تاريخ القبول : ٢٠٢٤/٢/١٤
تاريخ النشر : ٢٠٢٤/٧/١

واقع الوعي بإجراءات الأمن السيبراني كما يدركها طلبة كليات التربية بجامعة مطروح

إعـــداد

د / مروه توفيق محمد مشعل
أستاذ مساعد مناهج وطرق تدريس رياض الأطفال
قسم تعليم الطفولة المبكرة- كلية التربية
جامعة شقراء

د / مروه محمود الشناوي
مدرس مناهج الطفل
كلية التربية للطفولة المبكرة
جامعة مطروح

مستخلص الدراسة:

سعت الدراسة الحالية إلى التعرف علي واقع الوعي بإجراءات الأمن السيبراني كما يدركها طلبة كليات التربية بجامعة مطروح، وتم استخدام المنهج الوصفي لتحديد أهم بإجراءات الأمن السيبراني التي يتخذها الطلبة لحماية أنفسهم من المخاطر السيبرانية، وحددت الباحثتين عينة عشوائية من طلبة كليات التربية حيث بلغ عدد أفراد عينة الدراسة (١٢٥) طالب وطالبة، واستخدمت الدراسة إستبيان الوعي باجراءات الأمن السيبراني لدي طلبة كليات التربية وتم تقسيم الإستبيان غلي ثلاثة محاور (درجة وعي الطلاب بإجراءات الأمن السيبراني الخاصة بالأجهزة المتصلة بالإنترنت، درجة وعي الطلاب بإجراءات الأمن السيبراني بالطالب نفسه، سبل تعزيز الوعي السيبراني لدى طلاب الكلية)، وتوصلت الدراسة إلي وجود درجة وعي تتراوح بين متوسطة ومرتفعة لدى طلاب كليات التربية بإجراءات الأمن السيبراني اللازمة والخاصة بالأجهزة المتصلة بالإنترنت، كما يتضح وجود ضعف في وعي الطلاب ب إجراءات الأمن السيبراني اللازمة والخاصة بالطالب نفسه، ويرجع ذلك إما إلى عدم الوعي بخطورة الإجراء نفسه أو عدم الاهتمام باتخاذ الإجراء اللازم، أيضاً وجود عدة سبل يمكن عن طريقها تعزيز الوعي بإجراءات الأمن السيبراني لدى طلبة كليات

التربية، أهمها تقديم الدورات التدريبية بشكل دوري، وقيام كليات التربية بتوصيف مقرر عن الأمن السيبراني يتم تدريسه للطلبة، وتوفير نسخ أصلية من نظم التشغيل والبرامج بأسعار مخفضة لطلبة الكليات، وأوصت الدراسة بضرورة إدراج تعليم الأمن السيبراني كجزء من المناهج الدراسية في التعليم بشكل عام، إجراء برامج تدريبية للتوعية بالأمن السيبراني للمعلمين أثناء الخدمة، إعداد مناهج للأمن السيبراني لمعلمي المراحل المختلفة، توعية الأطفال باجراءات تطبيق الأمن السيبراني خاصة في المرحل المبكرة، تقديم نسخ مجانية أو مخفضة التكاليف من برامج الحماية وأنظمة التشغيل الأصلية للطلبة عند التحاقهم بالجامعة.

الكلمات المفتاحية: الوعي – إجراءات الأمن السيبراني – طلبة كليات التربية.

The reality of awareness of cybersecurity procedures as perceived by students of faculties of education at Matrouh University

by

Dr. Marwa Tawfiq Meshaal
Assistant Professor of Kindergarten Curricula and Teaching Methods
College of Education
Shaqra University

Dr. Marwa Mahmoud El Shenawy
Teacher of Child Curricula
Department of Educational Sciences
Faculty of Early Childhood Education
Matrouh University

Study Abstract:

The current study sought to identify the reality of awareness of cybersecurity procedures as perceived by students of faculties of education at Matrouh University, and the descriptive approach was used to determine the most important cybersecurity measures taken by students to protect themselves from cyber risks, and the researchers identified a random sample of students of faculties of education, where the number of members of the study sample reached (١٢٥) male and female students, and the study used a questionnaire awareness of cybersecurity measures among students of faculties of education, and the questionnaire was divided into three axes (the degree of students' awareness of cybersecurity procedures). for devices connected to the Internet, the degree of students' awareness of cybersecurity procedures in the student himself, ways to enhance cyber awareness among

college students), The study found that there is a degree of awareness ranging from medium to high among students of faculties of education of the necessary cybersecurity procedures for devices connected to the Internet, and it is clear that there is a weakness in students' awareness of the necessary cybersecurity measures for the student himself, due either to lack of awareness of the seriousness of the procedure itself or lack of interest in taking the necessary action, as well as the existence of several ways through which awareness of cybersecurity measures can be enhanced among students of faculties of education, the most important of which is the provision of training courses periodically, and the Faculties of Education with a course description on cybersecurity taught to students, and providing original copies of operating systems and programs at reduced prices for college students, and the study recommended the need to include cybersecurity education as part of the curriculum in education in general, conducting training programs to raise awareness of cybersecurity for in-service teachers, preparing cybersecurity curricula for teachers of different stages, educating children about the procedures for applying cybersecurity, especially in the early stage, providing free or reduced cost copies of protection programs and original operating systems for students When they join the university.

Keywords:

Awareness - Cybersecurity Procedures - Students of Faculties of Education.

مقدمة:

يعيش المجتمع الحديث في عصر رقمي يتميز بالتقدم التكنولوجي السريع، وأصبحت التكنولوجيا الرقمية جزءًا مهمًا من حياتنا اليومية. مع تزايد انتشار استخدام الإنترنت وتوسيع نطاق الاتصالات الرقمية، ظهرت تحديات جديدة تتعلق بأمن المعلومات والبيانات الرقمية. ومن بين هذه التحديات التي نتجت عن العصر الرقمي، أصبح الأمن السيبراني مجالًا مهمًا لحماية المعلومات وأنظمة الكمبيوتر من التهديدات الإلكترونية (التيماني، ٢٠٢١).

الأمن السيبراني مفهوم حديث تزامن مع الثورة الرقمية التكنولوجية العالمية حيث أصبح الفرد يعتمد على اعتماداً أساسياً على الانترنت في جميع احتياجاته، وهو مفهوم يتضمن مجموعة من الإجراءات والتقنيات المصممة لحماية المعلومات الرقمية وأنظمة الكمبيوتر من المتسللين والاستغلال غير القانوني. وتشمل هذه التهديدات السيبرانية الهجمات الإلكترونية والبرامج الضارة وسرقة الهوية والقرصنة وغيرها من الأنشطة غير القانونية التي تستهدف البيانات الحساسة وأنظمة الكمبيوتر (الحبيب، ٢٠٢٢).

وتكمن أهمية الأمن السيبراني في حماية المعلومات الحساسة والأصول الرقمية المهمة، سواء في القطاع العام أو القطاع الخاص. فالهجمات السيبرانية يمكن أن تتسبب في خسائر مالية فادحة وتأثيرات سلبية على الاستقرار الاقتصادي والسياسي، وعلاوة على ذلك قد يتعرض الأفراد والمؤسسات للتجسس الإلكتروني والابتزاز الرقمي، مما يشكل تهديدًا للخصوصية والسلامة الشخصية.

وفي عصر تكنولوجيا المعلومات الحديث، أصبح الإنترنت جزءا لا يتجزأ من حياتنا اليومية وعملية التعليم، مع تزايد استخدام تكنولوجيا المعلومات والاتصالات في التعليم، أصبح الأمن السيبراني أمرًا بالغ الأهمية، ومن المهم أن يكون لدى الطلاب – خاصة في كليات التربية – وعي وفهم جيدين لهذه التدابير الأمنية لضمان أمن بياناتهم الشخصية والمؤسسية ولضمان استخدامهم لتكنولوجيا المعلومات بشكل آمن ومسؤول. ويتفق كلاً من (الجندي ومحمد، ٢٠١٩) و(الصانع وآخرون، ٢٠٢٠) (Hasan & Tasji, ٢٠٢١) أن الجامعة تعتبر منبر للتقدم العلمي والثقافي ويتوقف

هذا التقدم على مدي مسايرة الجامعة للتطورات العلمية والتقنية، كما أن الجامعة مطالبة بإعداد الشباب للاندماج الجيد في مجتمع تهيمن عليه التكنولوجيا في مجالات الحياه، كما أنها مطالبة أيضاً بتطبيق ممارسات الأمن السيبراني وبتنمية مهارات الأمن المعلوماتي لدى الطلبة حيث طالب اليوم هو معلم الغد الذي تقع عليه مسؤولية المساهمة بشكل كبير وفعال في حماية الطلبة من المخاطر التي قد يتعرضوا لها أثناء استخدامهم للتقنيات الحديثة.

وتعد زيادة الوعي بإجراءات الأمن السيبراني بين الطلاب في كليات التربية أمرًا بالغ الأهمية لتطوير جيل يمكنه التعامل بفعالية مع التحديات التكنولوجية والأمنية المستقبلية. ولذلك ستساعد هذه الدراسة في تحديد الخطوات والإجراءات التي يمكن اتخاذها لزيادة وعي الطلاب بالأمن السيبراني وتطوير كفاءاتهم في هذا المجال.

يعد الأمن السيبراني والأمن الرقمي من أهم الأولويات بالنسبة للمؤسسات والحكومات حول العالم. ولذلك، فإن زيادة الوعي بالأمن السيبراني في التعليم يمكن أن يساعد في حماية البيانات والمعلومات الحساسة والحفاظ على سلامة أنظمة وشبكات التعليم. ومن المهم أيضًا أن يفهم الطلاب التحديات السيبرانية التي قد يواجهونها كمدرسين أو مديرين ومشرفين لتكنولوجيا التعليم في المستقبل (الخضري، ٢٠٢٠) (غوص، والشريف ، ٢٠٢٢).

الخلاصة يعد تحسين الوعي بالأمن السيبراني في كليات التربية أمرًا بالغ الأهمية لتحقيق تكامل تكنولوجيا التعليم وبناء بيئة تعليمية آمنة وموثوقة، ومن خلال زيادة الوعي والتعريف بالأمن السيبراني واجراءاته، يمكن للمؤسسات والطلاب أن يكونوا على استعداد أفضل لمواجهة التحديات السيبرانية والمساهمة في بناء مجتمع رقمي آمن ومستدام.

مشكلة الدراسة:

التعليم هو الطريق إلى تطوير مستقبل المجتمع إذ إنه يفتح الفرص ويعتبر حجر الزاوية لمجتمع مستنير ومحرك رئيسي للتنمية المستدامة. وهو الأساس الذي يمكن

من خلاله تطوير المهارات والمعرفة اللازمة في سوق العمل من خلال توفير تعليم عالٍ الجودة وربطه باحتياجات سوق العمل.

لقد تضاعف الاهتمام العالمي بشكل عام بجودة التعليم في السنوات الأخيرة، حيث ترى معظم الدول المعاصرة أن التركيز الأساسي في القرن الحادي والعشرين يجب أن ينصب على التعليم الحديث عالٍ الجودة والذي يركز على متطلبات العصر ويعمل على الاستفادة من الإمكانات المتاحة حالياً إلى أقصي حد.

وتعتبر كليات التربية إحدى المؤسسات التعليمية الهامة التي لها دور بارز ومؤثر في المجتمع حيث يتم بها إعداد المعلم الذي سيقوم بدوره في تربية وتنشئة الأجيال وإعدادهم للمستقبل، وكما أوضح (Duman,٢٠٢٢) حتي تقوم كليات التربية بدورها الصحيح في اعداد معلم المستقبل يجب أن تعمل على تزويد هؤلاء الطلاب بالمعارف والمعلومات والقيم والمهارات التي تؤهلهم للتعامل مع مستجدات العصر الحديث.

وحيث أن التعليم الآن أصبح معتمد بشكل كبير على الإنترنت في بعض المراحل التعليمية ولاسيما المرحلة الجامعة بشكل رئيس خاصة بعد انتشار فيروس كورونا كما أشار (Raju, et al., ٢٠٢٢) إلى تبني الأكاديميون والطلاب التعليم عبر الإنترنت من خلال الاعتماد على المنصات التعليمية وأن التحدي الرئيس الذي سيواجه الطلاب في عصر الرقمنة هو التحدي المتعلق بالأمن السيبراني، لذلك أصبح هناك ضرورة ملحة وحتمية لتزويد المعلم المستقبلي للتعامل الآمن مع شبكة الإنترنت والتعرف على مخاطر استخدامها مما يساعده في رفع الوعي لدى المتعلمين فيما بعد بمخاطر استخدام الإنترنت.

فوجود الوعي بإجراءات الأمن السيبراني لدى الطالب المعلم يساعده على تعرف المخاطر التي قد يتعرض لها ويمكنه من حماية نفسه وطلابه فيما بعد، وأكدت العديد من الدراسات (عبد السلام، ٢٠٢٣) (الصانع وآخرون، ٢٠٢٠) (الجندي ومحمد، ٢٠١٩) على أن التهديدات السيبرانية وصعوبة حماية الأجهزة بشكل كامل يستلزم زيادة الوعي المجتمعي بأمن المعلومات والتعرف على إجراءات الأمن السيبراني، وأوضح (الحبيب، ٢٠٢٢) أن الأمن السيبراني تظهر أهميته في توفير

أمن المعلومات والتخفيف من مخاطر اختراق المعلومات والهجمات الإلكترونية، وأشار (Haseski, ٢٠٢٠) إلى أن توفر مهارات الأمن السيبراني والوعي والمعرفة لدى معلمي ما قبل الخدمة غير كافية خاصة وأنهم يتعاملوا كثيراً مع أنشطة تعليمية في بيئة افتراضية ويجب أن يكونوا على معرفة بكيفية حماية بياناتهم الشخصية وتجنب المواقع غير الموثوق فيها، كما توجد قلة في الدراسات التي اهتمت بمسألة وعي الطلاب حول الأمن السيبراني في العالم العربي – في حدود علم الباحثتان – وأكد على ذلك دراسة (البراشدية، ٢٠١٩).

كما لاحظت الباحثتان من خلال عملهما مع طلبة كليات التربية قلة الوعي المعلوماتي لديهم وكيفية التعامل الآمن مع شبكة الإنترنت وحماية المعلومات والملفات الشخصية، ويؤكد على ذلك دراسة (الصحفي، ٢٠١٩) والتي أشارت إلى وجود قصور لدى معلمات الحاسب الإلى في الوعي بمفاهيم الأمن السيبراني.

وتأسيساً على ما سبق يتضح أهمية العمل على رفع الوعي لدى طلبة كليات التربية بإجراءات الأمن السيبرانية سواء عند استخدام الأجهزة في حال اتصالها بالإنترنت أو بالإجراءات التي يستخدمها الطالب لحماية نفسه من خطر التعرض للهجمات أو التهديدات السيبرانية ومخاطر التنمر الإلكتروني، وأيضاً سبل تعزيز الوعي السيبراني لدى الطلبة أنفسهم.

وتتمثل مشكلة الدراسة الحالية في الإجابة على التساؤل الرئيس التالي:

- ما درجة الوعي بإجراءات الأمن السيبراني كما يدركها طلبة كليات التربية بجامعة مطروح؟

ويتفرع منه الأسئلة التالية:

١–ما درجة وعي طلبة كليات التربية بإجراءات الأمن السيبراني الخاصة بالأجهزة المتصلة بالإنترنت؟

٢–ما درجة وعي طلبة كليات التربية بإجراءات الأمن السيبراني الخاصة بالطالب نفسه؟

٣-ما سبل تعزيز الوعي بإجراءات الأمن السيبراني لدى طلبة كليات التربية من وجهة نظرهم؟

٤-ما الفروق في درجات الوعي بإجراءات الأمن السيبراني بين طلبة كليات التربية تعزى إلى المتغيرات الديموغرافية للدراسة (العمر عند استخدام الإنترنت لأول مرة، الجنس، العمل بجانب الدراسة)؟

أهداف الدراسة :

١- التعرف على إجراءات الأمن السيبراني التي يمتلكها طلبة كليات التربية بجامعة مطروح.

٢- تنمية الوعي بإجراءات الأمن السيبراني لدى طلبة كليات التربية بجامعة مطروح.

٣- إعداد طلاب قادرين على الأخذ بالتدابير اللازمة وحماية أنفسهم من المخاطر السيبرانية.

٤- التعرف على سبل تعزيز إجراءات الأمن السيبراني لدى طلبة كليات التربية من وجهه نظرهم.

أهمية الدراسة:

قد تفيد هذه الدراسة في:

٥- إكساب الطلبة الوعي بإجراءات الأمن السيبراني لحماية أنفسهم من المخاطر السيبرانية.

٦- التعرف على أهم التدابير الوقائية التي يستخدمها الطلبة لحماية أنفسهم من المخاطر السيبرانية.

٧- تستهدف الدراسة شريحة مهمة من طلبة كليات التربية (معلم المستقبل) للتعرف على مدى وعيهم بالأمن السيبراني، وكيفية اتخاذ الإجراءات والتدابير المناسبة لحماية أنفسهم أثناء التعامل مع الإنترنت.

٨- تسليط الضوء على أهم إجراءات الأمن السيبراني الواجب إكسابها للطلبة ودور الجامعة في حمايتهم.

منهج الدراسة:

استخدمت الدراسة المنهج الوصفي نظراً لملائمته لطبيعة البحث.

أدوات الدراسة:

اعتمدت الدراسة الحالية على استبيان درجة وعي طلبة كلية التربية بإجراءات الأمن السيبراني إعداد الباحثتين.

حدود الدراسة:

تقتصر الدراسة الحالية على ما يلي:

- **حدود موضوعية** : واقع الوعي بإجراءات الأمن السيبراني كما يدركها طلبة كليات التربية بجامعة مطروح.
- **حدود مكانية:** كليات التربية بجامعة مطروح.
- **حدود زمانية** : الفصل الدراسي الأول للعام الجامعي ٢٠٢٣ / ٢٠٢٤.
- **حدود بشرية** : طلبة كليات التربية بجامعة مطروح.

مصطلحات الدراسة :

إجراءات:

جاء تعريفها في معجم المعاني بأنها "مجموعة من الخطوات المتتالية الواجبة الإتباع لتنفيذ عمل معين".

الأمن السيبراني :

طبقاً للهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية (٢٠١٨) فقد عرفته على أنه "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات، من

أي اختراق أو تعطيل أو دخول أو استخدام أو استغلال غير مشروع ، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الالكتروني والأمن الرقمي ونحو ذلك.

ويعرفه (الحبيب، ٢٠٢٢) مدي إدراك طلبة الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود لكيفية حماية بياناتهم وحساباتهم الشخصية المرتبطة بتقنيات الاتصالات والمعلومات من المخاطر السيبرانية

وتعرفه الباحثتان إجرائياً :

الوعي بمجموعة الإجراءات والتدابير التي يتخذها طلبة كليات التربية لحماية بياناتهم الشخصية وملفاتهم من التهديدات والاختراقات السيبرانية، بهدف ضمان سرية وسلامة معلوماتهم الرقمية، والحد من المخاطر المتعلقة بالاعتداءات السيبرانية.

طلبة كليات التربية :

تعرفه الباحثتان إجرائياً بأنهم:

الطلبة الذين يدرسون في كليات التربية في جامعة مطروح ويتم تزويدهم بالمعارف والمعلومات والمهارات التي تؤهلهم لممارسة مهنة التدريس بعد التخرج، وتتنوع تخصصاتهم فتشمل طلبة كليات (التربية للطفولة المبكرة– التربية النوعية– التربية– التربية الرياضية).

إجراءات الدراسة:

سارت الدراسة وفقاً للإجراءات التالية:

١– دراسة بعض البحوث والمراجع العربية والأجنبية التي اهتمت بمحاور الدراسة الحالية والاستفادة منها في تشكيل الإطار النظري، وفي كيفية إعداد الأدوات التي استخدمت فيها.

٢– تصميم أدوات جمع البيانات والتأكد من صدقها وثباتها.

٣– تطبيق الاستبيان على طلبة كليات التربية بجامعة مطروح.

٤– استخلاص نتائج الدراسة وتحليلها وتفسيرها واقتراح التوصيات والمقترحات المناسبة.

الإطار النظري للدراسة:

الأمن السيبراني:

في عالم اليوم لا غني لأي فرد من أفراد الأسرة عن استخدام الأجهزة الإلكترونية بكل أشكالها، وهذه الأجهزة تقوم بتخزين المعلومات والبيانات الشخصية حتى تمكن الفرد من أداء مهامه وأعماله اليومية بشكل مبسط، وإنجاز الأعمال المختلفة التي تتطلب إدخال البيانات الشخصية مثل مواقع التواصل الاجتماعي، والتعامل مع بعض المواقع الحكومية الإلكترونية، وسداد بعض الفواتير ... وكل ذلك يتم من خلال الاتصال بشبكة الإنترنت، كما زادت أهمية مواقع التواصل الاجتماعي ودورها المؤثر في حياة الأفراد خاصة بعد انتشار جائحة كورونا وفرض على العالم أجمع المكوث في المنازل لفترات طويلة، فكان الحل الوحيد لجميع شعوب العالم الاعتماد على شبكة الإنترنت ومواقع التواصل الاجتماعي للتواصل بين الأفراد، ومعرفة ومتابعة الأخبار المختلفة، من هنا أصبح الإنترنت له دور مؤثر وكبير في حياة جميع الأفراد وجميع الفئات في المجتمع الواحد، وجميع قطاعات هذا المجتمع.

هذا التوسع في استخدام الإنترنت بشكل رئيس في حياة الأفراد، يستلزم أن يكون لدى الأفراد الوعي والمعرفة بكيفية حماية أنفسهم من مخاطر استخدام الإنترنت أو الوقوع ضحية للتنمر الإلكتروني، أو الهجمات السيبرانية المختلفة التي تعمل على سرقة البيانات والملفات الشخصية إذا لم تتوفر عوامل الأمن والحماية الكافية من قبل المستخدمين (صائغ، ٢٠١٨).

وأشار كلاً من (الحارثي، ونصر، ٢٠٢١) أنه في عصر المعلومات وانتشار استخدام الإنترنت ظهرت العديد من الظواهر السلبية منها تعرض الأفراد لسلوك الإيذاء الإلكتروني من خلال الوسائط الإلكترونية والرقمية وتصاعد الإيذاء السيبراني وأصبحت مشكلة اجتماعية خطيرة، والطريقة التي يتصرف بها ضحايا الفضاء الإلكتروني غالباً ما تؤدي إلى ضعف الأداء الأكاديمي من قبل الطلاب الضحايا.

وحيث أن الجامعة تعد منبراً للتقدم العلمي والثقافي، ويتوقف هذا التقدم على مدى مسايرة مؤسسات التعليم العالي للتطورات العلمية والتقنية، وكلما أولت الجامعة اهتماماً بالمستحدثات التقنية الفعالة في دعم المحتوي التعليمي والممارسات التطبيقية

لذلك المحتوي وذلك من اجل إعداد الشباب للاندماج في مجتمع جديد يسيطر عليه التقدم العلمي والتقني كلما أصبحت الجامعة مطالبة باستقطاب التقنيات واستخدامها وممارستها بشكل تطبيقي في تحسين العملية التعليمية (الجندي، ومحمد، ٢٠١٩).

وكما أوضح (عبد السلام، ٢٠٢٣) أن الأمن السيبراني يشمل أشكال متعددة مثل حماية الحسابات الشخصية على مواقع التواصل الاجتماعي، والتأكد من صحة المعلومات، وعدم الدخول في روابط مجهولة قد تحتوي على فيروسات، وتدريب الأفراد على الاستخدام الإيجابي المنظم لشبكة الإنترنت في الأنشطة التعليمية، وامتلاك مهارات حماية الحساب الشخصي من هجمات القرصنة والتجسس الإلكتروني، وتفعيل برمجيات التحذير والحماية من الهجمات الإلكترونية.

وفي حين أن التكنولوجيا الحديثة تجلب فوائد هائلة، إلا أنها تفتح الباب أيضًا أمام زيادة التهديدات السيبرانية، فيمكن أن تأتي الهجمات الإلكترونية من مهاجمين يريدون سرقة معلومات حساسة أو تعطيل الخدمات أو تعطيل البنية التحتية للشبكة، ومع وجود كميات كبيرة من البيانات الحساسة المخزنة على الأنظمة الإلكترونية، أصبح الأمن السيبراني أمرًا بالغ الأهمية للمؤسسات والحكومات والأفراد (RICHARDSON, et al., ٢٠٢٠).

وتشمل تهديدات الأمن السيبراني مجموعة واسعة من الهجمات والتحديات، مثل البرامج الضارة والقرصنة والتصيد الاحتيالي، ولمكافحة هذه التهديدات، يتطلب الأمن السيبراني مجموعة من التدابير والأدوات التي تشمل الحماية من الهجمات، والكشف عن الانتهاكات، والاستجابة الفورية للحوادث الإلكترونية.

ويعد الوعي والتعليم السيبراني عنصرين أساسيين في مجال الأمن السيبراني، يجب أن يكون المستخدمون والمؤسسات على دراية بالمخاطر السيبرانية وأن يتبعوا ممارسات أمان البيانات والشبكات مثل استخدام كلمات مرور قوية، وتحديث البرامج الضارة، وتجنب الروابط غير الموثوق بها، تحديث البرامج والتطبيقات وإجراء عمليات فحص أمنية منتظمة.(المطرفي والفراني، ٢٠٢٣)

وبالإضافة إلى ذلك، يلعب التعاون بين جميع الجهات أيضًا دورًا مهمًا في تعزيز الأمن السيبراني، فيجب على الحكومات والشركات والمؤسسات التعليمية والمجتمع

المدني العمل معًا لتبادل المعلومات والخبرات والتعاون في مجال الأمن السيبراني، ويتطلب ذلك إنشاء شبكات اتصال فعالة وتنظيم الفعاليات وورش العمل لزيادة الوعي السيبراني وتحسين المهارات التقنية.

وبالرغم من ذلك لا يمكن التغلب على التهديدات السيبرانية بشكل كامل، ولكن يمكن تقليل المخاطر والحد من التأثيرات السلبية من خلال اتخاذ التدابير اللازمة، فيجب أن يكون الأمن السيبراني جزءًا من الثقافة المجتمعية، حيث يعمل على حماية بيانات الأفراد الشخصية والمعلومات الحساسة ويساعدهم على تطوير حلول أمنية مبتكرة (Raju, ٢٠٢٢)، و(التيماني، ٢٠٢١).

مفهوم الأمن السيبراني:

عرفه الغامدي (٢٠١٨) بأنه الطريقة المثلي المستخدمة لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية بهدف الولوج للمعلومات المهمة ومحاولة إتلافها أو ابتزاز المستخدمين من خلالها. نقلاً عن (الجندي ومحمد، ٢٠١٩).

وعرفه (علي، ٢٠١٧) بأنه تلك الطرق التي تستهدف كشف ومنع الهجمات على أي نظام حاسوبي والمعلومات المتضمنة فيه أو الوصول غير المصرح به، ويستهدف الأمن السيبراني حماية البيانات أو أي شكل من الأصول الرقمية المخزنة في حاسوب لأية جهة أو في أي جهاز يحتوي على ذاكرة رقمية.

ويعرف أيضا الأمن السيبراني بأنه التدابير المتخذة لحماية جهاز كمبيوتر أو شبكة ضد الوصول غير المصرح به للحفاظ على سلامة المعلومات المخزنة، يتضمن الأمن السيبراني التدخلات التقنية التي تحمي البيانات ومعلومات الهوية، والأجهزة من الوصول غير المصرح به أو الضرر بما في ذلك أمن الأصول في الفضاء السيبراني (RICHARDSON, et al., ٢٠٢٠).

عادة ما يتم استخدام مصطلح الأمن السيبراني للإشارة إلى نفس معني مصطلح "أمن المعلومات" ويرتبط مصطلح الأمن بحماية جميع الأصول، وقد عرف (Yilmaz and Sagiroglu, ٢٠١٣) الأمن السيبراني بأنه مجموع الأدوات والسياسات والمفاهيم والتدريب والتطبيقات والتقنيات المستخدمة لحماية المعلومات من أجل الوقاية من أضرار الهجمات السيبرانية (Karagozlu, ٢٠٢٠).

أهداف الأمن السيبراني:

ويهدف الأمن السيبراني إلى عدة نقاط من أهمها:

- توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات.
- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية والمؤسسات التعليمية.
- توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
- سد الثغرات في أنظمة أمن المعلومات.
- مقاومة البرمجيات الخبيثة ما تستهدفه من إحداث أضرار بالغة للمستخدمين.
- اتخاذ جميع التدابير اللازمة لحماية الأفراد من المخاطر المحتملة في المجالات المختلفة استخدام الإنترنت.
- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة (السمحان، ٢٠٢٠).

أهمية الأمن السيبراني:

تتجاوز أهمية الأمن السيبراني الحدود الجغرافية وتمتد إلى كافة القطاعات والمجالات في العصر الرقمي الحديث، ويوضح كلاً من (العتيبي، ٢٠٢٢)، و(الخضري، وآخرون، ٢٠٢٠) أن الأمن السيبراني ذو أهمية بالغة في عصرنا الحالي الذي يعتمد بشكل كبير على التكنولوجيا والاتصالات الإلكترونية، وهناك بعض الأسباب التي تبرز أهمية الأمن السيبراني:

- حماية البيانات الهامة: يتم تخزين كميات ضخمة من المعلومات الحساسة والبيانات الشخصية على الأنظمة الإلكترونية، ويشمل ذلك المعلومات المالية والطبية والتجارية والحكومية.
- الحماية الشخصية والخصوصية: في عصر التواصل الرقمي، يتم تبادل كميات كبيرة من المعلومات الشخصية عبر الإنترنت، ويساعد الأمن السيبراني في حماية الأفراد من الاختراقات والاحتيال وسرقة الهوية وضمان حماية خصوصيتهم الشخصية والمعلوماتية.
- الحماية من الهجمات السيبرانية المتطورة: يشهد العالم تطورًا مستمرًا في تقنيات الهجمات السيبرانية، والقرصنة والاحتيال الإلكتروني والبرمجيات الخبيثة تتطور بشكل سريع، والأمن السيبراني يلعب دورًا حاسمًا في تحديد ومواجهة هذه التهديدات والاستجابة لها بشكل فعال.

أهمية الأمن السيبراني في المؤسسات التعليمية:

المؤسسة التعليمية تعتبر مستودعات لمجموعات البيانات الكبيرة التي تحتوي على معلومات قيمة بالنسبة للطلبة وتشتمل على ما يلي:

(هوية الطالب، أرقام الضمان الاجتماعي للطلاب وأعضاء هيئة التدريس والموظفين، أرقام بطاقات الائتمان لأعضاء هيئة التدريس والموظفين والمدرسة، تاريخ التحصين والسجلات الطبية، التسجيل والحضور، أسماء الطلاب وأعضاء هيئة التدريس والموظفين، العناوين، تاريخ الميلاد، المدينة وبلد الإقامة، أرقام الهواتف، عناوين البريد الإلكتروني، درجات الاختبار، الإنجازات، المشاركة في الأنشطة المدرسية (التواريخ والأوقات)، بيانات أفراد الأسرة، الطلاب السابقون في المدرسة وبياناتهم) (RICHARDSON, et al., ٢٠٢٠).

ولخلق الوعي بالأمن السيبراني وتنمية الوعي الأمني لدى الأفراد لابد من توفير التعليم اللازم منذ الصغر، ويجب إدراج موضوع الأمن السيبراني في المناهج الدراسية في المدارس، ويجب دعم الأنشطة التعليمية والإعلامية بوسائل الإعلام.

ويقع الدور الأكثر في إعلام الطلبة بشأن الإجراءات الأمنية اللازمة على عاتق المعلمين بشكل عام (Karagozlu, ٢٠٢٠).

أهمية الأمن السيبراني للمعلم:

يجب أن يكون كل من يستخدم التكنولوجيا، على دراية بالأنواع الشائعة من عمليات الاحتيال، وأن يعرف كيفية حماية نفسه وبياناته وأجهزته. وعندما نكون على دراية بأحدث أنواع الهجمات نصبح قادرين على حماية أنفسنا ومساعدة طلابنا أيضا.

وبذلك يعد الأمن السيبراني للمعلم أمرًا مهمًا، حيث يتعامل المعلمون مع البيانات الشخصية للطلاب والمعلومات الحساسة في البيئة التعليمية الرقمية، ويذكر كلاّ من (Salvail, ٢٠٢٣) و(Haseski, ٢٠٢٠)، و(Kortjan, ٢٠١٣) الخطوات التي يمكن للمعلم اتخاذها في الفصل الدراسي للتوعية بالأمن السيبراني حيث يقوم بتدريب الطلبة على:

- استخدام كلمات مرور قوية يتم تغييرها على فترات مختلفة.
- عدم استخدام معلومات التعريف الشخصية، يتضمن ذلك الأسماء والعناوين وأرقام الهواتف وأي معلومات أخرى من شأنها أن تسمح لشخص غريب بمعرفة هويتك بالضبط.
- المحافظة على تحديث الأجهزة لحمايتها من الهجمات ، ويتم ذلك بإنشاء روتين لتحديث البرامج والتطبيقات بشكل منتظم.
- قاعدة فصل دراسي "عدم النقر أبدا على رابط مشبوه أو نافذة منبثقة، ينطبق هذا أيضا على رموز QR لأنها يمكن أن تحتوي على برامج ضارة وفيروسات.

وهناك بعض المفاهيم الأساسية التي يمكن للمعلم تعليمها للطلبة للتعريف بإجراءات الأمن السيبراني:

- **المواطنة الرقمية العامة:** تعليم الطلاب الأصغر سنا أهمية أن يكونوا مواطنين رقميين مسؤولين. وهذا يشمل احترام خصوصية الآخرين وكذلك اتباع القواعد والإرشادات التي وضعها آباؤهم أو مدرستهم أو مجتمعهم.
- **العناية بالجهاز:** تأكد من أن الأطفال يعرفون كيفية العناية بأجهزتهم ، بما في ذلك تتبعها وشحنها. لن يساعد هذا في منع الأجهزة المفقودة فحسب ، بل سيضع أيضا الأساس لإبقائها محدثة على الطريق.
- **الأمان عبر الإنترنت:** أخبر الطلاب أنهم بحاجة إلى توخي الحذر بشأن ما ينقرون عليه ، لأنه في بعض الأحيان ينقرون على أشياء مجهولة.
- **كلمات المرور:** ساعد الطلاب على إنشاء كلمات مرور قوية. شجعهم على استخدام مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز. في المدرسة الابتدائية العليا ، يجب تشجيع الطلاب على إعداد مصادقة متعددة العوامل عندما يكون ذلك ممكنا.
- **المعلومات الشخصية:** علم الطلاب توخي الحذر بشأن مشاركة المعلومات الشخصية عبر الإنترنت ، مثل الاسم الكامل والعنوان ورقم الهاتف وتاريخ الميلاد. شجعهم على مشاركة هذه المعلومات فقط مع مصادر موثوقة ، وذكرهم بعدم نشرها علنا. عند إنشاء اسم مستخدم ، يجب على الطلاب عدم استخدام أي جزء من اسمهم الحقيقي أو تاريخ ميلادهم.
- **الخصوصية عبر الإنترنت:** الاستمرار في تعزيز مفهوم الخصوصية عبر الإنترنت ، بما في ذلك المخاطر المرتبطة بمشاركة المعلومات الشخصية علنا على منصات التواصل الاجتماعي. أكد على أهمية ضبط إعدادات الخصوصية وتوخي الحذر بشأن ما يشاركونه عبر الإنترنت. تحدث عن كيفية استخدام المواقع والتطبيقات لتلك البيانات.

- **الوعي بالتصيد الاحتيالي:** تعريف الطلاب بمفهوم التصيد الاحتيإلى ووضح لهم كيفية التعرف على رسائل البريد الإلكتروني أو الرسائل أو الروابط المشبوهة التي قد تحاول سرقة المعلومات الشخصية. علمهم توخي الحذر عند النقر على روابط غير مألوفة أو مشاركة معلومات حساسة.
- **البرامج الضارة والفيروسات:** تقديم مفهوم البرامج الضارة والفيروسات، ومناقشة المخاطر المحتملة التي تشكلها على الأجهزة والمعلومات الشخصية. علم الطلاب أهمية استخدام برامج مكافحة الفيروسات وعدم تنزيل أي شيء يبدو مريبا.
- **أمان الإنترنت:** تغطية ممارسات أمان الإنترنت العامة ، بما في ذلك توخي الحذر بشأن تنزيل الملفات من مصادر غير معروفة ، والتعرف على مواقع الويب المزيفة ، وتجنب التفاعل مع الغرباء عبر الإنترنت.
- **البصمة الرقمية:** ساعد الطلاب على فهم كيف يمكن لأفعالهم عبر الإنترنت أن تترك أثرا دائما. عند دخولهم عالم وسائل التواصل الاجتماعي ، من الأسهل تصديق أن المنشورات والرسائل تختفي، لذلك يحتاج الأطفال إلى فهم أنهم لا يفعلون ذلك.

إجراءات الأمن السيبراني:

هناك العديد من الإجراءات التي يمكن اتخاذها لتعزيز الأمن السيبراني (Wadhwa & Arora, ٢٠١٧) (RICHARDSON, et al., ٢٠٢٠):

أ- حافظ على تحديث جهاز الكمبيوتر الخاص بك بأحدث التصحيحات والتحديثات:

من خلال تحديث جهاز الكمبيوتر الخاص بك بانتظام باستخدام التصحيحات واصلاحات البرامج الأخرى، فإنك تمنع المهاجمين من القدرة على الاستفادة من عيوب البرامج (نقاط الضعف) التي يمكنهم استخدامها لاقتحام نظامك، وتعد

الاستفادة من ميزات "التحديث التلقائي" في برنامجك بداية جيدة نحو الحفاظ على أمانك على الإنترنت.

ب–تأكد من تكوين جهاز الكمبيوتر الخاص بك بشكل آمن:

يعد تكوين تطبيقات الانترنت الشائعة مثل مستعرض الويب وبرامج البريد الإلكتروني أحد أهم المجالات التي يجب التركيز عليها.

ج– اختر كلمات مرور قوية وحافظ على سلامتها:

حقيقة نستخدم كلمات المرور على الإنترنت اليوم في كل شيء، يمكن أن تساعد النصائح التالية في جعل الاستخدام عبر الانترنت آمن:

- تتكون كلمات المرور القوية من ثمانية أحرف أو أكثر وتستخدم مجموعة من الأحرف والأرقام والرموز على سبيل المثال (# * % ؟).
- تجنب استخدام أي مما يلي ككلمة مرور خاصة بك: اسم تسجيل الدخول الخاص بك، وأي شيء يعتمد على معلوماتك الشخصية مثل اسم عائلتك والكلمات التي يمكن تخمينها، حاول تحديد كلمات مرور قوية وفريدة بشكل خاص لحماية أنشطة مثل الخدمة المصرفية عبر الإنترنت.
- احتفظ بكلمات المرور الخاصة بك في مكان آمن وحاول ألا تستخدم نفس كلمة المرور لكل خدمة تستخدمها عبر الإنترنت.
- تغيير كلمة المرور على أساس منتظم على الأكثر كل ٩٠ يوما.

د– حماية جهاز الكمبيوتر الخاص بك مع برامج الأمان:

هناك عدة أنواع من البرامج ضرورية للأمان الأساسي عبر الإنترنت والتي تشمل جدار الحماية وبرامج مكافحة الفيروسات، أصبحت مجموعات الأمان المتكاملة مثل Norton Internet Security والتي تجمع بين جدار الحماية ومكافحة الفيروسات وبرامج مكافحة التجسس مع ميزات أخرى مثل مكافحة البريد العشوائي والرقابة

الأبوية شائعة لأنها توفر جميع برامج الأمان اللازمة للحماية عبر الانترنت في حزمة واحدة.

هـ- حماية معلوماتك الشخصية للاستفادة من العديد من الخدمات عبر الإنترنت، سيتعين عليك حتما تقديم معلومات شخصية للتعامل مع الفواتير وشحن البضائع المشتراة نظرا لأن عدم الكشف عن أي معلومات شخصية نادراً ما يكون ممكنا تحتوي القائمة التالية على بعض النصائح لكيفية مشاركة المعلومات الشخصية بأمان عبر الإنترنت:

- ابتعد عن أية رسالة بريد إلكتروني مجهولة المصدر.
- لا ترد على الرسائل البريد الإلكتروني التي تطلب معلومات شخصية.
- الابتعاد عن مواقع الويب الاحتيالية المستخدمة لسرقة المعلومات الشخصية.
- إيلاء الاهتمام لسياسات الخصوصية على مواقع الويب وفي البرامج.
- حماية عناوين بريدك الإلكتروني.

كما أضاف كلاً من (المطرفي ، والفراني، ٢٠٢٣) (Ahang & Deng, ٢٠١٧)أنه توجد العديد من إجراءات تعزيز الأمن السيبراني، ومن هذه الإجراءات:

١. تثبيت تطبيقات من مصادر موثوقة المثدر ومعروفة.
٢. تسجيل الخروج من أي تطبيق اذا لم يكن قيد الإستخدام.
٣. المحافظة على تحديث جدران الحماية، والتي تمثل أنظمة الدفاع عن البنية التحتية للبيئة المعلوماتية.
٤. التأكد من إعدادات الحاسوب وشبكة الإنترنت.
٥. اختيار كلمات مرور قوية، وعمليات تحقق أمنية لمواقع التواصل الاجتماعي، والبريد الإلكتروني، والحسابات الشخصية على الحاسوب أو الهواتف الذكية.
٦. عدم الاستجابة لأية رسائل مجهولة المصدر ترد إلى البريد الإلكتروني.
٧. استخدام برامج الحماية ومضادات الفيروسات وتحديثها باستمرار.

٨. حماية المعلومات الشخصية ومنع الآخرين من الاطلاع عليها.
٩. تحديث كلمات المرور بشكل مستمر، على الأقل مرة أو مرتين شهريًا.
١٠. عدم إرسال أي معلومات شخصية عبر البريد الإلكتروني، أو الإفصاح عن معلومات خاصة عبر مواقع التواصل الاجتماعي.

دور الجامعة في التوعية بإجراءات الامن السيبراني للطلبة:

تلعب الجامعة دورًا حاسمًا في التوعية بإجراءات الأمن السيبراني للطلبة، فهي تمثل بيئة تعليمية وأكاديمية حيث يتفاعل الطلبة مع الكثير من المعلومات والخدمات الرقمية، وهناك بعض المتطلبات تتمثل في مجموعة الشروط الضرورية التي يلزم توافرها حتي يمكن تحقيق الأمن السيبراني بالجامعات (توفيق، ومرسي، ٢٠٢٣):

١. **دعم وتعزيز البنية التكنولوجية:** تحتاج الجامعات لأجهزة ذات كفاءة وقدرة عالية وشبكات اتصال متعددة وبرمجيات متطورة، بالإضافة إلى العنصر البشري المدرَّب من أجل البنية التحتية للأمن السيبراني، حيث تستطيع الجامعات بذلك التأثير على مختلف الكليات باستخدام القدرات الإلكترونية من جهة، وتأمين نفسها من الأخطار الممكنة من جهة أخري.

٢. **محاربة الفيروسات والقضاء على البرامج الخبيثة:** وهي برامج مصممة لتنفيذ عمليات قرصنة على أجهزة وشبكات بعض المؤسسات ومن ضمنها الجامعات، وتستخدم لتعطيل البنية التحتية، وسرقة البيانات والمعلومات.

٣. **القدرة على إجراء العمليات الإلكترونية:** وتتمثل في اختراق الشبكات ومهاجمة أنظمة المعلومات وتتطلب قدرة دفاعية فهي تتمثل في عمليات الحماية من الهجمات المختلفة وإمكانيات تشغيل الأجهزة ببرمجيات خاصة.

٤. المتطلبات البشرية:

- توعية أعضاء هيئة التدريس بمخاطر إرسال المعلومات الشخصية عبر الرسائل النصية أو البريد الإلكتروني.
- اختيار كلمة مرور قوية للحسابات الشخصية، تحتوي على حروف وأرقام ورموز.

- عقد لقاءات دورية للمختصين في تطبيق الأمن السيبراني لتعريفهم بالمستجدات في المجال.
- تبادل الخبرات مع الجامعات الأجنبية والعربية في مجال الأمن السيبراني.
- تنظيم حملات توعية لأعضاء هيئة التدريس للتعريف بالأمن السيبراني، ومخاطره، وتحقيق متطلباته.

وهناك بعض الأدوار التي يمكن أن تقوم بها الجامعة في التوعية بالأمن السيبراني للطلبة: (الخضري وآخرون، ٢٠٢٠)، و(Alharbi & Tassaddiq, ٢٠٢١)

١. **برامج التوعية والتدريب:** يمكن للجامعات تنظيم برامج توعية وتدريب متنوعة للطلبة حول أمن المعلومات والسلوك السيبراني الآمن. ويمكن أن تشمل هذه البرامج ورش عمل وندوات ومحاضرات حول أحدث التهديدات السيبرانية وكيفية التعامل معها.

٢. **موارد التوعية:** يمكن للجامعات توفير موارد التوعية مثل مواقع الويب والمواد الإرشادية وعروض الفيديو لشرح مفاهيم الأمن السيبراني الأساسية وإظهار أفضل الممارسات، ويمكن أن تتضمن هذه الموارد معلومات حول كلمات المرور القوية، واستخدام الشبكات اللاسلكية الآمنة، وتحديد رسائل البريد الإلكتروني المشبوهة، والمواضيع الأخرى ذات الصلة.

٣. **الدعم الفني وأنظمة الأمان:** يمكن للجامعات تزويد الطلبة بأنظمة وبرامج أمنية، بما في ذلك الإصدارات المرخصة من برامج مكافحة الفيروسات وجدران الحماية وأدوات الكشف عن التهديدات. يتوفر الدعم الفني أيضًا للطلبة في حالة ظهور مشكلات أو استفسارات أمنية.

٤. **سياسة الأمن السيبراني:** يجب أن يكون لدى الجامعات سياسات وإجراءات مناسبة للأمن السيبراني وتحديثها بانتظام. ويجب أن تتضمن هذه السياسات

توعية الطلبة بممارسات الأمن السيبراني والامتثال لقواعد الاستخدام الآمن للتكنولوجيا وشبكات الجامعة.

٥. **الاستجابة للحوادث الأمنية:** يجب أن تكون الجامعات مستعدة للاستجابة للحوادث الأمنية مثل المتسللين أو الهجمات الإلكترونية، ويجب توفير آليات الإبلاغ والتحقيق في الحالات المشبوهة، واتخاذ التدابير اللازمة لحماية البيانات والمعلومات.

ويهدف دور الجامعة في رفع مستوى الوعي بإجراءات الأمن السيبراني للطلبة إلى تزويدهم بالمهارات اللازمة للحفاظ على أمن المعلومات الشخصية والتفاعل مع التكنولوجيا والأمن السيبراني. وهذا يزيد من حماية الطلبة من المخاطر السيبرانية، ويساعدهم على اتخاذ قرارات أمنية مستنيرة طوال تجربتهم الأكاديمية.

ومن الجدير بالذكر أن الجامعة يجب أن تعمل على تنفيذ هذه الإجراءات بشكل شامل ومتكامل، وتضمن أن تكون متوفرة لجميع الطلبة سواء عن طريق توفير الموارد والتدريب اللازم أو عن طريق توفير الدعم الفني والتقني الملائم.

بشكل عام، يتعين على الجامعة أن تتبنى نهج شمولي للتوعية السيبرانية للطلبة، وتعزز ثقافة الأمن السيبراني بينهم من خلال توفير المعلومات والتدريبات والموارد اللازمة، ويمكن أن تشمل هذه الجهود:

١. تنظيم ورش عمل وندوات توعوية للطلبة حول أمن المعلومات والتهديدات السيبرانية الشائعة والطرق المناسبة للتعامل معها.

٢. توفير موارد تعليمية عبر الإنترنت متاحة للطلبة تشرح المفاهيم الأساسية للأمن السيبراني وتوفر نصائح وإرشادات عملية.

٣. إشراك الطلبة في تدريبات تفاعلية تعزز مهاراتهم في اكتشاف ومعالجة التهديدات السيبرانية المحتملة.

٤. توفير قنوات اتصال آمنة للطلبة للإبلاغ عن حالات الاختراق أو الاشتباه في نشاطات سيبرانية غير مشروعة.

٥. العمل على تطوير سياسات وإجراءات الأمن السيبراني المناسبة والتأكد من توافرها وفهمها من قبل الطلاب.

٦. التعاون مع الشركاء الخارجيين المتخصصين في مجال الأمن السيبراني لتوفير التوجيه والارشاد

في الختام، يمكن القول أن الأمن السيبراني أصبح تحديًا ملحًا في عالم يعتمد بشكل متزايد على التكنولوجيا، يتطلب الأمر جهودًا مستمرة لحماية البيانات والأنظمة الإلكترونية من الهجمات السيبرانية، وضمان استمرارية وسلامة المعلومات.

الدراسات السابقة:

هدفت دراسة (المطرفي، والفراني، ٢٠٢٣) إلى الكشف عن فاعلية مقرر إلكتروني مقترح لتنمية الوعي المعرفي بالأمن السيبراني لطالبات المرحلة الثانوية بمدينة جدة، واستخدمت الدراسة المنهج شبه التجريبي، وتكونت عينة الدراسة من (٢٦) طالبة بالصف الأول الثانوي بجدة، ولتحقيق أهداف الدراسة قامت الباحثتان بتطبيق اختبار الوعي المعرفي بالأمن السيبراني على عينة الدراسة قبل وبعد تطبيق المقرر الإلكتروني المقترح، أظهرت النتائج فاعلية المقرر الإلكتروني المقترح في تنمية الوعي المعرفي بالأمن السيبراني لطالبات المرحلة الثانوية بمدينة جدة، وقدمت الدراسة مجموعة من التوصيات من أهمها الاستفادة من المقرر الإلكتروني المقترح الذي أعدته الباحثتان كمقرر للأمن السيبراني لطالبات مدارس المرحلة الثانوية بمدينة جدة ومناطق المملكة العربية السعودية الأخرى.

بينما استهدفت دراسة (توفيق، ومرسي، ٢٠٢٣) التعرف على متطلبات تحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس، أهم المعوقات التي تحول دون تحقيق هذه المتطلبات من وجهة نظر أعضاء هيئة التدريس بجامعة بنها، واستخدمت الدراسة المنهج الوصفي لتحقيق أهدافها، من خلال إعداد استبانة لتعرف أهم متطلبات تحقيق الأمن السيبراني بجامعة بنها في ظل التحول الرقمي، على عينة بلغ قوامها (٢٤٨) عضو هيئة تدريس، وتوصل البحث إلى اتفاق العينة على متطلبات تحقيق الأمن السيبراني بجامعة بنها

في ظل التحول الرقمي، والتي تمثلت في مجموعة من المتطلبات التقنية والمادية والبشرية والمعرفية، ومعوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها.

في حين أن دراسة (عبد السلام، ٢٠٢٣) هدفت إلى معرفة الوضع الراهن لإستراتيجيات الأمن الأسري السيبراني التي يستخدمها أولياء الأمور (الآباء / الأمهات) في مواجهه أنماط التنمر الإلكتروني في المجتمع المصري، واستخدمت الدراسة المنهج الوصفي، وتكونت عينة الدراسة من (٩٥٤) من الآباء والأمهات من ثمانية محافظة بجمهورية مصر العربية، واعتمدت على مقياس التنمر الإلكتروني واستبانة استراتيجية الأمن الأسري السيبراني كأدوات للدراسة، وأشارت نتائج الدراسة إلى أن معظم أفراد عينة أولياء الأمور أكدوا انتشار أنماط التنمر الإلكتروني بدرجات مختلفة، وأكثر استراتيجيات التي يميل لاستخدامها أولياء الأمور هي (الحماية والتجنب) أكثر من (التأقلم والهجوم) في مواجهة التنمر الإلكتروني، وأكدت الدراسة على ضرورة تقديم برامج لتنمية وعي أفراد الأسرة بمفهوم الأمن السيبراني عبر وسائل الإعلام المختلفة، ضرورة عقد برامج تأهيلية للأسر عن استراتيجيات الأمن الأسري السيبراني لسلامة أبنائهم من التنمر الإلكتروني.

أما دراسة (Duman, ٢٠٢٢) هدفت إلى تحديد السلوكيات المتعلقة بالأمن السيبراني لمستخدمي الإنترنت من طلاب كلية علوم الرياضة، وتم استخدام مقياس توفير الأمن السيبراني الشخصي الذي طوره (إيرول)، ووفقاً لنتائج الدراسة تختلف سلوكيات الطلاب المتعلقة بالأمن السيبراني حسب الجنس والاستخدام اليومي للإنترنت ومستوي المعرفة حول الأمن السيبراني، كما أن طلاب علوم الرياضة لديهم وعي عال بالأمن السيبراني ولكنهم لا يتخذون إجراءات احتياطات كافية وحماية الخصوصية، لذلك على الطلاب على علم بممارسات الأمن السيبراني ونوع الاحتياطات التي ينبغي اتخاذها.

كما قام (Raju, ٢٠٢٢) بدراسة هدفت إلى التوعية بالأمن السيبراني في استخدام المنصات الرقمية بين الطلاب في مؤسسات التعليم العالي، واقتصرت الدراسة على طلاب كلية علوم الكمبيوتر والرياضيات بجامعة UiTM Terengganu وتكونت عينة الدراسة من (١١٠) طالب بالمرحلة الجامعية، واعتمدت على الاستبيان كأداة

للدراسة لتحليل مستوي الوعي بالأمن السيبراني، وأظهرت نتائج الدراسة على الرغم من أن طلاب كلية علوم الكمبيوتر أظهروا مستوي لائق من الوعي ببعض جوانب الأمن السيبراني مثل الهجوم السيبراني، والتسلط عبر الإنترنت، والمعلومات الشخصية إلا أنه لا يوجد عمق مناسب للمعرفة بالأمن السيبراني، ولا يزال الطلاب غير مدركين لكيفية حماية بياناتهم وخصوصياتهم.

ودراسة (العتيبي، ٢٠٢٢) هدفت إلى التعرف على درجة الوعي بماهية الأمن السيبراني لدى عينة من الأسر بمحافظة جده، وتحديد أهم الأشكال التي يتعامل معها الأمن السيبراني ولها علاقة بالمجتمع السعودي، واعتمدت الدراسة على منهج المسح الاجتماعي، وتكونت عينة الدراسة من (٦٨١) من الأسر السعودية بمحافظة جدة، واعتمدت على الاستبيان كأداة رئيسة لجمع المعلومات، وأشارت نتائج الدراسة أن الوعي بماهية الأمن السيبراني لدى العينة جاء بدرجة مرتفعة وتمثلت درجات الوعي في تجنب الكشف عن أي بيانات شخصية أو عائلية أثناء تصفح الإنترنت، ووجود معرفة لديهم بمخاطر فيروسات الهواتف الذكية، وأشارت عينة الدراسة إلى أن هناك معوقات اجتماعية لتحقيق الوقاية من جرائم الأمن السيبراني.

وهدفت دراسة (الحبيب، ٢٠٢٢) إلى التعرف على درجة الوعي بمفاهيم الأمن السيبراني وتطبيقاته، وأبرز سبل تعزيز الوعي بالأمن السيبراني لدى طلبة وطالبات الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية من وجهة نظرهم، واستخدمت الدراسة المنهج الوصفي المسحي، وتمثلت أهم نتائج الدراسة في أن عينة الدراسة يملكون درجة عالية من الوعي بمفاهيم وتطبيقات الأمن السيبراني، ويرجع ذلك إلى سعة اطلاع أفراد العينة، وأوصت الدراسة بتفعيل كلية التربية لعدد من الإجراءات التي تساهم في رفع درجة الوعي بالأمن السيبراني لدى طلبة الدراسات العليا بكلية التربية.

كما هدفت دراسة (Ahmed et al., ٢٠٢١) إلى التعرف على مستوى الوعي لدى معلمي المدارس بتطوير الأمن السيبراني لطلابهم بناء على دراسة حالة لمدارس إمارة عجمان الخاصة في دولة الإمارات العربية المتحدة، واعتمدت الدراسة على (١٧٢) معلم، واعتمدت على المنهج الوصفي، وتم تطبيق استبيان وعي المعلمين

بإجراءات الأمن السيبراني لطلابهم كأداة للدراسة، وأوضحت نتائج الدراسة أن مستوى وعي معلمي المدارس حظى بمستوى مقبول نحو حماية وسلامة طلابهم، ومستوى وعي المعلم بالأمن السيبراني يجب أن يكون بمستوي عال حتي يقابل مستوى طلبة المدارس حيث يتمتع طلاب المدارس بمستوي عال في دولة الإمارات بالوصول إلى الإنترنت، كما أشارت أيضاً إلى وجود علاقة بين التخصص ووعي المعلمين تجاه الأمن السيبراني يعزي إلى وجود دالة إحصائية بين استجابة معلمي الرياضيات واللغة العربية لصالح معلمي اللغة الرياضيات.

أما دراسة (Alharbi & Tassaddiq, ٢٠٢١) هدفت إلى تقصي وتقييم مستوي الوعي بالأمن السيبراني لدى عينة من طلاب المرحلة الجامعية في جامعة المجمعة باستخدام استبيان إلكتروني لقياس مدي وعي طلاب الجامعة بالأمن السيبراني وأمان استخدام الانترنت، وتكونت عينة الدراسة من (٥٧٦) طالب بجامعة المجمعة، وأشارت نتائج الدراسة إلى أن ضرورة زيادة مستوي الوعي بالأمن السيبراني لدى طلاب جامعة المجمعة وذلك من خلال تطوير أدوات فعالة وتقنيات وتقديم برامج توعية حول الأمن السيبراني للطلاب.

كما ألقى (التيماني، ٢٠٢١) الضوء على واقع الأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بأمن المعلومات، واستخدمت الدراسة المنهج الوصفي، واعتمدت على المقابلة كأداة لجمع المعلومات والبيانات على المختصين بالأمن السيبراني في مدينة الرياض، وتوصلت الدراسة إلى الاهتمام الحكومي بالأمن السيبراني بدأ بشكل مبكر قبل ادراك أفراد المجتمع لهذا المفهوم، وتوصلت الدراسة إلى أن أكثر العوامل التي تزيد من فرص حدوث الجرائم السيبرانية هو ضعف الوعي لدى الأفراد ومشاركتهم معلوماتهم الشخصية مع الآخرين .

كما قام (الحارثي، ونصر، ٢٠٢١) في دراسته من التحقق من فاعلية برنامج تجريبي لتعزيز بعض جوانب الصحة النفسية الإيجابية والهوية الثقافية، والأمن النفسي لدى طلاب جامعة الباحة المعرضين لخطر الإيذاء السيبراني، وتكونت عينة الدراسة من (٤٠) طالب من طلاب مرحلة البكالوريوس من كلية التربية جامعة الباحة، واعتمدت على المنهج شبه التجريبي، واستخدمت مقياس الهوية الثقافية، ومقياس الأمن

النفسي، ومقياس الإيذاء السيبراني، والبرنامج التدريبي التوكيدي، وأسفرت النتائج عن فاعلية التدريب في تعزيز الصحة النفسية الإيجابية لدى الطلبة عينة الدارسة بما يضمن لهم القدرة على التصدي لكل صور الإيذاء بعافية نفسية، وتحسين الهوية الثقافية لدى الطلبة وهوية الطالب الفردية والجماعية والاعتزاز بها في مواجهة ما يتعرضون له وتحررهم من الخوف كأكثر عوامل تهديد الأمن النفسي.

وأيضا دراسة (Hasan, Tasji, ٢٠٢١) هدفت إلى التحقق من إجراءات الأمن المعلوماتي في جامعة طيبة بالمملكة العربية السعودية، وتم إجراء استطلاع رأي على الإنترنت لقياس مدى وعي الطلاب وأعضاء هيئة التدريس والموظفين فيما يخص ثلاث محاور: السياسات الأمنية لجامعة طيبة، وجرائم أمن المعلومات، والإجراءات الأمنية الأساسية، وأظهرت النتائج نقص الوعي الأمني خاصة بين طلاب البكالوريوس، وأوصى الباحثان بتحسين التوعية الأمنية، وتقديم دورات تدريبية وورش عمل لرفع وعي الطلاب بالأمن السيبراني.

وهدفت دراسة (Haseski, ٢٠٢٠) إلى تحديد أثر مهارات الأمن السيبراني الفردية لدى معلمي ما قبل الخدمة على اتجاهاتهم نحو التعليم بمساعدة الحاسب، وتكونت عينة الدراسة من (٢٤١) معلم من معلمي ما قبل الخدمة في أقسام مختلفة بجامعة مانيسا جلال بايار، كلية التربية خلال العام الدراسي ٢٠١٩/ ٢٠٢٠، وتم جمع البيانات باستخدام "مقياس توفير الأمن السيبراني الشخصي"، "والموقف تجاه مقياس التعليم بمساعدة الكمبيوتر"، وأظهرت نتائج الدراسة ضرورة تحسين كفاءة المعلمين قبل الخدمة في مجال الأمن السيبراني، كما حصل المعلمون الذين يمتلكون كمبيوتر شخصي على أعلى درجات في الحفاظ على الأمن السيبراني الشخصي.

وأشارت دراسة (Karagozlu, ٢٠٢٠) إلى تحديد سلوكيات المعلمين قبل الخدمة فيما يتعلق بالأمن السيبراني، واعتمدت الدراسة على المنهج الوصفي، وتكونت عينة الدراسة من (١٤٤) معلم قبل الخدمة الملتحقين بكلية التربية جامعة قبرص بفصل الربيع ٢٠١٩ – ٢٠٢٠ ، وأشارت نتائج الدراسة أن الطلاب عينة البحث قد اتخذوا تدابير لحماية الخصوصية عندما لاحظوا أشخاص ومواقف غير موثوقة في بيئة الإنترنت، وأن الطلاب الذكور يظهرون سلوكيات أكثر وعياً فيما يتعلق بالبعد

الاحترازي ويستطيعون حماية أجهزتهم المتصلة بالإنترنت بشكل مناسب ضد الفيروسات.

أما دراسة (الخضري وآخرون، ٢٠٢٠) هدفت الدراسة إلى توجيه التربويين والمهتمين بالعملية التعليمية إلى أهمية الأمن السيبراني وطرق تطبيقه بين طلاب الجامعات السعودية، وتكونت عينة الدراسة من (٣٢٠) طالب في الجامعات السعودية و(٦٠) عضو هيئة تدريس و(٤٠) إداري بالجامعة، واعتمدت على الاستبيان كأداة لجمع المعلومات، وأوصت الدراسة بزيادة الاهتمام بتوعية المؤسسات الجامعية السعودية بتطبيق معايير أمن المعلومات، وتنظيم دورات تدريبية للطلاب وأعضاء هيئة التدريس والإداريين لتدريبهم على تطبيق أمن المعلومات.

وقامت دراسة (السمحان، ٢٠٢٠) بمعرفة متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، واستخدمت الاستبانة كأداة لجمع المعلومات من عينة عددها (٤٨٧) من العاملين بجامعة الملك سعود بالرياض لتعرف وجهة نظرهم حول كيفية تحقيق الأمن السيبراني بالجامعة، وأوصت الدراسة بضرورة إدراج مجال الفضاء السيبراني ضمن مناهج التعليم في بالمملكة، تشجيع مجالات البحث العلمي والابتكار في مجال الأمن السيبراني، وتوعية العاملين بكافة مؤسسات الدولة وتنمية المعايير المهنية الاحترافية لديهم بمجال الأمن السيبراني.

وقدم (الصانع، ٢٠٢٠) دراسة هدفت إلى معرفة درجة وعي المعلمين بالأمن السيبراني وعلاقته بتطبيق أساليب حديثة لحماية الطلبة من مخاطر الإنترنت، كأساليب تعزيز القيم والهوية الوطنية لديهم، وتكونت العينة من (١٠٤) معلم ومعلمة في مدارس مدينة الطائف الحكومية والأهلية، واستخدمت الدراسة المنهج الوصفي الارتباطي، ومقياس لتحديد درجة الوعي بالأمن السيبراني لدى المعلمين، وأساليب حماية الطلبة من مخاطر الإنترنت وأساليب تعزيز القيم والهوية الوطنية لدى الطلبة، وأظهرت نتائج الدراسة ارتفاع وعي المعلمين بالأمن السيبراني في مجال الأجهزة الخاصة والمحمولة من مخاطر الاختراق الإلكتروني والهجمات السيبرانية، وفي درجة استخدامهم لأساليب حماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية لدى الطلبة في مجالات الأهداف الدراسية، وطرق التدريس، والأنشطة،

والمشاريع، وأساليب التقويم، ووجدت علاقة ارتباطية موجبة ومتوسطة بين وعي المعلمين بالأمن السيبراني واستخدامهم لأساليب حماية الطلبة من مخاطر الإنترنت.

وفي دراسة (الجندي، ومحمد، ٢٠١٩) التي هدفت إلى التعرف على دور الممارسات التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة، وتكونت عينة الدراسة من (٨٠) طالبة من قسم الحاسب الآلى بالكلية الجامعية بأضم جامعة أم القري، واعتمدت الدراسة على المنهج شبه التجريبي، واستخدمت بطاقة ملاحظة مهارات الأمن المعلوماتي، مقياس دقة التطبيق العملي للأمن المعلوماتي كأدوات للدراسة، وتوصلت الدراسة إلى تأثير الممارسة التطبيقية للأمن السيبراني في تنمية مهارات ودقة التطبيق العملي للأمن المعلوماتي لدى الطالبات، قدرة الطالبة على استيعاب وامتلاك المقدرة على وصف سيناريو الهجوم القائم على الوصول عن بعد وتحديد الأجزاء المكونة للهجوم، وامتلاك الطالبة المعرفية الأولية حول سيناريوهات الهجوم مثل البرمجة عبر المواقع، واستغلال المتصفح الإلكتروني.

أما دراسة (صائغ، ٢٠١٨) هدفت الدراسة إلى الكشف عن العلاقة بين وعي أفراد الأسرة بمفهوم الأمن السيبراني وبين الاحتياطات الأمنية التي يتخذونها للوقاية من الجرائم الإلكترونية، واستخدمت الدراسة المنهج الوصفي التحليلي، واعتمدت على استبيان وعي أفراد الأسرة بمفهوم الأمن السيبراني وبين احتياطاتهم الأمنية من الجرائم الإلكترونية كأداة للدراسة، وتكونت عينة الدراسة من (٢١٥) فرد من أفراد الأسرة ذكور وإناث من فئات مختلفة من مدينة مكة المكرمة، وتوصلت الدراسة إلى وجود علاقة بين وعي أفراد الأسرة بمفهوم الأمن السيبراني وبين الاحتياطات الأمنية التي يتخذونها للوقاية من الجرائم الإلكترونية كما أن هذه الفروق ترجع للمستوي التعليمي لأفراد الأسرة.

في حين كشفت دراسة (YILMAZ, et al., ٢٠١٧) عن ملفات تعريف أمن الإنترنت والوعي باستخدام الكمبيوتر للطلاب الذين يدرسون في المدرسة الثانوية، واستخدمت الدراسة المنهج الوصفي، وتم جمع البيانات من (٢٠٢٩) طالبا بالمرحلة الثانوية يدرسون في المدارس الثانوية في مقاطعة بارتين في تركيا باستخدام

الاستبيان، وأشارت النتائج إلى أن غالبية الطلاب ليس لديهم وعي كافي فيما يتعلق بأمن المعلومات والوعي باستخدام الكمبيوتر.

ودراسة (Zhang, Li &Deng, ٢٠١٧) هدفت إلى فهم سلوك مستخدمي الهواتف الذكية فيما يختص بأمن المعلومات، وتم عمل استطلاع رأي على الإنترنت لدراسة هذا السلوك لمستخدمي الهواتف الذكية في الصين، وتم تحليل البيانات باستخدام التحليل الوصفي، واتضح من نتائج الدراسة وجود مخاوف جدية بشأن أمن المعلومات في استخدام الهواتف الذكية في الصين، بما في ذلك الجهل بالمعلومات الأمنية في تنزيل التطبيقات واستخدامها، وعدم كفاية إعدادات الهاتف، والتمكين غير الملائم للأدوات المساعدة الإضافية.

إجراءات الدراسة الميدانية:

أولا: منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي، وهو المنهج الملائم لطبيعة الدراسة وأهدافها، لأنه يعمل على تفسير وتحليل المعلومات واستخلاص دلالات، تفيد في الوقوف على درجة وعي أولياء الأمور بإجراءات الأمن السيبراني اللازمة للطفل في مرحلة الطفولة المبكرة حيث يعرف المنهج الوصفي: "بأنه عدد من الإجراءات البحثية التي تصف الظاهرة اعتماداً على جمع البيانات ولحقائق وتصنيفها ومعالجتها وتحليلها لاستخلاص دلالتها والوصول إلى نتائج وتعميمات عن الظاهرة موضع الدراسة" (الرشيدي، ٢٠٠٠، ٣٢).

ثانيا مجتمع وعينة الدراسة:

تألف مجتمع الدراسة من طلبة كليات التربية بجامعة مطروح، وقد تم اختيار عينة عشوائية بسيطة بحيث بلغ عدد أفراد عينة الدراسة (١٢٥) طالب وطالبة.

ثالثا: أدوات الدراسة:

استخدمت الباحثتان أداة الاستبانة في جمع البيانات وتم بناؤها من خلال المصادر التالية:

- الأدبيات المتعلقة بهذا الموضوع.

- الدراسات السابقة والإطار النظري.
- الاستعانة بذوي الاختصاص والخبرة في هذا المجال.

رابعا: وصف أداة الدراسة:

تم تصميم إستبيان الوعي باجراءات الأمن السيبراني لدي طلبة كليات التربية وهي إستبانه مغلقة مقسمة إلى ثلاث محاور كالتالي:

- تضمن بيانات عامة عن الطالب/ الطالبة.
- المحور الأول: يتضمن درجة وعي الطلاب بإجراءات الأمن السيبراني الخاصة بالأجهزة المتصلة بالإنترنت.
- المحور الثاني: يتضمن درجة وعي الطلاب بإجراءات الأمن السيبراني الخاصة بالطالب نفسه.
- المحور الثالث: يتضمن سبل تعزيز الوعي السيبراني لدى طلاب الكلية.

وقد استخدمت الدراسة "مقياس ليكرت ذو التدريج الخماسي" للتعبير عن استجابات أفراد عينة الدراسة على فقرات الاستبانة على هذا النحو: (موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة)، بحيث يتم إعطاء القيمة الوزنية (٥) إلى موافق بشدة، (٤) إلى موافق، (٣) محايد، (٢) إلى غير موافق، والقيمة الوزنية (١) إلى غير موافق بشدة.

صدق أداة الدراسة:

١- الصدق الظاهري للأداة: عرضت الأداة بعد تصميمها في صورتها الأولية بما يتناسب مع أهدافها على مجموعة من المحكمين المختصين. وقد أعدت استمارة خاصة لاستطلاع آرائهم والاستفادة من ملاحظاتهم في تعديل صياغة الأداة ووضعها في صورتها النهائية.

٢- الصدق البنائي للأداة: للتحقق من صدق الاتساق الداخلي للاستبانة، تم حساب معامل ارتباط بيرسون؛ للتعرف على درجة ارتباط كل عبارة من عبارات الاستبانة بالدرجة الكلية للمحور.

جدول (١) يوضح معاملات ارتباط بيرسون بين المعدل الكلي لفقرات الاستبانة ومعدل كل محور من محاور الدراسة.

المحاور	الارتباط
المحور الأول	.٨٦**
المحور الثاني	.٩٠**
المحور الثالث	.٤٢**

من خلال الجدول (١) يتضح بأن معامل الارتباط بين المعدل الكلي لفقرات الاستبانة ومعدل كل محور من محاور الاستبانة تتراوح بين (٠.٩٠- ٠.٤٢) وهذا يشير إلى صدق الاتساق الداخلي لمحاور الاستبانة، وأن معاملات الارتباط جميعها بين محاور الاستبيان وبين المجموع الكلي له، دالة إحصائياً عند مستوى (٠.٠٥)، وهذا يدل على أن المحاور جميعها تتميز بدرجة صدق عالية.

ثبات الاستبانة:

ولحساب ثبات الاستبانة تم تطبيقها على عينة من أولياء الأمور بلغ عددهم (٣٠) طالبة، وبعد أسبوعين تم إعادة التطبيق للاستبانة على العينة ذاتها، وأعطت معاملات ثبات مقبولة، وتم التأكد من ثبات الاستبانة من خلال طريقة معامل ألفا كرونباخ.

جدول (٢) معامل ثبات ألفا كرونباخ لمحاور الدراسة.

المحور	عدد البنود	معامل ثبات ألفا كرونباخ	النسبة
المحور الأول	١٣	٠.٨٠	%٨٠.٥
المحور الثاني	١٩	٠.٨٠	%٨٠.٤
المحور الثالث	٦	٠.٨٤	%٨٤.٣
المحور الكلي	٣٨	٠.٨٨	%٨٧.٩

ويتضح من جدول (٢) أن قيمة معامل ألفا كرونباخ للاستبانة كلية بلغت (٠.٨٨)، وهي نسبة مناسبة ومرتفعة، وهذا يؤكد على ثقة الباحثة لاستخدام الاستبانة كأداة لجمع المعلومات، والوثوق بنتائج تطبيقها، وبذلك تكون قد تأكدت من صدق وثبات الاستبانة في صورتها النهائية، وأنها صالحة للتطبيق على عينة الدراسة الأساسية، مما يجعلها على ثقة تامة بصحة الاستبانة وصلاحيتها لجمع البيانات اللازمة.

إجراءات تطبيق الدراسة:

بعد التأكد من صدق (الاستبانة) وثباتها، وصلاحيتها للتطبيق، تم تطبيقها ميدانياً باتباع ما يلي:

١. كتابة الاستبانة باستخدام نماذج جوجل.
٢. إرسال الرابط لطلبة كليات التربية بجامعة مطروح عبر البريد الإلكتروني بالإضافة إلى مجموعات الواتس آب.
٣. جمع الاستبانات، وقد بلغ عددها (١٢٥) استبانة.

أساليب المعالجة الإحصائية:

اعتمدت الباحثة في جمع بيانات ومعلومات الدراسة بالاعتماد على الإطار النظري والدراسات السابقة، وقامت بتبويبها وتفريغ البيانات في جداول، ثم استخدمت الباحثة لتحليل البيانات البرنامج الإحصائي الخاص بالعلوم الإنسانية والاجتماعية spss لتحليل البيانات، وبعد ذلك تم حساب المقاييس الإحصائية التالية:

- التكرارات، والنسب المئوية.
- المتوسط الحسابي الموزون (المرجح) "Weighted Mean".
- المتوسط الحسابي "Mean".
- الانحراف المعياري "Standard Deviation".
- معامل ارتباط بيرسون.
- معامل ألفاكرونباخ.

خامسا: تحليل النتائج وتفسيرها:

١- **للإجابة عن السؤال الأول: ما درجة وعي طلبة كليات التربية بإجراءات الأمن السيبراني الخاصة بالأجهزة المتصلة بالإنترنت؟**، تم حساب المتوسط الحسابي،

والانحراف المعياري، والرتب لاستجابات أفراد عينة الدراسة على عبارات المحور، وجاءت النتائج كما يلي:

جدول (٣) استجابات أفراد عينة الدراسة حول درجة وعي طلبة كليات التربية بإجراءات الأمن السيبراني الخاصة بالأجهزة المتصلة بالإنترنت.

م	العبـــارات	المتوسط الحسابي	الانحراف المعياري	الرتبة	الدرجة
١	أستخدم تطبيقات لحجب المواقع الإباحية.	٤.٠٠	١.٥٢	٦	مرتفعة
٢	أستخدم البرامج الأصلية من الشركات بدلا من البرامج الغير موثوقة.	٤.١٦	١.٠١	٤	مرتفعة
٣	أحذف البرامج مجهولة المصدر من الأجهزة الإلكترونية.	٤.٤٥	.٨٩	١	مرتفعة
٤	أعطل خدمات الوصول إلى موقعي في التطبيقات المحملة على جهازي.	٣.٦٦	١.٠٢	٩	متوسطة
٥	أحدث نظام التشغيل بصفة مستمرة.	٤.٢٥	.٨٨	٣	مرتفعة
٦	أحدث البرامج والتطبيقات بصفة مستمرة.	٤.٣٥	.٨٥	٢	مرتفعة
٧	أهتم بتحميل برامج آمنة لمكافحة الفيروسات.	٣.٤٥	١.٣١	١١	متوسطة
٨	أحدث البرامج المضادة للفيروسات بشكل مستمر.	٣.٥٩	١.٣٥	١٠	متوسطة
٩	أختار كلمة مرور قوية، وأهتم بتغييرها بصفة دورية.	٣.٦٩	١.٣٢	٨	مرتفعة
١٠	أقوم بإعداد نسخة احتياطية للبيانات المخزنة في جهازي على الخدمة السحابية.	٣.٨٤	١.٢٧	٧	مرتفعة
١١	أغير إعدادات جهازي بشكل مستمر كي لا تخترق شبكة الواي فاي.	٣.٢٣	١.٣٣	١٢	متوسطة
١٢	أستخدم في جهازي تقنية التحقق الثنائي (كلمة المرور – البصمة).	٤.٤٥	١.١٧	١	مرتفعة
١٣	أعي خطورة الاتصال بشبكات الإنترنت العامة.	٤.٠٠	١.٣٠	٥	مرتفعة

يتضح من جدول (٣) السابق: أن المتوسطات الحسابية الوزنية لاستجابات أفراد العينة على فقرات هذا المحور قد تراوحت بين (٤.٤٥– ٣.٢٣) وهو متوسط حسابي درجته من متوسطة إلى مرتفعة وهذا يشير إلى مدى درجة وعي طلاب كليات التربية

بإجراءات الأمن السيبراني اللازمة والخاصة بالأجهزة المتصلة بالإنترنت، حيث يتضح أن العبارة " أستخدم في جهازي تقنية التحقق الثنائي (كلمة المرور– البصمة)." قد أخذت المرتبة الأولى باستجابة مرتفعة بلغت (٤.٤٥)، وهذا يشير إلى وعي الطلاب بضرورة استخدام تقنية التحقق الثنائي للحد من المخاطر السيبرانية الخاصة بالأجهزة، ويتضح أيضا أن العبارة " أغير إعدادات جهازي بشكل مستمر كي لا تخترق شبكة الواي فاي." قد أخذت المرتبة الأخيرة باستجابة متوسطة بلغت (٣.٢٣)، وهذا يؤكد على تردد الطلاب حول اتخاذ إجراء يخص تغيير إعدادات الأجهزة بشكل مستمر كي لا يتم اختراق شبكة الواي فاي إما لقلة الاهتمام بذلك الأمر أو وقتهم المحدود نتيجة للدراسة، وهذا ما يختلف مع دراسة (YILMAZ, et al., ٢٠١٧)، حيث انتهت إلى أن غالبية الطلاب ليس لديهم وعي كافي فيما يتعلق بأمن المعلومات والوعي بالاستخدام الآمن للكمبيوتر.

يتبين من الجدول السابق وجود درجة وعي تتراوح بين متوسطة ومرتفعة لدى طلاب كليات التربية بإجراءات الأمن السيبراني اللازمة والخاصة بالأجهزة المتصلة بالإنترنت، وقد يرجع ذلك إلى عدة عوامل من أهمها: التوعية بالأمن السيبراني لدى تلك الفئة من جهة الجامعات.

٢- **وللإجابة عن السؤال الثاني:** ما درجة وعي طلبة كليات التربية بإجراءات الأمن السيبراني الخاصة بالطالب نفسه؟، تم حساب المتوسط الحسابي، والانحراف المعياري، والرتب لاستجابات أفراد عينة الدراسة على عبارات المحور، وجاءت النتائج كما يلي:

جدول (٤) استجابات أفراد عينة الدراسة حول درجة وعي طلبة كليات التربية بإجراءات الأمن السيبراني الخاصة بالطالب نفسه.

م	العبارات	المتوسط الحسابى	الانحراف المعياري	الرتبة	الدرجة
١٤	لا أنشر أي معلومة خاصة بأصدقائي بدون علمهم على الإنترنت.	٤.٦٩	.٧٧	١	مرتفعة
١٥	لا أنشر أو أردد الشائعات على مواقع التواصل الاجتماعى.	٤.٦٣	.٩٧	٢	مرتفعة
١٦	أتجنب الحديث مع الغرباء عبر مواقع التواصل الاجتماعى.	٤.٤٠	.٩٨	٥	مرتفعة
١٧	أرفض طلبات الصداقة من حسابات مجهولة المصدر.	٤.٦٢	.٨١	٣	مرتفعة
١٨	أحذف الحسابات المزعجة والرسائل المجهولة دون أن يفتحها.	٤.٣٩	.٩٦	٦	مرتفعة
١٩	أتجنب إرسال معلوماتي الشخصية عبر الرسائل النصية أو البريد الإلكتروني.	٤.٦٩	.٧٣	١	مرتفعة
٢٠	أتجنب نشر صوري الشخصية والعائلية من خلال تطبيقات التواصل الاجتماعى.	٤.٠٨	١.٠٢	٩	مرتفعة
٢١	أستطيع رفع بلاغ عن الإساءات التي قد أتعرض لها في مواقع التواصل الاجتماعى.	٤.٠٠	١.٢٦	١٠	مرتفعة
٢٢	أستخدم كلمات سر مختلفة لكل حساب شخصي على الإنترنت.	٣.٣٦	١.٤٥	١٣	متوسطة
٢٣	أبلغ عن أي صفحة تنشر أخبارا ملفقة عن الشخص.	٣.٢٨	١.٥٢	١٤	متوسطة
٢٤	أبلغ إدارة الموقع عن أية حسابات تضايقني وتتنمر على.	٣.٥٧	١.٣٤	٨	متوسطة
٢٥	على دراية بإجراءات التبليغ عن الجرائم الإلكترونية للجهات الرقابية في الدولة.	٣.٥٥	١.٤٥	١١	متوسطة
٢٦	أحدد عدد ساعات لاستخدام الأجهزة الإلكترونية في اليوم.	٢.٧٢	١.٤٣	١٦	متوسطة
٢٧	أغطى الكاميرا في حال عدم استخدامها.	٢.٣٠	١.٣٩	١٧	منخفضة
٢٨	أبلغ عن المرسل في حالة استلام محتوى ضار أو رسائل جنسية.	٤.٢٠	١.١٩	٨	مرتفعة
٢٩	الشراء عبر الإنترنت من مواقع موثوقة.	٣.٤٤	١.٣٩	١٢	متوسطة
٣٠	استخدام حسابات المصارف والفيزا ووسائل الدفع الأخرى في المواقع الموثوق فيها.	٣.٢٧	١.٦٦	١٥	متوسطة
٣١	تجنب وضع البيانات والصور الشخصية على مواقع التواصل الاجتماعي إلا للضرورة.	٤.٢٢	١.٠٤	٧	مرتفعة
٣٢	استخدام المحتوى المرخص من الناشر أو المؤلف.	٤.٥١	.٦٠	٤	مرتفعة

يتضح من الجدول (٤): أن المتوسطات الحسابية الوزنية لاستجابات أفراد العينة على فقرات هذا المحور قد تراوحت بين (٤.٦٩– ٢.٣٠) وهو متوسط حسابي درجته متوسطة وهذا يشير إلى مستويات متوسطة من وعي الطلاب بإجراءات الأمن السيبراني الخاصة بالطالب نفسه، حيث يتضح أن العبارة " أتجنب إرسال معلوماتي الشخصية عبر الرسائل النصية أو البريد الإلكتروني." قد أخذت المرتبة الأولى باستجابة مرتفعة بلغت (٤.٦٩)، وهذا يشير إلى وعي الطلاب بضرورة عدم إرسال أي معلومات شخصية عبر الرسائل لإمكانية وصولها لأشخاص غير مرغوبين، وبالتإلى يتم الاستيلاء على جميع الحسابات الشخصية التي تخص تلك المعلومات، وهذا يتفق مع دراسة (Raju, ٢٠٢٢) حيث انتهت إلى وجود مستوى لائق من الوعي بالأمن السيبراني لدى طلبة الكليات إلا أنه لا يوجد عمق مناسب للمعرفة بالأمن السيبراني، ولا يزال الطلبة غير مدركين لكيفية حماية بياناتهم الشخصية وخصوصياتهم.

وقد حصلت عبارة " أغطي الكاميرا في حال عدم استخدامها." على درجة منخفضة الاستجابة (٢.٣٠) وهذا يشير إلى عدم اهتمام الطلاب بتغطية الكاميرا في حال عدم استخدامها، وقد يرجع ذلك إلى عدم وعيهم بخطورة ذلك الإجراء، وما قد يحدث من المتطفلين إذا تمكنوا من فتح الكاميرا بأي وقت يرغبون فيه بذلك.

ومن الجدول السابق يتضح وجود ضعف في وعي الطلاب بكليات التربية ببعض إجراءات الأمن السيبراني اللازمة والخاصة بالطالب نفسه، ويرجع ذلك إما إلى عدم الوعي بخطورة الإجراء نفسه أو عدم الاهتمام باتخاذ الإجراء اللازم، واتفق ذلك مع دراسة (Hasan, Tasji, ٢٠٢١) التي انتهت إلى نفس النتيجة فيما يخص ضعف درجة وعي طلاب الجامعات بإجراءات الأمن السيبراني.

٣- **وللإجابة عن السؤال الثالث: ما سبل تعزيز الوعي بإجراءات الأمن السيبراني لدى طلبة كليات التربية من وجهة نظرهم؟**، تم حساب المتوسط الحسابي، والانحراف المعياري، والرتب لاستجابات أفراد عينة الدراسة على عبارات المحور، وجاءت النتائج كما يلي:

جدول (٥) استجابات أفراد عينة الدراسة حول سبل تعزيز الوعي بإجراءات الأمن السيبراني لدى طلبة كليات التربية من وجهة نظرهم.

م	العبارات	المتوسط الحسابي	الانحراف المعياري	الرتبة	الدرجة
٣٣	إنشاء كلية التربية قسم الأمن السيبراني.	٤.٢٨	.٦٧	٤	مرتفعة
٣٤	قيام كلية التربية بتوصيف مقرر عن الأمن السيبراني يقوم أعضاء هيئة التدريس بتدريسه للطلاب.	٤.٣٩	.٦٩	٢	مرتفعة
٣٥	حضور دورات في الأمن السيبراني بشكل دوري.	٤.٢٠	.٨٣	٥	مرتفعة
٣٦	القراءة الدورية عن المخاطر السيبرانية وكيفية الوقاية منها.	٤.١٨	.٧٦	٦	مرتفعة
٣٧	توفر الجامعة نسخ أصلية من نظم التشغيل والبرامج الأساسية بأسعار مخفضة لطلاب الكلية.	٤.٣٢	.٦١	٣	مرتفعة
٣٨	تقديم دورات تدريبية لطلاب الكلية عن الأمن السيبراني بشكل دوري.	٤.٥٠	.٦٠	١	مرتفعة

يتضح من الجدول (٥): أن المتوسطات الحسابية الوزنية لاستجابات أفراد العينة على فقرات هذا المحور قد تراوحت بين (٤.٥٠– ٤.١٨) وهو متوسط حسابي درجته مرتفعة وهذا يشير إلى اهتمام طلبة كليات التربية بتعزيز إجراءات الأمن السيبراني لديهم من خلال كافة السبل المتاحة، حيث يتضح أن عبارة " تقديم دورات تدريبية لطلاب الكلية عن الأمن السيبراني بشكل دوري."، قد أخذت المرتبة الأولى باستجابة مرتفعة بلغت (٤.٥٠)، وهذا يشير إلى ضرورة تقديم تلك الدورات بشكل مستمر ودوري لا طلاع الطلبة على كل جديد في مجال إجراءات الأمن السيبراني اللازمة لهم.

وقد حصلت عبارة " القراءة الدورية عن المخاطر السيبرانية وكيفية الوقاية منها." على درجة مرتفعة الاستجابة (٤.١٨) وهذا يؤكد على ضرورة توفير الكتب والمجلات المتخصصة في الأمن السيبراني بمكتبات الكليات لتوفير مصدر المعلومات في هذا الموضوع لطلبة الكليات، وهذا يتفق مع دراسة كل من (الخضري وآخرون، ٢٠٢٠)، و(الحبيب، ٢٠٢٢) حيث أوصت بتفعيل كليات التربية عدد من الإجراءات التي تساهم في رفع وعي الطلبة بالأمن السيبراني.

ومن الجدول السابق يتضح وجود عدة سبل يمكن عن طريقها تعزيز الوعي بإجراءات الأمن السيبراني لدى طلبة كليات التربية، أهمها تقديم الدورات التدريبية بشكل دوري، وقيام كليات التربية بتوصيف مقرر عن الأمن السيبراني يتم تدريسه للطلبة، وتوفير نسخ أصلية من نظم التشغيل والبرامج بأسعار مخفضة لطلبة الكليات.

وللإجابة على السؤال الرابع: ما الفروق في درجات الوعي بإجراءات الأمن السيبراني بين طلبة كليات التربية ترجع للمتغيرات الديموغرافية للدراسة (العمر عند استخدام الإنترنت لأول مرة، الجنس، العمل بجانب الدراسة)؟، تم حساب المتوسط الحسابي، والانحراف المعياري، ونتائج اختبار (ت)، وجاءت النتائج كما يلي:

جدول (٨) فروق في وعي طلاب كليات التربية بإجراءات الأمن السيبراني تعزى لمتغير العمر عند استخدام الإنترنت لأول مرة

العمر	العدد	المتوسط الحسابي	الانحراف المعياري	ت	الدلالة
أقل من ٥	٢	١٦٦.٠٠	١.٤١	١.٩٤٣	.١٠٨
٥– ٩	١٤	١٦١.٠٠	١٨.٩٦		
١٠– ١٤	٥٨	١٤٨.٠١	١٧.٢٣		
١٥– ١٩	٤٩	١٥٠.٧٩	١٩.٢٠		
٢٠ فأكثر	٢	١٦٠.٥٠	٦.٣٦		
المجموع	١٢٥	١٥١.٠٤	١٨.٣٨		

ويتضح من جدول (٨) وجود فروق دالة إحصائيا عند مستوى دلالة (٠,٠٥) في وعي طلاب كليات التربية بإجراءات الأمن السيبراني تعزى لمتغير العمر عند استخدام الإنترنت لأول مرة، ويمكن تفسير هذه النتيجة بأن كلما قل عمر الشخص عند استخدام الإنترنت لأول مرة زاد وعيه بإجراءات الأمن السيبراني اللازم اتخاذها، وقد يرجع ذلك مدى خبرة الفرد باستخدام الإنترنت الآمن ومروره بمواقف مختلف أكسبته تلك الخبرة، وانفردت الدراسة الحالية ببحث أثر ذلك المتغير على درجة وعي طلبة كليات التربية بالإجراءات اللازمة للأمن السيبراني.

جدول (٩) فروق في وعي طلاب كليات التربية بإجراءات الأمن السيبراني تعزى لمتغير الجنس

الجنس	العدد	المتوسط الحسابي	الانحراف المعياري	ت	الدلالة
ذكر	٢٨	١٤٩.٢٨	٢٣.٥٢	.٣٣٠	.٥٦٧
أنثى	٩٧	١٥١.٥٥	١٦.٧٢		
المجموع	١٢٥	١٥١.٠٤	١٨.٣٨		

ويتضح من جدول (٩) عدم وجود فروق دالة إحصائيا عند مستوى دلالة (٠.٠٥) في وعي طلاب كليات التربية بإجراءات الأمن السيبراني تعزى لمتغير الجنس، ويمكن أن يرجع ذلك إلى عدم وجود اختلاف بين الطلاب والطالبات في درجة وعيهم تجاه إجراءات الأمن السيبراني اللازم اتخاذها، وتختلف هذه النتيجة مع دراسة كل من (Karagozlu, ٢٠٢٠)، و(Duman, ٢٠٢٢) التي أثبتت تفوق الطلبة الذكور على الإناث في إظهار سلوكيات أكثر وعياً فيما يتعلق بالبعد الاحترازي وحماية أجهزتهم المتصلة بالإنترنت بشكل مناسب ضد الفيروسات.

جدول (١٠) فروق في وعي طلاب كليات التربية بإجراءات الأمن السيبراني تعزى لمتغير العمل بجانب الدراسة.

العمل بجانب الدراسة	العدد	المتوسط الحسابي	الانحراف المعياري	ت	الدلالة
أعمل	٣٣	١٤٩.١٢	١٨.٠٥	.٤٩	.٤٨
لا أعمل	٩٢	١٥١.٧٣	١٨.٥٤		
المجموع	١٢٥	١٥١.٠٤	١٨.٣٨		

ويتضح من جدول (١٠) توجد فروق دالة إحصائيا عند مستوى مستوى دلالة (٠.٠٥) في وعي طلاب كليات التربية بإجراءات الأمن السيبراني تعزى لمتغير العمل بجانب الدراسة لصالح الطلبة الذين لا يعملون بجانب الدراسة، وقد يرجع ذلك إلى توفر الوقت اللازم لدى الطلبة الذين لا يعملون بجانب الدراسة للاطلاع على إجراءات الأمن السيبراني اللازم اتخاذها وتنفيذها بالفعل، واتفقت هذه النتيجة مع دراسة (Zhang, Li &Deng, ٢٠١٧) التي انتهت إلى وجود فروق دالة بين أفراد مجموعة الدراسة تعزى إلى متغير العمل.

سادسا: توصيات الدراسة:

توصي الباحثتان بالتوصيات التالية:

- إدراج تعليم الأمن السيبراني كجزء من المناهج الدراسية في التعليم بشكل عام.
- إجراء برامج تدريبية للتوعية بالأمن السيبراني للمعلمين أثناء الخدمة.
- إعداد مناهج للأمن السيبراني لمعلمي المراحل المختلفة.
- توعية الأطفال باجراءات تطبيق الأمن السيبراني خاصة في المرحل المبكرة.
- توفير نسخ مجانية أو مخفضة التكاليف من برامج الحماية وأنظمة التشغيل الأصلية للطلبة عند التحاقهم بالجامعة.

سابعا: مقترحات الدراسة:

تقترح الباحثتان إجراء دراسات مستقبلية حول النقاط التالية:

- أثر برنامج تدريبي لتعزيز مهارات الأمن السيبراني في العملية التعليمية.
- برنامج لتنمية مهارات الأمن السيبراني وعلاقته بالتنمر الالكتروني لدي الأطفال.
- أثر إدمان الألعاب الإلكترونية على السلوك الاجتماعي لطلبة الجامعة.

المراجع

البراشدية، حفيظة سليمان أحمد. (٢٠١٩). الفيسبوك والجرائم الإلكترونية في عمان: هل هناك علاقة؟، مجلة دراسات المعلومات والتكنولوجيا، ١.

توفيق، صلاح الدين محمد، ومرسي، شيرين عيد. (٢٠٢٣). متطلبات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمية من وجهة نظر أعضاء هيئة التدريس: جامعة بنها أنموذجا، المجلة التربوية، ج ١٠٥.

التيماني، مداخل زيد عبد الرحيم. (٢٠٢١). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني. مجلة الخدمة الاجتماعية، ٧٦.

الجندي، علياء عبد الله إبراهيم ومحمد، نهير طه حسن. (٢٠١٩). دور الممارسات التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة. عالم التربية، ٦٧ (٣).

الحارثي، فهد محمد عبد المحسن ونصر، فتحي نصر محمد. (٢٠٢١). برنامج تجريبي توكيدي لتعزيز بعض جوانب الصحة النفسية الإيجابية والهوية الثقافية، والأمن النفسي لدى طلاب جامعة الباحة المعرضين لخطر الإيذاء السيبراني، العلوم التربوية، ٢٩ (٣).

الحبيب، ماجد عبد الله محمد. (٢٠٢٢). درجة الوعي بالأمن السيبراني لدى طالب وطالبات الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية وسبل تعزيزه من وجهه نظرهم. مجلة العلوم التربوية، ع٣٠.

الخضري، جيهان سعد محمد وكليبي، نعمة ناصر وسلامي، هدي جبريل. (٢٠٢٠). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية: دراسة مقارنة ، مجلة تطوير الأداء الجامعي، جامعة المنصورة، ١٢ (١).

الرشيدي، صالح بشير. (٢٠٠٠). مناهج البحص التربوي: رؤية تطبيقية مبسطة، دار الكتاب الحديث، الكويت.

السمحان، مني عبد الله. (٢٠٢٠). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، كلية التربية، ع ١١١.

الصانع، نوره عمر محمد وعسران، عواطف سعد الدين والسواط، حمد حمود حميد وعلي، إيناس محمد سليمان وأبو عيشه، زاهدة جميل. (٢٠٢٠). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. مجلة كلية التربية، جامعة أسيوط، ٣٦ (٦).

الصحفي، مصباح أحمد وعسكول، سناء صالح. (٢٠١٩). مستوي اللاوعي بالأمن السيبراني لدى معلمات الحاسب الإلى للمرحلة الثانوية بمدينة جده، مجلة البحث العلمي في التربية، ٢٠ (١٠).

عبد السلام، مندور عبد السلام فتح الله. (٢٠٢٣). استراتيجيات الأمن الأسري السيبراني التي يستخدمها أولياء الأمور في مواجهه أنماط التنمر الإلكتروني بجمهورية مصر العربية، القيادة العامة لشرطة الشارقة، ٣٢ (١٢٥).

العتيبي، سعود شباب سدر. (٢٠٢٢). مدي توفر الوعي بالأمن السيبراني لدى أفراد الأسر في المجتمع السعودي (دراسة استطلاعين على عينة من الأسر بمحافظة جده)، المجلة الدولية لنشر البحوث والدراسات، ٣ (٢٧).

المطرفي، بيان بخيت والفراني، لينا أحمد خليل. (٢٠٢٣). فاعلية مقرر الكتروني مقترح لتنمية الوعي المعرفي بالأمن السيبراني لدى طالبات المرحلة الثانوية في مدينة جده، مجلة العلوم التربوية والنفسية، ٧ (١٣).

الهيئة الوطنية للأمن السيبراني. (٢٠١٨). الضوابط الأساسية للأمن السيبراني، المملكة العربية السعودية.

صائغ، وفاء حسن عبد الوهاب. (٢٠١٨). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية، ١٤ (٣).

علي، إيهاب عبد الرحيم. (٢٠١٧). أمن المعلومات الصحية، مجلة التقدم العلمي، الكويت، ٩٩

غوص، أميرة عبد الرحمن والشريف، باسم نايف. (٢٠٢٢). فاعلية توظيف بعض التطبيقات التعليمية الذكية في تقديم وحده مقترحة عن الأمن السيبراني على

التحصيل المعرفي والاتجاه نحوه لدى طالبات المرحلة المتوسطة بالمدينة المنورة، مجلة التربية، جامعة الأزهر، ٣ (١٩٥).

معجم المعاني

https://www.almaany.com

المراجع الأجنبية:

Ahmed, Osman Sirajeldeen & Nasef, Saeed Ameen & Al Rawashdeh, Alaa Zuhir & Eltahir, Mohd. Elmagzoub. (٢٠٢١). Teacher's awareness to develop student cyber security: A Case Study, Turkish Journal of Computer and Mathematics Education, ١٢ (١٠).

Al-Barashdi, Hafidha S. (٢٠١٩). Facebook and the cyber-crimes: Is there a relationship?, Journal of Information Studies and Technology,٢(٧).

Alharbi, Talal & Tassaddiq, Asifa. (٢٠٢١). Assessment of Cybersecurity Awareness among Students of Majmaah University, Big Data Cognitive Computing, ٥ (٢٣).

Duman, Feray Küçükbaş. (٢٠٢٢). Determining Cyber Security-Related Behaviors of Internet Users: Example of the Faculty of Sport Sciences Students, European Journal of Education, ٥ (١).

Hasan, Daniah Anwar & Tasji, Linah Faisal. (٢٠٢١). Investigating the Information Security Awareness at Taibah University (TU), International Congress of Advanced Technology and Engineering (ICOTEN).

Haseski, Halil İbrahim. (٢٠٢٠). Cyber Security Skills of Pre-Service Teachers as a Factor in Computer-Assisted Education,

International Journal of Research in Education and Science (IJRES), ٦(٣)

Karagozlu, Damla. (٢٠٢٠). Determination of cyber security ensuring behaviours of pre-service teachers, Cypriot Journal of Educational Sciences, ١٥(٦).

Kortjan, Noluxolo. (٢٠١٣). A Cyber Security Awareness and Education Framework for South Africa, MAGISTER TECHNOLOGIAE, FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY, NELSON MANDELA METROPOLITAN UNIVERSITY.

Raju, Rajeswari & Abd Rahman, Nur Hidayah & Ahmad, Atif. (٢٠٢٢). Cyber Security Awareness In Using Digital Platforms Among Students In A Higher Learning Institution, Asian Journal of University Education (AJUE), ١٨ (٣).

RICHARDSON, MICHAEL D. & LEMOINE, PAMELA A. & STEPHENS, WALTER E. & WALLER, ROBERT E. (٢٠٢٠). PLANNING FOR CYBER SECURITY IN SCHOOLS: THE HUMAN FACTOR, Educational Planning, ٢٧ (٢).

Salvail, Laurie. (٢٠٢٣). Teachers' essential guide to cybersecurity: leaen about the basic every educator and student should know.

Wadhwa, Amit & Arora, Neerja. (٢٠١٧). A Review on Cyber Crime- Major Threats and Solutions, International Journal of Advanced Research in Computer Science, ٨ (٥).

Yilmaz, Seda & Sagiroglu , seref . (٢٠١٣). Siber Güvenlik Risk Analizi, Tehdit ve Hazirlik Seviyeleri, ٦th INTERNATIONAL

INFORMATION SECURITY & CRYPTOLOGY CONFERENCE, Ankara / TURKEY

YILMAZ, Ramazan & YILMAZ, F.Gizem KARAOĞLAN & ÖZTÜRK, H.Tuğba & KARADEMIR, Tuğra. (٢٠١٧).Examining Secondary School Students' Safe Computer and Internet Usage Awareness: An Example from Bartın Province, Pegem Eğitim ve Öğretim Dergisi, ٧(١).

Zhang, Xiao Juan & Li, Zhenzhen & Deng, Hepu (٢٠١٧). Information security behaviors of smartphone users in China: an empirical analysis, The Electronic Library, Vol. ٣٥ No. ٦.