها وشعبها في مختلف مجالات حياته اليومية، ومسيرته نحو التقدّم بأمان؛ كونه يرتبط ارتباطًا وثيقًا بسلامة مصادر الثروة المعلوماتية في العصر الحالي، والقدرة على الاتصال والتواصل، وهي المحور الذي يتكوّن حوله الإنتاج، والإبداع، والقدرة على المنافسة (الجبور، 2012 : 7).

وقد اهتمت دول العالم بدور المؤسسات التربوية؛ نظرًا لدور تلك المؤسسات في إعداد المعلمين بشكل يُمكّنهم من التعامل مع كافة التطورات التكنولوجية، التي يُتوقّع أن تصل إلى آفاق أبعد في عالم الغد، وما يتطلبه هذا التعامل من درجة وعي كافية بالأمن السيبراني.

ويشهد الواقع الاجتماعي في المملكة العربية السعودية تطورًا كبيرًا في استخدام نظم المعلومات بجميع أجهزة الدولة ومؤسساتها، حيث يُستخدم في الأعمال البنكية والاقتصادية والصناعية والإجراءات الحكومية المختلفة، وقد دخلت التكنولوجيا ونظم المعلومات في العلاج وحركة الطيران، وليس المجتمع السعودي بمنأى عن التأثيرات العالمية، فقد أصبح مستهدفًا من المنظمات الإجرامية الدولية؛ لما تتمتّع به المملكة من مكانة اقتصادية وجغرافية (البقمي، 2007، القحطاني، 2019).

ويعمل عدد من المنظمات الدولية باستمرار لمواكبة التطورات في شأن أمن الفضاء الإلكتروني، وقد أسست مجموعات عمل لوضع استراتيجيات لمكافحة جرائم الإنترنت. ويُستخدم مصطلح «الأمن السيبراني» لتلخيص الأنشطة المختلفة، كجمع المعلومات، ووضع السياسات العامة والتدابير الأمنية، والمبادئ التوجيهية، وطرق إدارة المخاطر، والحماية، والتدريب، ودليل لأفضل الممارسات المهنية، ومختلف التقنيات التي يمكن استخدامها لحماية شبكة الإنترنت. وتشمل هذه السياسات المعلومات

Corresponding Author: Manal Hassan Muhammad bin Ibrahim mhibrahim@uj.edu.sa, 00966566639993 المؤلف المراسل: منال حسن محمد بن إبراهيم

وأجهزة الكمبيوتر، والأفراد، والبنية التحتية، والخدمات، ومجمل المعلومات المنقولة أو المُخزّنة في الأجهزة الإلكترونية. ويهدف الأمن السيبراني إلى ضمان تحقيق سلامة المؤسسات والأفراد في مواجهة المخاطر الأمنية وكل ما يتعلّق بشبكة الإنترنت (المقصودي، 2017: 106).

وقد حقّقت المملكة العربية السعودية إنجازًا عالميًّا بحصولها على المركز الثالث عشر والأول عربيًّا من بين (175) دولة في المؤشر العالمي للأمن السيبراني (GCI)، الذي يصدره الاتحاد الدولي للاتصالات، التابع للأمم المتحدة لعام 2018م، متقدّمة (33) مرتبة عن تقييمها في الإصدار السابق للمؤشر العالمي لعام 2016م، وخصوصًا بعد إنشاء الهيئة الوطنية للأمن السيبراني في 2007/10/31م، حيث أطلقت الهيئة العديد من المبادرات والمشروعات المهمة، التي أسهمت في تعزيز هذا النوع من الأمن في المملكة، مؤكدة أنها تتطلّع إلى فضاء سيبراني سعودي آمن وموثوق من خلال مستوى نضج أعلى في الأمن السيبراني بجميع الجهات الوطنية، وبالتعاون مع الأطراف ذات العلاقة (جريدة سبق، 2019).

وقد أطلقت الهيئة الوطنية للأمن السيبراني - ممثلةً بالمركز الوطني الإرشادي للأمن السيبراني- بالتعاون مع وزارة التعليم حملة بعنوان: (بأمان_نتعلّم)، في إطار جهود المركز في رفع الوعي والمعرفة بالأمن السيبراني؛ لتجنّب المخاطر السيبرانية وتقليل آثارها، عن طريق إصدار التنبيهات بآخر الثغرات والمنشورات التوعوية وأخطرها. وتهدف الحملة التي جاءت متزامنة مع بداية العام الدراسي (2020) إلى رفع الوعي بالأمن السيبراني، وتقليل المخاطر التي قد يتعرّض إليها الطالب في أثناء ممارسة مهامه التعليمية اليومية باستخدام شبكة الإنترنت.

2. مشكلة الدراسة

لمّا كانت معظم الدول اليوم تعتمد على تكنولوجيا المعرفة والمعلوماتية في تسيير شؤونها العامة - لاسيما في العالم المتقدّم- فإن أي اختراق أو تعطيل للمنظومة التقنية المعتمدة فيها؛ يعدُّ تهديدًا مباشرًا لأمنها القومي؛ كونه سلوكًا موجهًا من قِبل مجموعات أو دول أخرى عمدًا؛ لإحداث خلل أو إرباك في الأطر العامة للدولة ومؤسساتها، بما يرقى إلى مستوى التهديد العام؛ وبالتالي فإن الاختراقات التي تصيب جزءًا منها، ستنفذ لا محالة إلى الأجزاء الأخرى، وهو ما يُعرّض الأمن الاستراتيجي العالمي بالمجمل إلى التهديدات، التي تستلزم وضع خطط وبرامج دفاعية تحذيرية؛ تحسبًا لأي سلوك تهديدي طارئ، له المقدرة العالية على التطويق والاستجابة والمعالجة (القيسي، 2020).

وقد سبّبت الهجمات الإلكترونية ضررًا كبيرًا على البنية التحتية في المملكة العربية السعودية، وتمثّلت أبرز الحوادث الرئيسة في هجمات استهدفت بداية شركة أرامكو السعودية، وعطّلت نشاطها لمدة شهر فيما يُشار إليه بأكبر اختراق في التاريخ، وتسبّبت هذه البرمجيات الخبيثة في حدوث خلل مرة أخرى في نوفمبر 2016، ويناير 2017.

واستنادًا إلى ما توصّلت إليه بعض الدراسات السابقة من نتائج، وما قدّمته من مقترحات، التي أكّدت جميعها أهمية الأمن السيبراني، وضرورة توعية الطلاب والمعلمين لحماية بياناتهم، والحفاظ على بيئة عمل آمنة من الاختراقات وعمليات التجسس والابتزاز، ومن هذه الدراسات: المنتشري وحريري (2020)، والقيسي (2020)، و.Richardson et al (2020)، والقحطاني (2019)، وصائغ (2018).

وقد أكّدت المنتشري وحريري (2020: 115) أن هناك مسؤولية مزدوجة تقع على عاتق المعلمات في عصر الثورة المعلوماتية، يتعلّق الجانب الأول من هذه المسؤولية بضرورة الوعي بالأمن السيبراني، بوصفه من الأمور اللازمة لكل مستخدم للإنترنت بشكل عام، فضلًا عن أهميته بالنسبة للمعلمة بشكل خاص؛ نظرًا لدورها المهم في إعداد الطالبات وتوعيتهن بمخاطر الأمن السيبراني وانتهاكاته.

وفي ضوء ما سبق؛ تبلورت مشكلة البحث في السؤال الرئيس الآتي: "ما فعالية البرنامج التدريبي المُقترح في تنمية جوانب الوعي بالأمن السيبراني في التعليم عن بُعد لدى معلمات العلوم بالمرحلة الابتدائية؟" ويتفرّع من السؤال الرئيس السابق الأسئلة الفرعية الآتية:

- ما جوانب الأمن السيبراني في التعليم عن بُعد اللازم تنميتها لدى معلمات العلوم بالمرحلة الابتدائية؟
- ما البرنامج التدريبي المُقترح لتنمية جوانب الوعي بالأمن السيبراني لدى معلمات العلوم بالمرحلة الابتدائية؟
- هل توجد فروق ذات دلالة إحصائية بين متوسطي درجات المعلمات (مجموعة الدراسة)، اللاتي خضعن للتدريب على البرنامج المُقترح في مقياس الوعي بالأمن السيبراني في التطبيقين القبلي والبعدي؟

3. أهداف الدراسة

- تصميم مقياس وعي يقيس الوعي لدى معلمات العلوم بجوانب الأمن السيبراني في التعليم عن بُعد.
- بناء برنامج تدريبي مُقترح لتنمية الوعي بجوانب الأمن السيبراني في التعليم عن بُعد لدى معلمات العلوم بالمرحلة الابتدائية.
- الكشف عن فعالية استخدام البرنامج التدريبي المُقترح في تنمية الوعي بجوانب الأمن السيبراني في التعليم عن بُعد لدى معلمات العلوم بالمرحلة الابتدائية.

4. أهمية الدراسة

- تعدُّ هذه الدراسة من الدراسات القليلة التي قدَّمت برنامجًا تدريبيًّا لتنمية الوعي بجوانب الأمن السيبراني لدى معلمات العلوم بالمرحلة الابتدائية.
- توجيه المعلمات إلى أهمية توفير بيئة عمل آمنة خالية من التهديد وخرق المعلومات في الفصول الافتراضية.
- إحداث نهضة علمية وثقافية من خلال تطوير قدرات المعلمات الشخصية والمهنية، وتدريبهن على تبني الافكار الجديدة، وفتح آفاق جديدة لتعزيز الأمن السيبراني.
- حداثة الدراسة ومواكبتها للتغير المحلي والعالمي في مجال الأمن السيبراني؛ قد يُساعد على تطوير المعلمين والمعلمات في هذا المجال، الذين يكونون قادرين على توعية الطلاب والطالبات أولًا ثم المجتمع.

5. حدود الدراسة

اقتصرت الدراسة الحالية على الحدود الآتية:

- **حدود بشرية**: معلمات العلوم بالمرحلة الابتدائية.
- **حدود مكانية**: معلمات المدارس بجدة ومكة والطائف.
- **حدود زمانية**: الفصل الدراسي الأول للعام الجامعي (2020-2021).
- **حدود موضوعية**: الاقتصار على مهارات الوعي بالأمن السيبراني في تدريس البرنامج المُقترح، ومقياس الوعي.

6. مصطلحات الدراسة

- **الأمن السيبراني (Cyber Security)**: عرّف التقرير الصادر عن الاتحاد الدولي للاتصالات (2011: 17) الأمن السيبراني بأنه: مجموعة من المهمات مثل: (تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات)، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين.
- **الوعي بالأمن السيبراني (Awareness of Cyber Security)**: عرّف العريفي (1996) الوعي بأنه: إدراك الإنسان لذاته ولما يحيط به إدراكًا مباشرًا، وهو أساس كل معرفة. كما يشير الوعي إلى الفهم وسلامة الإدراك، ويُقصد بهذا الإدراك إدراك الإنسان لنفسه وللبيئة المحيطة به. ويعني هذا فهم الإنسان لذاته وللآخرين عند تفاعله معهم؛ سعيًا لإشباع حاجاته، وقضاء مصالحه وهو مُدرك للعلاقات بينه وبين الآخرين والبيئة من خلال المواقف المختلفة. ويُعرّف الوعي بالأمن السيبراني إجرائيًّا بأنه: إدراك المعلمة بما يدور حولها من جرائم إلكترونية واختراقات للبيانات والحسابات الشخصية؛ سعيًا لتحقيق الأمن المعلوماتي، واتخاذ كافة الإجراءات الاحترازية؛ للوقاية من خرق الأجهزة والبيانات وكل ما يتعلّق بالتقنية ذات العلاقة بتوفير بيئة تعلّم عن بُعد آمنة للمعلمة وللمتعلمة، ويُقاس بالدرجة التي تحصل عليها المعلمة في المقياس المُعدّ لذلك.

7. الإطار النظري والدراسات السابقة

7.1. الإطار النظري:

7.1.1. مفهوم الأمن السيبراني

الأمن السيبراني هو: مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المُصرّح به وسوء الاستغلال، واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها؛ بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية البيانات الشخصية وسريتها وخصوصيتها، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. والأمن السيبراني سلاح استراتيجي بيد الحكومات والأفراد، لا سيما أن الحرب السيبرانية أصبحت جزءًا لا يتجزّأ من التكتيكات الحديثة للحروب والهجمات بين الدول (جريدة الوطن، 2020).

وعرّفت جبور (2012) الأمن السيبراني بأنه: أمن الشبكات، والأنظمة المعلوماتية، والبيانات والمعلومات، والأجهزة المتصلة بالإنترنت. إذًا فالأمن السيبراني هو المجال الذي يتعلّق بإجراءات الحماية ومقاييسها ومعايرها المفروض اتخاذها أو الالتزام بها؛ لمواجهة التهديدات ومنع التعدّيات؛ للحدّ من آثارها في أقسى الأحوال وأسوئها. وهو النشاط الذي يُؤمّن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحدّ من الخسائر والأضرار التي تترتب في حال تحقّق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقّف عجلة الإنتاج، ولا تتحوّل الأضرار إلى خسائر دائمة.

وتُعرّفه المنتشري وحريري (2020) بأنه يُشكّل جميع إجراءات حماية شبكات المعلومات ضد كافة الأعمال والممارسات التي تستهدف التلاعب بتلك المعلومات، والحاق الأذى بالمستخدمين، بما يشمل الحماية ضد الاختراق، وبثّ البرمجيات الخبيثة والفيروسات، والوصول غير المُصرَّح به، وغير ذلك من ممارسات سلبية.

وعرّفته الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية (2018) بأنه: حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوّناتها من أجهزة وبرمجيات، وما تقدّمه من خدمات، وما تحويه من بيانات من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع. كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحوها.

كما عُرّف الأمن السيبراني بأنه: التدابير المُتخذة لحماية جهاز كمبيوتر أو شبكة من الوصول غير المُصرَّح به؛ للحفاظ على سلامة المعلومات المُخزّنة وأمنها. ويتضمّن الأمن السيبراني التدخّلات الفنية التي تحمي البيانات ومعلومات الهوية والأجهزة من الوصول غير المُصرَّح به أو الضرر، بما في ذلك أمن الفضاء الإلكتروني (Richardson, et al., 2020).

وينبثق من الأمن السيبراني الوعي الأمني، الذي عرّفته الخياط (2018) بأنه: إدراك المعلم لذاته وللمسؤولية المُؤتمن عليها، وإدراكه للظروف الأمنية المحيطة به، وتكوين اتجاه عقلي إيجابي نحو الموضوعات الأمنية العامة للمجتمع، تُمثِّل سياجًا وقائيًّا وتحصينًا فكريًّا لمن يقوم بتدريسهم أو التعامل معهم.

7.1.2. أهمية الأمن السيبراني:

ذكر الصحفي والعسكول (2019) أن هناك أهمية تربوية كبيرة للأمن السيبراني، والواجب توافرها لضمان الحماية الكافية للمعلومات، ومنها:

- أولًا: السرية والأمن (Confidentiality): وتعني التأكد من أن المعلومات لا تُكشف ولا يُطلع عليها من قِبل أشخاص غير مُخوّلين بذلك.
- ثانيًا: التكاملية (Integration) وسلامة المحتوى (Content integrity): وهو التأكد من أن محتوى المعلومات صحيح ولم يُعدّل، وعلى نحو خاص لم يدمر أو يُغيّر أو يُعبث به في أي مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي مع المعلومات، أو عن طريق تدخّل غير مشروع.
- ثالثًا: استمرارية توافر المعلومات أو الخدمة (Continuation): إذ يجب التأكد من استمرار عمل النظام المعلوماتي، واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة للمواقع المعلوماتية، وأن المُستخدِم لن يتعرَّض إلى منع الاستخدام أو الدخول إلى النظام.
- رابعًا: عدم إنكار التصرّف المرتبط بالمعلومات ممن قام به: ويُقصد به ضمان إنكار الشخص المتصل بالمعلومات أو مواقعها بقيامه بتصرف ما، بحيث تتوافر قدرة إثبات هذا التصرف، وأن شخصًا ما في وقت معين قد قام به، كذلك عدم قدرة مستلِم رسالة معينة على إنكار استلامه لهذه الرسالة.

وأضافت المنتشري وحريري (2020: 103) بأنه مما يزيد من الأهمية التربوية للأمن السيبراني تعرّض المعلمين إلى الانتهاكات والمخاطر السيبرانية دون أن يكون لديهم دراية بتلك الانتهاكات والمخاطر، ومدى خطورتها على التصفّح الآمن للإنترنت؛ وهو ما يدعو إلى ضرورة رفع مستوى الوعي بأهمية الأمن السيبراني لدى هؤلاء المعلمين، وضرورة تضافر الجهود من قِبل المدرسة ووزارة التعليم في هذا الشأن.

وفي هذا الصدد، ذكر الشهري (2017: 5) أنَّ من الضروري أن تواكب التشريعات المختلفة هذا التطور الملحوظ في الجرائم المعلوماتية، فالمواجهة التشريعية ضرورية للتعامل من خلال نظم قانونية غير تقليدية لهذا الإجرام غير التقليدي. وتتعامل هذه المواجهة بشكل عصري متقدِّم مع جرائم الكمبيوتر المختلفة، التي يأتي في مقدمتها الدخول غير المشروع على شبكات الحاسب ونظم المعلومات، والتحايل على نظم المعالجة الآلية للبيانات، ونشر الفيروسات وإتلاف البرامج، وتزوير المستندات، ومهاجمة المراكز المالية والبنوك، وتعدتها إلى الحروب الإلكترونية، والإرهاب الإلكتروني، ونشر الشائعات والنيل من هيبة الدول، إضافة إلى نشر الرذيلة والإباحية، وغيرها من الجرائم الإلكترونية.

7.1.3. الصراع الإلكتروني في الفضاء السيبراني:

يُطلق على الفضاء السيبراني المستودع الكبير الذي تُجرى فيه جميع عمليات التواصل الإلكتروني، عبر شبكات الحواسيب. وبتعبير أكثر اتساعًا: هو منظومة من العناصر المتفاعلة فيما بينها، والمتكوّنة من أجهزة الكمبيوتر، وأنظمة الشبكات والبرمجيات، وحوسبة المعلومات، ونقل البيانات وتخزينها، ومستخدمي كل هذه العناصر. وتتداخل بنية الفضاء السيبراني بأنظمة البرمجيات، والعناصر المادية، والفضاء الرقمي؛ لتُشكِّل منظومة معلوماتية في إطار برمجيات التواصل الإلكتروني (القيسي، 2020: 153).

7.2. الدراسات السابقة:

أعدَّ Morris and Thomas (2015) مشروعًا لإنشاء فصل دراسي افتراضي قائم على الوسائط المتعددة في مختبر افتراضي لتعليم أمن (CPS)، وتساعد هذه القاعة الدراسية الافتراضية على وجه الخصوص طلاب الجامعات في المناطق الريفية محدودة الموارد على تعلّم أحدث معارف أمن (CPS)، من خلال التعلُّم عبر الإنترنت. وتشتمل حداثة هذا التطوير على ثلاث مميزات: أولًا: تستهدف جميع مواد التدريس الخاصة بأمن (CPS) التعلم المستند إلى التطبيق، ونختار تطبيقات (CPS) المهمة والمثيرة للاهتمام، بما في ذلك الرعاية الصحية، والطاقة المتجددة، والتحكّم في الصناعة وتحليل هجمات (CPS). ثانيًا: بناء محاضرات افتراضية مثيرة للاهتمام في الفصول الدراسية للمدارس الريفية. ثالثًا: بناء برنامج مساعد افتراضي تفاعلي للمختبر (يُسمى المختبر الافتراضي TA)؛ لتمكين الطلاب عن بُعد من إجراء مختبرات أجهزة افتراضية.

أما دراسة Rogers and Ashford (2015) فخلصت إلى أن المهاجمين السيبرانيين سيستمرون في النشاط. وتوجد مشكلة تتمثّل في أنهم كثيرو الإنتاج ومتزايدون في تعقيد هجماتهم؛ ويعني هذا أنه يجب على المؤسسات الأكاديمية أن تكون استباقية وفعّالة في التعامل مع هذا التهديد، وأن هناك حاجة مُلحّة للاستمرار في استخدام أحدث استراتيجيات تخفيف الهجمات، والاستمرار في توخي اليقظة. ويمكن استخدام المنتجات مفتوحة المصدر كلما أمكن ذلك؛ للتحكّم في التكاليف، ولكن قد يلزم شراء منتجات أكثر فاعلية مثل: (Splunk)، ونشرها وترقيتها بشكل فعّال مع تقدّم الوقت. وقبل كل شيء يجب أن تستمر مؤسسات التعليم العالي في تدريب المستخدمين؛ حتى يصبح هؤلاء المستخدمون بمنزلة دفاع آخر ضد الهجمات الإلكترونية.

أما دراسة Mangold (2016) فهدفت إلى تحديد الفعالية التعليمية لبرامج تعليم الأمن السيبراني للشباب؛ لزيادة المعرفة به لدى المشاركين من طلاب المدارس الثانوية. وتكوّنت مجموعة العينة من (37) طالبًا في مدرسة ثانوية بفلوريدا، وأظهرت نتائج الدراسة أن برنامج (Cyber Camp) أدّى إلى زيادة متوسطة في المعرفة بالأمن السيبراني بنسبة 36.1%. وأوصت الدراسة بضرورة أن تتضمّن الأبحاث المستقبلية عينات متنوعة من طلاب الجامعات والمعلمين.

وهدفت دراسة Lester (2018) إلى تحديد مستويات فهم ووجهات نظر المعلمين وأولياء الأمور ومقارنتها وفحصها بشأن قضايا الأمن السيبراني والتدريب، وأُجريت هذه الدراسة لتحديد ما إذا كانت هناك حاجة لمزيد من التدريب المتاح بسهولة حول القضايا المتعلّقة بالسلامة عبر الإنترنت للمعلمين وأولياء الأمور؛ لضمان سلامة الطلاب والأطفال في المدارس والمجتمعات من رياض الأطفال وحتى التعليم الثانوي. ووُجد أن العديد من المعلمين وأولياء الأمور يعملون لمعرفة المزيد عن السلامة على الإنترنت ومراقبة الطلاب والأطفال؛ ولكنهم يشعرون بالإحباط لأن التكنولوجيا تتغيّر بسرعة كبيرة، لدرجة أن جهودهم في بعض الأحيان تبدو غير كافية. وأوصت الدراسة بإضافة الموارد المجانية للمعلمين وأولياء الأمور؛ لتنمية الوعي لديهم. كما أوصت بأنه يجب على القنوات الإخبارية وبعض مديري المدارس بذل المزيد من الجهد لتثقيف مجتمعاتهم حول التغييرات التكنولوجية؛ لإبقاء المعلمين وأولياء الأمور على اطلاع، ومساعدة المجتمع على اتخاذ قرارات أفضل للطلاب والأطفال.

أما دراسة Marquardson and Gomillion (2018) فهدفت إلى توفير مبادئ مصممي الدورة التدريبية؛ لتطوير تمارين الأمن السيبراني بطريقة تزيد من نجاح الطلاب، مع تقليل المخاطر التنظيمية. وتوفير تدريب لمساعدة المعلمين والمسؤولين على تقييم الضوابط وأساليب التحكّم؛ مما يسمح بوصف أوضح للمخاطر التي تُخلِّص منها وتخفيفها وقبولها. وتستند المبادئ الواردة في هذه المقالة إلى تجربة تطوير برنامج جديد للأمن السيبراني في إحدى جامعات الغرب الأوسط.

وهدفت دراسة صائغ (2018) إلى الكشف عن العلاقة بين وعي أفراد الأسرة بمفهوم الأمن السيبراني والاحتياطات الأمنية التي يتخذونها للوقاية من الجرائم الإلكترونية، وأظهرت نتائج الدراسة وجود علاقة ارتباطية دالة بين وعي الأسرة بمفهوم الأمن السيبراني والاحتياطات الأمنية التي يتخذونها للوقاية من الجرائم الإلكترونية، ووجود فروق ذات دلالة إحصائية في درجة وعي أفراد الأسرة بمفهوم الأمن السيبراني، وذلك بالنسبة لمُتغيري: العمل والمؤهل التعليمي. وأوصت الدراسة بتعاون الجهات المعنية على تثقيف أفراد الأسرة وتوعيتهم بمفاهيم الأمن السيبراني، وتضمين تلك المفاهيم في المناهج الدراسية.

وهدفت دراسة الجثعمي (2018) إلى معرفة وعي طالبات المرحلة الثانوية في المدارس الحكومية بمدينة الرياض بقضايا أمن المعلومات، وأُعدت استبانة لذلك، وأظهرت نتائج الدراسة أن (43.1%) من الطالبات لديهن وعي ومعرفة بقضايا أمن المعلومات، وأن (94.4%) منهن لديهن علم بأن حواسيبهن يُمكن أن تُصاب بفيروسات، وأن (85.3%) منهن يعلمن بضرورة استخدام كلمة سر على أجهزتهن الإلكترونية من الاختراق والتجسس، وأوصت الدراسة بأهمية إدخال بعض المقررات الدراسية التي لها علاقة بقضايا أمن المعلومات؛ لإكساب الطلاب والطالبات مهارات الحماية من مخاطر التهديدات الإلكترونية وقضايا أمن المعلومات.

وهدفت دراسة الفريح (2018) إلى تقصي تصوّرات الطلبة المعلمين في كلية التربية بجامعة الكويت عن حوادث التنمّر السيبراني بمدارس التعليم العام. وتناولت تلك التصوّرات خمسة محاور، تمثّلت في: القلق، والثقة، والإعداد الجامعي، والتزام المدرسة، ودور المدرسة والمجتمع تجاه التعامل مع تلك الحوادث. كما هدفت إلى الكشف عما إذا كان هناك فروق ذات دلالة إحصائية في تصوّرات الطلبة المعلمين تُعزى لطبيعة المرحلة الدراسية التي يتدرّبون فيها، ومستوى كفاءتهم التكنولوجية. وتقصّت الدراسة أيضًا دور عامل الإعداد الجامعي في مجال التنمّر السيبراني؛ بوصفه متغيرًا تنبئيًّا لشعور الطلبة المعلمين بالقلق والثقة في التعامل مع حوادث التنمّر السيبراني. وطُبّقت استبانة- بعد التحقّق من صدقها وثباتها- على عينة مكوّنة من (279) طالبًا معلمًا من الملتحقين ببرنامج التربية العملية. وأظهرت النتائج: 1) وجود شعور بالقلق لدى الطلبة المعلمين من حوادث التنمّر السيبراني في المدارس، وأنهم في حاجة إلى رفع ثقتهم بأنفسهم، ورفع مستوى إعدادهم الجامعي في مواجهة تلك الحوادث. 2) تأكيد الطلبة المعلمين ضرورة التزام المدرسة والمجتمع تجاه تلك الحوادث. 3) وجود فروق ذات دلالة إحصائية في تصوّرات الطلبة المعلمين تجاه حوادث التنمّر السيبراني تُعزى للمرحلة الدراسية ومستوى الكفاءة التكنولوجية؛ لصالح الطلبة المعلمين الذين يتدرّبون في المرحلة الثانوية، ولصالح من يمتلك كفاءة تكنولوجية عالية. 4) كما تبيّن أن عامل الإعداد الجامعي في مجال التنمّر السيبراني كان مُتغيرًا تنبئيًّا في شعور الطلبة بالقلق والثقة في التعامل مع حوادث التنمّر السيبراني.

كما أجرى Hairston et al. (2020) دراسة هدفت إلى عمل برنامج لجعل الأمن السيبراني متاحًا لطلاب المدارس الثانوية الذين يعانون من إعاقات بصرية ومكفوفي (VIB). ويتطلّب مجال الأمن السيبراني الاهتمام والدراسة؛ لأنه له أهمية مُلحّة مع التقدّم والتطور التكنولوجي؛ ومع ذلك وُجدت حواجز يمكن أن تُثني الطلاب ذوي الإعاقة عن دراسة الأمن السيبراني؛ ولذلك أُطلق أول مخيم (GenCyber) طُوّر ووُجّه خصيصًا لطلاب المدارس الثانوية لمكفوفي (VIB) في صيف 2019. وأُنشئت بيئة تعليمية فريدة بالجمع بين الوسائل التعليمية التفاعلية وبيئات التطوير والاستراتيجيات التعليمية المبتكرة؛ بهدف إظهار الأمن السيبراني بوصفه خيارًا وظيفيًّا قابلًا للتطبيق لقوى عاملة متنوّعة. وتضمّنت نتائج البرنامج من هذا العمل فهمًا واضحًا لمفاهيم الأمن السيبراني (GenCyber)، وإثارة الاهتمام بمهن الأمن السيبراني، وبناء الثقة لمتابعة تلك المهن.

وأكّدت دراسة Richardson et al. (2020) أن الأمن السيبراني برز بوصفه واحدًا من أهم القضايا التي تواجه المدارس في القرن الحادي والعشرين. ويعدُّ أمان الكمبيوتر أداة أساسية لحماية الأطفال، وأن المدارس من مرحلة رياض الأطفال حتى نهاية التعليم الثانوي تعدُّ واحدة من أكثر البيئات جاذبية لجرائم اختراق خصوصية البيانات؛ بسبب ممارسات الأمن السيبراني الأقل فاعلية في المدارس. وأن العامل البشري هو السبب الأساسي وراء نجاح العديد من الهجمات على أجهزة الكمبيوتر والأنظمة المدرسية؛ لأن مستخدم الكمبيوتر غير المتعلم هو الحلقة الأضعف التي يستهدفها مجرمو الإنترنت، الذين يستخدمون الهندسة الاجتماعية. وأوصت الدراسة بضرورة تنمية الوعي الأمني السيبراني الرسمي؛ للتخفيف من استغلال نقاط الضعف البشرية من قِبل قراصنة الكمبيوتر والمهاجمين.

كما هدفت دراسة Pike et al. (2020) إلى إلقاء الضوء على المناهج الدراسية والتعلّم غير المنهجي في مجال الأمن السيبراني، والتحقّق من صحتها. وشارك في الدراسة (Cal Poly Pomona)، و(Coastline College) بوصفها مراكز للتميز الأكاديمي في الدفاع السيبراني (CAE-CD)، جنبًا إلى جنب مع مجموعة من الشركاء الأكاديميين والصناعيين في إنشاء مسارات التعلّم، التي تنقل المبتدئين المهتمين طوال الطريق إلى مهنة مثيرة في مجال الأمن السيبراني. كما صُمّمت المسارات لتضمين المناهج الدراسية، والمناهج الدراسية المشتركة، والتعلّم غير المنهجي في عملية يديرها الطلاب، يستهلك فيها الطلاب وحدات التعلم التي يرغبون فيها ويحتاجون إليها، التي تحرّكهم نحو أهداف التعلم التي اختاروها.

وذكرت دراسة Ameen et al. (2021) أن امتثال الموظفين للأمن السيبراني وسياسات الأمن السيبراني غير مفهوم جيدًا؛ ولذلك دعا الباحثون إلى اتباع نهج أكثر شمولية لأمن المعلومات، باقتراح نموذج أطلقوا عليه "نموذج الامتثال لأمان الهاتف الذكي (ESSC)"، الذي يُعمّق فهم سلوك أمن المعلومات للموظفين، من خلال مراعاة التأثيرات على المستويات الوطنية والتنظيمية والتكنولوجية (الخاصة بالهواتف الذكية) والشخصية. وركّز البحث على الاستخدام الآمن للهواتف الذكية في مكان العمل بين الموظفين (الذين تتراوح أعمارهم بين 18 و 35 عامًا) في سياق متعدد الثقافات: المملكة المتحدة، والولايات المتحدة، والإمارات العربية المتحدة، حيث طُبّق (1735) استبيانًا. وأشارت النتائج إلى أن أولئك الذين يرغبون

في فهم سلوك أمن الهواتف الذكية للموظفين يجب أن يأخذوا في الحسبان سياسات الأمن السيبراني الوطنية، والاختلافات الثقافية في البلدان المختلفة، والتهديدات الخاصة باستخدام الهواتف الذكية.

أوجه الاستفادة من الدراسات السابقة:

- أكدت جميع الدراسات أن الهجمات السيبرانية تؤثر في الأطفال والشباب بقدر تأثيرها في البالغين.
- أن الطلاب بمراحل التعليم العام والتعليم العالي في حاجة إلى رفع ثقتهم بأنفسهم، ورفع مستوى إعدادهم الجامعي في مواجهة الحوادث المتعلّقة بالأمن السيبراني.
- ضرورة تنمية وعي المعلمين والمعلمات بجوانب الأمن السيبراني والتدريب عليها.
- تطوير برامج جديدة للأمن السيبراني ودمجها في المقررات الدراسية.
- تثقيف اولياء الأمور والمعلمين بالمتغيرات التكنولوجية، وتنمية وعيهم بمخاطر الإنترنت.
- تطوير تدريبات للأمن السيبراني بطريقة تزيد من نجاح الطلاب في تقليل المخاطر الإلكترونية.
- ضرورة إضافة الموارد المجانية المتعلّقة بالأمن السيبراني للمعلمين وأولياء الأمور؛ لتنمية الوعي لديهم.
- تعرّف العديد من المراجع العربية والأجنبية التي يُمكن الاستعانة بها لمزيد من الاطلاع على موضوع الدراسة الحالية.

8. منهج الدراسة

تعدّ الدراسة الحالية من الدراسات التجريبية التي استخدمت المنهج التجريبي ذا التصميم شبه التجريبي ذي المجموعة الواحدة، الذي يتناسب مع أهداف هذه الدراسة.

9. مجتمع الدراسة وعينتها

أُختيرت عينة عشوائية بسيطة من معلمات المرحلة الابتدائية، وتعني العشوائية هنا أن الفرصة متساوية، ودرجة الاحتمال واحدة لأي فرد من أفراد مجتمع الدراسة ليُختار بوصفه أحد أفراد العينة دونما أي تأثر أو تأثير (العساف، 2006). وعلى هذا الأساس وُجّهت أداة الدراسة إلى عينة من معلمات الدراسة عبر موقع "جوجل درايف" Google Drive ليجبن عنها، وقد بلغن عددهن (30) معلمة، والجدول (1) يوضّح وصف العينة.

جدول (1): وصف عينة الدراسة.

المتغيرات	المستوى التعليمي	الإدارة التعليمية	العدد	النسبة
المؤهل الدراسي	بكالوريوس علوم+ دبلوم تربوي	إدارة التعليم بجدة	18	60%
		إدارة التعليم بمكة	6	20%
		إدارة التعليم بالطائف	6	20%
سنوات الخبرة	أقل من 5 سنوات	-	-	-
	من5سنوات إلى أقل من 10سنوات		30	100%
	أكثر من 10سنوات	-	-	-
دورات الامن السيبراني	لا يوجد		30	100%

ويتضح من الجدول (1) أن المعلمات الحاصلات على درجة البكالوريوس والدبلوم التربوي يمثّلن 100%. وبالنسبة لتوزيع أفراد العينة حسب عدد سنوات الخبرة، فإن جميع المعلمات الممثلات لعينة الدراسة لديهن خبرة تتراوح من (5) إلى (10) سنوات؛ حيث إن جميع المعلمات عائدات من الخدمة من المناطق النائية.

أما فيما يتعلّق بتوزيع أفراد العينة حسب عدد الدورات في مجال الأمن السيبراني، فيتبيّن أن نحو 100% من المعلمات لم يحصلن على أي دورة في مجال الأمن السيبراني؛ مما يجعل الحافز قويًّا لاختيار هذه العينة بالذات لتحقيق هدف الدراسة، وتوضيح أثر البرنامج لديهن.

10. أدوات الدراسة وموادها

10.1. أداة الدراسة: مقياس الوعي بجوانب الأمن السيبراني في التعليم عن بُعد (من إعداد الباحثة):

اتخذت الدراسة الحالية مقياس الوعي بجوانب الأمن السيبراني في التعليم عن بُعد لدى معلمات العلوم بالمرحلة الابتدائية - من إعداد الباحثة- وقد أُطلع على بعض الدراسات والمقاييس التي تقيس الوعي بالأمن السيبراني والاستفادة منها؛ وبناءً عليه حُدّد التعريف الإجرائي لمفهوم الأمن السيبراني وصياغة عبارات المقياس، وبلغ عدد عباراتها (44) عبارة، يتم الاستجابة عنها بالاختيار من بين خمسة بدائل، وهي: (بدرجة كبيرة جدًّا- بدرجة كبيرة- بدرجة متوسطة- بدرجة قليلة- بدرجة قليلة جدًّا). وتُقيّم درجات كل عبارة بالتقديرات (5- 4- 3- 2- 1) على الترتيب، كما ورد في ملحق(1).

10.1.1. صدق المقياس: الصدق المنطقي

للتحقّق من دلالات الصدق المنطقي للمقياس، وصلاحيته لقياس الوعي بالأمن السيبراني، عُرض على مجموعة من السادة المحكّمين(ن= 5) من ذوي الاختصاص في مجال طرائق التدريس؛ لتحكيم فقراته في صورته الأولية من ناحية الصياغة اللغوية لكل فقرة (مناسبة، تُعدّل، تُحذف). وتكوّن المقياس من (8) أبعاد تقيس: (جوانب الأمن السيبراني في التعليم عن بُعد، وتحصين بيئة المعلومات وسدّ ثغراتها الأمنية، والإجراءات الوقائية لتحصين الحاسب، وإرشادات أمنية لتقديم الدروس الافتراضية، والمنصة التعليمية في ظل أهم الجوانب الأمنية، والحفاظ على سرية رقم السجل المدني، وعلامات الخطر التي تدلّ على أن الجهاز مخترق، وخدمات مهمة في نظام التعليم عن بُعد). وأُعتمد معامل اتفاق بين المحكّمين لا يقلّ عن 80%، واقترح المحكّمون إجراء بعض التعديلات على عبارات المقياس ارتبطت بالصياغة اللغوية للفقرات؛ وبذلك تكوّن المقياس في صورته النهائية للتطبيق الاستطلاعي من (44) عبارة.

10.1.2. التحقّق من ثبات مقياس الوعي بجوانب الأمن السيبراني في التعليم عن بُعد

يُقصد بالثبات: مدى استقرار درجات الطلاب مهما تكررت مرات التطبيق، سواء بإعادة التطبيق، أو بالصور المتكافئة للاختبار، أو بالتجزئة النصفية. ولحساب الثبات طُبّق المقياس على العينة الاستطلاعية للدراسة، ثم حُسب معامل **ألفا كرونباخ (α)Cronbach's** ، والتجزئة النصفية وجتمان للمقياس وكان: (0.914، 0.960، 0.878) على التوالي؛ مما يؤكد تمتّع المقياس بدرجة مرتفعة من الثبات.

10.2. مادة التعليم والتعلّم: (البرنامج المُقترح: إعداد الباحثة):

تُعرّف الباحثة البرنامج إجرائيًّا بأنه: مجموعة من الإجراءات المعرفية والأنشطة والأشكال والمنظومات المترابطة المنظّمة المُعدّة بأسلوب التعلّم عن بُعد، واستخدام المنصات التعليمية؛ لتنمية الوعي بالأمن السيبراني لدى معلمات العلوم بالمرحلة الابتدائية. وتناولت الباحثة في هذا الجزء هدف البرنامج، ومرتكزاته، ومداخل تصميمه، ومصادره كالآتي:

10.2.1. هدف البرنامج

هدف البرنامج المُقترح إلى الكشف عن مدى فعاليته في تنمية مهارات الوعي بالأمن السيبراني لدى معلمات العلوم بالمرحلة الابتدائية في المملكة العربية السعودية.

10.2.2. أسس بناء البرنامج

عند إعداد البرنامج أُخذ في الحسبان مجموعة من الأسس كما يلي:

- أن يكون البرنامج ملبيًّا للاحتياجات التدريبية الفعلية للمعلمات.
- تنوّع أساليب تدريب المعلمات ووسائله.
- تنوّع الأنشطة المتضمّنة في البرنامج لتحاكي الموقف الحقيقي الذي يتعرّض إليه المعلمات.
- تزويد المعلمات بالمشكلات ذات الصلة التي تعزّز التعلم لديهن.
- توفير بيئة تعلّم إلكترونية آمنة قوامها المشاركة الفعّالة.
- أن يحتوي البرنامج على أساليب متنوّعة وفعّالة في التدريب.
- توظيف التعلّم عن بُعد، وتدريب المعلمات على الاستخدام الأمن للمنصات التعليمية.

10.2.3. مرتكزات البرنامج

يرتكز البرنامج المُقترح على تدريب المعلمات على مهارات الوعي بالأمن السيبراني، حيث يعدُّ من البرامج الموجّهة توجيهًا معرفيًّا: أي أنه يعتمد على التدخّل المقصود؛ لتحقيق مجموعة من الأهداف المحدّدة والمُخطّط لها

مسبقًا، وتُقدّم فيها مجموعة من الأنشطة بطريقة تساعد على تنمية المعرفة، وتوظيف المهارات بكفاءة؛ لإحداث عملية التعليم والتعلّم بطريقة شائقة وسهلة على المعلمات.

10.2.4. مداخل تصميم البرنامج

بُنيت جلسات البرنامج بمداخل مختلفة، مثل: التعليم عن بُعد، والتعليم الافتراضي، واستخدم المنصات التعليمية، والعصف الذهني، ونموذج المحاكاة، وورش العمل، والتعلّم القائم على المشكلة (PBL)، والتعلم القائم على السياق.

10.2.5. مصادر البرنامج

اطلعت الباحثة على الدراسات السابقة في هذا المجال، مثل: المنتشري وحريري (2020)، الجثعمي (2018)

Furnell et al. (2018), McCormac et al. (2017), Mangold, 2016), Peccoud (2018), Da Veiga (2019), Ameen et al. (2021)

10.2.6. مدة البرنامج

طُبّق البرنامج في (10) جلسات، مدة كل جلسة ساعتان، واستغرق تطبيق البرنامج خمسة أسابيع، بواقع جلستان أسبوعيًا، وطُبّق البرنامج بصورة جماعية على أفراد العينة عن طريق التعليم عن بُعد بتطبيق زوم.

10.2.7. محتوى البرنامج

يحتوي البرنامج على (10) جلسات، تتضمّن كل جلسة مجموعة من الإجراءات تتناغم مع التعليم الإلكتروني والتعليم عن بُعد؛ لتنمية الوعي بجوانب الأمن السيبراني.

11. نتائج الدراسة ومناقشتها

11.1. للإجابة عن السؤال الأول، الذي نصّ على: ما جوانب الأمن السيبراني في التعليم عن بُعد، اللازم تنميتها لدى معلمات العلوم بالمرحلة الابتدائية؟

اطلعت الباحثة على عدد من الدراسات ذات الصلة كدراسات: فاطمة المنتشري وحريري (2020)، والقيسي (2020)، و(Richardson, et.al., 2020)، والقحطاني (2019)، وصائغ (2018). كما اطلعت على الحملة التي أطلقتها الهيئة الوطنية للأمن السيبراني، ممثّلة بالمركز الوطني الإرشادي للأمن السيبراني، بالتعاون مع وزارة التعليم وعنوانها: «بأمان نتعلّم»، وذلك في إطار جهود المركز في رفع الوعي والمعرفة بالأمن السيبراني؛ لتجنّب المخاطر السيبرانية وتقليل آثارها، عن طريق إصدار التنبيهات بآخر الثغرات والمنشورات التوعوية وأخطرها.

وخلصت الباحثة إلى جوانب الأمن السيبراني في التعليم عن بُعد، اللازم تنمية الوعي بها لدى معلمات العلوم بالمرحلة الابتدائية، وعُرضت على عدد من السادة المحكّمين الزملاء في تخصص المناهج وطرق التدريس وتقنيات التعليم وأمن المعلومات، وهي على النحو الآتي الذي ورد في مقياس الوعي:

- نبذة معرفية مختصرة عن جوانب الأمن السيبراني في التعليم عن بُعد بالمملكة العربية السعودية.
- تجهيز شبكة المنزل، وتحصين بيئة المعلومات وسدّ ثغراتها الأمنية.
- أبرز الإجراءات الوقائية الواجب مراعاتها لتحصين الحاسب الشخصي والأجهزة الذكية.
- إرشادات أمنية حول أساسيات تجهيز وتخصيص مكان لتقديم الدروس الافتراضية.
- التعرُّف على المنصة التعليمية في ظلّ أهم الجوانب الأمنية الواجب مراعاتها.
- الحفاظ على سرية رقم السجل المدني المُستخدم في العديد من أنظمة التعليم الإلكترونية.
- تعرُّف علامات الخطر التي تدلّ على أن الجهاز مخترق.
- معرفة الروابط والإرشادات ذات العلاقة التي تحوي معلومات وخدمات مهمة في نظام التعليم عن بُعد.

11.2. للإجابة عن السؤال الثاني والذي ينص على: ما البرنامج التدريبي المُقترح لتنمية جوانب الوعي بالأمن السيبراني لدى معلمات العلوم بالمرحلة الابتدائية؟

قامت الباحثة ببناء برنامج تدريبي مقترح كما ورد في خطوات تصميم مادة التعليم والتعلم والجدول (2) يوضح ذلك.

جدول (2): البرنامج التدريبي المُقترح لتنمية الوعي بجوانب الأمن السيبراني في التعليم عن بُعد لدى معلمات العلوم بالمرحلة الابتدائية

رقم الجلسة	عنوان الجلسة	أهداف الجلسة	طرائق التدريس والاساليب المستخدمة	مصادر التعلم والأنشطة التعليمية	أساليب التقويم
1	التطبيق القبلي. خلفية نظرية	- توفير بيئة آمنة مشجعة للمعلمات، تقوم على الاحترام والثقة المتبادلة خالية من التهديد والتوتر. - التعرف على الميثاق الأخلاقي لكل جلسة، والاساليب التدريسة التي يمكن اتباعها في البرنامج. - التعرف على التجربة وأسس البرنامج والهدف منه.	الحوار والمناقشة العصف الذهني	التعليم عن بُعد	التطبيق القبلي
2	جوانب الأمن السيبراني في التعليم عن بُعد	بنهاية الجلسة ينبغي على المعلمة ان تكون قادرة على أن: تحدد مفهوم الأمن السيبراني. تناقش نشأة الأمن السيبراني. تحدد دواعي تأمين المعلومات. تحدد مفهوم التعليم عن بُعد. تستنتج دواعي استخدام التعليم عن بُعد	الحوار والمناقشة - لعب الأدوار	البحث على الإنترنت، فيديو، المواقع التعليمية، https://www.youtube.com/watch?v=ZBbrJ5sZpCg	اختبارات إلكترونية
3	تحصين بيئة المعلومات وسد ثغراتها الأمنية	بنهاية الجلسة ينبغي على المعلمة ان تكون قادرة على أن: - تحدد مفهوم بيئة المعلومات. - تناقش أساليب تحصين بيئة المعلومات. - تستنتج الثغرات الأمنية. - توضح أساليب تجهيز شبكة المنزل.	السرد القصصي – الحوار والمناقشة - لعب الأدوار	داتا شو، خرائط مفاهيمية، كاميرا، السبورة الذكية،	أسئلة شفوية وأسئلة قصيرة
4	الإجراءات الوقائية لتحصين الحاسب	بنهاية الجلسة ينبغي على المعلمة ان تكون قادرة على أن: - توضح الاجراءات الوقائية لتحصين الحاسب الشخصي. - تحدد الاجراءات الوقائية لتحصين الهاتف الذكي. - تمهر في اتباع الإجراءات الوقائية لتحصين الحاسب. - تطرح أمثلة للاجراءات الوقائية لتحصين الجواسب	العصف الذهني	فيديو وافلام تعليمية	أسئلة شفوية وأسئلة قصيرة
5	إرشادات أمنية لتقديم الدروس الافتراضية	بنهاية الجلسة ينبغي على المعلمة ان تكون قادرة على أن: -تحدد الشروط الواجب توافرها في الجلسة الافتراضية. - تقترح فنيات الفصول الافتراضية. - تعدد الشروط الواجب توافرها لنجاح جلسة الفصول الافتراضية.	السرد القصصي – الحوار والمناقشة - لعب الأدوار	داتا شو، خرائط مفاهيمية، كاميرا، السبورة الذكية،	أسئلة شفوية وأسئلة قصيرة
6	المنصة التعليمية في ظل أهم الجوانب الأمنية	بنهاية الجلسة ينبغي على المعلمة ان تكون قادرة على أن: - تطلع على المنصات التعليمية المختلفة. - تناقش مميزات المنصات التعليمية . - تتبع الجوانب الأمنية عند استخدام المنصات التعليمية. - تحدد طرق الحماية من الاختراق اثناء استخدام المنصات التعليمية. - تتبع الاجراءات الأمنية بعد استخدام المنصة التعليمية.	العصف الذهني	فيديو وافلام تعليمية	أسئلة شفوية وأسئلة قصيرة
7	الحفاظ على سرية رقم السجل المدني	بنهاية الجلسة ينبغي على المعلمة ان تكون قادرة على أن: -تقترح اساليب حماية رقم السجل المدني. - تحدد كيفية اختيار كلمة السر وشروط تغييرها. - تتبع أفضل الممارسات لتكون كلمة سر قوية و يسهل تذكرها.	العصف الذهني	فيديو وافلام تعليمية https://ncdcr.gov.sa المركز الوطني الارشادي للأمن الوطني.	أسئلة شفوية وأسئلة قصيرة
8	علامات الخطر التي تدل على أن الجهاز مخترق	بنهاية الجلسة ينبغي على المعلمة ان تكون قادرة على أن: - تحدد علامات اختراق الجهاز - تقترح الاجراءات الأمنية للحفاظ على الجهاز من الاختراق. - تناقش مواعيد العناية الدورية لصيانة الجهاز. - تتجنب مؤشرات اختراق جهاز الكمبيوتر.	العصف الذهني- مناقشة وحوار-	فيديو وافلام تعليمية https://web1.internet.sa/ar	أسئلة شفوية وأسئلة قصيرة
9	خدمات مهمة في نظام التعليم عن بُعد	بنهاية الجلسة ينبغي على المعلمة ان تكون قادرة على أن: - تشرح نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية. - تناقش نظام التعاملات الاليكترونية في المملكة العربية السعودية. - تحدد طرق الابلاغ عن الجرائم الالكترونية. - تنشر الوعي حول دور المركز الوطني الارشادي للأمن الوطني	العصف الذهني- مناقشة وحوار-	https://ncdcr.gov.sa المركز الوطني الارشادي للأمن الوطني.	اختبارات إلكترونية
10	الجلسة الختامية والتطبيق البعدي	- تقديم الشكر للمعلمات على التعاون مع الباحثة. - التأكيد على اتباع الإجراءات الأمنية مستقبلاً. - المشاركة الايجابية في التطبيق البعدي.	الحوار المناقشة	فيديو وافلام تعليمية	مقياس الوعي بالأمن السيبراني

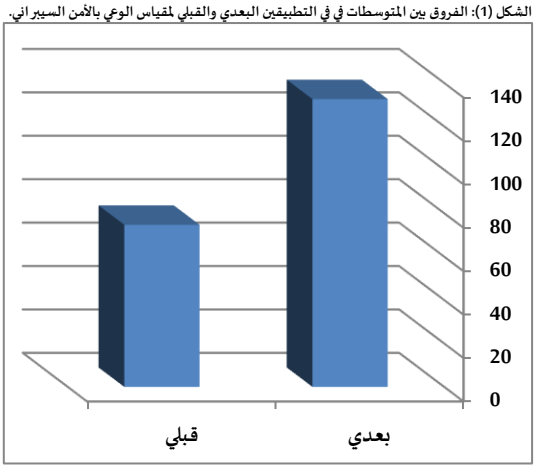
11.3. وللإجابة عن السؤال الثالث، الذي نصّ على: هل توجد فروق ذات دلالة إحصائية بين متوسطي درجات المعلمات (المجموعة التجريبية)، اللاتي خضعن للتدريب على البرنامج في مقياس الوعي بالأمن السيبراني في التطبيقين القبلي والبعدي؟

حسبت الباحثة الفروق بين درجات المجموعة التجريبية في التطبيقين البعدي والقبلي في مقياس الوعي بالأمن السيبراني، كما هو موضح في الجدول (3).

جدول (3): المتوسطات، والانحراف المعياري، وقيمة "ت"، ودلالتها الإحصائية بين درجات المجموعة التجريبية في التطبيقين البعدي والقبلي لمقياس الوعي بالأمن السيبراني.

المتغير		العدد	المتوسط الحسابي	الانحراف المعياري	اختبار"ت"	مستوى الدلالة
الوعي بالأمن السيبراني	بعدي	30	132.57	5.04	32.60	دال عند مستوى 0.01
	قبلي	30	74.67	8.32		

الشكل (1): الفروق بين المتوسطات في في التطبيقين البعدي والقبلي لمقياس الوعي بالأمن السيبراني.



يتبيّن من الجدول رقم (3)، والشكل (1) أن قيمة (ت) (32.60)، وهي قيمة ذات دلالة إحصائية عند مستوى (0.01)؛ لصالح التطبيق البعدي في مقياس الوعي بالأمن السيبراني؛ مما يشير إلى وجود فرق دال إحصائيًّا لصالح التطبيق البعدي.

وتعزو الباحثة هذه النتيجة إلى التغيير الذي أحدثه البرنامج التدريبي لتنمية الوعي لدى المعلمات بالأمن السيبراني، وتوفير أنشطة متكاملة تختص بالأمن المعلوماتي؛ تُعزّز الحماية والتثقيف بالأمن السيبراني، وكذلك توفير فيديوهات تعليمية حول مخاطر الأمن السيبراني وتهديداته، ووجود تعليمات للحفاظ على الأمن السيبراني في المدارس والمؤسسات التعليمية بشكل عام. كما تجلّت المشاركة الإيجابية للمعلمات بالبرنامج التدريبي في تنمية وعيهن للحفاظ على بيئة إلكترونية آمنة، من خلال اتباع الإجراءات اللازمة لتأمين المعلومات، وتطبيق ذلك عمليًّا في المنزل والمدرسة.

وتتفق هذه النتيجة مع العديد من الدراسات، ومنها دراسة: (Bicak et al., 2015)، التي هدفت إلى تطوير مناهج الأمن السيبراني بإدخال التخصّصات في برنامج الدراسات العليا، وخلصت إلى تعزيز الأمن السيبراني عبر إدخال ثلاثة تخصصات في منهج الدراسات العليا للأمن السيبراني، وهي: تحليل بيانات الأمن السيبراني، والذكاء السيبراني، وأمن معلومات الرعاية الصحية وخصوصيتها، وإدخال برامج لتنمية الاتجاه نحو مناهج الأمن السيبراني المستقبلية.

كما تتفق مع دراسة Mangold (2016) ، التي توصّلت إلى تحسّن إيجابي في اكتساب المعرفة بالأمن السيبراني للمشاركين في البرنامج التدريبي، وأوصت بأنه يجب على الباحثين بشكل عام تركيز المزيد من الجهود على تصميم برامج الأمن السيبراني ضمن الأطر التربوية، والتأكّد من أن تلك الأطر قابلة للقياس، والإبلاغ عن نتائجها وآثارها الايجابية. ويجب كذلك على الباحثين الاستمرار في تطوير طرق تقييم كمية جديدة؛ للتقليل من عدم الدقة وأعباء الوقت التي تتكبّدها المسوحات.

وتتفق الدراسة أيضًا مع دراسة Pike et al. (2020)، التي توصّلت إلى فاعلية التعليم غير المنهجي والحقائب التعليمية في تعليم الأمن السيبراني، وأثبتت النتائج تمكّن الطلاب من المناهج الدراسية الرسمية مع رحلة التعلّم الخاصة بهم، وتخطيط مهام التعلّم المنهجية والمناهج الدراسية وغير المنهجية التي تناسب خطتهم، وتسمح لهم بتحقيق أهدافهم الأكاديمية والوظيفية.

11.3. للإجابة عن التساؤل الرئيس، الذي نصّ على: "ما فعالية البرنامج التدريبي المُقترح في تنمية جوانب الوعي بالأمن السيبراني في التعليم عن بُعد لدى معلمات العلوم بالمرحلة الابتدائية (عينة الدراسة)؟

أُستخدم مربع إيتا ($\eta 2$)، ومعامل كوهين Cohen's d؛ لحساب حجم تأثير المُتغيّر المستقل، وهو (استخدام البرنامج التدريبي للأمن السيبراني)، في المُتغيّر التابع، وهو (الوعي بالأمن السيبراني). ويبيّن الجدول (4) النتائج الإحصائية التي تُوصّل إليها.

جدول (4): قيمة "ت"، ودرجة الحرية، وحجم التأثير"مربع إيتا $\eta 2$، ومعامل كوهين Cohen's d" لطلاب المجموعة التجريبية في التطبيق البعدي لمقياس الوعي بالأمن السيبراني.

المستوى	التطبيق	قيمة "ت"	درجة الحرية	مربع إيتا$\eta 2$	قيمة d	حجم التأثير
الوعي بالأمن السيبراني	البعدي	32.60	58	0.95	8.72	كبير

ويتضح من الجدول السابق (4)، أن حجم تأثير البرنامج التدريبي في جوانب الوعي بالأمن السيبراني في التعليم عن بُعد لدى معلمات العلوم كبير جدًّا، حيث تُشير قيمة مربع إيتا إلى أن نسبة التباين المفسّر الذي تُحدثه المعالجة التجريبية (البرنامج التدريبي) في التباين المنظّم للمُتغيّر التابع (الوعي بالأمن السيبراني) لدى عينة البحث؛ يُقدّر بـ(95%). وترجع هذه النِّسب من التباين الكلي للفروق بين المتوسطات؛ لصالح التطبيق البعدي، كما جاءت قيمة (d>1) مساوية (8.72)؛ مما يُشير إلى فاعلية كبيرة للمعالجة التجريبية. وتتفق هذه النتيجة مع نتائج دراسات: المنتشري وحريري (2020)، والقحطاني (2019)، والصحفي وعسكول (2019)، وصائغ (2018).

Pike et al. (2020), Bicak et al. (2015).

12. توصيات الدراسة

في ضوء النتائج السابقة توصي الباحثة بما يأتي:

- توفير البرمجيات والبرامج والتطبيقات التي تستطيع المعلمات التعامل معها باحترافية.
- إضافة موضوعات متنوّعة عن الأمن السيبراني في المناهج الدراسية بالمراحل التعليمية المختلفة.
- دمج الأمن السيبراني في البرامج التربوية وبرامج إعداد المعلم.
- إلحاق المعلمات بدبلومات بالأمن السيبراني؛ يرفع مستوى الفهم والوعي والتطبيق لديهن.
- توفير برامج تدريبية مجانية للمعلمات اللاتي في داخل الخدمة، وتنمية وعيهن نحو الأمن السيبراني وأمن المعلومات.
- ربط الترقية في وظائف التعليم بالوزارة بأخذ دورات تدريبية عن الأمن السيبراني.
- تعاون الجهات المعنية بتثقيف المعلمين بشكل عام ومعلمات المرحلة الابتدائية بشكل خاص.
- تصميم وإعداد برامج توعوية تثقيفية للمعلمات بوزارة التعليم؛ لإطّلاعهن على أصول التعامل مع الإنترنت، ومواقع التواصل الاجتماعي، ومخاطر الإنترنت.

نبذة عن المؤلفة

منال حسن محمد بن إبراهيم

قسم المناهج والتدريس، كلية التربية، جامعة جدة، جدة، المملكة العربية السعودية، 00966566639993، mhibrahim@uj.edu.sa

د. بن إبراهيم، سعودية،حاصلة على البكالوريوس و الماجستير من جامعة الملك عبدالعزيز، والدكتوراة من جامعة طيبة، استاذ المناهج و طرق تدريس العلوم المساعد، شغلت منصب مديرة وحدة التطوير والتنمية المستدامة بالكلية، أشرفت على قسم اللغة الانجليزية، مستشار بأوقاف جامعة جدة، أشرفت على برنامج الدبلوم العام في التربية، أشرفت و ناقشت عدد من الرسائل العلمية، مدرب معتمد في عدد من المجالات، حضرت عدد من المؤتمرات و الدورات و ورش العمل، قدمت عدد من الدورات وورش العمل، حكمت عدد من المسابقات العلمية.

المراجع

البقمي، ناصر محمد. (2007). *فاعلية التشريعات العقابية في مكافحة الجرائم*

المعلوماتية. الرياض، السعودية: مكتبة الملك فهد الوطنية.

الجبور، منى الأشقر. (2012). الأمن السيبراني: التحديات ومستلزمات المواجهة. في: *اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني*، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية. بيروت، 27–2012/08/28.

الجثعمي، مها دخيل الله. (2017). مستوى الوعي بقضايا أمن المعلومات لدى طالبات المرحلة الثانوية بالمدارس الحكومية بمدينة الرياض. *مجلة العلوم الإنسانية والاجتماعية، جامعة الإمام محمد بن سعود الاسلامية - عمادة البحث العلمي*، **بدون رقم مجلد**(47)، 355–400.

جريدة الوطن. (2020). *ما هو الأمن السيبراني*. متوفر بموقع: https://www.almowaten.net/2017/10/ (تاريخ الاسترجاع: 2020/09/25).

الخياط، عالية محمد. (2018). تنمية الوعي الأمني للمعلم في ضوء التحديات الفكرية المعاصرة. *مجلة الإرشاد النفسي*، **4**(6)، 1–25.

سبق. (2019). *السعودية تحقق المركز 13 عالميًا في مؤشر الأمم المتحدة الأمن السيبراني*. متوفر بموقع: https://sabq.org/SR5xKt (تاريخ الاسترجاع: 2019/03/27).

الشهري، حسن أحمد. (2017). قانون دولي موحد لمكافحة الجرائم الإلكترونية (تصور مقترح). *المجلة العربية للدراسات الأمنية والتدريب*، **27**(53)، 1–90.

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

الصحفي، مصباح أحمد حامد والعسكول، سناء صالح. (2019). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. *مجلة البحث العلمي في التربية، كلية البنات للآداب والعلوم والتربية، جامعة عين شمس*، **20**(10)، 493–534.

العريفي، محمد سعود. (1996). *العلاقة بين الوعي الاجتماعي والحد من انتشار العقاقير المخدرة*. رسالة ماجستير، جامعة الملك سعود، الرياض، السعودية.

الفريح، سعاد عبد العزيز. (2018). التنمّر السيبراني في مدارس التعليم العام: من منظور الطلبة المعلّمين بجامعة الكويت. *المجلة التربوية*، **32**(126)، 15– 58.

القحطاني، نوره ناصر. (2019). مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. *مجلة جمعية الاجتماعيين في الشارقة*، **36**(144)، 85–120.

القيسي، محمد وائل. (2020). مستقبل الأمن الاستراتيجي العالمي في ظل التحديات التكنو - معلوماتية والفضاء السيبراني. *مجلة دراسات إقليمية: جامعة الموصل، مركز الدراسات الإقليمية*، **13**(44)، 139–173.

المقصودي، محمد بن أحمد. (2017). الأمن السيبراني والجهود الدولية لمكافحة الجرائم عابرة القارات. *جامعة نايف العربية للعلوم الأمنية*، **37**(427)، 102–7.

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

الهيئة الوطنية للأمن السيبراني. (2018). *تقرير الضوابط الأساسية للأمن السيبراني*. الرياض، السعودية: الهيئة الوطنية للأمن السيبراني.

Al-Arifi, M.S. (1996). *Alealaqat Bayn Alwaeyi Alaijtimaeii Walhadi Min Aintishar Aleaqaqir Almukhdirati* 'The Relationship between Social Awareness and the Reduction of Drug Prevalence'. Master's Dissertation, King Saud University, Riyadh, Saudi Arabia. [in Arabic]

Al-Buqami, N.M. (2007). *Faeiliat Altashrieat Aleiqabiat Fi Mukafahat Aljarayim Almaelumatiati*' The Effectiveness of Punitive Legislation in Combating Information Crimes'. Riyadh, Saudi Arabia: King Fahd National Library. [in Arabic]

Al-Fraih, S.A. (2018). Altanamur alsiyburaniu fi madaris altaelim aleami: Min manzur altalabat almuealimin bijamieat alkuayt 'Cyber bullying in public education schools: from the perspective of student teachers at Kuwait University'. *The Educational Journal*, **32**(126), 15–58. [in Arabic]

Al-Jabour, M.A. (2012). Al'amn alsybrany: Altahadiyat wamustalzimat almuajahati 'Cybersecurity: Challenges and requirements for confrontation'. In: *The First Annual Meeting of Professionals in the Security and Safety of Cyberspace. The League of Arab States: Arab Center for Legal and Judicial Research*, Beirut, Lebanon, 27–28 /08/2012. [in Arabic]

Al-Jathmi, M.D. (2017). Mustawaa alwaey biqadaya 'amn almaelumat ladaa talibat almarhalat alththanawiat bialmadaris alhukumiat bimadinat alriyad 'The level of awareness of information security issues among secondary school students in government schools in Riyadh'. *Journal of Human and Social Sciences, Imam Muhammad bin Saud Islamic University: Deanship of Scientific Research*, **n/a**(47), 355–400. [in Arabic]

Al-Khayyat, A.M. (2018). Tanmiat alwaey al'amnii lilmaelam fi daw' altahadiyat alfikriat almueasirati 'Developing teacher security awareness in light of contemporary intellectual challenges'. *Journal of Psychological Counseling*. **4**(6), 1–25. [in Arabic]

Al-Maqsoudi, M.A. (2017). Al'amn alsaybraniu waljuhud alduwaliat limukafahat aljarayim eabirat alqarat 'Cybersecurity and international efforts to combat transcontinental crime'. *Naif Arab University for Security Sciences*, **37**(427), 102–7. [in Arabic]

Al-Muntashari, F.Y. and Hariri, R. (2020). Darajatan waeaa muealimat almarhalat almutawasitat bial'amn alsiybranaa fa almadaris aleamat bimadinat jidat min wijhat nazar almuelamati 'The degree of awareness of middle school teachers about cybersecurity in public schools in Jeddah from the teachers 'point of view'. *The Arab Journal of Specific Education, the Arab Foundation for Education, Science and Arts*, **n/a**(14), 95–140. [in Arabic]

Al-Qahtani, N.N. (2019). Madaa tuafur alwaey bial'amn alsiybiranaa ladaa tullab watalibat aljamieat alsewdyt min manzur aijtmaei: dirasat midaniati 'The extent of the availability of awareness of cybersecurity among students of Saudi universities from a social perspective: A field study'. *Journal of the Social Society of Sharjah*, **36**(144), 85–120. [in Arabic]

Al-Qaisi, M.W. (2020). Mustaqbal al'amn al'iistratijii alealamii fi zili altahadiyat altknw- maelumatiat walfada' alsayubrani 'The future of global strategic security in light of the challenges of techno-information and cyberspace'. *Regional Studies Journal, University of Al Mosul, Regional Studies Center*, **13**(44), 139–73. [in Arabic]

Alsahfiu, M.A. and Al-Askoul, S.S. (2019). Mustawaa alwaey bial'amn alsiyubranii ladaa muealamat alhasib alalii lilmarhalat alththanawiat bimadinat jidat 'The level of awareness of cybersecurity among secondary school computer teachers in Jeddah'. *Journal of Scientific Research in Education. Girls College of Arts, Sciences and Education. Ain Shams University*, **20**(10), 493–534. [in Arabic]

Al-Shehri, H.A. (2017). Qanun dawliin muahad limukafahat aljarayim al'iiliktrunia (tsawr muqtrh) 'A unified international law to combat cybercrime (proposed scenario)'. *The Arab Journal of Security Studies and Training*, **27**(53), 1–90. [in Arabic]

Al-Watan Newspaper. (2020). *Ma Hu Al'amn Alsayubran* 'What is Cybersecurity'. Available at: https://www.almowaten.net/2017/10/ (accessed on 25/09/ 2020). [in Arabic]

Ameen, A., Tarhini, B., Shah, M., Madichie, D., Paul, J. and Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, **114**(n/a), January 2021, doi.org/10.1016/j.chb.2020.106531

Bicak, A., Liu, M. and Murphy, D. (2015). Cybersecurity curriculum development: Introducing specialties in a graduate program. *Information Systems Education Journal (ISED)*, **13**(3), 99–110.

Council of the Great City School. (2017). *Cyber-Security in Today's K-12 Environment*. Washington, DC: By Member Districts of the Council of the Great City Schools.

Da Veiga, A. (2019). Achieving a security culture. In I. Vasileiou and S. Furnell (eds.) *Cybersecurity Education for Awareness and Compliance* (pp. 72–100). Hershey, PA: IGI Global.

Furnell S., Khern-Am-Nuai W., Esmael R., Yang W. and Li N. (2018). Enhancing security behaviour by supporting the user. *Computers and Security*, **75**(2018), 1–9. DOI:10.1016/j.cose.2018.01.016.

Hairston, R., Williams, T., Smith, D., Sabados, W. and Forney, S, (2020). Teaching cybersecurity to students with visual impairments and blindness. *Journal of Science Education for Students with Disabilities*, **23**(1), 1–15.

Lester, T. (2018). *An Investigation on Cyber Safety Awareness among Teachers and Parents*. PhD Thesis, Gardner-Webb University, Boiling Springs, North Carolina, USA.

Mangold, L.V. (2016). *An Analysis of Knowledge Gain in Youth Cybersecurity Education Programs*, PhD Thesis**,** Northcentral University San Diego, California, USA.

Marquardson, J. and Gomillom, D. (2018). Cyber security curriculum development: protecting students and institutions while providing hands-on experience. *Information Systems Education Journal*, **16**(5), 12–21.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, **69**(2017), 151–6.

Morris, T. and Hu, F. (2015). 'Towards a multimedia-based virtual classroom on cyber-physical system (cps) security education for both city and rural schools'. *In: 2015 ASEE Annual Conference & Exposition,* Seattle, Washington, 14-17-/06/2015.

National Cybersecurity Authority. (2018). *Taqrir Aldawabit Al'asasiat Lil'amn Alsybrany* 'Basic Cybersecurity Controls Report'. Riyadh, Saudi Arabia: The National Cybersecurity Authority. [in Arabic]

Peccoud, J., Gallegos, J., Murch, R., Buchholz, W. and Raman, S. (2018).

Cyberbiosecurity: From naive trust to risk awareness. *Trends in Biotechnology*, **36**(1), 4–7.

Pike, R., Brandon, B., West, I. and Zentner, A., (2020). *Digital Badges and E-Portfolios in Cybersecurity Education*. Available at: https://files.eric.ed.gov/fulltext/EJ1258232.pdf (accessed on 01/11/2020)

Richardson, M., Lemoine, P., Stephens, W. and Waller, R. (2020). Planning for cyber security in schools: The human factor. *Educational Planning*, **2**(2), 23–39.

Rogers, G, and Ashford, T. (2015). 'Mitigating higher ed cyber attacks. Association supporting computer users in education'. *In*: *The Annual Meeting of the Association Supporting Computer Users in Education* (ASCUE), Myrtle Beach, South Carolina, USA, 14–8/06/2015.

Sabaq. (2019). *Alsewdyt Tuhaqiq Almarkaz 13 Ealmyana Fi Muashir Al'umam Almutahidat Al'amn Alsiyubrani* 'Saudi Arabia Ranks 13th Globally in the United Nations Cybersecurity'. Available at: https://sabq.org/SR5xKt (accessed on 27/03/2019). [in Arabic]

Sayigh, W.H.A. (2018). Waey 'afrad al'usrat bimafhum al'amn alsayburanii waealaqatih biaihtiatatihim al'amniat min aljarayim al'iiliktruniati 'Family members' awareness of the concept of cybersecurity and its relationship with their security precautions from cybercrime'. *Arab Journal of Social Sciences, Arab Foundation for Scientific Consulting and Human Resource Development*, **14**(3), 18–70. [in Arabic]