درجة الوعي بالأمن السيبراني ودور تكنولوجيا التعليم في تنميته لدى طلبة كلية التربية الأساسية بدولة الكويت

تاريخ استلام البحث: ٢٧\١٠\٢٠٢٤ تاريخ قبول البحث للنشر: ٢٣\١١\٢٠٢٤

د. عايدة عبد الكريم العيدان (١)

د. بدور مسعد المسعد (٢)

المستخلص

هدفت الدراسة إلى تعرف درجة وعى طلبة كلية التربية الأساسية بدولة الكويت بمفاهيم الأمن السيبراني وبمخاطر انتهاكات الأمن السيبراني، وتعرف دور تكنولوجيا التعليم في تنمية هذا الوعي لديهم. وقد تم استخدام المنهج الوصفي المسحي، وقد أعدت استبانة خصيصًا لخاصة بالدراسة تضمنت (٤٣) عبارة. وُزعت على (٣) محاور. وتم التطبيق على عينة تكونت العينة من (٧٢٠) طالبًا وطالبة. وأسفرت النتائج عن أن الطلبة يمتلكون وعيا بالأمن السيبراني بدرجة متوسطة ولديهم معرفة ووعي كبيرين بمخاطر وتهديدات الأمن السيبراني. وقد أفاد الطلبة بأن دراسة مقررات تكنولوجيا التعليم والحاسوب يمكن تسهم بدرجة متوسطة في تنمية الوعي بالأمن السيبراني لديهم. كما كشفت النتائج عن عدم وجود اختلافات بين تقديرات العينة حول الوعي بالأمن السيبراني ومخاطره تبعًا لمتغير النوع، في حين وجدت فروق تبعًا لمتغير التخصص لصالح مجموعة الطلبة تخصص تكنولوجيا التعليم، وتبعًا لمتغير الفرقة الدراسية لصالح طلبة الفرقتين الثالثة والرابعة. وعلى ضوء هذه النتائج أوصت الباحثتان بضرورة إدراج مقررات دراسية خاصة بمفاهيم الأمن السيبراني ضمن البرامج الأكاديمية بالكلية، وإعداد برامج تربوية ودورات تدريبية للطلبة تتناول مفاهيم ومخاطر وانتهاكات الأمن السيبراني.

الكلمات المفتاحية: الأمن السيبراني، الوعي، المخاطر، التهديدات.

The degree of awareness of cybersecurity and the role of educational technology in its development among students of the College of Basic Education in the State of Kuwait

Dr. Ayda Abdulkareem Al-Eidan Dr. Budour M. Almisad

Abstract

The study aimed to identify the level of awareness of students of the College of Basic Education in the State of Kuwait about the concepts of cybersecurity and the risks of cybersecurity violations, and to identify the role of educational technology in developing this awareness among them. The descriptive survey approach was used, and a questionnaire was prepared specifically for the study, which included (43) statements. It was distributed over (3) axes. It was applied to a sample consisting of (720) male and female students. The results showed that students have an average level of awareness of cybersecurity and have great knowledge and awareness of the risks and threats of cybersecurity. The students reported that studying educational technology and computer courses can contribute to a moderate level in developing their cybersecurity awareness. The results also revealed no differences between the sample estimates regarding awareness of cybersecurity and its risks according to the gender variable, while differences were found according to the specialization variable in favor of the group of students specializing in educational technology, and according to the study year variable in favor of students in the third and fourth years. In light of these results, the researchers recommended the necessity of including courses on cybersecurity concepts within the college's academic programs, and preparing educational programs and training courses for students that address the concepts, risks, and violations of cybersecurity.

Keywords: Cybersecurity, awareness, risks, threats.

(١) أستاذ مشارك - قسم تكنولوجيا التعليم- كلية التربية الأساسية - الهيئة العامة للتعليم التطبيقي والتدريب- الكويت.
aa.aleidan@paaet.edu.kw

(٢) أستاذ مشارك - قسم تكنولوجيا التعليم- كلية التربية الأساسية - الهيئة العامة للتعليم التطبيقي والتدريب- الكويت .
b.almisad@paaet.edu.kw

المقدمة

أدت الثورة الرقمية المعاصرة إلى تطورات هائلة غير مسبوقة، شملت جميع مجالات النشاط الإنساني العلمية والتربوية والسياسية والاقتصادية. ومن أهم إفرازات هذه الثورة ما يعرف بالفضاء السيبراني، الذي ساهم في تكوين العلاقات الاجتماعية في حدود المجتمع الافتراضي الذي تغلب على الحدود والحواجز والاختلافات الثقافية والعرقية والدينية بين الجماعات. وعلى المستوى التعليمي أصبح الفضاء السيبراني وسيلة تعليمية يمكن للطلاب اللجوء إليها لمساعدتهم في أداء واجباتهم.

وعلى الرغم من الإيجابيات التي يحملها الفضاء السيبراني إلا أنه يقبع خلفه واقع افتراضي مخيف؛ إذ يسكن المجرمون وتجار المخدرات ومنظمات الإرهاب واللصوص، والمتنمرون، الأمر الذي شكل مصدر تهديد لمستخدمي الشبكة العنكبوتية، عبر ما يعرف بالهجمات السيبرانية أو الجرائم السيبرانية التي يمكن من خلالها إيقاع خسائر فادحة، قد يصل إلى التلاعب بالبيانات أو تزييفها، أو محوها من أجهزة الحواسيب (خليفة، ٢٠١٧). وتزداد خطورته في أنه يعرض خصوصية الأفراد للاختراق وشخصيتهم للابتزاز، وارتكاب بعض السلوكيات والانحرافات، بالإضافة إلى بعض التهديدات، والقرصنة، والمواد الإباحية، وسرقة الهوية، ناهيك عن الآثار السلبية مثل الاكتئاب والقلق؛ والكثير من الأضرار الصحية والجسمية والاجتماعية (خورشيد، ٢٠٢٠).

في سياق ذلك؛ ظهر ما يعرف بالأمن السيبراني الذي يهدف إلى حماية البيانات التي تخص الأفراد والمؤسسات في العالم وحماية أجهزة الكمبيوتر والشبكات والبرمجيات من الوصول غير المصرح به أو الهجمات التي تهددها (Haseski, 2020). وأصبح حديث العالم بأسره، وأصبح جزءا أساسيا من أي سياسات أمنية واقتصادية أو سياسية أخرى، حيث يلامس اهتمام كل من له علاقة بالعالم الرقمي، سواء كان من الأفراد أو المنظمات أو الحكومات، لذلك بات من الأهمية بمكان تحقيق الأمن السيبراني من خلال استخدام الآليات والوسائل الممكنة التي تساعد على تحقيقه (هوساوي، ٢٠٢٠).

على جانب آخر؛ يشهد التعليم في جميع أنحاء العالم تحولات كبيرة في الممارسات التعليمية للتدريس والتعلم تحت مظلة بيئة التعلم المدعومة بالتكنولوجيا. وأصبح هناك توجه للتحول إلى مجتمع منتج ومشارك للمعرفة والمعلومات، وذلك من خلال دمج التقنية في المؤسسات التعليمية والعمل على توظيفها بالطريقة المثلى، ودمجها في المقررات الدراسية؛ لتحقيق الأهداف المنشودة، وتحسين مخرجات التعليم، وجعل المتعلم هو محور العملية التعليمية (غوص والشريف، ٢٠٢٢). وهذا فرض على التربية إجراء تغيير في الأهداف والوسائل والطرق التي تسير عليها؛ فلم تعد الأهداف قاصرة على الأهداف الاجتماعية والسياسية والاقتصادية؛ بل تخطى ذلك إلى تحقيق الأهداف الرقمية التي تهتم بإعداد الجيل رقميًا، وتأهيله تكنولوجيًا من خلال تزويده بمهارات رقمية وإكساب المؤسسات التعليمية ميزة تنافسية.

ومع تنامي الجهود المبذولة نحو تحقيق التحول الرقمي، فقد أصبح هناك ضرورة لتوفير الحماية من الهجمات السيبرانية، والمحافظة على الهوية الإلكترونية، خاصة وأن التعليم الرقمي يعتمد بشكل كبير على شبكة الإنترنت، وتوفير هذه الحماية يستوجب توعية المتعلمين بمخاطر استخدام شبكات الإنترنت، وكيفية اتخاذ إجراءات وقائية لحماية البيانات والمعلومات من الفيروسات، أو اختراقها، أو استغلالها في الإساءة إلى الآخرين. وما يؤثر سلبًا على سلامة البنى التحتية للمعلومات الشخصية والوطنية، وعلى أمن الطلبة، ولتفادي وقوعهم كضحايا للجرائم الإلكترونية (الصانع وآخرون، ٢٠٢٠).

وفي إطار هذا السياق؛ فقد أصبح الأمن السيبراني من المواضيع التي لا يمكن إغفال أهميتها في الجانب التعليمي في ظل الثورة الرقمية والتكنولوجية المعاصرة. ويتعاظم ذلك التوجه في المؤسسات التعليمية التي تعاني من ضعف وجود نشاط توعوي واضح بتحديات الجرائم السيبرانية. وعلي ذلك، فقد أصبح الأمن السيبراني من التخصصات المهمة لدوره الحيوي في حماية البيانات من القرصنة والتلف، وحماية سرية البيانات الحساسة، ومعلومات التعريف

الشخصية، والملكية الفكرية، والبيانات وأنظمة المعلومات، وغير ذلك (الدمرداش، ٢٠٢٢). وظهرت الحاجة إلى رفع مستوى الوعي بالأمن السيبراني لتثقيف الطلبة، لتحسين إجراءات الأمان التفاعلية والاستباقية للحد من اختراق البيانات الشخصية، أو مشاركها دون حماية كافية، حيث يواجه الطلبة انتهاكات كبيرة في الخصوصية. وأصبح من الضروري تطوير الوعي الأمني السيبراني لدى الطلبة، وإدراج موضوع الأمن السيبراني في المناهج المدرسية، وتوجيه الطلبة لاستخدام الكمبيوتر والإنترنت بطريقة آمنة، واتخاذ التدابير الأمنية اللازمة (Karagozlu,2020) بما يتوافق مع المتغيرات التقنية المتسارعة في ضوء حاجات المتعلمين وخبراتهم، وذلك للتقليل من خطورة الهجمات السيبرانية في المؤسسات التعليمية، والعمل على تلافيها (السعادات والتميمي، ٢٠٢٢) حيث إن الوعي بالأمن السيبراني يعمل على حماية البيئة الرقمية وجعلها آمنة قادرة على التصدي لجميع هجمات وجرائم الفضاء السيبراني بمختلف أشكالها(فرج، ٢٠٢٢).

وقد أشارت دراسات (O'Brien, 2019؛Black & Clark,2018&Solms & Solms,2015 ؛Pusey & Sadera,2011) إلى افتقار الطلاب إلى أساسيات الأمن السيبراني، وإلى أهمية الأمن السيبراني، وضرورة تعزيز مفاهيمه في التعليم، وضرورة إكساب الوعي به للمعلمين والمتعلمين بما يضمن الحماية الشخصية للبيانات. وقد أوصت دراسة (القحطاني، ٢٠١٩) بضرورة الاهتمام بتعليم الطلبة مفهوم الأمن السيبراني، وكيفية التعامل مع المواقع الالكترونية المختلفة. كما أوصت بعض المؤتمرات والملتقيات التي عقدت في مجال الأمن السيبراني كمؤتمر الأمن السيبراني ٢٠١٩ بالرياض، ومؤتمر التكنولوجيا وحلول البرمجيات ٢٠١٩ بالقاهرة، والمؤتمر الدولي للثورة الصناعية الرابعة ٢٠١٨ بسلطنة عمان، ومؤتمر " تكنولوجيا وتقنيات التعليم والتعليم الإلكتروني" ٢٠١٨ بالشارقة.

وتأسيسا على ما سبق؛ تبرز أهمية تنمية الوعي بالأمن السيبراني من خلال مؤسسات الإعداد الأكاديمي خاصة التي تعد الطلبة ليكونوا معلمي الغد، ومن خلال المقررات المتصلة بتكنولوجيا التعليم بشكل خاص. ومن هنا تأتي أهمية دور كلية التربية الأساسية وما تقدمه من مقررات تتعلق بتكنولوجيا التعليم في إعداد معلمين يمكنهم التعامل مع التطور التقني المتسارع، وما يتطلبه هذا التعامل من وعي بمفاهيم ومهارات الأمن السيبراني. ومن ثم جاءت الدراسة الحالية للوقوف على مدى إسهام مقررات تكنولوجيا التعليم في تنمية الوعي بمفهوم الأمن السيبراني وإجراءاته لدى الطلبة المعلمين للحماية من خطر التهديدات والجرائم الإلكترونية.

مشكلة الدراسة وأسئلتها

من خلال عمل الباحثتين وخبرتيهما في الميدان التعليمي كأعضاء هيئة تدريس لتكنولوجيا التعليم بكلية التربية الأساسية، فقد لاحظتا أن الأمن السيبراني أصبح يمثل أحد التحديات التي تواجه الطلبة أثناء استخدام الشبكة العنكبوتية. وقد قامت الباحثتان باستكشاف من خلال توزيع استبانة مختصرة على عينة استطلاعية حجمها (٥٠) طالبة بالكلية، وكان الهدف منها: الكشف عن مدى الوعي بمفاهيم الأمن السيبراني، ومدى تمكنهم من التعامل مع الأجهزة الحاسوبية والهاتف النقال، التي تتطلب الحماية الشخصية والمسؤولية الرقمية. وجاءت النتيجة مشيرة إلى أن حوالي (٩٠٪) من الطلبة ليس لديهم إلمام كافٍ بمفردات الأمن السيبراني، ووجود قصور لديهم في مهارات الأمن السيبراني، وأن الكثير منهم لا يمتلكون الوعي الجيد بقضايا الأمن السيبراني، وكيفية اتخاذ إجراءات للتعامل مع التهديدات المختلفة أو حماية أجهزتهم الإلكترونية. وعلى ذلك، أمكن تحديد مشكلة هذه الدراسة في ضعف مستوى الوعي بالأمن السيبراني لدى طلبة كلية التربية الأساسية.

يؤكد ذلك ما كشفت عنه نتائج عديد من الدراسات؛ التي أسفرت عن أن الطلاب يتعرضون للآثار السلبية أثناء التعامل مع الفضاء السيبراني؛ منها دراسات (الصحفي وعسكول، ٢٠١٩؛ المنتشري وحريري، ٢٠٢٠؛ السعيد، ٢٠٢٠؛ إبراهيم، ٢٠٢١) التي أسفرت عن وجود ضعف في الوعي بمفاهيم الأمن السيبراني والمعلوماتي لدى الطلاب، وأن مستويات الوعي بالأمن السيبراني في المؤسسات التعليمية لا ترتقي للمستوى المطلوب. وأكدت على ضرورة إكساب الطلاب الوعي

بتلك المفاهيم. وضرورة التوعية بمخاطر الفضاء السيبراني، وتعليم الطلاب الممارسات الصحيحة، وعلى تنمية الوعي بأخلاقيات وآداب السلوك الرقمي وإدراج مقررات دراسية خاصة بهذه المفاهيم.

وعلى ضوء ذلك، جاءت الدراسة الحالية الوقوف على مدى إسهام تدريس مقررات تكنولوجيا التعليم في إمكانية تنمية هذا الوعي لدى طلبة كلية التربية الأساسية بدولة الكويت. خاصة وأن الباحثتان – في حد علمهما- لم يعثرا على أي من الدراسات التي عالجت هذا الدور، وصولا إلى عدد من التوصيات التي يمكن أن تعزز هذا الوعي لدى الطلبة.

ويمكن صياغة أسئلة الدراسة على النحو الآتي:

١- ما درجة وعى طلبة كلية التربية الأساسية بدولة الكويت بالأمن السيبراني؟

٢- ما المخاطر والانتهاكات السيبرانية التي يتعرض لها الطلبة أثناء التعامل مع الفضاء السيبراني؟

٣- ما إسهامات دراسة مقررات تكنولوجيا التعليم في تنمية الوعي بالأمن السيبراني لدى طلبة كلية التربية الأساسية؟

٤- هل توجد فروق ذات دلالة إحصائية بين متوسطات أفراد عينة الدراسة حول تقدير مستوى الوعي بالأمن السيبراني ومخاطر انتهاكات الأمن السيبراني ودور تكنولوجيا التعليم في تنميته تعزى لمتغيرات (النوع، التخصص، الفرقة الدراسية)؟

أهداف الدراسة

تهدف الدراسة إلى تعرف درجة وعى طلبة كلية التربية الأساسية بدولة الكويت بمفاهيم الأمن السيبراني ومخاطر وانتهاكات الأمن السيبراني، ورصد أهم إسهامات دراسة مقررات تكنولوجيا التعليم على تنمية الوعي بالأمن السيبراني لدى الطلبة، وتعرف مدى وجود تباين بين تقديرات العينة في ذلك تبعا لمتغيرات (النوع، التخصص، الفرقة الدراسية).

أهمية الدراسة

تتحدد أهمية الدراسة في العناصر الآتية:

- تأتي هذه الدراسة استجابة للتوجهات العالمية في تعزيز ورفع درجة الوعي بالأمن السيبراني لدى مستخدمي الفضاء السيبراني.
- تسليط الضوء على دور كلية التربية الأساسية بدولة الكويت في تنمية الوعي بالأمن السيبراني لدى الطلبة.
- تتزامن الدراسة الحالية مع تزايد خطر الهجمات الإلكترونية التي تهدد الأمن السيبراني للمستخدمين.
- قد تساعد نتائج هذه الدراسة في إعداد الفعاليات التي تعمل على زيادة الوعي بالأمن السيبراني وتعميقه لدى طلبة كلية التربية الأساسية بدولة الكويت
- قد يستفيد من نتائج هذه الدراسة القائمين على برامج إعداد المعلم في كلية التربية الأساسية، خاصة في تعرف أهمية إدراج مفاهيم الأمن السيبراني ضمن هذه البرامج.
- تقدم الدراسة أداة لقياس الوعي بالأمن السيبراني ومخاطره تهديداته ودور دراسة مقررات تكنولوجيا التعليم في تنميته.

منهج الدراسة

تستعين الدراسة بالمنهج الوصفي المسحي لملاءمته لطبيعة الدراسة، وللإجابة عن أسئلتها؛ إذ هو المنهج الذي يقوم على جمع البيانات من مجتمع الدراسة، عن طريق العينة الممثلة لهم، وذلك بهدف وصف الظاهرة محل الدراسة (الوعي بالأمن السيبراني) من حيث درجته لدى أفراد العينة، ومدى تقديرهم لمخاطر الهجمات والتهديدات السيبرانية في الواقع، وتعرف مدى أهمية دراسة مقررات تكنولوجيا التعليم في تنمية هذا الوعي، فضلا عن تعرف تأثير المتغيرات الديموجرافية المتعلقة بالنوع والتخصص والفرقة الدراسية في ذلك .

التعريفات الإجرائية للدراسة

تتناول الدراسة التعريفات الإجرائية الآتية:

- يعرف الأمن السيبراني إجرائيا في الدراسة الحالية بأنه: الإجراءات التي يقوم بها الطلبة لمنع اختراق شبكات المعلومات بواسطة البرمجيات الخبيثة كالفيروسات، وغير ذلك من الممارسات السلبية. والتي تعمل على توفير الحماية الأمنية، وعدم وإلحاق الأذى، ومنع الدخول غير المشروع للأجهزة والهواتف الذكية، والمحافظة على الهوية الإلكترونية، واستعادة المعلومات الرقمية وذلك بهدف ضمان سرية، وتوافر وسلامة البيانات، واتخاذ جميع الاحتياطات اللازمة لحماية الطالبات من التهديدات السيبرانية
- يُعرَّف الوعي بالأمن السيبراني إجرائيا في الدراسة الحالية بأنه: معرفة وفهم طلبة الكلية لمختلف الإجراءات الإنسانية والتقنية والقانونية اللازمة لحماية أجهزتهم الإلكترونية وبياناتهم من أي اختراقات أو انتهاكات مرتبطة باستخدام التكنولوجيا لأغراض العملية التعليمية، أو تلف أو تدمير، وتزويدهم بالمعارف التي تضبط السلوكيات والتصرفات التي تحميهم من المخاطر السيبرانية، أثناء التعامل مع الانترنت وشبكات التواصل الاجتماعي.

الإطار النظري

يعرض هذا الجزء من الدراسة لمحورين أساسيين، يوضحان الإطار الفكري والمفاهيمي للدراسة، وهما الأمن السيبراني، وتكنولوجيا التعليم، وقد تم تناولهما على النحو الآتي:

الأمن السيبراني cyber security

حسب قاموس المورد (٢٠١٦، ٣٠٧) فإن لفظ السيبرانية: هي كلمة يونانية الأصل تعني علم الضبط. والسبرنة مصدرها (Cybernetic) تعني الضبط الأوتوماتكي لعملية ما، والتحكم من بعد عن طريق استخدام الحاسوب. و كلمة Cyber تعبير يصف جميع الأمور المتعلقة بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، وحماية البيانات والمعلومات والأجهزة باستخدام آليات وتجهيزات وتطبيقات وبرمجيات من خلال شبكات الحواسيب والاتصالات والإنترنت .

ويعرف Pusey and Sadera (2011, 82) الأمن السيبراني بأنه " الإجراءات التقنية الهادفة إلى حماية البيانات، والهوية الشخصية والمعدات التقنية من أي شكل من أشكال الوصول غير المسموح به إلى تلك المعلومات أو المعدات". ويعرف Crompton, Thompson and Zou, (2016,3) " الأمن السيبراني على أنه العملية أو الحالة التي تكون بموجبها المعلومات وأنظمة المعلومات محمية بشكل تام ضد أي شكل من أشكال الإتلاف أو الوصول غير المسموح به لتلك المعلومات والأنظمة أو التلاعب بها أو إساءة استخدامها" . ويعرف Buczak and Guven (2016. 1153) " الأمن السيبراني على أنه مجموعة من التكنولوجيا والعمليات المصممة لحماية أجهزة الحاسوب والشبكات والبرامج والبيانات من الهجمات، والوصول غير المرخص به، والعبث أو التدمير". ويعرف Richardson et al.,(2020) " الأمن السيبراني بأنه " مجموعة الأدوات والسياسات والتدابير المتخذة، وأفضل الممارسات التي يمكن استخدامها لإدارة المخاطر، وحماية البيئة السيبرانية والحواسيب، والمستخدمين، والبنية التحتية، والتطبيقات، من الوصول غير المصرح به؛ وذلك بهدف الحفاظ على سلامة ونزاهة البيانات المخزنة". في حين تحدده المنتشري (٢٠٢٠، ٤٦٢) بأنه: "مفهوم أمنى خاص بحماية المعلومات وكل ما له صلة بتلك المعلومات من عمليات وخدمات وأجهزة وتقنيات ضد أي شكل من أشكال الوصول غير المسموح به، أو استخدام تلك المعلومات بشكل سلبي أو بما يمثل خطرا على الهجمات أو الأفراد ذوي الصلة بتلك المعلومات". ويرى كلاع (٢٠٢٢، ٢٨٤) " أن الأمن السيبراني يعني ممارسة حماية البرامج والشبكات والأنظمة والبيانات وكل ما يرتبط بشبكة الإنترنت ووضع السياسات الأمنية؛ بهدف الحد من الهجمات السيبرانية وإلحاق الأذى بالمستخدمين بما في ذلك الطلاب والطالبات من أجل حمايتهم من التلاعب بالمعلومات والانتهاكات التي يترتب عليها العديد من الأضرار سواء كانت مادية، أو نفسية أو معنوية " .

ومن ذلك يتبين أن الأمن السيبراني يتمثل في كونه مجموعة إجراءات تقنية أو عمليات مصممة أو مجموعة أدوات وسياسات. لكن جميعها تدور حول مفهوم أمني خاص يتعلق بحماية البيانات والمعلومات ويمنع الوصول غير المسموح به عبر ما يعرف بالهجمات أو التهديدات السيبرانية. وأن سياسات الأمن السيبراني تعتمد على شقين أساسين هما الجانب التقني والجانب التنظيمي، وتأثير ذلك على جوانب الوعي والتطبيق لدى الأفراد والمنظمات.

وبصفة عامة؛ ترى الباحثتان أن مفهوم الأمن السيبراني هو مفهوم أمني يتضمن مجموعة إجراءات وتطبيقات تعمل على حماية البيانات المعلومات من مخاطر القرصنة عن طريق الوصول غير المشروع للتلاعب بها، وحماية الأشخاص من التجسس والتنمر أو التصيد والنصب والاحتيال والتشهير بالإساءة.

وعادة ما يذكر عددٍ من المصطلحات مع مفهوم الأمن السيبراني؛ مثل: الفضاء السيبراني، والتحقق الذي يعد شرطا أساسيا للوصول إلى الموارد في النظام، ومصطلح النسخ الاحتياطية، والتشفير، والمخاطر السيبرانية، والهجوم السيبراني، والصمود الأمني السيبراني، وأرشفة البيانات، والدفاع الأمني، وقواعد نقل النص التشعبي الآمن، ونظام الحماية المتقدمة، والبرمجيات الضارة، وجدار الحماية لتطبيقات الويب (الشمري، ٢٠٢٣). هذه المصطلحات تمثل منظومة تعمل في فلك حماية الفضاء السيبراني من الأخطار والتهديدات التي يمكن أن يتعرض لها المستخدمون، والتي ينبغي أن يتم مواجهتها من خلال توعية الأفراد بجوانب الاستخدام الآمن، في ضوء ما يعرف بالمواطنة الرقمية.

أهداف الأمن السيبراني

تعد حماية مصالح الأفراد، والدول وأمنها الوطني الرقمي، والحفاظ على سرية وخصوصية بيانات المستخدمين، من أهم البواعث التي تدفع إلى وضع حلول للثغرات الأمنية الرقمية والتهديدات التي يمكن أن تؤثر على المستخدمين، ويعد ذلك من أهم أهداف تحقيق الأمن السيبراني . وفي هذا الصدد يشير العتيبي(٢٠٢٢) إلى أن أهم أهداف الأمن السيبراني تتمثل في:

- سد كافة الثغرات الموجودة في أنظمة أمن المعلومات.
- توفير بيئة للتعاملات في مجتمع المعلومات تكون آمنة وموثوقة.
- تأمين البنية التحتية لتحقيق بيئة رقمية آمنة تصمد أمام الهجمات الإلكترونية.
- مقاومة البرمجيات الخبيثة، وما تستهدفه من إحداث أضرار بالغة للمستخدمين .

ويضيف (صائغ ، ٢٠١٨؛ المنتشري وحريري، ٢٠٢٠) إلى ذلك الأهداف الآتية:

- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات.
- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف المستخدمين والمؤسسات.
- توفير المتطلبات اللازمة للحد من المخاطر والجرائم السيبرانية التي تستهدف المستخدمين.
- الحد من التجسس والتخريب الإلكتروني على مستوى الأفراد والمؤسسات.
- التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة.

أهمية الأمن السيبراني

في ظل انتشار الاستخدام المتزايد لشبكة الإنترنت والهواتف الذكية أصبح الأمن السيبراني ضرورة وحلٌ أمثل لمتابعة الاستخدام الواسع للإنترنت وتطبيقاته وأنظمته المختلفة للتقليل من المخاطر التي تنشأ من سوء الاستخدام، وميل البعض منهم لسلوكيات منحرفة. وتبرز أهمية الأمن السيبراني من حيث دوره في المحافظة على سرية البيانات الخاصة بالأفراد والمؤسسات، ومنع الوصول إلا لمن هم مسموح لهم الاطلاع عليه(غوص والشريف، ٢٠٢٢).

كما تبرز أهمية الأمن السيبراني في حماية جميع أنواع الأجهزة الخاصة المحمولة والمعدات التقنية، ووسائط التخزين من خطر الهجمات والاختراقات الإلكترونية، والتدمير الجزئي والكلي، وتوفير فرص التعامل الآمن مع خدمات تصفح الإنترنت من خلال نشر المعلومات

والإجراءات التي تعمل على حماية الأفراد (الصانع وآخرون ٢٠٢٠) من الوقوع كضحايا للمخاطر والانتهاكات السيبرانية.

الأهمية التربوية للأمن السيبراني

مع تزايد استخدام وسائل الوصول إلى شبكة الإنترنت عبر العديد من الأجهزة المحمولة بالإضافة إلى الحواسيب، تنامت فرص وقوع العديد من الطلبة والمعلمين حول العالم ضحية لأحد أشكال المخاطر والانتهاكات السيبرانية، مما ترتب عليه كثير من المخاطر والانتهاكات والأضرار المادية والنفسية والمعنوية التي تؤثر على المعلم والمتعلم، وعلى المؤسسة التعليمية (Wilson, 2014). فضلا عن الخسائر العلمية للأبحاث والوثائق التعليمية عند التسلل إلى شبكات المعلومات الخاصة بالمؤسسات التعليمية. وكذلك تعطيل التعلم، وسرقة الملكية الفكرية، بما يؤدي إلى ضرر جسدي وعاطفي للمستخدمين. وهذا في مجمله يؤثر سلبًا على الطلبة والمعلمين والمؤسسة التربوية، ويعمل على تدمير الأخلاق والقيم، والبنى التحتية، وتؤدي إلى خسائر مادية ومعنوية (المنتشري وحريري، ٢٠٢٠). الأمر الذي يزيد من أهمية وضرورة توفير الأمن السيبراني في مجال التعليم والتعلم، خاصة للمؤسسات التعليمية التي تفتقر إلى البنية التحتية اللازمة لتحقيق الأمن السيبراني، والتي يجعلها غير قادرة على مواجهة التهديدات.

ويذكر عبد الجواد وآخرون(٢٠٢٤) أن الأهمية التربوية للأمن السيبراني تتمثل في ضمان سرية وخصوصية الوثائق التعليمية والحفاظ على سلامتها بشكل مستمر، ومتابعة ومراقبة وتطوير وضبط نظام المعلومات والأمن السيبراني في المؤسسات التعليمية وحمايته من الهجمات السيبرانية، من خلال تثقيف الطلبة والمعلمين والقائمين على أمر المؤسسات التعليمية بعدم التعرض للانتهاكات والمخاطر السيبرانية، وتوفير طرق الوقاية ضد الهجمات السيبرانية للحفاظ على أمن المؤسسة التعليمية بعناصرها المختلفة.

المخاطر والتهديدات السيبرانية

تشير الأدبيات (العتيبي، ٢٠٢٢؛ المنتشري وحريري، ٢٠٢٠) إلى أن أهم مخاطر وتهديدات الأمن السيبراني التي يتعرض لها الأفراد والمؤسسات عند التعامل مع الفضاء السيبراني، تتمثل في:

١- التنمر الإلكتروني: الذي يتم من خلاله استخدام تكنولوجيا الاتصالات لأغراض الإيذاء كالتحرش، المضايقة الإزعاج، التهديد، الابتزاز وغيرها.

٢- التشهير الالكتروني: الذي يقوم على بث أفكار وأخبار من شأنها الإضرار الأدبي أو المعنوي بشخص أو جهة معينة .

٣- الاحتيال الإلكتروني: وهو نوع من أنواع النصب على الضحية؛ للتمكن من الاستيلاء عليه .

٤- التصيد الإلكتروني: وهو أحد أشكال الجرائم السيبرانية يتم من خلاله استهداف المستخدمين وخداعهم للحصول على معلوماتهم الحساسة وسرقة أموالهم وابتزازهم .

٥- الهندسة الاجتماعية (اختراق العقول): وهي مجموعة من الأساليب التي يستخدمها الجناة لإقناع الضحايا بتنفيذ بعض الإجراءات التي تساعد على اختراق أنظمتهم والإضرار بها .

٦- الإرهاب الإلكتروني: وهو إحداث الخوف والاضطرابات وزعزعة الأمن والإيمان في نفوس الناس من خلال بث الأخبار المحبطة والمسيئة ونشر الشائعات بغرض الحصول على الأنباء الصحيحة التي تخص هذا الموضوع .

٧- التغرير والاستدراج: حيث يوهم الجناة ضحاياهم من الصغار برغبتهم في تكوين علاقة صداقة على الإنترنت، لاستغلالهم وابتزازهم .

٨- التجسس الإلكتروني: حيث يتم بواسطة برامج معينة تقوم بالحصول سرا على معلومات تخص المستخدم، ومراقبة حركته، ومن ثم يقوم بنقل هذه المعلومات إلى الجهة التي تريد مهاجمته .

الوعي بالأمن السيبراني

من أجل حماية البيانات الخاصة بالأفراد، والتعرف على السلوكيات الصحيحة للاستخدام الآمن للإنترنت، للحد من المخاطر والتهديدات السيبرانية، وما يترتب عليها من آثار سلبية لا تقف حدودها عند الأفراد، بل تتعداها إلى المؤسسات والدول؛ تبرز أهمية توافر الوعي الكافي بجوانب الأمن السيبراني لضمان ممارسات رقمية سليمة.

ويعرف الوعي بالأمن السيبراني على أنه "مزيج من المعرفة والسلوكيات اللازمة لحماية المعلومات أو الأصول السيبرانية الشخصية" (Garcia & Bongo, 2022, 116) وأنه "الإحساس والدراية بالأعمال والممارسات غير المشروعة والتي تهدف للاختراق، أو التعطيل، أو التعديل، أو الاستغلال غير المصرح به للبيانات، أو المعلومات؛ للحماية والوقاية منها" (السعادات والتميمي، ٢٠٢٢، ٢٦٤). كما يعرف بأنه: "معرفة وفهم المعلمين بشكل عميق لمختلف أشكال التهديدات السيبرانية المرتبطة بالتعلم الإلكتروني، واستخدام التكنولوجيا لأغراض عمليتي التعليم والتعلم، وقدرتهم الفعلية والسلوكية على اتخاذ الإجراءات اللازمة للتعامل مع هذه التهديدات بالشكل المناسب" (الضفيري وآخرون، ٢٠٢٤، ١٠).

وفي المجال التربوي يعرّف الوعي بالأمن السيبراني بأنه "مدى إدراك الطلبة لكيفية حماية بياناتهم وحساباتهم الشخصية المرتبطة بتقنيات الاتصالات والمعلومات من المخاطر السيبرانية" (الحبيب، ٢٠٢٢، ٢٧٩).

وينطوي الوعي بالأمن السيبراني بشكل رئيس على مكونين رئيسين؛ هما: الجانب المعرفي، وهو المعرفة والفهم الشاملين للمشكلات والتحديات المتعلقة بالأمن السيبراني وتداعياتها، وكذلك ما يجب القيام به للتعامل معها. والجانب السلوكي الذي يشير إلى الإجراءات المتخذة فعليا، والسلوك الذي يظهره الأفراد لحماية أجهزتهم من التهديدات السيبرانية استنادًا إلى معرفتهم وفهمهم (Khan et al., 2022)

أهمية الوعي بالأمن السيبراني في المجال التعليمي

تبرز أهمية الوعي بالأمن السيبراني في المجال التعليمي، من حيث إن فرص وقوع الفرد كضحية للجرائم السيبرانية تزداد في ضوء غياب هذا الأمن مع تزايد الاعتماد على توظيف شبكة الإنترنت في معظم جوانب العملية التعليمية.

ومن الممكن الوقوف على مستوى الوعي بالأمن السيبراني لدى المتعلمين من خلال الممارسات التي تعكس هذا الوعي عند التعامل مع الفضاء السيبراني، والتي من أهمها (الحبيب ، ٢٠٢٢):

- التأكد من إعدادات الحاسوب وشبكة الإنترنت.
- اختيار كلمات مرور قوية، وتحديثها بشكل مستمر، والتحقق من أمن مواقع التواصل الاجتماعي، والبريد الإلكتروني، والحسابات الشخصية على الحاسوب أو الهواتف الذكية.
- عدم الاستجابة لأي رسائل مجهولة المصدر ترد إلى البريد الإلكتروني، وعدم الرد بإرسال أي معلومات شخصية عبر البريد الالكتروني، أو الإفصاح عن معلومات خاصة بالمستخدم .
- استخدام برامج الحماية ومضادات الفيروسات وتحديثها باستمرار.
- حماية المعلومات الشخصية ومنع الآخرين من الاطلاع عليها.
- المحافظة على تحديث جدران الحماية للبنية التحتية للبيئة المعلوماتية.
- تأمين وتحديد إمكانية الوصول إلى النظام، حيث يمكن تقييده بالعديد من وسائل التعرف على شخصية المستخدم وتحديد نطاق الاستخدام.

تكنولوجيا التعليم: المفهوم والأسس والمرتكزات

تكنولوجيا التعليم في الأساس تعني منهجية في التفكير لوضع منظومة تعليمية، أي إتباع منهج وأسلوب وطريقة في العمل تسير وفق خطوات منظمة، مستعملة كافة الإمكانيات التي تقدمها التكنولوجيا. وهي تمثل منظومة متكاملة تشمل توظيف واستثمار كل ما هو جديد من الأجهزة والأدوات والمعدات والمواد الإلكترونية، والتطبيقات التكنولوجية في مجال التعليم، وفي

تصميم البيئات التعليمية، والأساليب التعليمية التي يستخدمها المعلم والمتعلم (الشيبي، ٢٠٢٢). ومن ثم فهي عملية مركبة متكاملة يشترك فيها الأفراد والأساليب والأفكار والأدوات والتنظيمات بغرض مواجهة المشكلات التي تتصل بجميع جوانب التعلم الإنساني وإيجاد الحلول المناسبة لها ثم تنفيذها وتقويمها (عليان وآخرون، ٢٠٠٣) وغايتها تتمحور حول الإفادة من المعرفة العلمية وطرائق البحث العلمي في تخطيط وحدات النظام التعليمي وتنفيذها وتقويمها ككل متكامل، لأجل زيادة قدرات المعلم والمتعلم على التفاعل مع العملية التعليمية، وتقديم الحلول الإبداعية المبتكرة ، توسيعا لفرص التعليم، وتخفيضا لكلفته، ورفعا لكفاءته، وزيادة فاعليته بصورة تتناسب مع طبيعة العصر (الصرايرة، ٢٠٢٣) وعلى المستوى الإجرائي تمثل تكنولوجيا التعليم كل ما يستخدم في مجال التعليم من تقنية معلوماتية، تيسر أمر تحقيق أهداف العملية التعليمية بفاعلية، والحصول على مخرجات ذات جودة عالية.

وقد أصبحت تكنولوجيا التعليم علما له طبيعته بين العلوم التربوية، وله أسسه ومرتكزاته ومبادئه التي يقوم عليها؛ التي من أهمها:

- أن تكنولوجيا التعليم علم أكاديمي متخصص يسعى إلى فهم وتحديد المشكلات الناتجة عن المواقف التعليمية وتحليلها وتفسيرها، والبحث في أسباب حدوثها، والعوامل المؤثرة فيها، وإيجاد الحلول المناسبة لها، والتنبؤ بالمشكلات المتوقعة، واقتراح حلول مستقبلية بناء على دراسة العلاقات الموجودة بين عناصر الموقف التعليمي.
- أن تكنولوجيا التعليم لها أهدافها المحددة والمتمثلة في تحسين وتطوير عملي في التعليم والتعلم والتغلب على المشكلات التي تواجه العملية التعليمية.
- أن تكنولوجيا التعليم أصبحت مهنة مستقلة لها قواعدها، أصولها وأخلاقياتها ومسؤوليتها، ووظائفها، فهناك أخصائي تكنولوجيا التعليم والذي يتم إعداده بكليات التربية للقيام بهذه الوظيفة(البجاوي والمسعودي، ٢٠٢٠).

أهمية توظيف تكنولوجيا التعليم في العملية التعليمية

وتوظيف التكنولوجيا في العملية التعليمية ينطوي على تضمين التكنولوجيا كأداة لتعزيز عملية التعلم. ويتحقق التوظيف الفعال للتكنولوجيا عندما يصبح الطلبة قادرين على الاستفادة من الأدوات التكنولوجية المناسبة لمساعدتهم في الحصول على المعلومات في الوقت المناسب، وتحليل وتركيب وعرض المعلومات بطريقة احترافية(Medina et al., 2018) .

وتبرز أهمية توظيف تكنولوجيا التعليم من حيث إنها تساعد على:

- تحسين نوعية التعليم؛ حيث تسهم تكنولوجيا التعليم في تعليم الأعداد الكبيرة من المتعلمين باستخدام الأجهزة التعليمية الحديثة، وتوفر فرصًا لمراعاة الفروق الفردية بين المتعلمين من خلال تنويع مصادر التعليم وفقا للقدرات المختلفة للمتعلمين.
- تؤدى تكنولوجيا التعليم دور المرشد الذي يساعد المعلم في توجيه المادة العلمية للمتعلم واستبدال طريقته التقليدية للتعليم في شرح الدروس بطريقة حديثة تفعل دور المتعلم وتجعله نشطا في العملية التعليمية.
- تساعد تكنولوجيا التعليم في توفير فرصة لاكتساب الخبرات الحسية وبشكل أقرب إلى الخبرات الواقعية، التي تقرب الواقع إلى أذهان المتعلمين ، ومن ثم تساعد في نمو المفاهيم العلمية لدى المتعلمين.
- تعمل تكنولوجيا التعليم على تحسين مستوى الخريجين، إذ تعمل على توفير الجو التربوي والنفسي، وتشويق المتعلمين وإثارة انتباههم وزيادة فهمهم للمادة العلمية، وتشجيع المتعلمين على التفكير السليم، حيث تركز الانتباه في الموضوع الذي تعالجه، وحصر التفكير، وعدم تشتيت الانتباه.
- تثير تكنولوجيا التعليم اهتمام المتعلمين وهواياتهم وتجديد نشاطاتهم ومشاركتهم وإشباع حاجاتهم التعليم تساعد في نمو المفاهيم وتكوين الاتجاهات العملية المرغوبة.
- كما تساعد تكنولوجيا التعليم على تعليم أعداد كبيرة من الطلبة داخل الصفوف أو خارجها، وتعمل على تلاقي ضعف الكفاية المهنية لدى بعض المعلمين(عبد الفتاح ،٢٠٢٢).

تكنولوجيا التعليم وتنمية الوعي بالأمن السيبراني

إن دراسة تكنولوجيا التعليم يمكن أن تسهم في تنمية وعي الطلبة بالأمن السيبراني وتزويده بسبل الحماية من مخاطر الهجمات السيبرانية، وذلك من خلال:

- توعية الطلبة فيما يتعلق بحماية البيانات الشخصية.
- التعريف بمخاطر وأوجه القصور المحتملة عند مشاركة الطلبة في الأنشطة على شبكة الإنترنت .
- استخدام التقنيات المختلفة والحديثة التي تساعد على التأمين والحماية.
- نشر سياسات وإجراءات الأمن الرقمي وتحديثها بكل جديد
- نشر مفاهيم الأمن السيبراني واهم التهديدات والأخطار الناتجة عنه من خلال إرسال الرسائل النصية للمواطنين (الجندي، ٢٠١٩).
- تدريب الطلبة على إعداد كلمات مرور قوية يصعب وصول القراصنة إليها.
- تعزيز جوانب المواطنة الرقمية التي تؤكد على تعرُّف مجموعة القواعد والضوابط والمعايير والأعراف والمبادئ المتبعة في الاستخدام الأمثل للتكنولوجيا الرقمية والتي يحتاجها الطلبة، كي يتعلموا طريقة التعامل مع التقنيات ليحفظوا أمنهم السيبراني من الاختراق، وليساهموا في المحافظة على أمن الوطن.
- إكساب الطلبة مهارة عمل نسخ احتياطية من البيانات والملفات الخاصة بنظم المعلومات أو الحالة التقنية، مثل: كلمات المرور الخاصة، والبريد الإلكتروني، والبيانات المخزنة داخل أو خارج النظام.
- تدريب الطلبة على استخدام أساليب الوقاية من الفيروسات التي تهاجم النظام، وذلك بمعرفة طرق تثبيت برامج التحقق من الفيروسات في الذاكرة وتحديثها باستمرار لضمان قدرتها على مواجهة الفيروسات الحديثة والمتطورة، وتجهيز نسخ احتياطية من البرمجيات لاسترجاعها في حال تعرض النسخة الأصلية للتلف، ومن خلال التوعية بعدم تحميل أي برنامج غير موثوق به في حساباتهم، أو فتح روابط مجهولة.
- الإرشاد والتوعية بأساسيات الأمن السيبراني لأجل رفع مستوى الوعي بالجرائم السيبرانية، والتوعية بالمخاطر الأمنية، من خلال تفعيل إقامة الندوات والمؤتمرات الخاصة بالأمن السيبراني، ودعوة الكفاءات البشرية في مجال الأمن السيبراني للاشتراك في هذه الندوات والمؤتمرات، وإدراج مقررات دراسية خاصة بمفاهيم الأمن السيبراني ضمن البرامج التعليمية المختلفة (الصانع وآخرون، ٢٠٢٠).

إجراءات العمل الميداني

أداة الدراسة

بعد الاطلاع على أدبيات البحث المتصلة بموضوع الدراسة منها (الصحفي وعسكول، ٢٠١٩؛ المنتشري وحريري، ٢٠٢٠؛ العتيبي، ٢٠٢٢؛ عرايضه، ٢٠٢٢؛ الحباشنة، ٢٠٢٣). أمكن إعداد أداة خاصة بالدراسة الحالية، وهي عبارة عن استبانة اشتملت (٤٨) عبارة.

صدق الأداة

للوقوف على صدق الاستبانة:

١- تم عرض الصورة الأولية منها (٤٨) عبارة على مجموعة من الأساتذة المختصين في تكنولوجيا التعليم بكلية التربية الأساسية، وكلية التربية جامعة الكويت، بغية إبداء الرأي حول مناسبة العبارات للمحاور ولهدف الدراسة. وقد أفاد المحكمون بتعديل بعض العبارات وحذف (٥)، ومن ثم أصبحت الأداة (٤٣) عبارة في صورتها النهائية. وُزعت على (٣) محاور؛ هي: - المحور الأول: درجة الوعي بالأمن السيبراني (١٤) عبارة، والمحور الثاني: مخاطر وانتهاكات الأمن السيبراني (١٣) عبارة، و المحور الثالث: دور تكنولوجيا التعليم في تنمية الوعي بالأمن السيبراني (١٦) عبارة.

٢- تم تطبيق الأداة على عينة استطلاعية حجمها (٣٦) طالبة من مجتمع الدراسة، ومن خارج العينة الأساسية ، وتم التحقق من صدق الاتساق الداخلي بحساب معاملات الارتباط الخطي بين درجة كل عبارة والدرجة الكلية للأداة، باستخدام برنامج المعالجات الإحصائية SPSS، ووجد أنها تتراوح بين (٠.٥٧٤- ٠.٨٢٣) وكانت جميعها دالة عند مستوى (٠.٠١).

ثبات الأداة

تم التأكد من ثبات الاستبانة، من خلال حساب معامل ألفا كرونباخ لدرجات إجابات العينة الاستطلاعية على أداة الدراسة ، وقد كانت قيم مرتفعة تدل على ثبات مرتفع للأداة، وقد كانت كما هو موضح في جدول (١) الآتي:

جدول(١) معاملات ثبات ألفا كرونباخ

المحور	عدد العبارات	معامل ألفا كرونباخ
درجة الوعي بالأمن السيبراني	١٤	٠.٩٠١
مخاطر وانتهاكات الأمن السيبراني	١٣	٠.٩٢٣
دور تكنولوجيا التعليم في تنمية الوعي بالأمن السيبراني	١٦	٠.٨٨٩
الاستبانة ككل	٤٣	٠.٩٣٥

مجتمع الدراسة وعينتها

تألف مجتمع الدراسة من طلبة كلية التربية الأساسية بفرعيها (بنين/بنات) في الفصل الدراسي الأول من العام الدراسي ٢٠٢٤/٢٠٢٥ البالغ حجمه (٢٣٦٧٤) طالبا وطالبة منهم (٧١٩٣) ذكور و(١٦٤٨١) إناث. وباستخدام معادلة " ستيفن ثامبسون" لحساب حجم العينة التي تمثل هذا المجتمع تمثيلا جيدا، وجد أن ذلك العدد هو (٣٧٨) مفردة، وقد طرحت أداة الدراسة إلكترونيا على مواقع التواصل الاجتماعي، وتم إعلام الطلبة بذلك وطلب منهم الإجابة على بنودها. وعلى مدار أسبوعين تم استجابة (٧٣٤) طالبا وطالبة، ومن ثم فقد تم الاكتفاء بالعدد الذي استجاب لأداة الدراسة بالإجابة على بنودها، وتم تفريغ الإجابات وفرزها، وقد وجد أن هناك (١٤) فردًا لم يكملوا الإجابات، فتم استبعادهم، وعلى ذلك أصبح عدد الإجابات المكتملة (٧٢٠) مفردة، وجميعها كانت صالحة لعملية التحليل الإحصائي، ومن ثم فقد تم اعتماد هذا العدد كعينة للدراسة الحالية. وتوزيع العينة حسب المتغيرات يوضحه جدول (٢) الآتي:

جدول(٢) توزيع العينة حسب متغيرات النوع والتخصص والفرقة الدراسية

المتغير	الفئات	العدد	النسبة المئوية
النوع	ذكر	٣١٤	٤٣.٦١٪
	أنثى	٤٠٦	٥٦.٣٩٪
التخصص الدراسي	تكنولوجيا التعليم	٢٠٩	٢٩.٠٣٪
	تخصصات علمية	٢٥١	٣٤.٨٦٪
	تخصصات أدبية	٢٦٠	٣٦.١١٪
الفرقة الدراسية	الأولى	١٠٣	١٤.٣١٪
	الثانية	١١٧	١٦.٢٥٪
	الثالثة	٢١٥	٢٩.٨٦٪
	الرابعة	٢٨٥	٣٩.٥٨٪
الإجمالي		٧٢٠	١٠٠٪

الأساليب الإحصائية المستخدمة

بعد تفريغ الإجابات، تم إدخال البيانات التي توفرت لدى الباحثتين إلى الحاسب الآلي، واستخدام حزمة البرامج الإحصائية للعلوم الاجتماعية (SPSS)، وتم استخدام أساليب الإحصاء الوصفي (المتوسط الحسابي) وتم استخدام أساليب الإحصاء الاستدلالي (اختبار t-test – اختبار ONE WAY ANOVA – واختبار شيفيه للمقارنات البعدية).

وقد تم استجابة أفراد العينة على أداة الدراسة وفق مدرج ليكرت ثلاثي يقيس درجة الوعي بالأمن السيبراني ومخاطر وتهديدات الفضاء السيبراني، وسبل تنميته ودور تكنولوجيا التعليم في ذلك بدرجة (كبيرة –متوسطة- قليلة) وقد أعطي لهذه الاختيارات تقديرات كمية

(٣، ٢، ١) على الترتيب. وقد تم حساب المدى لهذه الدرجات (المدى = ٣ – ١ = ٢) وتم تقسيمه إلى ثلاث فئات متساوية الطول، طول كل منها (٠.٦٧) تقريبا، وقد تم اعتماد المعيار الآتي لتصيف مستويات المتوسطات الحسابية لبيان درجة الوعي بالأمن السيبراني وتنميته:

- المتوسط الحسابي الوزني (١ – ١.٦٦) هو متوسط حسابي درجته قليلة .
- المتوسط الحسابي الوزني (١.٦٧- ٢.٣٣) هو متوسط حسابي درجته متوسطة
- المتوسط الحسابي الوزني (٢.٣٤- ٣.٠٠) هو متوسط حسابي درجته كبيرة

عرض النتائج ومناقشتها :

إجابة السؤال الأول

للإجابة على السؤال الأول الذي نصه: ما درجة وعى طلبة كلية التربية الأساسية بدولة الكويت بالأمن السيبراني؟ تم حساب المتوسطات الحسابية لدرجات إجابات العينة على عبارات المحور الأول" الوعي بالأمن السيبراني "، وتم رصد نتائج ذلك في جدول (٣)الآتي:

جدول (٣) ترتيب تقديرات الطلبة حول الوعي بالأمن السيبراني حسب المتوسطات الحسابية

العبارات	المتوسط الوزني	الدرجة	الترتيب
أعرف كيفية إعداد كلمات مرور قوية لحماية الصفحات الالكترونية	٢.٦٨	كبيرة	١
أعرف كيفية تغيير كلمة المرور كل فترة	٢.٥٤	كبيرة	٢
أدرك أهمية توفر الأمن السيبراني عند التعامل مع شبكة الانترنت	٢.٥١	كبيرة	٣
أميّز الروابط الإلكترونية مجهولة المصدر	٢.٤٤	كبيرة	٤
أعرف كيف أحافظ على بياناتي الشخصية أثناء تصفحي على الإنترنت	٢.٣٥	كبيرة	٥
لديّ خبرة لتمييز المواقع غير الأخلاقية	٢.٣٤	كبيرة	٦
لدي خبرة بكيفية كشف إصابة الأجهزة الإلكترونية بالفيروسات	٢.٣٣	متوسطة	٧
أعرف كيفية التأكد من أمن المتصفح الذي استخدمه	٢.٢٦	متوسطة	٨
أعي كيف أفحص أي محتوى إلكتروني قبل المشاركة فيه	٢.٢٥	متوسطة	٩
أميّز مرفقات رسائل البريد الإلكتروني مجهولة المصدر	٢.٢٤	متوسطة	١٠
أعي كيفية التأكد من صحة المعلومة بالرجوع إلى مصدرها إلكترونيا	٢.٢٤	متوسطة	١١
أدرك أبعاد الأمن السيبراني	٢.٠١	متوسطة	١٢
لديّ معرفة بقواعد حفظ الملكية الفكرية أثناء استخدام شبكة الإنترنت	١.٦٤	قليلة	١٣
أعرف طرق الإبلاغ عن المواقع المشكوك فيها للجهات المختصة	١.٥٨	قليلة	١٤
المتوسط الحسابي للمحور ككل	٢.٢٤	متوسطة	

تشير النتائج في جدول (٣) إلى أن أفراد العينة يمتلكون وعيا بالأمن السيبراني بدرجة متوسطة، حيث جاءت إجاباتهم بمتوسط حسابي قدره (٢.٢٤) من أصل (٣) درجات، وهو متوسط حسابي درجة متوسطة يقع في الشريحة المتوسطة (١.٦٧- ٢.٣٣) من الشرائح الثلاثة لتصنيف مستويات المتوسط الحسابي المعتمد في الدراسة الحالية .

وتتفق هذه النتيجة مع نتائج دراسة (المنتشري وحريري، ٢٠٢٠) التي كشفت عن أن درجة الوعي بمفاهيم الأمن السيبراني لدى العينة كانت بدرجة متوسطة بشكل عام. ودراسة (الشهري، ٢٠٢١) التي كشفت عن معرفة بالأمن السيبراني بدرجة متوسطة لدى طلبة كلية التربية بجامعة الإمام محمد بن سعود الإسلامية، ودراسة (الضفيري، وآخرون، ٢٠٢٤) التي كشفت عن أن مستوى الوعي بالأمن السيبراني لدى أفراد العينة هو بدرجة متوسطة. في حين تختلف مع نتائج دراسات (الصانع، ٢٠٢٠؛ البيشي، ٢٠٢١؛ الظويفري، ٢٠٢١؛ العتيبي، ٢٠٢٢؛ عرايضه، ٢٠٢٢؛ الحبيب، ٢٠٢٢) التي كشفت عن أن مستوى الوعي بماهية الأمن السيبراني لدى الأفراد كان بدرجة مرتفعة. وكذلك تختلف مع نتائج دراسة (الصحفي وعسكول ، ٢٠١٩) التي بينت ضعف مستوى الوعي بمفاهيم الأمن السيبراني لدى العينة.

ويمكن عزو هذه النتائج إلى ضعف خبرة الطلبة ومحدودية درايتهم بأهمية مفهوم الأمن السيبراني، لعدم تلقى الطلبة خبرات مباشرة حول مفاهيم الوعي بالأمن السيبراني، وقد يكون ذلك لعدم وجود خطة محكمة لنشر الوعي بالأمن السيبراني داخل الكلية وخارجها، وندرة الدورات التدريبية التي تختص بتعزيز هذا المفهوم، كمصطلح تقني جديد، ولعل السبب في ذلك قد يرجع إلى وجود عدد من المشكلات نتيجة ندرة المتخصصين في هذا المجال ، وعدم وجود منظومة أمن معلومات في الكلية تقدم التوعية والحماية بالأمن السيبراني، وعدم القيام بفعاليات من أجل توعية للطلبة بالكلية بجوانب ومضامين الأمن السيبراني، مع عدم الاهتمام الكافي بتثقيف الطلبة بوسائل حماية بياناتهم ومعلوماتهم على أجهزتهم الخاصة، وتوجيههم لكيفية التصفح الآمن للإنترنت، وكيفية التحقق من مصدر المعلومة المتداولة قبل مشاركتها مع الآخرين، مع عدم كفاية التوعية بحقوق الملكية الفكرية، والتأكيد على أهمية احترامها، وإمكانية لجوئهم إلى الجهات التي يمكن الرجوع إليها عند التعرض لأي من الجرائم الإلكترونية، فضلا عن ضعف استخدام برامج الحماية والجدار الناري وتحديثها بشكل مستمر، وضعف التدريب عليها. وعدم توافر فرص لإجراء ممارسات تختص بالوعي بالأمن السيبراني تحت إشراف مشرفين متخصصين بالكلية، وضعف متطلبات تحقيق الوعي بأهمية الأمن السيبراني في البيئة التعليمية، ووجود قصور في القناعة بأن الأمن السيبراني ومفاهيمه أصبح ضرورة لدى الطلبة والبيئة التعليمية ككل، بالإضافة إلى عدم توافر أدلة تطبيقية لأجل تطبيق الأمن السيبراني في المجال التعليمي. وأن ما يتم من سبل تنمية الوعي الأمن السيبراني يتم بجهود فردية من خلال دراسة بعض المقررات الدراسية.

وهذا في مجملة يكشف عن حاجة الطلبة للتوعية والتثقيف بالموضوعات ذات العلاقة بالأمن السيبراني، وتطوير معارفهم ومهاراتهم في هذا المجال، وكيفية استخدامها أثناء ممارساتهم التعليمية .

إجابة السؤال الثاني

للإجابة على السؤال الثاني الذي نصه: ما المخاطر والانتهاكات السيبرانية التي يتعرض لها الطلبة أثناء التعامل مع الفضاء السيبراني؟ تم حساب المتوسطات الحسابية لدرجات إجابات العينة على عبارات المحور الثاني المتعلق بذلك، وكانت النتائج كما هو مدون في الجدول(٤).

جدول (٤) ترتيب مخاطر وانتهاكات الفضاء السيبراني التي يتعرض لها الطلبة

العبارات	المتوسط الوزني	الدرجة	الترتيب
التنمر الإلكتروني بقصد إلحاق الأذى بالآخرين	٢.٩١	كبيرة	١
نشر العروض والمواد الإباحية	٢.٨٨	كبيرة	٢
التجسس الإلكتروني لنقل أخبار المستخدم وبياناته إلى جهة أخرى مهاجمة	٢.٨٦	كبيرة	٣
التشهير الإلكتروني بنشر أخبار مسيئة على شبكة الانترنت	٢.٨٥	كبيرة	٤
التصيد الإلكتروني للحصول على معلومات مهمة عن الشخص للاستغلال ضده	٢.٧٢	كبيرة	٥
انتحال الشخصيات وسرقة بيانات الشخص والتأثير عليه	٢.٧١	كبيرة	٦
اختراق الحسابات الشخصية للأفراد وتخريب محتوياتها	٢.٦٥	كبيرة	٧
إنشاء مواقع إلكترونية وهمية لتزييف الحقائق حول الأفراد والدول	٢.٦٣	كبيرة	٨
الابتزاز المالي من خلال التهديد بنشر شائعات عن الضحية	٢.٦٢	كبيرة	٩
الابتزاز الجنسي من خلال التهديد بنشر مقاطع أو صور تخص الضحية	٢.٤٩	كبيرة	١٠
بث الأفكار الهدامة والمتطرفة	٢.٤٦	كبيرة	١١
التغرير والاستدراج للصغار من مستخدمي الإنترنت للسيطرة عليهم وتوجيههم لأفعال سيئة	٢.٢٣	متوسطة	١٢
تجارة المخدرات عن طريق الإنترنت	١.٥٤	قليلة	١٣
المتوسط الحسابي للمحور ككل	٢.٥٨	كبيرة	

تشير النتائج في جدول (٤) إلى أن أفراد العينة يمتلكون وعيا بمخاطر وانتهاكات الفضاء السيبراني بدرجة كبيرة، حيث جاءت إجاباتهم على المحور الثاني المتعلق برصد المخاطر التي يعرض لها الطلبة بمتوسط حسابي قدره (٢.٥٨) من أصل (٣) درجات، وهو متوسط حسابي درجة كبيرة يقع في الشريحة العليا(٢.٣٤-٣.٠٠) من شرائح تصنيف مستويات المتوسط الحسابي.

وتتفق هذه النتيجة مع نتيجة دراسة (العتيبي، ٢٠٢٢) التي كشفت عن أن أفراد العينة يتعرضن للعديد من أشكال الجرائم التي يتعامل معها الأمن السيبراني بدرجة مرتفعة. ودراسة (المنتشري وحريري، ٢٠٢٠) التي كشفت عن تقدير أفراد العينة لإمكانية تعرضهم لقدر كبير من انتهاكات الأمن السيبراني. ومع نتيجة دراسة (Spiering ٢٠١٣ التي أشارت إلى وجود العديد من المشكلات والانتهاكات السيبرانية والتهديدات المختلفة التي يتعرض لها الأفراد نتيجة نقص الوعي بالأمن السيبراني، ودراسة (Safaria, 2018) التي وضحت ظهور العديد من المخاطر السيبرانية لدى الطلبة، مما يتطلب الحماية من تلك المخاطر والتوعية اللازمة.

ويمكن عزو هذه النتيجة إلى أن درجة الوعي لدى الطلبة بمحددات الأمن السيبراني ليست على المستوى الذي يضمن لهم الأمن والسلامة عند التعامل مع شبكة الانترنت، خاصة فيما يتعلق بإجراءات إعداد كلمات مرور قوية لا يمكن اختراقها، وتشفير الملفات، وعدم وجود تدريب للطلبة على تفادي المخاطر التي تهدد الأمن السيبراني، وعدم استخدام برامج الحماية، وتبادل الملفات مع الزملاء عبر أجهزة الحواسيب وعبر الهواتف الذكية، وعدم فحصها جيدا قبل استخدامها للتصفح الآمن، فضلا عدم وجود منظومة متكاملة تختص بالوعي بالأمن السيبراني، وتوفير البرمجيات والبرامج والتطبيقات الجيدة المحصنة ضد الاختراق التي يستطيع الطلبة التعامل معها باحترافية، وعدم وضع برامج لتوعية الطلبة حول مخاطر وتهديدات الأمن السيبراني. وهذا أكدته دراسة(المنتشري وحريري، ٢٠٢٠). ولا شك في أن إهمال تلك الإجراءات يؤدي إلى وقوع الطلبة ضحايا للمخاطر والانتهاكات السيبرانية. وأن عدم التوعية بالانتهاكات السيبرانية قد يكون له أثر سلبي على أمن الأفراد والمؤسسات . وعلى ضوء ذلك تبرز أهمية سن تشريعات لمكافحة المخاطر الانتهاكات السيبرانية، وضرورة توعية الطلبة بها، حتى يتسنى لهم استخدامها في الوقت المناسب.

إجابة السؤال الثالث

للإجابة على السؤال الثالث الذي نصه: ما إسهامات دراسة مقررات تكنولوجيا التعليم في تنمية الوعي بالأمن السيبراني لدى طلبة كلية التربية الأساسية؟ تم حساب المتوسطات الحسابية لدرجات إجابات العينة على عبارات المحور الثالث، وتم رصد نتائج ذلك في جدول (٥)الآتي:

جدول(٥) ترتيب العبارات حول دور تكنولوجيا التعليم في تنمية الوعي بالأمن السيبراني

العبارات	المتوسط الوزني	الدرجة	الترتيب
تدريب الطلبة على تحديث برنامج الحماية الموجودة على الحاسب بشكل دوري	٢.٣٤	متوسطة	١
إكساب الطلبة مهارة الاحتفاظ بالملفات في أكثر من مكان لتفادي السرقة أو التلف	٢.٣٣	متوسطة	٢
تدريب الطلبة على كيفية إعداد كلمة سر قوية، وتحديثها باستمرار	٢.٣٢	متوسطة	٣
إكساب الطلبة مهارة توظيف الألعاب التعليمية الإلكترونية الهادفة في فهم الدروس	٢.٣٠	متوسطة	٤
تأكيد أهمية الاحتفاظ بسجل الأعمال الالكتروني portfolio لتوثيق الأعمال	٢.٢٩	متوسطة	٥
تعريف الطلبة بكيفية تجميع معلومات من الإنترنت بطريقة منظمة	٢.٢٨	متوسطة	٦
توجيه الطلبة لتوظيف الوسائط المتعددة لعرض المحتوى التعليمي عبر الأجهزة الإلكترونية	٢.٢٧	متوسطة	٧
إكساب الطلبة مهارة تصميم مقاطع فيديو أو كتابة منشورات أو التغريدات	٢.٢٥	متوسطة	٨
التأكيد على استخدام برامج للحماية من ملفات التجسس	٢.٢٤	متوسطة	٩
تدريب الطلبة لاستخدام برمجيات حماية الأجهزة الإلكترونية من الاختراق	٢.٢٣	متوسطة	١٠
إكساب الطلبة مهارة استخدام تقنيات التواصل الاجتماعي بغرض تحسين التفاعل التعليمي	٢.٢٢	متوسطة	١١

العبارات	المتوسط الوزني	الدرجة	الترتيب
توجيه الطلبة لاستخدام برامج المحاكاة الحاسوبية لتعزيز تعلم محتوى المنهج	٢.٢٢	متوسطة	١٢
إكساب الطلبة مهارة نسخ الملفات احتياطيا في ذاكرة خارجية	٢.٢١	متوسطة	١٣
إكساب الطلبة مهارة وضع نظام يمنع الوصول إلى الحساب الشخصي	٢.٠١	متوسطة	١٤
إكساب الطلبة مهارة وضع إجراءات وسياسات لحفظ الأمن السيبراني	١.٩٧	متوسطة	١٥
إكساب الطلبة مهارة التشفير للملفات المهمة التي يمكن إرسالها من خلال شبكة الإنترنت	١.٨٥	متوسطة	١٦
المتوسط الحسابي للمحور ككل	٢.٢١	متوسطة	

تشير النتائج في جدول (٥) إلى أن أفراد العينة يرون أن مقررات تكنولوجيا التعليم يمكن أن تسهم بدرجة متوسطة في تنمية الوعي بالأمن السيبراني، حيث جاءت إجاباتهم بمتوسط حسابي قدره (٢.٢١) من أصل (٣) درجات، وهو متوسط حسابي درجة متوسطة يقع في الشريحة الوسطى من شرائح تصنيف مستويات المتوسط الحسابي المعتمد في الدراسة الحالية.

وجاءت هذه النتيجة متفقة مع نتائج دراسات (الضفيري، وآخرون، ٢٠٢٤؛ الصرايرة ،٢٠٢٣، الشيبي ٢٠٢٢) التي أشارت إلى أن درجة الاستفادة من توظيف التكنولوجيا في تنمية الوعي بالأمن السيبراني ومخاطره، وكيفية مواجهة هذه التهديدات والمخاطر، كانت درجة متوسطة.

ويمكن عزو ذلك إلى ضعف خبرة الطلبة في الكلية بصفة عامة بجدوى توظيف تكنولوجيا التعليم في تنمية الأمن السيبراني، نظرا لأن غالبية الأقسام العلمية بالكلية لا يدرسن مقررات تتصل بتكنولوجيا التعليم، ودورها في تصميم بيئات التعلم، وعدم وجود نماذج واضحة لهذا التوظيف، وضعف ثقة بعض الطلبة في قدرتهم على توظيف تطبيقات تكنولوجيا التعليم، ومدى انعكاس ذلك على امتلاك الطلبة للعديد من المهارات اللازمة للتعامل مع الفضاء السيبراني.

وفي هذا الصدد نشير إلى ضرورة دراسة مقرر عام في تكنولوجيا التعليم لطلبة الكلية يمثل مدخل عام لطلبة الكلية نحو توظيف المستحدثات التكنولوجية في العملية التعليمية، ويوضح لهم كيفية التعامل مع الفضاء السيبراني، إذ أصبح أمرا واقعا اليوم في ضوء التحول نحو التعلم الرقمي والتعليم عن بعد. على أن يهدف هذا المقرر إلى توجيه الطلبة لمعرفة المواقع الإلكترونية التي تعمق القيم الدينية والأخلاقية المتعلقة بالتصرف الأخلاقي في الفضاء السيبراني، وتوعية الطلبة بالممارسات السلبية البعيدة عن منظومة القيم أثناء استخدام شبكة الانترنت، وتنمية قيم التعبير عن الرأي وتقبل الرأي الأخر واحترام وجهات النظر المختلفة وتثقيف الطلبة بوسائل حماية بياناتهم معلوماتهم على أجهزتهم الخاصة، وكيفية استعمال برامج الحماية والجدار الناري وتحديثها بشكل مستمر، وتوعية الطلبة بمشكلات استخدام الإنترنت ، وتعريفهم بسبل التصفح الآمن للإنترنت لفترات طويلة، وبكيفية التحقق من مصدر المعلومة المتداولة في مواقع التواصل الاجتماعي قبل إرسالها للآخرين، وتعريف الطلبة بالجهات التي يرجعون إليها عند التعرض لأي من الجرائم الإلكترونية، وكيفية احترام الطلبة لحقوق الملكية الفكرية للآخرين.

إجابة السؤال الرابع

للإجابة على السؤال الرابع؛ الذي نصه: هل توجد فروق ذات دلالة إحصائية بين متوسطات أفراد عينة الدراسة حول تقدير مستوى الوعي بالأمن السيبراني ومخاطر وانتهاكات الأمن السيبراني ودور تكنولوجيا التعليم في تنميته تعزى لمتغيرات (النوع- التخصص- الفرقة الدراسية)؟ تم استخدام أساليب الإحصاء الاستدلالي، لبحث مدى وجود هذه الفروق، وكانت على النحو الآتي:

(١)الفروق تبعا لمتغير النوع

تم استخدام اختبار (t-test)، بعدما تم التأكد توفر شروط استخدام هذا الاختبار فيما يتصل بتجانس العينة، ومناسبة حجمها، والجدول (٦) الآتي يبين نتائج ذلك:

جدول (٦) نتائج اختبار (t-test) للفروق بين متوسطات تقديرات العينة تبعا النوع (ذكر/أنثى)

المحور	النوع	العدد	المتوسط الحسابي	الانحراف المعياري	ت	درجة الحرية	الدلالة الإحصائية	ملاحظات
الوعي بالأمن السيبراني	ذكر	٣١٤	٣١.٣٥	٤.٠٣	١.٥٣٣	٧١٨	٠.١٢٦	غير دالة
	أنثى	٤٠٦	٣١.٨٢	٤.١٢				
الوعي بالمخاطر والتهديدات السيبرانية	ذكر	٣١٤	٣٣.٦١	٤.٣٤	٠.٢٧٨	٧١٨	٠.٧٨١	غير دالة
	أنثى	٤٠٦	٣٣.٥٢	٤.٢٨				
دور تكنولوجيا التعليم في تنمية الوعي بالأمن السيبراني	ذكر	٣١٤	٣٥.٢١	٤.٦٥	٠.٠٠٢	٧١٨	٠.٩٩٨	غير دالة
	أنثى	٤٠٦	٣٥.٦٢	٤.٧٤				

يتضح من الجدول(٦) أنه لا توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات العينة حول الوعي بالأمن السيبراني في جميع المحاور تبعا لمتغير النوع، وذلك استنادا إلى قيم (ت) حيث كانت غير دالة عند مستوى (٠.٠٥). ويستدل من ذلك على أن أفراد العينة من الجنسين لديهم نفس المستويات من الوعي بالأمن السيبراني وبمخاطره التهديدات السيبرانية وكذلك حول سبل تنميته في كلية التربية الأساسية بدولة الكويت.

وتتفق هذه النتيجة مع نتائج دراسات (العتيبي، ٢٠٢٢؛ عرايضة، ٢٠٢٢؛ العقلا وعلي، ٢٠٢٢؛ الضفيري وآخرون، ٢٠٢٤) التي كشفت عن عدم وجود فروق ذات دلالة إحصائية بين آراء أفراد العينة نحو الوعي بالأمن السيبراني والمخاطر والتهديدات وأشكال الجرائم التي تنتج عن عدم وجود الأمن السيبراني تعزى لمتغير "النوع. في حين تختلف مع نتائج دراسة (الثوابية والفراهيد، ٢٠٢١) التي كشفت عن وجود فروق ذات دلالة إحصائية في درجة تأثير الفضاء السيبراني على العلاقات الاجتماعية تعزى لمتغير الجنس لصالح الإناث، ومع نتائج دراسة (الحباشنة، ٢٠٢٣) التي كشفت عن وجود فروق دالة إحصائيا في درجة الوعي بالأمن السيبراني تعزى لمتغير النوع لصالح الذكور.

ويمكن تفسير هذه النتائج بتجانس الخبرات والفرص التي تعرض لها الطلبة على اختلاف نوعهم، فيما يتعلق بالوعي بالأمن السيبراني، وأن جميع الطلبة لهم اهتمامات متشابهة بموضوع الأمن السيبراني والفضاء الإلكتروني، وأن مدى امتلاكهم المهارات التي تساعدهم على حماية معلوماتهم وبياناتهم في هذا الفضاء، ويرجع تساوي الفرص المتاحة لاكتساب الجوانب المعرفية والأدائية الخاصة بالوعي بالأمن السيبراني، إلى أن العوامل المؤثرة في تزويد الطلبة من الجنسين بالجوانب المعرفية والمهارية في مجال الأمن السيبراني ومخاطره ودور تكنولوجيا التعليم في إكساب الطلبة مهارات التعامل مع هذه، هي عوامل متشابهة إلى حد كبير لدى الجنسين، إذ إن الجنسين يتعرضان لنفس برامج الإعداد في الكلية. وأن كلا منهما يعاني من افتقار المقررات بالمعارف العلمية المتعلقة بالوعي السيبراني، وعدم وجود خطة عامة لتنمية هذا الوعي لدى طلبة الكلية في الأقسام العلمية المختلفة.

(٢) الفروق تبعا للتخصص

تم استخدام تحليل التباين الأحادي لمناسبته لتعرف أثر متغير التخصص كمتغير مستقل على متغير وهو الوعي بمفاهيم الأمن السيبراني ومخاطره وسبل تنميته، وأن العينة بشرائحها المختلفة هي مجموعات مستقلة وقد تم اختيارها بطريقة عشوائية من مجتمع الدراسة.. وتم رصد نتائج ذلك في جدول (٧) الآتي:

جدول(٧) نتائج اختبار (ONE WAY ANOVA) للفروق بين متوسطات تقديرات العينة تبعا لمتغير التخصص (تكنولوجيا التعليم/ علمي/ أدبي)

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	ف	ملاحظات
الوعي بالأمن السيبراني	بين المجموعات	٥٢.١٥٦	٢	٢٦.٠٧٨	٦.٣٢٢	دالة
	داخل المجموعات	٢٩٥٧.٦٢٥	٧١٧	٤.١٢٥		
	المجموع	٣٠٠٩.٧٨١	٧١٩			
الوعي بالمخاطر والتهديدات السيبرانية	بين المجموعات	١٠.٨٣٦	٢	٥.٤١٨	١.٤٩٥	غير دالة
	داخل المجموعات	٢٥٩٨.٤٠٨	٧١٧	٣.٦٢٤		
	المجموع	٢٦٠٩.٢٤٤	٧١٩			
دور تكنولوجيا التعليم في تنمية الوعي بالأمن السيبراني	بين المجموعات	١٠٤.٥١٨	٢	٥٢.٢٥٩	٨.١٢١	دالة
	داخل المجموعات	٤٦١٣.٨٩٥	٧١٧	٦.٤٣٥		
	المجموع	٤٧١٨.٤١٣	٧١٩			

تشير نتائج تحليل التباين الأحادي في جدول(٧) أنه لا توجد فروق دالة إحصائية بين متوسطات درجات العينة حول تقديراتهم لمخاطر وتهديدات الأمن السيبراني تبعا لمتغير التخصص الدراسي، حيث كانت قيم (ف) غير دالة عند مستوى (٠.٠٥). في هذا المحور. ويستدل من ذلك على اتفاق العينة من طلبة الأقسام العلمية المختلفة حول تعرضهم للمخاطر والانتهاكات والتهديدات السيبرانية.

في حين تكشف النتائج في جدول (٧) عن وجود فروق دالة إحصائيا بين تقديرات العينة حول الوعي بالأمن السيبراني ودور تكنولوجيا التعليم في تنميته تبعا لمتغير التخصص الدراسي، حيث كانت قيم (ف) في هذين المحورين دالة عند مستوى (٠.٠٥). ولتعرف مصادر هذه الفروق، فقد تم استخدام اختبار شيفيه لمقارنة المتوسطات الحسابية لتقديرات العينة في هذه المحاور لمناسبته لذلك، وتم رصد نتائج ذلك في جدول (٨) الآتي:

جدول(٨) نتائج اختبار شيفيه للمقارنات البعدية للمتوسطات حسب متغير التخصص

المحور	التخصص	المتوسط الحسابي	علمي	أدبي
الوعي بالأمن السيبراني	تكنولوجيا تعليم	٣٤.٧٨	❖٤.٥٦	❖٤.٢٧
	علمي	٣٠.٢٢		
	أدبي	٣٠.٥١		
دور تكنولوجيا التعليم في تنمية الوعي بالأمن السيبراني	تكنولوجيا تعليم	٣٩.٣٥	❖٦.٥٣	❖٦.٣٠
	علمي	٣٢.٨٢		
	أدبي	٣٣.٠٥		

❖ دالة عند مستوى (٠.٠٥)

توضح نتائج اختبار شيفيه الواردة في جدول (٨) إلى أن الفروق كانت لصالح مجموعة الطلبة في تخصص تكنولوجيا التعليم مقابل مجموعات الطلبة في التخصصات الأخرى(علمي/ أدبي). ويستدل من ذلك على أن طلبة تخصص تكنولوجيا التعليم لديهم مستوى أعلى من الوعي بالأمن السيبراني والمفاهيم المتصلة به، وبسبل تعزيزه لدى الطلبة في الكلية من خلال إسهام دراسة مقررات تكنولوجيا التعليم في تنمية هذا الوعي.

وتتفق هذه النتيجة مع نتائج دراسات (الشيبي، ٢٠٢٢؛ الضفيري وآخرون، ٢٠٢٤) التي تشير إلى وجود فرق دال إحصائيا فيما يتعلق بالوعي بالأمن السيبراني، وفقا لمتغير "التخصص".

ويمكن عزو هذه النتيجة إلى أن الطلبة تخصص تكنولوجيا التعليم يتيح للطلبة فرصا أكبر لتكوين خلفية ثقافية ووعيا حول أهمية دراسة الفضاء السيبراني وما يتعلق به من مستوى بالوعي الأمني وكيفية تنميته وتعزيزه، لضرورته في عالم اليوم، وأن دراسة المقررات في هذا التخصص يتيح للطالب فرصا أكبر لمعرفة كيفية التعامل مع التقنيات الحديثة والوعي بكيفية توظيفها وكيفية مواجهة التهديدات السيبرانية المرتبطة مما يوفر فرصا أكبر للمعلمين لتوظيف التكنولوجيا في التدريس. وعلى ضوء ذلك نرى أن هذا أمرا منطقيا أن يكون لدى الطلبة الدارسين في قسم تكنولوجيا التعليم وعيا واتجاهات إيجابية نحو الأمن السيبراني، وأنهم يقدرون بشكل أكثر واقعية السبل التي تتم في الواقع لتنمية الوعي بالأمن السيبراني،

وكيف أن دراسة مقررات تكنولوجيا تسهم بدرجة كبيرة في تنمية هذا الوعي؛ على خلاف الطلبة في الأقسام العلمية الأخرى الذي لا يتعرضون لدراسة مثل هذه المقررات.

(٣) الفروق تبعا لمتغير الفرقة الدراسية

تم استخدام تحليل التباين الأحادي لتوافر شروط استخدام هذا الاختبار، وتم رصد نتائج ذلك في جدول (٩) الآتي:

جدول(٩) نتائج اختبار (ONE WAY ANOVA) للفروق بين متوسطات تقديرات العينة تبعا لمتغير الفرقة الدراسية (الأولى - الثانية - الثالثة- الرابعة)

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	ف	ملاحظات
الوعي بالأمن السيبراني	بين المجموعات	٧٢.٣٦٣	٣	٢٤.١٢١	٤.٥٢٩	دالة
	داخل المجموعات	٣٨١٣.٤١٦	٧١٦	٥.٣٢٦		
	المجموع	٣٨٨٥.٧٧٩	٧١٩			
الوعي بالمخاطر والتهديدات السيبرانية	بين المجموعات	١٠.٠٦٨	٣	٣.٣٥٦	١.٠١٨	غير دالة
	داخل المجموعات	٢٣٦٠.٦٥٢	٧١٦	٣.٢٩٧		
	المجموع	٢٣٧٠.٧٢٠	٧١٩			
دور تكنولوجيا التعليم في تنمية الوعي بالأمن السيبراني	بين المجموعات	١٩٠.٢٧٥	٣	٦٣.٤٢٥	٧.١٢٤	دالة
	داخل المجموعات	٦٣٧٤.٥٤٨	٧١٦	٨.٩٠٣		
	المجموع	٦٥٦٤.٨٢٣	٧١٩			

تشير نتائج تحليل التباين الأحادي في جدول(٩) أنه لا توجد فروق دالة إحصائية بين متوسطات درجات العينة حول تقديراتهم الوعي بالمخاطر والتهديدات السيبرانية تبعا لمتغير الفرقة الدراسية، حيث كانت قيم (ف) غير دالة عند مستوى (٠.٠٥). في هذا المحور. في حين تكشف النتائج عن وجود فروق دالة إحصائيا بين تقديرات العينة حول الوعي بالأمن السيبراني وسبل وتعزيزه من خلال دور تكنولوجيا التعليم في ذلك تبعا لمتغير الفرقة الدراسية، حيث كانت قيم (ف) في هذين المحورين دالة عند مستوى (٠.٠٥). ولتعرف مصادر هذه الفروق، فقد تم استخدام اختبار شيفيه لمقارنة المتوسطات الحسابية لتقديرات العينة في هذين المحورين، وتم رصد نتائج ذلك في جدول (١٠) الآتي:

جدول(١٠) نتائج اختبار شيفيه للمقارنات البعدية للمتوسطات حسب متغير الفرقة الدراسية

المحور	الفرقة	المتوسط الحسابي	الأولى	الثانية
الوعي بالأمن السيبراني	الأولى	٢٧.٤٢		
	الثانية	٢٧.٦٣		
	الثالثة	٣٤.٩٨	٧.٥٦*	٧.٣٥*
	الرابعة	٣٥.١٥	٧.٧٣*	٧.٥٢*
دور تكنولوجيا التعليم في تنمية الوعي بالأمن السيبراني	الأولى	٣٠.٥٣		
	الثانية	٣٠.٢٦		
	الثالثة	٣٩.٩٥	٩.٤٢*	٩.٦٩*
	الرابعة	٤٠.٨٤	١٠.٣١*	٩.٥٨*

* دالة عند مستوى (٠.٠٥)

تشير نتائج اختبار شيفيه في جدول (١٠) إلى أن الفروق كانت لصالح مجموعة الطلبة في الفرقتين الثالثة والرابعة مقابل مجموعات الطلبة في الفرقتين الدراسيتين الأولى والثانية. ويستدل من ذلك على أن طلبة الفرقتين الثالثة والرابعة يمتلكون وعيا بمستوى أعلى بالأمن السيبراني ولديهم تقديرات أكبر ومعرفة بسبل تنمية هذا الوعي في الكلية، وأنهم يقدرون دورا أكبر لإسهام دراسة مقررات في تكنولوجيا التعليم في تنمية هذا الوعي، عما يراه الطلبة في الفرقتين الأولى والثانية.

وتتفق هذه النتائج مع نتائج دراسة (عرايضة، ٢٠٢٢) التي كشفت عن وجود فروق ذات دلالة إحصائية بين متوسطات تقديرات أفراد عينة الدراسة حول الوعي بالأمن السيبراني لصالح تقديرات الطلبة في الصفوف العليا. في حين تختلف مع نتائج دراسات (الصحفي وعسكول،

٢٠١٩؛ المنتشري، ٢٠٢٠؛ العتيبي، ٢٠٢٢؛ العقلا وعلي، ٢٠٢٢؛ الضفيري وآخرون، ٢٠٢٤). التي كشفت عن عدم وجود فروق في مستوى الوعي بالأمن السيبراني استخدام التقنيات الحديثة في تنمية هذا الوعي تبعا لمتغير المستوى التعليمي.

ويمكن عزو ذلك الاختلاف إلى تباين الخبرات والفرص التي يتعرض لها الطلبة على اختلاف عدد سنوات الدراسة فيما يتعلق بالوعي بالأمن السيبراني، حيث إن الطلبة في الفرقة الأولى يدرسون مقررات عامة، تعد مداخل لدراسة التخصصات ككل، وكذلك في الفرقة الثانية يبدأ الطالب في دراسة مقررات تقترب من التخصص الدراسي للطالب، وهذه المقررات لا توفر لديهم فرص جيدة تتعلق بتكوين خلفية ثقافية ووعيا جيدا حول الأمن السيبراني وتهديداته، بينما الطلبة في الفرقتين الثالثة والرابعة وخاصة في تخصص تكنولوجيا التعليم والحاسوب يدرسون خطط دراسية منظمة وبرامج تقوم على مجموعة مقررات متخصصة بشكل دقيق، تعمل على إعداد خريج في هذه التخصصات للعمل في ميدان تكنولوجيا التعليم، ومن ثم يكون لديهم فرصا أكبر لاكتساب الجوانب المعرفية والأدائية الخاصة بالوعي بالأمن السيبراني، وما يتعلق بالفضاء السيبراني، وأهم المخاطر والتهديدات التي تواجه الطلبة في التعامل مع هذا الفضاء، كما أن دراسة المواد المتخصصة في تكنولوجيا التعليم بشكل خاص تساعد الطلبة على امتلاك المهارات والكفايات التي تعزز من قدرات الطلبة على توظيف المستحدثات التكنولوجية في التعليم، بخلاف الطلبة في الفرق الأقل الذين قد لا يكون قد تكون لديهم وعي بتلك المستحدثات، أو لديهم قصور في كفايات توظيفها .

توصيات الدراسة

على ضوء نتائج الدراسة نوصي بالآتي:

- ضرورة توفير برامج تعليمية لتنمية مفهوم الأمن السيبراني لدى الطلبة في مؤسسات التعليم العالي.
- ينبغي إدراج مجال الفضاء السيبراني ضمن مناهج التعليم في الكليات الجامعية بشكل إلزامي.
- إدراج مقررات دراسية خاصة بمفاهيم الأمن السيبراني ضمن برامج الإعداد الأكاديمي بالكلية.
- إعداد برامج تربوية دورات تدريبية للطلبة تتناول الوعي بمفاهيم ومخاطر وانتهاكات الأمن السيبراني.
- إدراج أنشطة تعليمية ملزمة للطلبة تستلزم استخدام التكنولوجيا في التدريس وتوظيف المعارف والمهارات المرتبطة بالوعي بالأمن السيبراني
- ضرورة تدشين حملات إعلامية واسعة لتعريف طلاب وأعضاء هيئة التدريس بالفضاء السيبراني ومخاطره وتوعيتهم بأساليب الحماية والبرامج التي ينبغي استخدامها
- تدريب أعضاء هيئة التدريس حول كيفية تفعيل دورهم في إكساب الطلبة مهارات التعامل مع الفضاء السيبراني، وحماية البيانات من المخاطر والتهديدات السيبرانية.

المقترحات

وتقترح الباحثتان:

- إجراء دراسة تتناول واقع مداخل وإستراتيجيات تنمية الوعي بالأمن السيبراني لدى الطلبة
- إجراء تحليل محتوى لمقررات تكنولوجيا التعليم التي تدرس للشعب العامة (علمي وأدبي) والتعرف على مدى تناولها لمفاهيم الأمن السيبراني .
- إجراء دراسة تتناول مدى جاهزية كلية التربية الأساسية بدولة الكويت لمواجهة التهديدات السيبرانية
- إجراء بحث حول برنامج مقترح لتنمية الوعي بالأمن السيبراني وبحث مدى فاعليته في ذلك .
- إجراء بحث يتعلق بوضع تصور يتضمن مجموعة من الآليات التي يمكن من خلالها تنمية الوعي بالأمن السيبراني لدى الطلبة.

المراجع

إبراهيم، منال حسن محمد. (٢٠٢١). الوعي بجوانب الأمن السيبراني في التعليم عن بعد المجلة العلمية لجامعة الملك فيصل. *مجلة العلوم الإنسانية والإدارية*، ٢٢ (٢)، ٢٩٩ –٣٠٧.

البجاوي، صباح عبد الصمد والمسعودي، محمد حميد مهدي. (٢٠٢٠). تكنولوجيا التعليم المعاصر أفكار وتطبيقات . دار الصفاء للنشر والتوزيع .

البيشي، منير عبد الله. (٢٠٢١). الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس دراسة على جامعة بيشة. *مجلة الجامعة الاسلامية للدراسات التربوية والنفسية*، ٢٩ (٦)، ٢٧٢- ٣٥٣.

الثوابية، احمد محمود والفراهيد، أمل عبد الحميد موسى. (٢٠٢١). الفضاء السيبراني وعلاقته بالأداء الأكاديمي والعلاقات الاجتماعية والعاطفية لدى طلبة جامعة الطفيلة التقنية. *مجلة الدراسات والبحوث التربوية*، ١١ (٣)، ٣٧٤- ٤٠٤.

الجندي، علياء عبد الله إبراهيم. (٢٠١٩). دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة. *عالم التربية*، (٦٧)، ج٣، ١٤- ٨٤.

الحباشنة، عبير احمد عبد الرحمن.(٢٠٢٣). درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية "والتعليم قصبة الكرك. *مجلة الزرقا للبحوث والدراسات الإنسانية*، ٢٣ (٣)، ٦٦٢- ٦٧٩.

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

خليفة، إيهاب. (٢٠١٧). *القوى الإلكترونية كيف يُمكن أن تدير الدول شؤونها في عصر الانترنت*. العربي للنشر والتوزيع.

خورشيد، عصمت مصباح. (٢٠٢٠). تطبيقات أدب الطفل في تعليم الإتيكيت الرقمي لمرحلة الطفولة المبكرة (دراسة وصفية تحليلية). *المؤتمر الدولي (الافتراضي) لمستقبل التعليم الرقمي في الوطن العربي*، ٣٠ أكتوبر – ٢ نوفمبر، ٣٢٧ – ٣٤١.

الدمرداش، تانمي صابر. (٢٠٢٢). أثر تفاعل العناصر الافتراضية المدعومة بالذكاء الاصطناعي وأدوات إدارة المعرفة في تنمية مهارات الأمن السيبراني وحل المشكلات لدى طلاب الحاسبات والذكاء الاصطناعي. *مجلة البحوث في مجالات التربية النوعية*،(٤١)، ١٣٣١- ١٤٢٧.

السعادات، خليل، والتميمي، ندى. (٢٠٢٢). رفع الوعي بالأمن السيبراني لدى المعلمين في ضوء مبادئ تعليم الكبار. *آفاق جديدة في تعليم الكبار* ، (٣٢)، ٢٥٥-٢٨٠.

السعيد، أميرة رضا مسعد. (٢٠٢٠). برنامج مقترح قائم على التعلم المدمج لتنمية مهارات الاستخدام الأمن للانترنت والوعي بأخلاقيات التكنولوجيا المعاصرة لدى تلاميذ الحلقة الإعدادية. *المجلة العربية للتربية النوعية*، ٤(١٥)، ٣٩- ٧٦.

الشمري، فيصل بن فهد بن محمد.(٢٠٢٣). أثر تدريس مقرر الأمن السيبراني على تنمية الوعي المعلوماتي والمهاري للأمن السيبراني لدى طلاب دبلوم الحاسب في كلية التربية بجامعة حائل. *مجلة العلوم التربوية*، (١)، ج ٤، ٢٠٧- ٢٣٢.

الشهري، مريم محمد فضل. (٢٠٢١). دور إدارة الجامعة في تعزيز الوعي بالأمن السيبراني لدى طلبة كلية التربية بجامعة الإمام محمد بن سعود الإسلامية. *مجلة العلوم الإنسانية والإدارية*، (٢٥)، ٨٣- ١٠٤ .

الشيبي منى. (٢٠٢٢). واقع استخدام التقنيات الحديثة في تدريس العلوم من وجهة نظر معلمات ومشرفات الصفوف الأولية في المرحلة الابتدائية بمدينة مكة المكرمة . *مجلة القراءة والمعرفة*، (٢٤٠)، ١٤٣-١٧٢.

الصانع، نوره عمر وآخرون. (٢٠٢٠). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الانترنت وتعزيز القيم والهوية الوطنية لديهم. *المجلة العلمية لكلية التربية*، ٣٦ (٦) ، ٤١- ٩٠.

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

الصحفي، مصباح أحمد حامد، وعسكول، سناء بنت صالح. (٢٠١٩). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. *مجلة البحث العلمي في التربية*، ١٠ (٢٠)، ٤٩٣-٥٣٤ .

الصرايرة هديل. (٢٠٢٣). *واقع استخدام مستحدثات التكنولوجيا في تدريس الرياضيات للمرحلة الأساسية من وجهة نظر المعلمين في لواء المزار الجنوبي* [رسالة ماجستير غير منشورة]. جامعة مؤتة.

الضفيري، ناجي بدر والعنزي، إبراهيم غازي والعنزي، دلال فرحان. (٢٠٢٤). الوعي بالأمن السيبراني لدى معلمي المرحلة المتوسطة بدولة الكويت وعلاقته بمستوى توظيفهم للتكنولوجيا في التدريس. *مجلة الدراسات والبحوث التربوية*، ٤(١١)، ١ — ٤٢.

الظويفري، مشاعل شبيب مطيران. (٢٠٢١). واقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية. *المجلة الدولية للدراسات التربوية والنفسية*، ١٠ (٣)، ٦٣٥- ٦٥٥.

عبد الجواد، سيد نوح سيد وأبو الهدى، حسام الدين حسين وإسماعيل، الغريب زاهر ومحمود، أيمن جبر. (٢٠٢٤). تصميم بيئة تعلم الكترونية تكيفية لتنمية مهارات الأمن السيبراني لدى اخصائى تكنولوجيا التعليم. *مجلة جامعة الفيوم للعلوم التربوية والنفسية*، ١٨ (٩)، ٣١٧ - ٣٦٨.

العتيبي، سعود شباب سدر. (٢٠٢٢). مدى توافر الوعي بالأمن السيبراني لدى أفراد الأسر في المجتمع السعودي (دراسة استطلاعية على عينه من الأسر بمحافظة جدة . *المجلة الدولية لنشر البحوث والدراسات*، ٣ (٢٧)، ٥٧٥- ٦١٣.

عليان، ربحي مصطفى والدبس، محمد عبد.(٢٠٠٣). وسائل الاتصال وتكنولوجيا التعليم. دار صفاء للنشر.

غوص، أميرة عبد الرحمن حسن والشريف، باسم نايف محمد. (٢٠٢٢). فاعلية توظيف بعض التطبيقات التعليمية الذكية في تقديم وحدة مقترحة عن الأمن السيبراني على التحصيل المعرفي والاتجاهات نحوه لدى طالبات المرحلة المتوسطة بالمدينة المنورة. *مجلة التربية*، (١٩٥)، ج(٣)، ٦٨٥- ٧٣٤.

فرج، علياء عمر كامل ابراهيم. (٢٠٢٢). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي. *المجلة التربوية*، ١ (٩٤)، ٥٠٩- ٥٣٧.

البعلبكي، منير.(٢٠١٦) *قاموس المورد* (ط.٤١). دار العلم للملايين.

القحطاني، نورة. (٢٠١٩). مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي. *دراسة ميدانية شؤون اجتماعية*، ٣٦ (١٤٤)، ٨٥ — ١٢٠

كلاع، شريفة. (٢٠٢٢). الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني. *مجلة الحقوق والعلوم الإنسانية*، ١٥ (١)، ٢٩٢- ٣١٤ .

المديرس، عبد الله والمطيري فيصل، والحمَّار، أمل.(٢٠٢١). اتجاهات معلمي المرحلة الثانوية بدولة الكويت نحو استخدام التكنولوجيا الرقمية في التدريس، *مجلة كلية التربية*، (١١٤)١، ٣١٦-٣٤٩.

المنتشرى فاطمة يوسف، وحريري، رندة. (٢٠٢٠). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للتربية النوعية* ، (١٤) ٩٥ — ١٤٠.

المنتشري، فاطمة يوسف. (٢٠٢٠). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للعلوم التربوية والنفسية*، ٤ (١٧) ، ٢٧٥- ٤٨٥.

هوساوي، ياسر محمد. (٢٠٢٠). دور التوعية بالأمن السيبراني في الحد من اثر تعقيد وسائل التحقق الرقمي من الهوية على سلوك المستخدم الطرفي. *مجلة جامعة أم القرى للهندسة والعمارة*، ١ (١)، ٣٩ -٥١ .

Black.M., Chapman,D. & Clark, A.(2018).The enhanced virtual laboratory: extending cyber security awareness through a web-based laboratory. *Information systems education journal (ISED), 16* (6), 4-12.

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153-1176.

Crompton, B., Thompson, D., Reyes, M., Zhou, X. & Zou., X. (2016). *Cybersecurity awareness Shrewsbury public schools*. School of professional studies. Paper 3.

Garcia, A. B., & Bongo, S. M. C. (2022). A Cyber Security Cognizance among College Teachers and Students in Embracing Online Education. *In 2022 8th International Conference on Information Management (ICIM)* (pp. 116-119). IEEE

Haseski, H. İ. (2020). Cyber security skills of pre-service teachers as a factor in computer assisted education. *International. Journal of Research in Education and Science (IJRES)* 6(3), 484-500.

Karagozlu, D. (2020). Determination of cyber security ensuring behaviors of pre-service teachers. *Cypriot Journal of Educational Science. 15*(6) , 1698-1706. https://doi.org/10.18844/cjes.v1 5i6.5327

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2022). Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Security Journal*, 1-33.

Mangold, L. V. (2016). *An analysis of knowledge gain in youth cybersecurity education programs.* (Order No. 10250476).

Medina, S. E., Andreasen, K. J., & Newell, J. M. (2018). *An Investigation of Professional Development to Prepare Secondary Administrators to Be Instructional Leaders in Technology Integration* [Doctoral dissertation]. Saint Louis University.

O'Brien, C. (2019) .*Teachers' perceptions about use of digital games and online resources for cybersecurity basics education*: A case study (Order No. 13807207

Pusey, P. & Sadera, W. (2011). Cyberethics, Cybersaftey, and Cybersecutity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. J*ournal of digital learning in teacher education. 28*(2), p.82- 88 .

Richardson, M., Lemonine, P., Stephens, W. & Waller, R. (2020): Planning for Cyber Security in Schools: The Human Factor. *Educational Planning 27*(2),23-39.

Safaria, T. (2016). Prevalence and Impact of Cyberbullying in a Sample of Indonesian Junior High School Students. *The Turkish Online Journal of Educational Technology*. *15*(1), 82- 91.□

Solms. R. & Solms, S.(2015). Cyber safety education in developing countries. *Journal of systemics, cybernetics and informatics*. *13*(2), 14-19.

Spiering, A. (2013). Improving cyber saftey awareness education at duch elementary school. *Unpublished master thesis*. Leiden: Leidein university.□

Wilson, C. (2014). Cybersecurity education the emergence of an accredited academic discipline. Journal of the colloquium information system security education. 2(1), 13- 25.