درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالأمن السيبراني

د. علي سويعد علي القرني

أستاذ المناهج وتقنيات التعليم المشارك

جامعة ام القرى

مستخلص البحث

هدف البحث إلى الكشف عن درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالأمن السيبراني، من خلال الكشف عن وعيهم بالمفاهيم المرتبطة به، التهديدات السيبرانية، وطرق حماية بياناتهم ومعلوماتهم أثناء استخدام الانترنت. وقد استخدم المنهج الكمي الوصفي في البحث، واستخدمت أداة الاستبانة في جمع البيانات من أفراد العينة الذين وصل عددهم إلى ١٩٨٠ طالبًا وطالبة من مختلف مناطق المملكة. وبعد جمع البيانات وتحليلها أظهرت النتائج مستوى وعي عالي لدى المستجيبين لمفاهيم الأمن السيبراني، التهديدات السيبرانية، وطرق حماية البيانات والمعلومات. كما أظهرت جوانب قصور لديهم في إلمامهم ببعض المفاهيم والممارسات التي تحميهم من التهديدات السيبرانية. كما أشارت النتائج إلى عدم وجود فروق ذات دلالة إحصائية عند مستوى ٠،٠٥ بين متوسطات استجابات أفراد العينة تبعا لمتغيرات الصف الدراسي، المنطقة الجغرافية، فترات استخدام الانترنت يوميًا، ونوع الجنس ما عدا في طرق حماية البيانات والمعلومات أظهر الطلاب تفوقًا على الطالبات. واختتم البحث بتوصيات بضرورة تقديم دورات في الأمن السيبراني لسد بعض جوانب القصور التي ظهرت في البحث، بالإضافة إلى تعزيز المقررات بموضوعات متعلقة بالأمن السيبراني.

كلمات مفتاحية: *أمن المعلومات؛ تهديدات سيبرانية؛ حماية البيانات؛ الوعي السيبراني*

Abstract

The research aimed to reveal the degree of awareness of secondary school students in Saudi Arabia about cyber security, by revealing their awareness of related concepts, cyber threats, and ways to protect their data and information while using the Internet. The descriptive quantitative method was used in the research, and the questionnaire tool was used to collect data from the sample, who numbered 1980 male and female students from different regions of Saudi Arabia. After collecting and analyzing the data, the results showed a high level of awareness among the respondents of cyber security concepts, cyber threats, and ways to protect data and information. They also showed deficiencies in their knowledge of some concepts and practices that protect them from cyber threats. The results also indicated that there were no statistically significant differences at the level of 0.05 between the averages of the respondents' responses according to the variables of class, geographic region, daily internet use periods, and gender, except for the methods of data and information protection, where male students showed superiority over female students. The research concluded with recommendations that it is necessary to offer courses in cyber security to bridge some of the deficiencies that appeared in the research, in addition to strengthening the courses with topics related to cyber security.

Keywords: *Information Security; Cyber Threats; Data Protection; Cyber Awareness*

١. المقدمة

ساعدت التطورات المتسارعة في وسائل الاتصالات وتقنية المعلومات في تقارب المسافات بين دول العالم، حيث أصبح العالم بثقافته المتنوعة ولهجاته المختلفة مجتمعًا واحدًا يجمعه هدف مشترك وهو الوصول لمجتمع تقني متقدم. ومن هذا المنطلق، سعت العديد من الدول إلى الانتقال لمجتمع تكون لغة الصفر والواحد هي لغته السائدة، فطورت البنية التحتية الرقمية القوية كأساس لهذا المجتمع، وهيأت الخدمات الرقمية التي تعين الأفراد على إنجاز المهام عن بعد، وهو ما يطلق عليه بالتحول الرقمي الذي عرفته فرج (٢٠٢٢) بأنه الانتقال من النظام التقليدي إلى نظام رقمي قائم على تكنولوجيا المعلومات والاتصال في إنجاز الأعمال، وذلك بالتكامل بين المتطلبات الإدارية، التقنية، والبشرية.

ونتيجة لهذا التحول الرقمي وإتاحة التقنية للأفراد والمؤسسات؛ تزايدت المعلومات والمعارف في فضاء الانترنت بشكل كبير، حيث أشار أحمد (٢٠١٧) أن المعرفة تتضاعف كل إحدى عشرة ساعة، وتتضاعف صفحات الويب كل ثلاثة أشهر؛ وذلك أن إضافة محتوى لفضاء الانترنت لا يتطلب سوى اشتراك فعال للانترنت وحساب مستخدم، والذي يعتبر إيجابي لما فيه من إثراء للمعرفة، وتعدد للمصادر.

ولكن من جهة أخرى، هذا الوصول المتاح لأي مستخدم، قد يعين بعض المستخدمين على نشر المعلومات المضللة، أو التعدي على خصوصيات الآخرين والإضرار بهم، وهذا يعني إمكانية وجود مخاطر للانترنت على المستخدمين، وانخفاض موثوقية المعلومات المتاحة، وتعطيل أو تقليل أداء بعض الأجزاء البرمجية أو المادية للحواسيب (العضياني، ٢٠٢١). فعلى سبيل المثال، في عام ٢٠١٢، تعرضت أرامكو لهجوم عن طريق فايروس shamoon تسبب في تعطل ٣٠٠٠٠ من أنظمة تشغيل ويندوز (Bronk & Tikk-Ringas، ٢٠١٣)، كما أشارت التقارير الصادرة عن Overseas Security Advisory Council عام ٢٠١٦ إلى تعرضها لهجمات إلكترونية أخرى أدت إلى تعطيل ٥٠٠٠٠ قرص صلب، وتعليق استخدام الانترنت لمدة

خمسة أشهر تقريبًا، كما تعرضت العديد من الشركات داخل المملكة العربية السعودية عام ٢٠١٧ إلى هجمات إلكترونية من Mamba Ransomware (أبوزيد، ٢٠١٩). وفي ذات السياق، تعرض موقع وزارة الصحة في المملكة العربية السعودية لهجوم سيبراني في الربع الثالث من عام ٢٠١٨ تسبب في تعطيله لساعات، وفي المجمل، أغلب الشركات في الشرق الأوسط وأفريقيا سبق لهم التعرض لهجوم سيبراني في عام ٢٠١٧ بحسب ما أورده تقرير Cisco لعام ٢٠١٨ (Dawson، ٢٠٢٢).

ونظرًا للدور الكبير الذي يوفره الأمن السيبراني في الحفاظ على بيانات المستخدمين، وتحقيق التنمية الاجتماعية والاقتصادية لكافة الدول؛ فقد حرصت كافة القطاعات المختلفة على تعزيز أمنها السيبراني (فرحات، ٢٠١٨). فعلى سبيل المثال، أشار فتوح (٢٠٢١) لأهمية تعزيز الأمن السيبراني لقطاع المصارف والمؤسسات المالية، وأن يكون متوافقًا مع أحدث المعايير العالمية المتبعة؛ وذلك للوصول إلى ثقة المستخدمين من جهة، وإنتاجية أكبر للمؤسسات من جهة أخرى. وفي المجال الطبي، أشار Jones وآخرون (٢٠٢٢) إلى أن الأمن السيبراني الطبي قضية كبرى على المستوى العالمي؛ نتيجة اتصال الأجهزة الطبية بشبكات الاتصال بشكل دائم، كما أكد على استخدام الشبكات المحلية الافتراضية (VLAN) للحد من الوصول للأجهزة أو المعلومات الطبية، بالإضافة إلى توعية الموظفين الذين يعملون على هذه الأجهزة بالإجراءات الأساسية للأمن السيبراني. وفي المجال التجاري، أكدت نتائج دراسة Phair و Alavizadeh (٢٠٢٢) على ضرورة اكتساب مدراء المنظمات التجارية معارف ومهارات تقنية، بالإضافة إلى تعزيز مهاراتهم السيبرانية وذلك لحفظ معلومات منظماتهم.

ولا شك أن المجال التعليمي من المجالات الهامة التي حظيت باهتمام المختصين في مجالي الأمن السيبراني والتعليمي على المستويين المعرفي والتقني. من ذلك محاولة اكساب الطلاب بعض مهارات الأمن السيبراني عن طريق الألعاب

الرقمية التعليمية (الشهراني وفلمبان، ٢٠٢٠؛ Alghamdi & Younis، ٢٠٢١)، والتطبيقات التعليمية على الأجهزة الذكية (عرفة والعراقي، ٢٠٢١؛ غوص والشريف، ٢٠٢٢)، وبعض التطبيقات المعتمدة على الذكاء الاصطناعي (الدمرداش، ٢٠٢٢)، والممارسات العملية (الجندي ومحمد، ٢٠١٩)، والعمل على رفع مستوى الوعي لدى الطلاب بطرق الاختراقات السيبرانية وكيفية الوقاية منها (الشهري، ٢٠٢١؛ Alammari وآخرون، ٢٠٢٢؛ Bhatnagar & Pry، ٢٠٢٠؛ Khader وآخرون، ٢٠٢١؛ McCrohan وآخرون، ٢٠١٠). ولم يكتف المهتمون بتثقيف وإكساب المهارات للطلاب العاديين فقط، بل حرصوا كذلك على تثقيف واكساب الطلاب من ذوي الإعاقة بعض مفاهيم الأمن السيبراني، بالإضافة إلى زيادة اهتمامهم بالوظائف المتعلقة به (القحطاني، ٢٠٢٢؛ Hairston وآخرون، ٢٠٢٠). ومن جانب آخر، فقد حظي الكادر التدريسي من المعلمين والمعلمات بالاهتمام البالغ من التربويين، حيث حرصوا على قياس مدى وعيهم بمهارات الأمن السيبراني، بالإضافة إلى إكسابهم المهارات اللازمة لحماية بياناتهم من خلال بعض البرامج التدريبية (السعادات والتميمي، ٢٠٢٢؛ الصانع وآخرون، ٢٠٢٠؛ الصحفي وعسكول، ٢٠١٩؛ العقلاء وعلي، ٢٠٢٢). ومؤخرًا أعلنت الهيئة الوطنية للأمن السيبراني عن مبادرة بالتعاون مع وزارة التعليم، تهدف إلى تدريب المعلمين والمعلمات في مجال الأمن السيبراني؛ وذلك بهدف تزويدهم بالمهارات والمعارف الأساسية لحماية بياناتهم ونقل هذه الخبرات على نطاق واسع في المجتمع (الهيئة الوطنية للأمن السيبراني، ٢٠٢٣).

٢. مشكلة البحث

مع التطور المتسارع في التقنية ووسائل الاتصالات، بالإضافة إلى ما أنتجته جائحة كورونا من حيث توسع الاعتماد على التقنية في الميدان التربوي، وتجهيز المنصات التعليمية –كمنصة مدرستي- لتصبح بيئة تعليمية افتراضية متكاملة، يتعامل معها الطلاب والطالبات بشكل يومي من خلال الاطلاع على المحتوى الذي

أعده المعلمون والمعلمات أو الأنشطة المطلوب تنفيذها بعد العودة للمنزل، بالإضافة لتوجه وزارة التعليم بالمملكة العربية السعودية للاكتفاء ببعض المقررات الإلكترونية المتاحة على المنصة دون الحاجة لطباعتها ورقيًا كمقرر تفسير١، التفكير الناقد، تقنية رقمية١- ١، وغيرها من المقررات في المرحلة الثانوية، كل هذه المعطيات ساهمت بشكل كبير في ارتفاع استخدام الانترنت من قبل الطلاب والطالبات، وقد تكون حاجزًا أمام بعض القيود التي وضعت من قبل الوالدين تجاه استخدام الانترنت في المنزل، وهذا الوصول المتكرر للانترنت يعني أن فرص اختراق خصوصياتهم وسرقة بياناتهم كبيرة؛ لذلك من المهم معرفة مدى وعيهم بهذه المخاطر وطرق الوقاية منها.

بالإضافة إلى أن مراجعة الأدبيات التي اهتمت بالأمن السيبراني في الميدان التربوي، أظهرت اهتمامًا كبيرًا بدرجة وعي المعلمين والمعلمات وأعضاء هيئة التدريس بمخاطر الأمن السيبراني على حساب الطلاب (إبراهيم، ٢٠٢١؛ البيشي، ٢٠٢١؛ السعادات والتميمي،٢٠٢٢؛ الصانع وآخرون، ٢٠٢٠؛ الصحفي وعسكول، ٢٠١٩؛ العقلاء وعلي، ٢٠٢٢؛ الكردي، ٢٠٢١؛ المطيري، ٢٠٢١؛ Maina وآخرون، ٢٠٢١)، بالإضافة لمبادرة الهيئة الوطنية للأمن السيبراني التي تستهدف تدريب المعلمين والمعلمات، كما ورد ذكره سابقًا. وفي ذات السياق، ركزت الدراسات على طلاب المرحلة الجامعية أكثر من التعليم العام، حيث أظهرت الأدبيات حرصًا من الباحثين على رفع مستوى وعي طلاب وطالبات المرحلة الجامعية بهذه المخاطر وإكسابهم المهارات الضرورية لذلك (الجندي ومحمد، ٢٠١٩؛ الحبيب، ٢٠٢٢؛ الدمرداش، ٢٠٢٢؛ شعبان، ٢٠٢١؛ الشهري، ٢٠٢١؛ الصبان والحربي، ٢٠١٩؛ عرفة والعراقي، ٢٠٢١؛ غوص والشريف، ٢٠٢٢؛ Alammari وآخرون، ٢٠٢٢؛ Younis & Alghamdi، ٢٠٢١؛ Pry & Bhatnagar، ٢٠٢٠؛ Hairston، ٢٠٢٠؛ Yoon وآخرون، ٢٠١٢). وهناك بعض الدراسات التي أظهرت اهتمامًا بهذا الموضوع على طلاب وطالبات مراحل التعليم العام خارج المملكة العربية السعودية (Bhuyan، ٢٠٢٠؛ Kritzinger،

٢٠١٧؛ Tekerek A. & Tekerek M.، ٢٠١٣؛ Yildiz، ٢٠١٩)، إلا أن الدراسات التي أجريت على طلاب التعليم العام في المملكة تكاد تكون معدودة (السواط وآخرون، ٢٠٢٠؛ الشهراني وفلمبان، ٢٠٢٠؛ Aldosari وآخرون، ٢٠٢٠)، ومع ندرتها فإنها استهدفت طلاب في مراحل تعليمية تختلف عن المرحلة المستهدفة في هذه الدراسة، كالمرحلة الابتدائية والمتوسطة في دراسة السواط وآخرون، والشهراني وفلمبان، أو منطقة جغرافية محدودة كدراسة Aldosari وآخرون التي طبقت في مدينة الرياض، ودراسة السواط وآخرون في مدينة الطائف؛ لذلك لا تزال هناك فجوة تحتاج دراسات إضافية لسدها.

كذلك فيما تشير نتائج الدراسات السابقة إلى أن مستوى الوعي بمهارات الأمن السيبراني، وكيفية حماية البيانات والأجهزة المتصلة بالإنترنت مرتفعة لدى بعض الطلاب (الحبيب، ٢٠٢٢؛ السواط وآخرون، ٢٠٢٠)، إلا أن هناك دراسات أخرى تشير إلى أن درجة الوعي لا تزال دون المأمول (القحطاني، ٢٠١٩؛ Tekerek M. & Tekerek A.، ٢٠١٣)، ويدعم هذه النتائج ما توصلت إليه الصحفي وعسكول (٢٠١٩) ودراسة العقلاء وعلي (٢٠٢٢) التي أجريت على معلمات ومعلمي الحاسب الآلي بمدينة جدة وحائل على التوالي، وأظهرت درجة وعي ضعيفة إلى متوسطة على التوالي؛ ونظرًا لهذا التباين في النتائج تظهر الحاجة لإجراء المزيد من الأبحاث لدعم الأدبيات في هذا الجانب.

بالإضافة لما سبق، أظهرت توصيات بعض الدراسات ضرورة الاهتمام بالوعي بمهارات الأمن السيبراني لدى الطلاب (السواط وآخرون، ٢٠٢٠؛ الشهري، ٢٠٢١؛ القحطاني، ٢٠١٩؛ فرج، ٢٠٢٢؛ Aldosari وآخرون، ٢٠٢٠)؛ لذا سعى هذا البحث إلى الكشف عن درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالأمن السيبراني.

٣. أسئلة البحث

سعى البحث إلى الإجابة عن السؤال الرئيس التالي: ما درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالأمن السيبراني؟ وذلك عن طريق الإجابة عن الأسئلة الفرعية التالية:

١- ما درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بمفاهيم الأمن السيبراني؟

٢- ما درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية؟

٣- ما درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت؟

٤- هل توجد فروق ذات دلالة إحصائية عند مستوى ٠,٠٥ بين متوسطات استجابات أفراد العينة تعزى لمتغيرات (الجنس، الصف الدراسي، المنطقة الجغرافية، فترات استخدام الانترنت)؟

٤. أهداف البحث

هدف البحث إلى:

١- التعرف على درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بمفاهيم الأمن السيبراني.

٢- التعرف على درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية.

٣- التعرف على درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت.

٤- الكشف عن وجود فروق ذات دلالة إحصائية عند مستوى ٠,٠٥ بين متوسطات استجابات أفراد العينة تعزى لمتغيرات (الجنس، الصف الدراسي، المنطقة الجغرافية، فترات استخدام الانترنت).

٥. أهمية البحث

تأتي أهمية هذا البحث في أنه قد يسد الفجوة البحثية والمعرفية للوعي بالأمن السيبراني في مرحلة تعتبر من أهم المراحل الدراسية. وذلك من خلال التعرف على درجة الوعي بالأمن السيبراني لطلبة المرحلة الثانوية. كما أن هذا البحث قد يسهم في تزويد القارئ بمعرفة شاملة عن مستوى الوعي بالأمن السيبراني في مناطق جغرافية مختلفة بالمملكة العربية السعودية. وبالإضافة لما سبق، فإن هذا البحث قد يسهم في تزويد الباحثين ببعض النتائج التي توضح العلاقة بين بعض المتغيرات والوعي بالأمن السيبراني.

من جهة أخرى، فإن نتائج هذا البحث قد تسهم في وضع الإطار العام لبرنامج تدريبي للوعي بالأمن السيبراني، بحيث يستهدف طلبة المرحلة الثانوية بالمملكة، مع التركيز على جوانب القصور لديهم والعمل على معالجتها.

٦. مراجعة الادبيات

٦-١: مفهوم الأمن السيبراني

أوردت الأدبيات العديد من التعريفات التي تصف مفهوم الأمن السيبراني منها ما أورده Kemmerer (٢٠٠٣) أنه عبارة عن الأساليب الدفاعية المستخدمة لاكتشاف المتسللين، وهو بهذا الوصف يركز على آليات وأساليب وطرق تتبع البيانات ورصد أي مستخدم غير شرعي يحاول الوصول لها، ويظهر في هذا الوصف أن Kemmerer أهتم بالشمولية ونظر إلى الأمن السيبراني بمفهومه الشامل. وفي ذات السياق، ذهب De Zan إلى الشمولية كذلك في وصفه لمفهوم الأمن السيبراني إلا أنه أضاف الوسط التي تتم فيه حماية هذه البيانات حيث أشار إلى أن الأمن

السيبراني يتطلب حماية شبكات الحاسوب وما تحويه من معلومات من الاختراق أو التلف أو التشويه (كما هو موثق في Maina وآخرون، ٢٠٢١).

كما ظهرت لاحقًا بعض التعريفات التي بينت مفهوم الأمن السيبراني بتفصيل أكبر من حيث شموله على قوانين وأدوات تستخدم للحد من السلوكيات الضارة، وحماية المستفيدين. حيث ذكر Adams (٢٠١٧) أن الأمن السيبراني عبارة عن مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المؤسسة والمستخدم، بما في ذلك الحوسبة الأجهزة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المرسلة أو المخزنة في البيئة السيبرانية. ويتفق معه Mat وآخرون (٢٠٢٢) من حيث وصف الأمن السيبراني حيث أشار إلى أنه عبارة عن جميع التقنيات والعمليات والسياسات التي تهدف إلى منع وتقليل التأثير السلبي للأعمال العدائية المتعمدة من قبل جهات فاعلة غير مسؤولة.

كما تعرفه الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية (٢٠٢١، ٥) على أنه "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع". ويظهر من هذا التعريف التفصيل الدقيق لمفهوم الأمن السيبراني، حيث شمل حماية الوسط الذي تنتقل به البيانات والمعلومات، بالإضافة إلى المعلومات وكل ما يتعلق بها من معالجات وتخزين، وتقنيات التشغيل بمكوناتها المادية والبرمجية.

وفي هذا البحث يعرف الأمن السيبراني إجرائيًا بحماية الأجهزة المتصلة بالإنترنت من التهديدات السيبرانية المحتملة، واتباع الطرق والأساليب الآمنة

لاستخدام الانترنت؛ لحماية الأجهزة والبرمجيات من التعطيل أو التدمير، والبيانات والمعلومات من الاختراق أو الفقدان أو التعديل والتشويه.

٦-٢: التهديدات السيبرانية

إن ارتباط معظم أجهزة الحاسب بالإنترنت ساهم بشكل كبير في زيادة الهجمات والتهديدات السيبرانية التي تعني إمكانية الوصول لبيانات الضحية بطريقة غير مشروعة وذلك من خلال ثغرات في نظامه (القحطاني، ٢٠١٥). وتعتبر الهندسة الاجتماعية من أبرز الأساليب المستخدمة في الهجمات السيبرانية التي ظهرت مؤخرًا، ويعرفها Mouton وآخرون (٢٠١٦) بأنها عملية خداع المستخدمين باستخدام تقنيات التلاعب النفسي، كما يعرفها القحطاني (٢٠١٥، ٢٥٠) بأنها "استخدام المهارات الاجتماعية لإقناع الأشخاص بالإفصاح عن المعلومات السرية". ومن طرق الهندسة الاجتماعية الشائعة ما تسمى برسائل الاصطياد الإلكتروني Phishing Mails (Cheng & Wang، ٢٠٢٢)، حيث يتم إرسال بريد إلكتروني للضحية، والذي يحتوي غالبًا على ملف أو رابط ضار (Pollock وآخرون، ٢٠٢٢)، ويستخدم شعارات وعلامات لجهات معروفة لتشتيت انتباه المستخدم عن عنوان البريد الإلكتروني الخاطئ، وإيهامه بأن البريد الوارد مرسل من الجهة الرسمية (Wright & Marett، ٢٠١٠). ومن جانب آخر، قد يستخدم المهاجمون شكل آخر من أشكال الهندسة الاجتماعية يعتمد على التواصل مع الضحية بشكل مباشر أو عن طريق الهاتف، متظاهرًا بأنه يعمل في جهة رسمية ويطلب منه بعض المعلومات الحساسة التي تساعده في الحصول على بعض المعلومات السرية واستخدامها لاحقًا عند تنفيذ عملية الهجوم (القحطاني، ٢٠١٥).

كما ذكر Cheng وWang (٢٠٢٢) بعض الهجمات السيبرانية مثل تشويه موقع الويب وذلك عن طريق تعديل غير مصرح به لصفحات الويب، بما في ذلك إضافة المحتوى الحالي أو إزالته أو تغييره. أو رفض الخدمة (Denial-of-Service (DoS)) وهو محاولة تكثيف البيانات غير المهمة بالموقع وذلك بهدف تأخير تنفيذ

خدمة ما أو جعل الخادم الذي يقدم الخدمة غير قادرٍ على العمل بشكل صحيح. ويضيف القحطاني (٢٠١٥) أشكال أخرى للتهديدات مثل استخدام برامج التجسس، الفيروسات، حصان طروادة، ديدان الحاسب الآلي، والبرامج الضارة (Malware).

وإضافة لما سبق، تعتبر كلمات المرور إحدى أهم التهديدات السيبرانية للمستخدمين والتي يمكن من خلالها إيجاد ثغرات للهجوم السيبراني. فعندما لا يراعي مستخدم الانترنت القواعد الأساسية لكتابة كلمة المرور الخاصة به، فإنه بذلك يعين المهاجم على الوصول إليها بسهولة. في دراسة قام بها Hoonakker وآخرون (٢٠٠٩) على ٩٠٠ موظفًا بشركة تجارية، وجدوا أن الموظفين في كلمات المرور يتبعون إحدى الطرق التالية: كتابة كلمات مرور بسيطة يسهل تذكرها، ولكن يسهل اختراقها، كلمة مرور واحدة طوال الوقت، إعادة استخدام كلمات مرور قديمة، ومشاركة كلمات المرور مع الآخرين. وفي دراسة أخرى قام بها Shen وآخرون (٢٠١٦) لاختبار ضعف ٦,٥ مليون كلمة مرور حقيقية سُرِقَت من شبكة التطوير البرمجي الصينية Chinese Software Development Network، وجدوا كلمة المرور "١٢٣٤٥٦٧٨٩" اُستخدِمت بنسبة ٣,٦٦٪، و"١٢٣٤٥٦٧٨" بنسبة ٣,٣١٪، وكلمات مرور مطابقة لاسم المستخدم بنسبة ٤,٤٥٪، وكلمات مرور اُستخدِم فيها كلمات مشهورة باللغة الإنجليزية بنسبة ٢١,٦٥٪.

٦-٣: أساليب حماية البيانات والمعلومات

إن وعي المستخدم بالأمن السيبراني يسهم في التصدي لهذه التهديدات والهجمات، ويساعد في حماية أجهزته وبياناته من المتطفلين (صائغ، ٢٠١٨). بمعنى آخر، من المهم أن يستوعب المستخدم أساليب الهندسة الاجتماعية التي يستخدمها المنتحلون حتى يكون بمأمن من الوقوع في شراكهم، والانسياق لمطالبهم (الشايع، ٢٠١٩؛ العضياني، ٢٠٢١؛ المنتشري وحريري، ٢٠٢٠)، وإضافة معايير التحقق الثنائية والثلاثية للحفاظ على سرية بياناته تعزز من الحفاظ عليها بعيدًا عنهم، والقدرة على عمل نسخ احتياطية للبيانات والمعلومات المهمة وحفظها على وسائط

تخزين خارجية، تضمن للمستخدم استرجاعها وعدم فقدانها عند وصول المتطفلين لهذه البيانات وتشويهها (المبيض، ٢٠٢٠). كما أشار القحطاني (٢٠١٥) إلى إتباع بعض الإرشادات التي تعزز من مستوى حماية البيانات والمعلومات منها تفعيل جدار الحماية الناري، استخدام الشبكات الخاصة الافتراضية (VPNs)، تشفير البيانات المهمة، حجب الإعلانات والنوافذ المنبثقة، واستخدام برامج مضادة للتجسس ومضادة للفيروسات.

من جانب آخر، وعي المستخدم بإرشادات كتابة كلمة مرور قوية يصعّب على قراصنة البيانات والمعلومات تخمينها والوصول لها (Tekerek, M & Tekerek, A، ٢٠١٣). حيث أظهرت دراسة McCrohan وآخرون (٢٠١٠) أن وعي المستخدمين وتزويدهم بمعلومات مفصلة حول التهديدات التي قد يتعرضون لها، ساهم في رفع جودة كلمات مرورهم الشخصية بنسبة ٣٦٪. لذلك ينبغي عند كتابة كلمات المرور مراعاة ألا تقل عن ثمانية خانات، وأن تكون مزيجاً من الأحرف والأرقام بالإضافة إلى الرموز الخاصة، وألا تكون جزءا من هوية المستخدم كالاسم أو تاريخ الميلاد أو رقم الهوية الشخصية، وألا تحوي بعض الكلمات المشهورة التي يسهل تخمينها (المبيض، ٢٠٢٠؛ Hoonakker وآخرون، ٢٠٠٩).

٧. إجراءات البحث

٧-١: منهج البحث

اتبع هذا البحث المنهج الكمي، بنوعه الوصفي التحليلي، ويهتم بوصف ظاهرة معينة وتفسيرها، ويتم فيه جمع البيانات حول الظاهرة بهدف التعرف على آراء أو توجهات المجتمع بشكل عام عن الظاهرة (Creswell، ٢٠١٤).

٧-٢: المشاركون في البحث (عينة البحث)

تكون مجتمع البحث من جميع طلاب وطالبات المرحلة الثانوية بالمملكة العربية السعودية، وبلغت عينة الدراسة ١٩٨٠ من طلبة المرحلة الثانوية، تم جمعهم

بطريقة العينة العشوائية البسيطة. وفيما يلي وصف لخصائص العينة الديموغرافية:

٧-٢-١: خصائص العينة بحسب الجنس

جدول١

وصف للعينة بحسب نوع الجنس

نوع الجنس	العدد	النسبة
الذكور	٩٠٥	٪ ٧،٤٥
الإناث	١٠٧٥	٪ ٣،٥٤
الإجمالي	١٩٨٠	٪ ١٠٠

يظهر الجدول (١) خصائص العينة بحسب الجنس، والذي يظهر فيه نسبة الذكور ٧،٤٥٪ من العينة، ونسبة الإناث ٣،٥٤٪ من العينة.

٧- ٢- ٢: خصائص العينة بحسب الصف الدراسي

جدول٢

وصف للعينة بحسب الصف الدراسي

الصف الدراسي	العدد	النسبة
الأول ثانوي	٥٧٠	٪ ٨،٢٨
الثاني ثانوي	٨٦٥	٪ ٧،٤٣
الثالث ثانوي	٥٤٥	٪ ٥،٢٧
الإجمالي	١٩٨٠	٪ ١٠٠

يظهر من الجدول٢ أن عدد الطلبة الذين يدرسون في الصف الثاني ثانوي يمثلون نسبة أكبر من الصفين الآخرين، حيث تبلغ ٧،٤٣٪، في حين كانت نسبة الصف الأول والثالث ٨،٢٨٪ و٥،٢٧٪ على التوالي.

٧-٢-٣ : خصائص العينة بحسب المنطقة التي تتبع لها العينة

جدول٣ : وصف للعينة بحسب الصف الدراسي

المنطقة	العدد	النسبة
الوسطى	٣٧٥	٪ ٩،١٨
الغربية	٤٥٠	٪ ٧،٢٢
الجنوبية	٤١٥	٪ ٢١ ،٠
الشمالية	٤٤٠	٪ ٢،٢٢
الشرقية	٣٠٠	٪ ٢،١٥
الإجمالي	١٩٨٠	٪ ١٠٠

يوضح جدول٣ توزيع العينة على مناطق المملكة العربية السعودية حيث تمثل نسبة العينة من المنطقة الوسطى ٩،١٨٪، الغربية ٧،٢٢٪، الجنوبية ٠، ٢١٪، الشمالية ٢،٢٢٪، والشرقية ٢،١٥٪.

٧- ٢- ٤ : خصائص العينة بحسب فترات استخدام الانترنت يوميًا

جدول٤ : وصف للعينة بحسب فترات استخدام الانترنت يوميًا

الفترة	العدد	النسبة
أقل من خمس ساعات	١٠٣٥	٪ ٣،٥٢
أكثر من خمس ساعات	٩٤٥	٪ ٧،٤٧
الإجمالي	١٩٨٠	٪ ١٠٠

يوضح جدول٤ توزيع العينة بحسب ساعات استخدامهم للانترنت يوميًا، حيث يظهر الجدول أن نسبة الذين يستخدمون الانترنت أقل من خمس ساعات يوميا تبلغ ٣،٥٢٪، أما البقية فهم يستخدمونه أكثر من خمس ساعات في اليوم.

٧- ٣ : أداة البحث

استخدمت أداة الاستبانة في جمع البيانات من أفراد العينة، وقد اعتمد في بنائها على الأدبيات السابقة ذات الصلة بالوعي بالأمن السيبراني (السواط وآخرون،

٢٠٢٠؛ العضياني، ٢٠٢١؛ المبيض، ٢٠٢٠). وتكونت الاستبانة من ثلاثة محاور: الوعي بمفاهيم الأمن السيبراني وتكون من ١١ فقرة، الوعي بالتهديدات السيبرانية وتكون من ١٣ فقرة، والوعي بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت وتكون من ١١ فقرة.

وقد استخدم مقياس ليكرت الذي يتكون من الرقم ١ و٢ للمحور الأول، بحيث ترمز الإجابة الصحيحة برقم ٢، وبقية الإجابات برقم ١، أما المحورين الثاني والثالث فاستخدم فيها مقياس ليكرت الخماسي.

٧-٣-١: صدق أداة البحث

تم عرض الأداة بصورتها الأولية على مجموعة من المتخصصين في مجال تقنيات التعليم والحاسب الآلي؛ وذلك للتأكد من سلامة الفقرات والتعرف على مدى انتماء كل فقرة للمحور الذي تندرج تحته، وإضافة أو تعديل الفقرات التي تحتاج لتصويب، وقد تم التعديل على بعض الفقرات وفقاً لما وصل من المحكمين.

بعد ذلك تم توزيع أداة الاستبانة على عينة استطلاعية بهدف حساب صدق الاتساق الداخلي للأداة، وكانت النتيجة كما يلي:

- محور درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بمفاهيم الأمن السيبراني

يوضح الجدول٥ الاتساق الداخلي بين فقرات المحور الأول والدرجة الكلية للمحور كما يلي:

جدول٥ : الاتساق الداخلي بين فقرات محور درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بمفاهيم الأمن السيبراني والدرجة الكلية للمحور

م	الفقرة	معامل الارتباط	الدلالة الإحصائية
١.	كلمة سيبراني تعني	٨٨،٠	دالة عند ٠,٠١
٢.	مفهوم الأمن السيبراني هو المفهوم الحديث لأمن المعلومات، ما رأيك بهذه العبارة	٦٣،٠	دالة عند ٠,٠١
٣.	الذين يعملون على سرقة أو تخريب أو تحريف بيانات خاصة بدول أو منشأة أو أفراد آخرين لأغراض مالية أو سياسية أو للتسلية يطلق عليهم	٦٢،٠	دالة عند ٠,٠١
٤.	البرامج غير المرغوبة أو الملفات التي يمكن أن تسبب ضررا لجهاز الحاسب أو تهدد البيانات المخزنة عليه تسمى	٥٧،٠	دالة عند ٠,٠١
٥.	العيوب في البرامج الثابتة أو الأجهزة التي يمكن أن يستغلها المهاجم لأداء إجراءات غير مصرح بها في النظام تسمى	٦٦،٠	دالة عند ٠,٠١
٦.	الحصول على معلومات الضحية ثم استخدامها ضده مقابل الحصول على المال أو يتم دفع الفدية تسمى	٦٨،٠	دالة عند ٠,٠١
٧.	التحايل على مستخدم الحاسب بغرض الحصول على معلومات المفترض ألا يفصح عنها تسمى	٦٥،٠	دالة عند ٠,٠١
٨.	تصميم مواقع أو إرسال رسائل بريد إلكتروني مطابقة للمواقع الأصلية بغرض الاحتيال تسمى	٨٨،٠	دالة عند ٠,٠١
٩.	ترميز البيانات وجعلها غير قابلة للفك بدون مفتاح الترميز تسمى	٧٧،٠	دالة عند ٠,٠١
١٠.	الممارسات التي تقع ضد فرد أو مجموعة بهدف التسبب بالأذى لسمعة الضحية عمداً أو إلحاق الضرر النفسي أو البدني به تسمى	٨٨،٠	دالة عند ٠,٠١
١١.	عند طلب الدخول لبعض المواقع يلزم إدخال كود مرسل لهاتفك بعد إدخال اسم المستخدم وكلمة المرور، هذه الخاصية تسمى	٧٨،٠	دالة عند ٠,٠١

من خلال الجدول يتضح بأن معاملات الارتباط بين معدل كل فقرة من المحور الأول مع المعدل الكلي لفقرات المحور كانت تتراوح بين ٠,٥٧ و٠,٨٨، وأن جميع معاملات الارتباط بين الفقرات المكونة لهذا المحور وبين المجموع الكلي للمحور دالة إحصائياً عند ٠,٠١، مما يشير إلى أنها تتمتع بدرجة صدق مرتفعة ومناسبة للتطبيق الميداني.

- **محور درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية:**

يوضح الجدول٦ الاتساق الداخلي بين فقرات المحور الثاني درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية والدرجة الكلية للمحور كما يلي:

جدول٦ : الاتساق الداخلي بين فقرات محور درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية والدرجة الكلية للمحور

م	الفقرة	معامل الارتباط	الدلالة الإحصائية
١.	عند وصول رسالة إلى بريدي الإلكتروني تفيد بحصولي على جائزة مالية، فإنني أقوم بتعبئة بياناتي على الرابط المرفق في الرسالة لاستكمال حصولي على الجائزة.	٦٠،٠	دالة عند ٠,٠١
٢.	عند استعراض الأوسمة (الهاشتاقات) في تويتر ووجود خبر عن فضيحة أحد المشاهير، فإنني أضغط على الرابط المرفق مع التغريدة لمشاهدة الخبر.	٦٢،٠	دالة عند ٠,٠١
٣.	عند الاتصال بي من شخص يدعي أنه يعمل بأحد الجهات الحكومية أو البنوك، ويطلب مني بعض المعلومات الشخصية، فإنني لا أتردد في التعاون معه وتزويده بهذه المعلومات.	٥٨،٠	دالة عند ٠,٠١
٤.	عند وصول رابط إلكتروني إلى بريدي الإلكتروني، أو أحد حساباتي في وسائل التواصل الاجتماعي، فإنني	٧١،٠	دالة عند ٠,٠١

	أقوم بالضغط عليه وفتحه للتعرف على محتوى الموقع الإلكتروني.		
٥.	أقوم بفتح الملفات التي يتم تنزيلها من الانترنت بشكل مباشر، وذلك للاطلاع على محتويات هذه الملفات.	٦٢،٠	دالة عند ٠,٠١
٦.	أقوم بحفظ كلمات المرور Password على المتصفح (على سبيل المثال متصفح Google Chrome) حتى أتمكن من الدخول مستقبلا دون الحاجة لكتابتها مرة أخرى.	٥٢،٠	دالة عند ٠,٠١
٧.	أنشئ كلمات المرور لحساباتي المختلفة بحيث ترتبط ببعض بياناتي الشخصية كتاريخ ميلادي أو المدينة التي أعيش فيها لسهولة حفظها وتذكرها	٦٢،٠	دالة عند ٠,٠١
٨.	أستخدم كلمة مرور واحدة لأكثر من حساب أملكه على الانترنت ليسهل تذكرها	٦،٠	دالة عند ٠,٠١
٩.	أستخدم أرقام أو حروف متتابعة (مثال: ABC أو ٢٣٤) في كلمة المرور الخاصة بي.	٦٣،٠	دالة عند ٠,٠١
١٠.	أستخدم بعض الكلمات المشهورة في كلمة المرور الخاصة بي (مثل: love).	٦٢،٠	دالة عند ٠,٠١
١١.	أستخدم شبكات الانترنت العامة المجانية المتاحة في الأماكن العام وذلك لتصفح الانترنت.	٦٣،٠	دالة عند ٠,٠١
١٢.	لا أتابع التحديثات المستمرة لنظام تشغيل جوالي والتطبيقات المثبتة عليه.	٥٤،٠	دالة عند ٠,٠١
١٣.	لا يوجد برنامج حماية من الاختراق على جهاز الحاسب الخاص بي، وإن وجد فلم يتم تحديثه منذ أن تم تنصيبه.	٥٣،٠	دالة عند ٠,٠١

من خلال جدول٦ يتضح بأن معاملات الارتباط بين معدل كل فقرة من المحور الثاني المتعلق بدرجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية مع المعدل الكلي لعبارات المحور كانت تتراوح بين ٥٢،٠ و٧١،٠، وجميع

معاملات الارتباط بين الفقرات المكونة لهذا المحور وبين المجموع الكلي للمحور دالة إحصائياً عند ٠,٠١، مما يشير إلى أن عبارات هذا المحور تتمتع بدرجة صدق مرتفعة.

- **محور درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية:**

يوضح جدول٧ الاتساق الداخلي بين فقرات المحور الثاني درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية والدرجة الكلية للمحور كما يلي:

جدول٧: الاتساق الداخلي بين فقرات درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت والدرجة الكلية للمحور

م	الفقرة	معامل الارتباط	الدلالة الإحصائية
١.	أقوم بإنشاء كلمة مرور مختلفة في كل مرة يطلب مني انشاء حساب باسم مستخدم وكلمة مرور لموقع على الانترنت	٥٨،٠	دالة عند ٠,٠١
٢.	أستخدم في كلمات المرور الخاصة بي مزيجاً من الأحرف الكبيرة والصغيرة والرموز الخاصة مثل (@ + !).	٦،٠	دالة عند ٠,٠١
٣.	أخرج من حسابي بعد الانتهاء من استخدام الانترنت.	٥٤،٠	دالة عند ٠,٠١
٤.	أقوم بمتابعة التحديثات لنظام تشغيل جوالي والتطبيقات المثبتة عليه بشكل دوري.	٦٧،٠	دالة عند ٠,٠١
٥.	أقوم بعمل نسخة احتياطية لمحرك القرص الصلب بالحاسب الخاص بي بشكل دوري؛ وذلك تجنبا لفقدان البيانات والمعلومات المخزنة فيه.	٦٤،٠	دالة عند ٠,٠١
٦.	أستخدم نظام التحقق الثنائي في معظم حساباتي على الانترنت ملاحظة: (شرح لمفهوم التحقق الثنائي: أي أن النظام يطلب منك إدخال كود مرسل لجوالك بعد التحقق من إدخال اسم المستخدم وكلمة المرور بشكل صحيح).	٥٢،٠	دالة عند ٠,٠١
٧.	أستخدم برامج مكافحة الفيروسات على جهازي الشخصي، وأقوم بتحديثها بشكل مستمر.	٦٦،٠	دالة عند ٠,٠١

٨.	أحرص على عدم فتح الملفات التي تصلني من مصادر مجهولة أو غير موثوقة إلا بعد فحصها ببرنامج الحماية من الفيروسات	٦٦،٠	دالة عند ٠,٠١
٩.	أستخدم بريد إلكتروني خاص للاستخدامات الرسمية والهامة.	٥٧،٠	دالة عند ٠,٠١
١٠.	أحرص على عدم تصفح الانترنت ومواقعي الشخصية عن طريق الشبكات المتاحة في الأماكن العامة.	٥٥،٠	دالة عند ٠,٠١
١١.	أحرص على عدم فتح الروابط التي تصلني من مصادر مجهولة أو غير موثوقة.	٤٩،٠	دالة عند ٠,٠١

من خلال جدول٧ يتضح لنا بأن معاملات الارتباط بين معدل كل فقرة من المحور الثالث المتعلق بدرجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت مع المعدل الكلي لعبارات المحور كانت تتراوح بين ٠,٤٩ و٠,٦٧، وجميع معاملات الارتباط بين الفقرات المكونة لهذا المحور وبين المجموع الكلي للمحور دالة إحصائياً عند ٠,٠١، مما يشير إلى أنها تتمتع بدرجة صدق مرتفعة وصالحة للتطبيق.

٧-٣-٢: ثبات أداة الدراسة

تم حساب ثبات أداة الدراسة بعد جمع البيانات من العينة الاستطلاعية، وذلك باستخدام معامل الفا كرونباخ (Cronbach's Alpha)، وكانت النتائج كما هي موضحة في الجدول التالي:

جدول٨: معامل الفا كرونباخ للأداة

م	المقاييس	عدد الفقرات	معامل ألفا	النسبة
١	المحور الأول: درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بمفاهيم الأمن السيبراني	١١	٠,٨٥١	٨٥,١٪
٢	المحور الثاني: درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية	١٣	٠,٨٨٥	٨٨,٥٪
٣	المحور الثالث: درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت	١١	٠,٩١٠	٩١,٠٪
المحور ككل		٣٥	٠,٩٢٢	٩٢,٢٪

يتضح من جدول٨ أن قيمة معامل الفا كرونباخ للأداة عالية تصل إلى ٢،٩٢٪، وهذا يعني أن معامل الثبات مرتفع وأن الأداة صالحة للتطبيق.

٨. نتائج البحث

الإجابة عن السؤال الأول: الذي ينص على "ما درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بمفاهيم الأمن السيبراني لدى طلاب المرحلة الثانوية بالمملكة العربية السعودية؟"، تمت الإجابة عليه باستخدام المتوسطات الحسابية والانحرافات المعيارية، وجاءت النتائج كما في الجدول التالي:

جدول٩ : استجابات أفراد الدراسة على عبارات درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بمفاهيم الأمن السيبراني مرتبة تنازلياً حسب المتوسطات الحسابية

رقم الفقرة	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	الدرجة
٤	البرامج غير المرغوبة أو الملفات التي يمكن أن تسبب ضررا لجهاز الحاسب أو تهدد البيانات المخزنة عليه تسمى:	١,٨٦	٠,٣٥	١	عالية
٦	الحصول على معلومات الضحية ثم استخدامها ضده مقابل الحصول على المال أو يتم دفع الفدية تسمى:	١,٨٢	٠,٣٨	٢	عالية
٣	الذين يعملون على سرقة أو تخريب أو تحريف بيانات خاصة بدول أو منشأة أو أفراد آخرين لأغراض مالية أو سياسية أو للتسلية يطلق عليهم:	١,٧٩	٠,٤١	٣	عالية
٩	ترميز البيانات وجعلها غير قابلة للفك بدون مفتاح الترميز تسمى:	١,٧٨	٠,٤١	٤	عالية
٥	العيوب في البرامج الثابتة أو الأجهزة التي يمكن أن يستغلها المهاجم لأداء إجراءات غير مصرح بها في النظام تسمى:	١,٦٩	٠,٤٦	٥	عالية
١٠	الممارسات التي تقع ضد فرد أو مجموعة بهدف التسبب بالأذى لسمعة الضحية عمداً أو إلحاق	١,٥٤	٥،٠	٦	عالية

	الضرر النفسي أو البدني به تسمى :				
١١	عند طلب الدخول لبعض المواقع يلزم إدخال كود مرسل لهاتفك بعد إدخال اسم المستخدم وكلمة المرور، هذه الخاصية تسمى:	١,٥٣	٥،٠	٧	عالية
١	كلمة سيبراني تعني	٣،١	٠,٤٦	٨	منخفضة
٢	مفهوم الأمن السيبراني هو المفهوم الحديث لأمن المعلومات، ما رأيك بهذه العبارة؟	١,٢٥	٠,٤٣	٩	منخفضة
٨	تصميم مواقع أو إرسال رسائل بريد إلكتروني مطابقة للمواقع الأصلية بغرض الاحتيال تسمى :	١,١٩	٠,٣٩	١٠	منخفضة
٧	التحايل على مستخدم الحاسب بغرض الحصول على معلومات المفترض ألا يفصح عنها تسمى	١,٠٦	٠,٢٤	١١	منخفضة
	الدرجة الكلية للمحور	١,٥٣	٠,٤١		عالية

يتضح من جدول٩ أن درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية عالية، حيث بلغ المتوسط الحسابي الكلي للمحور ٥٣،١، والانحراف المعياري ٤١،٠، وهذا المتوسط يقع ضمن الفئة العالية التي تقع ما بين ١,٥١ و٢.

من الجدول يظهر أن الفقرة رقم ٤ حصلت على أعلى متوسط حسابي حيث بلغت ٨٦،١ وانحراف معياري ٣٥،٠، فيما حصلت الفقرات ٧، ٨، ٢، و١ على متوسطات حسابية منخفضة حيث بلغت ٠٦،١، ١٩،١، ٢٥،١، و٣،١ على التوالي، وبانحرافات معيارية بلغت ٢٤،٠، ٣٩،٠، ٤٣،٠، و٤٦،٠ على التوالي.

الإجابة على السؤال الثاني: والذي ينص على "ما درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية؟"، وتمت الإجابة بحساب المتوسطات الحسابية والانحرافات المعيارية وتحديد الرتب والدرجة لاستجابات أفراد الدراسة، وجاءت النتائج كما في الجدول١٠.

جدول١٠ : استجابات أفراد الدراسة على عبارات محور درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية مرتبة تنازلياً حسب المتوسطات الحسابية

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	الدرجة
٣	عند الاتصال بي من شخص يدعي أنه يعمل بأحد الجهات الحكومية أو البنوك، ويطلب مني بعض المعلومات الشخصية، فإنني لا أتردد في التعاون معه وتزويده بهذه المعلومات.	٤,٦٤	٠,٩٧	١	عالية جداً
١	عند وصول رسالة إلى بريدي الإلكتروني تفيد بحصولي على جائزة مالية، فإنني أقوم بتعبئة بياناتي على الرابط المرفق في الرسالة لاستكمال حصولي على الجائزة.	٤,٥٢	١،١	٢	عالية جداً
١٠	أستخدم بعض الكلمات المشهورة في كلمة المرور الخاصة بي (مثل: love).	٤,٤٥	١,١٣	٣	عالية جداً
٢	عند استعراض الأوسمة (الهاشتاقات) في تويتر ووجود خبر عن فضيحة أحد المشاهير، فإنني أضغط على الرابط المرفق مع التغريدة لمشاهدة الخبر.	٤,٢٨	١,٠٩	٤	عالية جداً
٤	عند وصول رابط إلكتروني إلى بريدي الإلكتروني، أو أحد حساباتي في وسائل التواصل الاجتماعي، فإنني أقوم بالضغط عليه وفتحه للتعرف على محتوى الموقع الإلكتروني.	٤,١٦	١,٢٠	٥	عالية
٥	أقوم بفتح الملفات التي يتم تنزيلها من الانترنت بشكل مباشر، للاطلاع على محتويات هذه الملفات.	٣,٨١	١,٣٢	٦	عالية
١١	أستخدم شبكات الانترنت العامة المجانية المتاحة في الأماكن العام وذلك لتصفح الانترنت.	٣,٧٣	١,٣٢	٧	عالية
١٢	لا أتابع التحديثات المستمرة لنظام تشغيل جوالي والتطبيقات المثبتة عليه.	٣,٦٨	١,٣٦	٨	عالية

١٣	لا يوجد برنامج حماية من الاختراق على جهاز الحاسب الخاص بي، وإن وجد فلم يتم تحديثه منذ أن تم تنصيبه.	٣,٦٤	٤،١	٩	عالية
٩	أستخدم أرقام أو حروف متتابعة (مثال: ABC أو ٢٣٤) في كلمة المرور الخاصة بي.	٣,٥٦	١,٥١	١٠	عالية
٧	أنشئ كلمات المرور لحساباتي المختلفة بحيث ترتبط ببعض بياناتي الشخصية كتاريخ ميلادي أو المدينة التي أعيش فيها لسهولة حفظها وتذكرها	٣,١٤	١,٥٥	١١	متوسطة
٨	أستخدم كلمة مرور واحدة لأكثر من حساب أملكه على الانترنت ليسهل تذكرها	٢,٨٧	١,٤٤	١٢	متوسطة
٦	أقوم بحفظ كلمات المرور Password على المتصفح (على سبيل المثال متصفح Google Chrome) حتى أتمكن من الدخول مستقبلا دون الحاجة لكتابتها مرة أخرى.	٢,٥٨	١,٤٥	١٣	منخفضة
الدرجة الكلية لمحور درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية		٣,٧٧	٠,٧٨	عالية	

من جدول١٠ يتضح أن طلبة المرحلة الثانوية بالمملكة العربية السعودية لديهم وعي عالي بالتهديدات السيبرانية، حيث بلغ المتوسط الحسابي الكلي للمحور ٧٧،٣ وبانحراف معياري ٧٨،٠. وحصلت العبارتين الاولى والعاشرة على أعلى متوسط حسابي حيث بلغ٥٢،٤ و٤٥،٤، وبانحراف معياري ١،١ و١٣،١ على التوالي؛ مما يشير إلى الوعي العالي جدًا لهذه التهديدات.

من جهة أخرى، حصلت الفقرة السادسة في المحور على أقل متوسط حسابي حيث بلغ ٥٨،٢ وبانحراف معياري ٤٥،١، وهذا يدل على أن وعي أفراد العينة تجاه هذا التهديد منخفض. كذلك على الرغم من أن الجدول يوضح وعي أفراد العينة تجاه التهديد السيبراني المحتمل نتيجة استخدام كلمة مرور واحدة لأكثر من حساب جاء بدرجة متوسطة إلا أن المتوسط الحسابي للفقرة يوضح قربها من الفئة المنخفضة حيث بلغ متوسطها الحسابي ٨٧،٢ وبانحراف معياري ٤٤،١.

الإجابة على السؤال الثالث: والذي ينص على "ما درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت؟"، وتمت الإجابة بحساب المتوسطات الحسابية والانحرافات المعيارية وتحديد الرتب والدرجة لاستجابات أفراد الدراسة، وجاءت النتائج كما في الجدول ١١.

جدول١١ : استجابات أفراد الدراسة على عبارات محور درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت مرتبة تنازلياً حسب المتوسطات الحسابية

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	الدرجة
١١	أحرص على عدم فتح الروابط التي تصلني من مصادر مجهولة أو غير موثوقة.	٤،٤	١,٢٥	١	عالية جداً
٦	أستخدم نظام التحقق الثنائي في معظم حساباتي على الانترنت.	٤,٢١	١,١٧	٢	عالية جداً
٨	أحرص على عدم فتح الملفات التي تصلني من مصادر مجهولة أو غير موثوقة إلا بعد فحصها ببرنامج الحماية من الفيروسات	١،٤	١,٣٦	٣	عالية
٩	أستخدم بريد إلكتروني خاص للاستخدامات الرسمية والهامة.	٣,٩١	١,٤٢	٤	عالية
٤	أقوم بمتابعة التحديثات لنظام تشغيل جوالي والتطبيقات المثبتة عليه بشكل دوري.	٣,٩	١,٣٦	٥	عالية
٢	أستخدم في كلمات المرور الخاصة بي مزيجاً من الأحرف الكبيرة والصغيرة والرموز الخاصة مثل (@ +١).	٣,٨١	١,٤١	٦	عالية
١٠	أحرص على عدم تصفح الانترنت ومواقعي الشخصية عن طريق الشبكات المتاحة في الأماكن العامة.	٣,٧٨	١,٤٢	٧	عالية
٧	أستخدم برامج مكافحة الفيروسات على جهازي الشخصي، وأقوم بتحديثها بشكل مستمر.	٣,٤٦	١,٥٤	٨	عالية

٥	أقوم بعمل نسخة احتياطية لمحرك القرص الصلب بالحاسب الخاص بي بشكل دوري ؛ وذلك تجنبا لفقدان البيانات والمعلومات المخزنة فيه.	٣,٣٣	١,٥٥	٩	متوسطة
١	أقوم بإنشاء كلمة مرور مختلفة في كل مرة يطلب مني انشاء حساب باسم مستخدم وكلمة مرور لموقع على الانترنت	٣,٢٤	١,٤٦	١٠	متوسطة
٣	أخرج من حسابي بعد الانتهاء من استخدام الانترنت.	٢,٦٩	١,٥٨	١١	متوسطة
	الدرجة الكلية لمحور درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت	٣,٧١	٠,٨٣		عالية

يظهر جدول١١ وعي عالي لأفراد العينة بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت، حيث بلغ المتوسط الكلي للمحور ٧١،٣ وبانحراف معياري ٨٣،٠. وكان اتفاق أغلب المستجيبين على الفقرة الحادية عشر من المحور، حيث حصلت على أعلى متوسط حسابي بلغ ٤،٤ وانحراف معياري ٢٥،١. من جانب آخر، كانت الفقرة الثالثة في المحور أقل فقرة اتفق عليها أفراد العينة، حيث بلغ متوسطها الحسابي ٦٩،٢ وانحرافها المعياري ٥٨،١.

الإجابة على السؤال الرابع: والذي ينص على: "هل توجد فروق ذات دلالة إحصائية عند مستوى ٠,٠٥ بين متوسطات استجابات أفراد العينة تعزى لمتغيرات (الجنس، الصف الدراسي، المنطقة الجغرافية، فترات استخدام الانترنت)؟" وتمت الإجابة عليه باستخدام اختبار (ت) لمجموعتين مستقلتين Independent T-test، وتحليل التباين الأحادي One Way ANOVA لأكثر من مجموعتين وجاءت النتائج كالآتي:

أولًا: الفروق بالنسبة لمتغير الجنس:

للإجابة على هذا الجزء من السؤال، استخدم اختبار ت للكشف عن درجة دلالة الفروق الإحصائية بين متوسطات استجابات أفراد العينة، وكانت النتيجة كما في جدول١٢.

جدول١٢ : اختبارت للنتائج المتعلقة بمتغير الجنس

المقاييس		المتوسط الحسابي	الانحراف المعياري	اختبارت	مستوى الدلالة
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بمفاهيم الأمن السيبراني	ذكر	١,٤٦٧	٠,١٥٦	٠,٤٨٣	٠,٦٢٩
	أنثى	١,٤٧٥	٠,١٦١		
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية	ذكر	٣,٧٥	٠,٨٥	٠,٥٦	٠,٥٨
	أنثى	٣,٧٩	٠,٧١		
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت	ذكر	٣,٨٢	٠,٨	٢,٤٨	٠,٠١
	أنثى	٣,٦٢	٠,٨٥		

يوضح جدول١٢ عدم وجود فروق ذات دلالة إحصائية عند مستوى ٠٥،٠ بين متوسطات استجابات أفراد العينة تبعا لنوع الجنس من حيث درجة وعيهم بمفاهيم الامن السيبراني والتهديدات السيبرانية المحتملة، في حين يظهر الجدول وجود فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد العينة في وعيهم بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت، وهذه الفروق جاءت لصالح الطلاب حيث بلغ المتوسط الحسابي لهذه الفئة ٨٢،٣ وبانحراف معياري ٨،٠، في حين كان المتوسط الحسابي للطالبات ٦٢،٣ وبانحراف معياري ٨٥،٠.

ثانيًا : الفروق بالنسبة لمتغير الصف الدراسي:

للإجابة على هذا الجزء من السؤال، استخدم أسلوب تحليل التباين الأحادي للكشف عن درجة دلالة الفروق الإحصائية بين متوسطات استجابات أفراد العينة، وكانت النتيجة كما في جدول١٣.

جدول١٣

اختبار (ANOVA) للفروق التي تعزى لمتغير الصف الدراسي

المقاييس	مصدر التباين	مجموع مربع الانحرافات	درجات الحرية	متوسط المربعات	F	مستوى الدلالة
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بمفاهيم الأمن السيبراني	بين المجموعات	٠,٠١	٢	٠,٠٠٥	٠,٢١	٠,٨١
	داخل المجموعات	٩,٩٢	١٩٧٧	٠,٠٢٥		
	المجموع	٩,٩٣	١٩٧٩			
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية	بين المجموعات	٦٨،١	٢	٨٤،٠	٤،١	٢٥،٠
	داخل المجموعات	٧٩،٢٣٦	١٩٧٧	٦،٠		
	المجموع	٤٨،٢٣٨	١٩٧٩			
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت	بين المجموعات	١,٠٧٠	٢	٠,٥٣	٠,٧٧	٠,٤٦
	داخل المجموعات	٢٧٤,١٨	١٩٧٧	٧،٠		
	المجموع	٢٧٥,٢٥	١٩٧٩			

يظهر من جدول١٣ عدم وجود فروق ذات دلالة إحصائية عند مستوى٠،٠٥، بين متوسطات استجابات أفراد العينة تبعا للصف الأول، الثاني، والثالث ثانوي تجاه المحاور الثلاثة للاستبيان.

ثالثًا: الفروق بالنسبة لمتغير المنطقة الجغرافية:

للإجابة على هذا الجزء من السؤال، استخدم أسلوب تحليل التباين الأحادي للكشف عن درجة دلالة الفروق الإحصائية بين متوسطات استجابات أفراد العينة، وكانت النتيجة كما في جدول١٤.

جدول ١٤ : اختبار (ANOVA) للفروق التي تعزى لمتغير المنطقة التي تتبع لها

المقاييس	مصدر التباين	مجموع مربع الانحرافات	درجات الحرية	متوسط المربعات	F	مستوى الدلالة
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بمفاهيم الأمن السيبراني	بين المجموعات	٠,٠٥٥	٤	٠,٠١٤	٠,٥٤٧	٠,٧٠١
	داخل المجموعات	٩,٨٧	١٩٧٥	٠,٠٢٥		
	المجموع	٩,٩٣	١٩٧٩			
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية	بين المجموعات	٦٩،٣	٤	٩٢،٠	٥٤،١	١٩،٠
	داخل المجموعات	٧٩،٢٣٤	١٩٧٥	٦،٠		
	المجموع	٤٨،٢٣٨	١٩٧٩			
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت	بين المجموعات	٣,٢٠٧	٤	٠,٨	١,١٥	٠,٣٣
	داخل المجموعات	٢٧٢,٠٥	١٩٧٥	٧،٠		
	المجموع	٢٧٥,٢٥	١٩٧٩			

يظهر من جدول١٤ عدم وجود فروق ذات دلالة إحصائية عند مستوى٠،٠٥، بين متوسطات استجابات أفراد العينة تبعا للمنطقة الجغرافية التي يتبع لها أفراد العينة تجاه المحاور الثلاثة للاستبيان.

رابعًا : الفروق بالنسبة لمتغير فترات استخدام الانترنت

للإجابة على هذا الجزء من السؤال، استخدم اختبار ت للكشف عن درجة دلالة الفروق الإحصائية بين متوسطات استجابات أفراد العينة، وكانت النتيجة كما في جدول١٥.

جدول١٥ : اختبار (ت) للنتائج المتعلقة بمتغير فترات استخدام الانترنت يومياً

المقاييس		المتوسط الحسابي	الانحراف المعياري	اختبار ت	مستوى الدلالة
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بمفاهيم الأمن السيبراني	أقل من خمس ساعات	١,٤٨	٠,١٦	٠,٦٨	٠,٣٩
	أكثر من خمس ساعات	١,٤٧	٠,١٥		
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بالتهديدات السيبرانية	أقل من خمس ساعات	٣,٧٢	٠,٨٢	١,٣٣	٠,١٨
	أكثر من خمس ساعات	٣,٨٣	٠,٧٣		
درجة وعي طلبة المرحلة الثانوية بالمملكة العربية السعودية بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت	أقل من خمس ساعات	٣,٧٦	٠,٧٩	١,١٧	٠,٢٤
	أكثر من خمس ساعات	٣,٦٦	٠,٨٨		

يظهر من جدول١٥ عدم وجود فروق ذات دلالة إحصائية عند مستوى٠,٠٥، بين متوسطات استجابات أفراد العينة تبعا للصف الأول، الثاني، والثالث ثانوي تجاه المحاور الثلاثة للاستبيان.

٩. مناقشة النتائج

يتضح أن أفراد العينة لديهم وعي عالي بمفاهيم الأمن السيبراني بشكل عام (الحبيب، ٢٠٢٢)، ولكن هناك بعض المصطلحات التي لا تزال تمثل تحدي لديهم. بمعنى آخر، تشير البيانات التي جمعت أن هناك معرفة عالية ببعض المصطلحات المتعلقة بالأمن السيبراني، مثل الفيروسات والابتزاز الإلكتروني، ولكن من جهة أخرى، يواجه المشاركون صعوبات في التعرف على بعض المفاهيم. مثال على ذلك، أغلب المستجيبين لا يعرفون المعنى الصحيح لكلمة سيبراني، ولا يدركون الفرق بين أمن المعلومات والأمن السيبراني، كما يظهر من استجاباتهم عدم معرفتهم بمصطلح

الهندسة الاجتماعية، وقد يرجع ذلك إلى أن المفاهيم غالبًا مرتبطة بالمعرفة أكثر من الممارسات. بمعنى آخر، عدم تعرض الطلاب والطالبات في المناهج الدراسية لموضوعات عن الأمن السيبراني، أو عدم التحاقهم بدورات متخصصة في مجال الأمن السيبراني، تجعلهم غير مدركين لهذه المفاهيم التي قد تكون أعمق نوعًا ما من غيرها من المفاهيم (Tekerek A. & Tekerek M.، ٢٠١٣).

كما يظهر من نتائج البحث أن المستجيبين لديهم الوعي العالي بالتهديدات السيبرانية المحتملة أثناء استخدام الانترنت. يعكس ذلك اتفاق أغلبهم على عدم التعاون مع المتصلين الغرباء وإعطائهم بياناتهم الشخصية، وعدم التفاعل مع رسائل الاصطياد الإلكتروني التي تصل على بريدهم (السواط وآخرون، ٢٠٢٠)، بالإضافة إلى البعد عن استخدام بعض الكلمات المشهورة في كلمات المرور التي تخصهم. وعلى الرغم من درجة وعيهم العالية بالتهديدات السيبرانية، إلا أنهم - وبحسب ما أظهرته النتائج- مستمرون في بعض الممارسات الخاطئة التي قد تسبب انتهاكًا لخصوصياتهم، حيث خلصت النتائج إلى أن معظم أفراد العينة يعمدون إلى حفظ كلمات المرور على المتصفح بشكل دائم؛ وذلك لسهولة الدخول مستقبلًا دون الحاجة لكتابتها مرة أخرى. وقد يعود ذلك إلى عدم الحصول على دورات في آليات وممارسات الأمن السيبراني؛ وبالتالي فهم يجهلون أن هذه الممارسة قد تؤدي إلى وصول الغرباء لبياناتهم (Hoonakker، ٢٠٠٩). وفي ذات السياق، تظهر النتائج أن كثير من أفراد العينة يستخدمون كلمة مرور واحدة لأكثر من حساب شخصي. وقد يعود ذلك إلى كثرة المواقع القائمة على الحوسبة السحابية، والتي تحتاج إلى اسم مستخدم وكلمة مرور للوصول، ولخوفهم من نسيان كلمة المرور، يعمدون إلى هذه الممارسة الخاطئة والتي قد يفقدون بها حساباتهم المختلفة على الانترنت في حال وصول المخترق لإحداها، وتتفق هذه النتيجة مع ما توصلت إليه دراسة Hoonakker (٢٠٠٩) وShen وآخرون (٢٠١٦).

كما تشير النتائج إلى وجود وعي عالي لأفراد العينة بطرق وأساليب حماية بياناتهم ومعلوماتهم أثناء استخدام الانترنت. ظهر ذلك من خلال حصول معظم الفقرات على درجات اتفاق عالية وعالية جدًا، أبرزها اتفاقهم على تجاهل الروابط والملفات التي تصلهم من مصادر غير موثوقة، واستخدام المصادقة الثنائية في معظم حساباتهم على الانترنت (السواط وآخرون، ٢٠٢٠؛ الشهري، ٢٠٢١). وبرغم هذه الدرجة العالية من الوعي بحماية بياناتهم، إلا أنهم يمارسون بعض الأخطاء التي قد تؤدي إلى فقدان بياناتهم أو تشويهها نتيجة وصول المهاجمون لها. حيث أظهرت النتائج أن معظم أفراد العينة لا يخرجون من حساباتهم بعد الانتهاء من استخدام الانترنت، وهي من الممارسات التي تقلل من الأمان أثناء استخدام الانترنت (المبيض، ٢٠٢٠)؛ وقد يعود ذلك إلى ضعف في معرفة وممارسة بعض طرق حماية البيانات والمعلومات التي قد تغيب عنهم نتيجة عدم خضوعهم لدورات في الأمن السيبراني.

وفي ذات السياق، أظهرت النتائج عدم وجود فروق ذات دلالة إحصائية عند مستوى ٠،٠٥ بين متوسطات استجابات أفراد العينة تبعا لمتغيرات المنطقة الجغرافية، الصف الدراسي، وفترات استخدام الانترنت. في حين وجدت الفروق بين استجابات أفراد العينة تبعا لمتغير الجنس في المحور المتعلق بالوعي بطرق حماية البيانات والمعلومات، وكانت لصالح الطلاب. بمعنى آخر، أن الطلاب لديهم وعي أكبر بطرق حماية البيانات والمعلومات أثناء استخدام الانترنت أكثر من الطالبات، وقد يعود ذلك إلى تقديم دورات أو نشرات توعوية من قبل إدارات التعليم أو المدارس للبنين.

وتلخيصًا لما سبق، فقد أظهرت النتائج وجود وعي عالي لمفاهيم الأمن السيبراني، التهديدات السيبرانية، وطرق حماية البيانات والمعلومات للمستجيبين، مع وجود بعض النقص المعرفي لديهم وبعض الممارسات الخاطئة التي لا تقلل من مستوى وعيهم. وهذه النتيجة اتفقت مع نتائج دراسة الحبيب (٢٠٢٢) والسواط وآخرون (٢٠٢٠)، وBhatnagar (٢٠٢٠)، إلا أنها تختلف مع ما توصل إليه بحث الصحفي وعسكول (٢٠١٩). وقد يكون لهذا الاختلاف مبررًا مقبولًا من حيث اختلاف العينة حيث أجريت على المعلمات بينما مجتمع هذا البحث طلبة المرحلة الثانوية، أضف إلى

ذلك، وقت تطبيق البحث حيث أجري قبل جائحة كورونا، في حين هذا البحث بعد الجائحة، ولا شك أن الخبرة والاهتمام بالتقنية لدى مستخدمي الانترنت اختلفت بعد الجائحة عنها قبلها.

١٠. توصيات البحث

بناء على ما توصلت إليه نتائج البحث، يوصى بما يلي:

- تقديم دورات تدريبية متخصصة بالأمن السيبراني لطلبة المرحلة الثانوية؛ وذلك لمعرفة بعض المفاهيم المتعلقة بالأمن السيبراني، وتصحيح بعض الممارسات الخاطئة في استخدام الانترنت والتي قد تتسبب في تهديد سيبراني لهم.
- تكثيف الموضوعات المتعلقة بالأمن السيبراني في المقررات الدراسية للمرحلة الثانوية.
- حث مكاتب تعليم البنات وإدارات المدارس الثانوية للطالبات بتقديم دورات ونشرات توعوية لهن؛ بهدف رفع مستوى وعيهن لطرق حماية بياناتهن.

١١. مقترحات مستقبلية

بناء على ما توصل إليه البحث، يُقترح بناء وحدة للأمن السيبراني ويتم تنفيذها على عينة من طلبة المرحلة الثانوية، بالإضافة إلى بناء برنامج إلكتروني يهدف إلى تعزيز مستوى الوعي بالأمن السيبراني لدى الطلبة.

المراجع العربية

إبراهيم، منال (٢٠٢١). الوعي بجوانب الأمن السيبراني في التعليم عن بعد. *المجلة العلمية لجامعة الملك فيصل*، ٢٢، ٢، ٢٩٩- ٣٠٧. https://doi-org.sdl.idm.oclc.org/10.37575/h/edu/0089

أبوزيد، عبدالرحمن (٢٠١٩) الأمن السيبراني الوطن العربي :دراسة حالة المملكة العربية السعودية.آفاق سياسية،ع٤٨، ٥٥- ٦١.

أحمد، أبوبكر (٢٠١٧). *إدارة المعرفة*. الطبعة الأولى، الرياض، المملكة العربية السعودية: مركز البحوث والتواصل المعرفي.

البيشي، منير (٢٠٢١). الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة. *مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، مج٢٩* ،ع٦ ،٣٥٣ - ٣٧٢.

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

الدمرداش، نانسي (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، ع٤١، ١٣٣١_ ١٤٢٧.

السعادات، خليل، والتميمي، ندى (٢٠٢٢). رفع الوعي بالأمن السيبراني لدى المعلمين في ضوء مبادئ تعليم الكبار.آفاق جديدة في تعليم الكبار، ع٣٢، ٢٥٥_ ٢٨٠.

الشايع، خالد (٢٠١٩). الأمن السيبراني- مفهومه وخصائصه وسياساته. الطبعة الأولى، القاهرة، مصر، الدار العالمية

الشهراني، بيان ، وفلمبان، فدوى (٢٠٢٠). أثر برنامج تدريبي قائم على تصميم ألعاب تعليمية إلكترونية باستخدام برنامج Marek Game لإكساب مفاهيم الامن السيبراني لدى طالبات المرحلة المتوسطة. *مجلة البحث العلمي في التربية*، ع٢١، ج٩، ٦١٤- ٦٥١.

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

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

الصحفي، مصباح، وعسكول، سناء (٢٠١٩). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. *مجلة البحث العلمي في التربية*، ع٢٠، ج١٠، ٤٩٣- ٥٣٤.

الصبان، عبير، الحربي، سماح (٢٠١٩). إدمان الطلاب على استخدام مواقع التواصل الاجتماعي وعلاقته بالأمن النفسي والتورط في الجرائم السيبرانية. *المجلة الدولية للدراسات التربوية والنفسية*، ج٦، ع٢، ٢٦٧- ٢٩٣.

العضياني، فهد (٢٠٢١). الأمن السيبراني وتحديات الذكاء الاصطناعي (الطبعة الأولى). شركة تكوين للطباعة والنشر والتوزيع.

غوص، أميرة، والشريف، باسم (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، ع ١٩٥* ، ج ٣، ٦٨٥ - ٧٣٤.

فتوح، وسام. (٢٠٢١). الأمن السيبراني في المنطقة العربية: توعية المصارف والمؤسسات المالية لإتباع المعايير العالمية .*مجلة اتحاد المصارف العربية، ع.٩٠*، ٥.

فرج، علياء (٢٠٢٢). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي: جامعة الأمير سطام بن عبد العزيز نموذجا. المجلة التربوية بجامعة سوهاج، مجلد ٩٤، ٥٠٩_ ٥٣٧.

فرحات، علاء الدين (٢٠١٨). أثر الجرائم الإلكترونية على البنى السوسيو اقتصادية. دفاتر السياسة والقانون، عدد خاص،. 167 - 148

القحطاني، ذيب (٢٠١٥). أمن المعلومات. مدينة الملك عبدالعزيز للعلوم والتقنية، الرياض.

القحطاني، عبدالله (٢٠٢٢). درجة الوعي بالأمن السيبراني لدى الأشخاص ذوي الإعاقة البصرية في المملكة العربية السعودية من وجهة نظرهم. *مجلة التربية الخاصة والتأهيل*، مج ١٤ ، ع ٥٠ – ١، ٣١.

القحطاني، نورة (٢٠١٩). مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية، *جمعية الاجتماعيين في الشارقة*، ٣٦ (١٤٤)، ٨٥- ١٢٠.

المبيض، محمد (٢٠٢٠). الوصايا العشر في الأمن السيبراني (الطبعة الأولى). مكتبة الملك فهد الوطنية.

المطيري، مشاعل (٢٠٢١). و اقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية. *المجلة الدولية للدراسات التربوية والنفسية*، ج١٠، ع٣، ٦٣٥- ٦٥٥. https://doi-org.sdl.idm.oclc.org/10.31559/EPS2021.10.3.7

المنتشري، فاطمة، حريري، رندة (٢٠٢٠). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للتربية النوعية*، ٤(١٣)، ٩٥- ١٤٠.

الهيئة الوطنية للأمن السيبراني. استعادة بتاريخ ١٤ يناير ٢٠٢٣. https://nca.gov.sa/news?item=366

الهيئة الوطنية للأمن السيبراني (٢٠٢١). استعادة بتاريخ ٣١ مارس ٢٠٢٣
https://cert.gov.sa/ar/awareness/awareness-materials/عرض- الموظفين/

References

Adams, Mackenzie (2017). Big Data and Individual Privacy in the Age of the Internet of Things. Technology Innovation Management Review, 7(4), 12-24.

Alammari, A. (1), Younes, S. (1,3), & Sohaib, O. (2). (2022). Developing and evaluating cybersecurity competencies for students in computing programs. PeerJ Computer Science, 8. https://doi-org.sdl.idm.oclc.org/10.7717/PEERJ-CS.827

Aldosari, F. F., Aldaihan, M. A., & Alhassan, R. A. (2020). Availability of ISTE Digital Citizenship Standards among Middle and High School Students and Its Relation to Internet Self-Efficacy. Journal of Education and Learning, 9(5), 59–74.

Alghamdi, M. Y., & Younis, Y. A. (2021). The use of computer games for teaching and learning cybersecurity in higher education institutions. Journal of Engineering Research (2307-1877), 9(3A), 143–151. https://doi-org.sdl.idm.oclc.org/10.36909/jer.v9i3A.10943

Bhatnagar, N., & Pry, M. (2020). Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study. Information Systems Education Journal, 18(1), 48–58.

Bhuyan, J., Wu, F., Thomas, C., Koong, K., Hur, J. W., & Wang, C. (2020). Aerial Drone: An Effective Tool to Teach Information Technology and Cybersecurity through Project Based Learning to Minority High School Students in the

U.S. TechTrends: Linking Research and Practice to Improve Learning, 64(6), 899–910.

Bronk, C., & Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. Survival, Vol. 55, Issue 2, 81-96.

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. Information (2078-2489), 13(4), 192. https://doi-org.sdl.idm.oclc.org/10.3390/info13040192

Dawson, M. (2022). An Argument for Cybersecurity in Saudi Arabia. Revista Academiei Fortelor Terestre, 27(1), 78–83. https://doi-org.sdl.idm.oclc.org/10.2478/raft-2022-0011

Hairston, J. R., Smith, D. W., Williams, T., Sabados, W. T., & Forney, S. (2020). Teaching Cybersecurity to Students with Visual Impairments and Blindness. Journal of Science Education for Students with Disabilities, 23(1).

Hoonakker, P., Bornoe, N., and Carayon. P. (2009). Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users. *Proceedings of the Human Factors and Ergonomics Society 53rd Annual Meeting*, October 19–23, San Antonio, Texas.

Jones, D., Greenhill, R., Shaw, C., Flores, D., & Schmidt, R. N. (2022). Cybersecurity Threats in the Healthcare Industry. Journal of Business & Educational Leadership, 12(1), 57–67.

Kemmerer, R. A. 2003. Cybersecurity. *Proceedings of the 25th IEEE International Conference on Software Engineering*: 705-715. http://dx.doi.org/10.1109/ICSE.2003.1201257

Khader M, Karam M, Fares H. (2021). Cybersecurity Awareness Framework for Academia. Information (2078-2489). 12(10):417. doi:10.3390/info12100417

Kritzinger, E. (2017). Cultivating a Cyber-Safety Culture among School Learners in South Africa. Africa Education Review, 14(1), 22–41.

Maina, F., Smit, J., & Serwadda, A. (2021). Professional Development for Rural STEM Teachers on Data Science and Cybersecurity: A University and School Districts' Partnership. Australian and International Journal of Rural Education, 31(1), 30–41.

Mat, B., Pero, S. D. M., Zengeni, K. T., & Fakhrorazi, A. (2022). Towards an Understanding of Emerging Cybersecurity Challenges of a Small State: A Case Study of Malaysia. Tamkang Journal of International Affairs, 25(3), 45–107. https://doi-org.sdl.idm.oclc.org/10.6185/TJIA.V.202204_25(3).0002

McCrohan, K., Engel, K., & Harvey, J. (2010). Influence of Awareness and Training on Cyber Security. Journal of Internet Commerce, 9(1), 23–41. https://doi-org.sdl.idm.oclc.org/10.1080/15332861.2010.487415

Mouton, F., Leenen, L., & Venter, H.S. (2016). Social Engineering Attack Examples, Templates and Scenarios. *Computers & Security*, Vol.59, p.186

Phair, N., & Alavizadeh, H. (2022). Cybersecurity skills of company directors — ASX 100. Journal of Risk Management in Financial Institutions, 15(4), 429–436.

Pollock, T., Levy, Y., Wei Li, & Kumar, A. (2022). Pilot testing of experimental procedures to measure user's judgment errors in simulated social engineering attacks. Online Journal of Applied Knowledge Management, 10(2), 23–40. https://doi-org.sdl.idm.oclc.org/10.36965/ojakm.2022.10(2)23-40

Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User Practice in Password Security: An Empirical Study of Real Life Passwords in the Wild. Computers & Security, 61, 130–141.

Tekerek, M, Tekerek, A (2013). A Research on Students' Information Security Awareness. Turkish Journal of Education, 2(3), 61-70

Wright, R., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems, 27*(1), 273–303. https://doi.org/10.2753/MIS0742-1222270111