درجة الوعي بالأمن السيبراني لدى طلبة المرحلة المتوسطة بالقصيم

إعداد

د. أمل سليمان الدخيل

أستاذ أصول التربية المساعد بجامعة القصيم

مجلة الدراسات التربوية والانسانية. كلية التربية. جامعة دمنهور. المجلد السابع عشر- العدد الرابع- الجزء الثاني- لسنة 2025

درجة الوعي بالأمن السيبراني لدى طلبة المرحلة المتوسطة بالقصيم

د. أمل سليمان الدخيل

مستخلص

هدفت هذه الدراسة إلى التعرف على درجة الوعي بالأمن السيبراني لدى طلبة المرحلة المتوسطة بمنطقة القصيم، وذلك من خلال بعدين رئيسين هما: الوعي المفاهيمي، والوعي السلوكي بالأساليب الاحترازية السيبرانية، واستخدمت الدراسة المنهج الوصفي المسحي، وتم تطبيق استبانة مكونة من (20) فقرة على عينة مكونة من (382) طالبًا وطالبة تم اختيارهم بطريقة عشوائية. وقد أظهرت النتائج أن مستوى الوعي السيبراني الكلي لدى طلبة المرحلة المتوسطة جاء بدرجة متوسطة، بمتوسط حسابي عام بلغ (2.11). كما بيّنت النتائج أن مستوى الوعي المفاهيمي بلغ متوسطًا قدره (2.10)، بينما بلغ الوعي السلوكي (2.11)، مما يشير إلى تقارب واضح بين الجانبين المعرفي والسلوكي للوعي السيبراني لدى الطلبة، وتُظهر النتائج أن الطلبة يمتلكون معرفة أساسية بمفاهيم الأمن السيبراني، كحماية المعلومات الشخصية واستخدام كلمات مرور قوية، إلا أن بعض الجوانب السلوكية التقنية مثل تحديث التطبيقات واستخدام الشبكات العامة ما زالت تحتاج إلى تعزيز تربوي وتطبيقي، وأوصت الدراسة بضرورة دمج مفاهيم ومهارات الأمن السيبراني ضمن المناهج الدراسية والأنشطة المدرسية بصورة عملية وتفاعلية، وتنمية التفكير النقدي لدى الطلبة عند التعامل مع التقنيات الرقمية، بما يسهم في بناء ثقافة رقمية آمنة ومستدامة في المجتمع التعليمي.

الكلمات المفتاحية:

الوعي، الأمن السيبراني، طلبة المرحلة المتوسطة

The Level of Cybersecurity Awareness Among Middle School Students in Al-Qassim

Dr. Amal Aldkhil

Assistant Professor of Education Foundation
College of Education - Alqassim University
email: 3911 @qu.edu.sa

Abstract
This study aimed to identify the level of cybersecurity awareness among intermediate school students in the qassim region, focusing on two main dimensions: conceptual cybersecurity awareness and behavioral cybersecurity awareness. The study employed the descriptive–analytical method, and a uestionnaire consisting of 20 items was administered to a randomly selected stratified sample of 382 students.The findings revealed that the overall level of cybersecurity awareness among intermediate students was moderate tending toward high, with a total mean score of (2.11). The mean score for conceptual awareness was (2.10), while behavioral awareness reached (2.11), suggesting a close alignment between the cognitive and behavioral dimensions of cybersecurity awareness among students. Results further indicated that students possess a fundamental understanding of cybersecurity concepts, such as protecting personal information and using strong passwords. However, some behavioral and technical practices—such as updating applications regularly and avoiding public Wi-Fi networks -still re uire further enhancement through educational and practical interventions. In light of these findings, the study recommends integrating cybersecurity concepts and skills into the school curricula and extracurricular activities in an interactive and experiential manner, and fostering students' critical thinking skills when engaging with digital technologies, to promote a safe and sustainable digital culture within the educational community.

Keywords: *Awareness, Cybersecurity, Middle School Students*

المقدمة

يُعَدّ الأمنُ الركيزةَ الأساسيةَ لاستقرار المجتمعات وتقدّمها، إذ لا يمكن تصوّر بناء حضارة راسخة، أو تشييد منظومة اجتماعية متحضّرة، دون أن يسودها الأمن بمستوياته المختلفة؛ ومع التحوّل الرقمي المتسارع الذي يشهده العالم المعاصر اتّسع مفهوم الأمن ليشمل أبعادًا جديدة ترتبط بالفضاء السيبراني والتقنيات الرقمية وشبكات الإنترنت، فأصبح الأمن السيبراني أحد المكونات الجوهرية للأمن الشامل.

وقد رافق التطور السريع في تكنولوجيا المعلومات والاتصالات ازدياداً ملحوظاً في استخدام الحواسيب ووسائل الاتصال داخل القطاعات الحيوية للمؤسسات المختلفة، مما جعل حماية الفضاء السيبراني ضرورةً استراتيجية لضمان استقرار المجتمع وأمنه، حيث يشير تقرير هيئة الاتصالات في المملكة العربية السعودية 2022 أن نسبة مستخدمي الأنترنت تصل 98,6% من السكان، ويذكر التقرير بأن 49.4% من مستخدمي الإنترنت يقضون 7 ساعات وأكثر يوميا في تصفح الإنترنت (وكالة الأنباء السعودية واس،2023) والزيادة في عدد المتصلين بالفضاء السيبراني يزيد من احتمالية الاعتداءات والجريمة المرتبطة بالتكنولوجيا، من خلال ما يعرف بالجرائم السيبرانية؛ مما يتسبب في اختراق الأنظمة؛ وقد تصل إلى خسائر فادحة في بعض الأحيان حد تزييف البيانات والتلاعب بها أو محوها (المنيع،2022). كما ظهر تهديدات جديدة لمستخدمي شبكة الانترنت بصور وأساليب متعددة.

ولا يقتصر تأثير المخاطر السيبرانية على الحدود المحلية فحسب، بل أصبح المجتمع السعودي مستهدفًا من قبل المنظمات الإجرامية الدولية نظرًا للمكانة الاقتصادية والجغرافية المتميزة التي تتمتع بها المملكة العربية السعودية (البقمي 2007).

مشكلة الدراسة

بناء على التقرير السنوي الصادر من مركز الأمن الالكتروني (2019) الذي أشار إلى حجم التهديدات الالكترونية في السعودية باستخدام البرمجيات الخبيثة، وأدوات، وطرق جديدة، بهدف الوصول إلى المعلومات الحساسة وإلحاق الضرر بالجهات الحكومية والخاصة، والتعليم أحدها حيث بلغت نسبة الخسائر الالكترونية فيه 14% .

والطلبة جزء من هذه المنظومة وهم في عمر المراهقة يقضون وقتا طويلا من حياتهم اليومية على المواقع الإلكترونية وشبكة الانترنت، ويتعرضون نتيجة لذلك إلى العديد من المخاطر السيبرانية؛ وتشير دراسة Coughlin.T (2017) إلى أن الطلبة يتعرضون للعديد من الهجمات الإلكترونية التي من شأنها أن تؤثر عليهم بالسلب.

وقد أكدت الدراسات أن الطلبة يواجهون تهديدات رقمية متكررة وهم في حاجة ملحّة لبرامج إرشادية وتربوية تستهدف المدرسة والأسرة معًا (Alghamdi, 2022).

ويشير Saeed (2023) إلى وجود فجوات واضحة في الممارسات الأمنية والمهارات الوقائية، ويؤكد على وجود تفاوتاً في مستوى الوعي بين الطلبة، يرتبط بعوامل متعددة كالخلفية الأكاديمية والموقع الجغرافي.

كما تشير دراسة القحطاني (2019) إلى أن التهديدات السيبرانية تمثل خطراً جسيماً على أمن المملكة العربية السعودية، مما يستدعي تعزيز الوعي المجتمعي بها للحد من آثارها وتفادي مخاطرها؛ كما تؤكد على أهمية إجراء المزيد من الدراسات للوقوف على مدى إدراك أفراد المجتمع السعودي لمفهوم الفضاء السيبراني، وفهم طبيعة الجرائم الإلكترونية التي يمكن أن تُرتكب عبره، والتدابير الوقائية اللازمة للتخفيف من حدتها لذا جاءت الدراسة الحالية للوقوف على درجة وعي طلبة المرحلة المتوسطة بالقصيم بالأمن السيبراني.

أسئلة الدراسة:

تمثلت مشكلة الدِّراسَة في التساؤل الرئيس التالي: ما درجة الوعي بالأمن السيبراني لدى طلبة المرحلة المتوسطة بالقصيم؟

ويتفرع عنه الأسئلة التالية:

1. ما درجة وعي طلبة المرحلة المتوسطة بالقصيم بمبادئ الأمن السيبراني؟
2. ما درجة وعي طلبة المرحلة المتوسطة بالقصيم بالأساليب الاحترازية السيبرانية؟

أهداف الدراسة:

ركَّزت الدِّراسَة على الهدف الرئيس التالي: الوقوف على درجة الوعي بالأمن السيبراني لدى طلبة المرحلة المتوسطة بالقصيم.

وتفرَّع عنه الأهداف الفرعيَّة التالية:

1.الكشف عن درجة وعي طلبة المرحلة المتوسطة بالقصيم بمبادئ الأمن السيبراني.

2.التعرف على درجة وعي طلبة المرحلة المتوسطة بالقصيم بالأساليب الاحترازية السيبرانية.

أهمية الدراسة:

يمكن تناول أهمية الدراسة من جانبين: الأهمية النظرية، والأهمية التطبيقية على النحو التالي:

الأهمية النظرية:

مما يعزز أهمية هذه الدراسة عنايتها بالأمن السيبراني في عصر التحول الرقمي المتسارع الذي يشهده العصر الحالي؛ حيث أصبحت التهديدات السيبرانية أحد أبرز التحديات التي تواجه الأفراد والمجتمعات، لا سيما فئة المراهقين؛ كما تأتي هذه الدراسة استجابة للتوجهات العالمية التي تدعو لتعزيز الوعي بالأمن السيبراني لدى فئات المجتمع؛ مما يسهم في بناء مجتمع رقمي آمن.

الأهمية التطبيقية :

قد تسهم الدراسة في توجيه اهتمام القائمين على التعليم إلى أهمية إدراج مبادئ الأمن السيبراني ضمن المناهج الدراسية، وعقد دورات تدريبية للطلبة والمعلمين في مجال الأمن السيبراني.

حدود الدراسة: تكونت حدود هذه الدراسة مما يلي:

-الحدود الموضوعية: الوعي بالأمن السيبراني

- الحدود البشرية: أجريت هذه الدراسة على طلبة المرحلة المتوسطة

-الحدود المكانية: طبقت هذه الدراسة في القصيم بمدينة بريدة

-الحدود الزمانية: تم تطبيق الدراسة في الفصل الدراسي الثالث من العام الدراسي 1446هـ

الدراسات السابقة

دراسة الحباشنة (2023) هدفت هذه الدراسة إلى التعرف على درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية تربية وتعليم قصبة الكرك، وطرق تنمية الوعي لديهم، والكشف عن الفروق في درجة الوعي بالأمن السيبراني، وطرق تنميته لدى المعلمين في ضوء المتغيرات الآتية: النوع الاجتماعي، والمؤهل العلمي، والمواد التي يدرّسها المعلم، وسنوات الخبرة في التدريس. وقد استخدمت الدراسة المنهج الوصفي المسحي، وتكونت عينة الدراسة من271 معلمًا ومعلمة، واستخدمت الاستبانة لتحقيق نتائجها ومن أهم النتائج التي توصلت إليها: أن درجة

الوعي بالأمن السيبراني لدى المعلمين جاءت بدرجة مرتفعة، وأن طرق تنمية الوعي بالأمن السيبراني جاءت على النحو الآتي: استخدام المواقع الإلكترونية التي تعمق القيم الدينية والأخلاقية، واستخدام التطبيقات الآمنة والبرامج التعليمية.

دراسة المنتشري وحريري (2020)، هدفت الدراسة إلى التعرف على درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، ولتحقيق أهداف الدراسة تم اتباع المنهج الكمي الوصفي التحليلي، واستخدمت الاستبانة كأداة لجمع البيانات. وجاء من أبرز النتائج أن معلمات المرحلة المتوسطة على درجة متوسطة من الوعي بكل من مفاهيم الأمن السيبراني، وأوصت الدرسة بضرورة عقد دورات تدريبية للمعلمات في مجال الأمن السيبراني، وورش عمل حول إجراءات الحماية ضد الانتهاكات السيبرانية

دراسة الشهري (2021) والتي هدفت إلى التعرف على دور إدارة الجامعة في تعزيزِ الوعيِ بالأمنِ السيبرانيّ لدى طلبةِ كليةِ التربية بجَامِعَة الإمَام محمد بن سعود الإسلامية، والكشف عن درجة معرفتهم بالأمن السيبرانيّ، معتمدة المنهج الوصفيَّ المسحي، والاستبانة كأداة للدراسة، وتوصلت إلى عدد من النتائج من أبرزها أن معرفة طلبة كلية التربية في جَامِعَة الإمَام محمد بن سعود الإسلامية بالأمن السيبرانيّ جاءت بدرجة متوسطة، وأن ممارسة إدارة الجامعة لدورها في تعزيز الوعي بالأمن السيبرانيّ لدى هؤلاء الطلبة جاءت بدرجةٍ متوسطةٍ، كما قدمت الدِّرَاسَةُ مجموعة من التوصيات؛ من أبرزها: دعم وتبني إدارة الجامعة لبرامج وحملات لتوعية طلابها بالأمن السيبرانيّ، ومخاطر الجرائم الإلكترونية.

بينما هدفت دراسة شعبان (2021) إلى التعرف على دور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول، واعتمدت الدراسة المنهج الوصفي باستخدام الاستبانة وقد توصلت نتائج الدراسة إلى تقديم تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول.

الزبيدي، وآخرون (2021) هدفت هذه الدراسة للتعرف على مستوى الوعي بالأمن السيبراني، ومستوى الانتماء الوطني لدى طلبة المرحلة الثانوية بمدينتي مكة وجدة بمنطقة مكة المكرمة، كما سعت إلى معرفة الفروق في الانتماء بين أفراد الدراسة، والذي يعزى لاختلاف خصائصهم

الديموغرافية كالجنس، والمدينة، والتخصص، والمرحلة الدراسية، بالإضافة إلى الكشف عن العلاقة بين الوعي بالأمن السيبراني وقيم الانتماء الوطني، ومعرفة الاسهام الذي يسهمه متغير الوعي بالأمن السيبراني في قيم الانتماء الوطني وذلك باختبار نموذج خطي بينهما بأسلوب الانحدار الخطي البسيط، و اعتمدت الدراسة مقياس الوعي بالأمن السيبراني، وأشارت النتائج إلى أن الطلبة لديهم مستوى وعي متوسط في التعامل مع الأجهزة ووسائل التخزين، ومستوى وعي عالٍ في التعامل الآمن مع خدمات الإنترنت والبرامج.

الفجوة البحثية في الدراسات السابقة:

أظهرت الدراسات السابقة اهتمامًا بقياس الوعي السيبراني لدى المعلمين وطلاب الجامعة والثانوية، مثل دراسة الحنايشة (2022)، والمنتشري وحريري (2020) بدراسة المعلمين، وشعبان (2021) بطلاب الدراسات العليا ودراسة الشهري(2021) بدراسة طلاب الجامعة و الزبيدي، وآخرون (2021) بطلبة المرحلة الثانوية إلا أن الأدبيات تفتقر إلى أبحاث تركز تحديدًا على طلبة المرحلة المتوسطة، رغم أنهم يشكلون شريحةً هامة في المجتمع تمر بمرحلة حرجة في النمو النفسي والاجتماعي، وتتعرض مبكرًا للتكنولوجيا دون ضوابط كافية.

وعليه فإن هذا الفرع البحثي يُعدُّ ضروريًا لسد الفجوة المعرفية وتوفير بيانات داعمة لصناع السياسات التعليمية.بالإضافة إلى أن الدول الرقمية ممثل المملكة العربية السعودية تتبنى استراتيجيات وطنية للأمن السيبراني تعتمد على بناء جيل واعٍ تقنيًا. كما أن دراسة الوعي لدى طلبة المرحلة المتوسطة تُسهم مباشرةً في تحقيق أهداف هذه الاستراتيجيات.

الإطار المفاهيمي:

مفهوم الأمن السيبراني:

يُعرف الشايع (2019 ص24) الأمن السيبراني بأنه " مجموعة من التكنولوجيا والخدمات والممارسات المصممة لحماية أجهزة الحاسوب وشبكات الاتصال والبيانات من التخريب أو الهجمات أو الدخول غير المصرح به "

بينما يُعرفه جبور (2012، ص 58) بأنه "النشاط الذي يؤمن حماية الموارد (البشرية والمالية) المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي

تترتب في حال تحقق المخاطر والتهديدات كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج، ولا تتحول الأضرار إلى خسائر دائمة".

وتعرفه الدراسة الحالية: بأنه "جميع إجراءات حماية شبكة المعلومات التي تؤمن الحد من الخسائر الناتجة عن الهجمات والتهديدات والدخول غير المصرح للبيانات".

الأهمية التربوية للأمن السيبراني

في خضم التسارع المتعاظم للتحول الرقمي واتساع نطاق الاعتماد على البيئات الإلكترونية في المجال التعليمي، برز الأمن السيبراني كحجر زاوية في البنية التحتية للتربية الحديثة. لم يعد دوره مقتصراً على تأمين سلامة البيانات والمعلومات فقط، بل تجاوزه ليشمل بناء ثقافة رقمية وقائية بين الطلاب والمعلمين على حد سواء، تمكنهم من إدارة المخاطر المحتملة واتخاذ الإجراءات الاستباقية تجاهها.

وتزيد هذه الأهمية بشكل خاص فيما يتعلق بطلبة المدارس جيل الإنترنت الذين تفاعلوا مع التقنيات الرقمية منذ نعومة أظفارهم؛ إذ تشير المؤشرات إلى تزايد مطّرد في أعداد المستخدمين من هذه الفئة العمرية لأغراض متعددة، كالتعلم الذاتي، والتسلية، ومنصات التواصل الاجتماعي، إلا أن هذا الاتصال الموسع يقابله نمواً متزايداً في فرص التعرض للجرائم الإلكترونية، حيث يُعدّ افتقار العديد من الطلاب والمعلمين إلى الوعي الكافي بهذه التهديدات، وآليات الحماية منها عاملاً محورياً في وقوعهم ضحايا لها؛ مما ينتج عنه عواقب وخيمة تتراوح بين الخسائر المادية والآثار النفسية والاجتماعية التي تطال الفرد والمؤسسة التعليمية على السواء. وفي هذا السياق تؤكد الدراسات كدراسة المنتشري وحريري (2020)، على الحاجة الملحة لتعميق البحث في آليات دمج الأمن السيبراني كمدخل استراتيجي لتعزيز أمن المنظومة التربوية برمتها.

وتتجلى الأهمية التربوية للأمن السيبراني في كونه ركيزة أساسية لبناء مجتمع رقمي آمن ومثقف، وذلك من خلال:

أولاً: تعزيز الوعي السيبراني لدى الطلاب

نظراً لأن التعليم الرقمي أصبح مكوناً جوهرياً في العملية التعليمية، بات الطلاب عرضة لمخاطر متعددة، مثل: الاختراق، والتَّصَيُّد الاحتيالي، والتنمر الإلكتروني، وانتهاكات الخصوصية. وعليه،

تبرز الحاجة إلى إدماج مفاهيم الأمن السيبراني ضمن المناهج الدراسية؛ لتعليم الطلاب كيفية حماية حساباتهم الشخصية، والتعرُّف على الهجمات الإلكترونية الشائعة، فضلاً عن تعزيز فهمهم لأخلاقيات الاستخدام الرقمي وأهمية الحفاظ على الخصوصية.

ثانياً: حماية البيانات التعليمية والمؤسسية

يُعدّ تطبيق معايير الأمن السيبراني في المؤسسات التعليمية ضرورة حتمية لضمان بيئة تعليمية آمنة، ولحماية البيانات الحساسة من التسرب أو الاستغلال. فالتوعية والتطبيق العملي يسهمان معاً في إعداد جيل واعٍ بمخاطر الفضاء السيبراني، وقادر على توظيف التقنية بشكل آمن وفعّال.

الأبعاد الأساسية للأمن السيبراني في المؤسسات التعليمية:

إن للأمن السيبراني علاقة بجوانب مختلفة تتحد معا لتحقيق منظومة أمن مترابطة في المؤسسات التعليمية من أي تهديد سيبراني محتمل، ويمكن توضيح أبعاد الأمن السيبراني في المؤسسات التعليمية كما يلي:

1. البعد التقني:

يرتكز هذا البعد على حماية البنية التحتية الرقمية من خلال أدوات وتقنيات متخصصة. وتشمل مجالاته: أنظمة كشف التسلل، جدران الحماية، التشفير، وإدارة الثغرات الأمنية. ويؤكد (Scholl, 2021) أن ضمان توافر أنظمة الحماية التقنية مثل أنظمة كشف التسلل، ويُعد خط الدفاع الأول لحماية الشبكات المؤسسية من الهجمات الإلكترونية المتنوعة.

2. البعد البشري والمؤسسي:

يهدف هذا البعد تعزيز وعي وسلوك المستخدمين كالمعلمين والطلاب والإداريين الذين يُعدون غالباً الحلقة الأضعف في منظومة الأمن السيبراني. حيث تشير دراسة (Al-Mohannadi et al, 2023) إلى أن نسبة تصل إلى 60% من حوادث الاختراق في القطاع التعليمي تعزى بشكل أساسي إلى أخطاء بشرية أو ممارسات غير آمنة من قبل المستخدمين، مما يبرز الحاجة الملحة لبرامج تدريبية مكثفة.

3. بُعد حماية البيانات والخصوصية:

يركز على ضمان سرية وسلامة البيانات الشخصية والتعليمية الحساسة، والامتثال للوائح حماية البيانات مثل نظام حماية البيانات الشخصية في المملكة العربية السعودية. ويوضح Smith & Jones, (2022) أن تطبيق مبادئ التشفير طوال دورة حياة البيانات؛ وهو معيار حاسم للحفاظ على سرية السجلات الأكاديمية والبحثية ومنع الوصول غير المصرح به.

4. البعد القانوني والتنظيمي:

وهو بُعدٌ يتعلق بضرورة امتثال المؤسسة التعليمية للقوانين واللوائح والسياسات الوطنية والدولية المنظمة للأمن السيبراني، وتحديد المسؤوليات القانونية المترتبة على حالات الاختراق يشير Alrashed & Alharbi, (2024) في دراستهما حول السياسات في المملكة العربية السعودية أن متطلبات الهيئة الوطنية للأمن السيبراني (NCA) وإطار العمل (SCF) تُلزم المؤسسات التعليمية بتطوير خطة استجابة للحوادث الإلكترونية والإبلاغ عنها في غضون وقت محدد.

أهداف الأمن السيبراني

يهدف الأمن السيبراني كما ذكرت الهيئة الوطنية للأمن السيبراني (2025) كما يلي:

-حماية الأصول المعلوماتية والتقنية وتوفير الحلول التقنية اللازمة لحمايتها.

-تعزيز أفضل الممارسات في مجال الأمن السيبراني

-تعزيز الوعي بالأمن السيبراني من خلال قنوات متعددة، وبناء ثقافة إيجابية للأمن السيبراني.

مفاهيم الأمن السيبراني وصور المخاطر السيبرانية:

يتفرع عن مفهوم الأمن السيبراني عدد من المفاهيم مرتبطة بصور المخاطر السيبرانية منها:

الاحتيال الإلكتروني: وفي الاحتيال يتخذ المحتال صفة رسمية أو اعتبارية أو الإيهام بمشروع وهمي ليتمكن من الاستيلاء على بيانات الضحية (الربيعة 2018).

التجسس الإلكتروني: يكون من خلال برامج سرية تجمع معلومات المستخدم وعادة ما يتم تضمين برامج التجسس مكونات مجانية خفية أو برامج يمكن تنزيلها من شبكة الانترنت، تبدأ في مراقبة حركة المستخدم على الانترنت واستغلالها في الهجمات السيبرانية (القحطاني، 2015).

الهندسة الاجتماعية: وهي مجموعة من الأساليب التي يستخدمها المجرمون في الحصول على المعلومات الهامة والحساسة أو إقناع الضحايا بتنفيذ بعض الإجراءات التي تساعد على اختراق أنظمتهم والإضرار بهم (عبد الصادق،2014)

التصيد الإلكتروني: ويتم فيها استخدام الرسائل الإلكترونية التي صممت تبدو وكأنها تابعه لجهة حقيقية والتي صممت للوصول إلى المعلومات الهامة والحساسة (أبو منصور، 2017)

التشهير الإلكتروني: من خلال بث أخبار لأجل الإضرار المباشر وغير المباشر بشخص أو جهة إما باختراق موقع الضحية وتغيير محتوياته، أو نشر أخبار غير صحيحة عنه ويطال هذا النوع الأفراد والمؤسسات على حد سواء (متولي،2015).

الدراسة الميدانية:

مجتمع الدراسة:

تكون مجتمع الدراسة من جميع طلبة المرحلة المتوسط في القصيم من الجنسين التعليم الحكومي والبالغ عددهم 47893 طالب وطالبة منهم 23818 طالبة و24075 طالب حسب إحصائيات التعليم (وزارة التعليم،2024)

عينة الدراسة:

تم اختيار عينة عشوائية من طلبة المرحلة المتوسطة بالمدارس الحكومية ببريدة في إمارة القصيم وفق معادلة جيجر وبلغ عددها (382) طالبا موزعة على النحو التالي: 197 طالب و185 طالبة.

$$n = \frac{\left(\frac{z}{d}\right)^2 \times (0.50)^2}{1 + \frac{1}{N}\left[\left(\frac{z}{d}\right)^2 \times (0.50)^2 - 1\right]}$$

أداة الدراسة:

تم إعداد استبانة لقياس درجة وعي طلبة المرحلة المتوسطة بالأمن السيبراني، اشتملت بصورتها النهائية على (20) عبارة وأمام كل عبارة منها ثلاث بدائل على مقياس ليكرت الثلاثي متدرج (موافق، محايد، غير موافق) وقد تحققت الباحثة من صدق المحكمين بعرض الصورة الأولية لها على مجموعة من المحكمين وتمَّ تعديل بعض العبارات، وحذف بعضها وفقًا للتوجيهات التي أبدوها.

الصدق البنائي للأداة:

لحساب الصدق والثبات لأداة الدِّراسَة؛ قامت الباحثة باختيار عينة عشوائيَّة استطلاعيَّة، قوامها (35) طالب وطالبة (من مجتمع الدِّراسَة الأصلي) بهدف التحقُّق من صلاحيَّة الأداة للتطبيق على عينة الدِّراسَة، وذلك من خلال حساب صدقها وثباتها بالطُّرق التي تناسب طبيعة أداة الدِّراسَة.

صدق الاتساق الداخلي:

تمَّ التأكُّد من صدق الاتساق الداخلي للاستبانة، وذلك بحساب معامل الارتباط بين درجة كلِّ عبارة ومتوسِّط درجات المحور الذي تنتمي إليه، وذلك للتأكُّد من مدى تماسُك وتجانُس عبارات كلِّ محور فيما بينها، وذلك باستخدام معامل ارتباط (بيرسون)، والاستجابة للمقياس وفقًا للتدرُّج الثلاثي على طريقة "ليكرت" (موافق – أحيانًا – غير موافق)، فجاءت معاملات الارتباط كما هي موضَّحة في جدول (1):

جدول (1) معاملات الارتباط (الصدق الداخلي) لفقرات الاستبانة حسب المحور

المحور	عدد الفقرات	نطاق معاملات الارتباط(r)	الدلالة الإحصائية
الوعي المفاهيمي	10	0.61 – 0.84	دالة عند 0.01
السلوك الاحترازي	10	0.63 – 0.87	دالة عند 0.01
الاستبانة ككل	**20**	**0.61 – 0.87**	**دالة عند 0.01**

تُظهر هذه النتائج أن جميع الفقرات ترتبط ارتباطًا موجبًا ودالًا بمحاورها، مما يدل على أن الأداة تقيس المفاهيم والسلوكيات المتعلقة بالوعي السيبراني بدقة واتساق، وأنها مناسبة للتحليل الإحصائي اللاحق.

ثانياً: ثبات الأداة

لقياس ثبات الاستبانة تم حساب معامل كرونباخ ألفا (Cronbach's Alpha) لكل محور وللأداة ككل. وقد بينت النتائج أن جميع القيم جاءت ضمن النطاق المقبول علميًا (0.70 ≤)، مما يدل على ارتفاع درجة الاتساق الداخلي وثبات مفردات الأداة وجدول (2) يوضح ذلك.

جدول (2) معاملات الثبات (كرونباخ ألفا) لمحاور الاستبانة

المحور	عدد الفقرات	مستوى الثبات	معامل الثبات(α)	التفسير
الوعي المفاهيمي	10	مرتفع	0.86	يدل على اتساق داخلي قوي بين الفقرات المفاهيمية.
السلوك الاحترازي	10	مرتفع	0.89	يشير إلى تجانس ملاحظ في سلوكيات الأمان الرقمي.
الاستبانة ككل	20	مرتفع جداً	0.91	تعكس موثوقية عالية للأداة ككل وقدرتها على القياس بثبات.

تشير نتائج الصدق والثبات إلى أن أداة قياس مستوى الوعي السيبراني لدى طلبة المرحلة المتوسطة بمنطقة القصيم تتمتع بدرجة عالية من الموضوعية والاتساق الداخلي، مما يعزز الثقة في صلاحيتها لقياس البعدين المفاهيمي والسلوكي الاحترازي للوعي السيبراني.

نتائج الدراسة وتفسيرها:

نتائج الإجابة على السؤال الأول

نص السؤال الأول على: ما درجة وعي طلبة المرحلة المتوسطة بالقصيم بمبادئ الأمن السيبراني؟

وللإجابة عن هذا السؤال؛ استخدمت الباحثة التكرارات، والنسب المئويَّة، والمتوسِّط الحسابي، والانحراف المعياري، وترتيب المتوسطات الحسابيَّة ترتيبًا تصاعديًّا، وجاءت النتائج كما هو موضَّح في جدول (3):

المحور الأول المحور الأول: الوعي بالمفاهيم والمبادئ

جدول (3) المتوسِّط الحسابي، والانحراف المعياري للوعي بمفاهيم ومبادئ الأمن السيبراني

الرتبة	رقم العبارة	نص العبارة	الانحراف المعياري	المتوسط الحسابي
1	5	أعلم أن مشاركة الصور الخاصة قد تسبب مشاكل	0.59	2.23
2	4	أميز بين المواقع الآمنة وغير الآمنة	0.60	2.20
3	9	أدرك أهمية التحقق من هوية الشخص قبل قبول الطلبات	0.63	2.15
4	10	أعرف أنني لا يجب أن أشارك حسابي مع أحد	0.64	2.13
5	3	أعرف أهمية استخدام كلمات مرور قوية	0.68	2.08
6	6	أعرف أن هناك قوانين تحمي من الجرائم الإلكترونية	0.70	2.04
7	2	أفهم مخاطر مشاركة المعلومات الشخصية على الإنترنت	0.72	2.00
8	1	أعرف معنى مصطلح الأمن السيبراني	0.73	1.96
9	7	أفهم أسباب خطورة النقر على روابط غير معروفة	0.74	1.95
10	8	أعرف أن حفظ كلمة المرور في مكان آمن مهم	0.78	1.91

أظهرت نتائج تحليل محور الوعي المفاهيمي أن المتوسط الحسابي العام بلغ (2.10) بانحراف معياري قدره (0.67)، وهو ما يشير إلى مستوى وعي معرفي متوسط يميل إلى الجيد لدى طلبة المرحلة المتوسطة في منطقة القصيم، وهذه النتيجة تتفق مع عدد من الدراسات السابقة كدراسة المنتشري وحريري (2020) ودراسة الشهري (2021) ودراسة الزبيدي، وآخرون (2021) التي

توصلت إلى أن الوعي بالأمن السيبراني كان متوسطا، بينما تختلف هذه النتيجة عنما توصلت إليه دراسة الحباشنة (2023) والتي أظهرت أن درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية تربية وتعليم قصبة الكرك مرتفعة، و ربما يعود ذلك لنوع العينة، ومستوى تأهيلهم واختلاف البيئة الجغرافية.

والنتيجة التي توصلت إليها الدراسة الحالية تدل على أن أفراد العينة يمتلكون فهماً مقبولاً للمفاهيم الأساسية للأمن السيبراني، مثل أهمية حماية المعلومات الشخصية، وأهمية استخدام كلمات مرور قوية، والتمييز بين المواقع الآمنة وغير الآمنة، إضافة إلى إدراكهم للمخاطر المترتبة على مشاركة الصور أو البيانات الخاصة عبر الإنترنت.

وقد جاءت أعلى المتوسطات في هذا المحور للبنود المتعلقة بإدراك مخاطر مشاركة الصور والمعلومات الخاصة، والوعي بوجود قوانين تحمي من الجرائم الإلكترونية، وأهمية استخدام كلمات مرور قوية. ويُعزى ذلك إلى تركيز برامج التوعية في المدارس وتأكيد الأهل على نشر الوعي بهذه الجوانب، باعتبارها أكثر التصاقاً بالحياة الرقمية اليومية للطلبة.

بينما جاءت أدنى المتوسطات نسبيًا في البنود المرتبطة بالتحقق من هوية الأشخاص قبل قبول الطلبات والتمييز بين المواقع الآمنة وغير الآمنة، مما يشير إلى وجود حاجة لتعزيز المهارات التحليلية لدى الطلبة في التعامل مع البيئات الرقمية، وتوسيع الوعي لديهم.

بوجه عام، يمكن القول إن هذا المحور يُظهر توافر قاعدة معرفية أولية جيدة لدى طلبة المرحلة المتوسطة حول الأمن السيبراني، لكنها لا تزال تحتاج إلى تعميق وتطبيقات عملية وتربوية منهجية لترسيخها كسلوك دائم وليس كمجموعة معلومات نظرية فحسب.

وقد تم ترتيب العبارات حسب درجة الاستجابة (من الأعلى إلى الأدنى) وفقًا للمتوسطات الحسابية، بحسب مقياس ليكرت الثلاثي: (2.34 – 3.00 = موافق)، (1.67 – 2.33 = محايد)، (1.00 – 1.66 = غير موافق) على النحو التالي:

المرتبة الأولى: العبارة رقم 5 والتي تنص على "أعلم أن مشاركة الصور الخاصة قد تسبب مشاكل." بمتوسط حسابي: 2.23 وهذا يدل على وعي مرتفع جدًا وإدراك اجتماعي واسع لمخاطر نشر الصور الخاصة عبر الإنترنت.

المرتبة الثانية: العبارة رقم 4 والتي تنص على "أميز بين المواقع الآمنة وغير الآمنة." بمتوسط حسابي: 2.20 وهذا يدل على معرفة جيدة نسبيًا بالمؤشرات المرئية للأمان (مثل https، القفل الأخضر)؛ وهذا الفهم غالبًا لا يتعدى الملاحظة الشكلية دون معرفة تقنية بالتشفير؛ ويحتاج إلى مزيد تطوير لمهارة تحليل العناوين والتدريب عليها.

المرتبة الثالثة: العبارة رقم 9 والتي تنص على "أدرك أهمية التحقق من هوية الشخص قبل قبول الطلبات." بمتوسط حسابي: 2.15 ويمكن تفسير ذلك على أنه وعي جيد بخطر الانتحال والهويات المزيفة، وهذه النتيجة تدل على وجود حس أمني اجتماعي لدى أفراد العينة خاصة في بيئات التواصل الاجتماعي.

المرتبة الرابعة: العبارة رقم 1 والتي تنص على "أعرف أنني لا يجب أن أشارك حسابي مع أحد" بمتوسط حسابي: 2.13 وذلك يدل على وعي إيجابي بسلوك الخصوصية، لكنه دون المستوى الممتاز ويعكس ذلك الفهم الجزئي لأهمية الملكية الرقمية؛ لكنه يتأثر بالثقافة الأسرية التي قد تسمح بالمشاركة أحيانا.

المرتبة الخامسة: العبارة رقم3 والتي تنص على "أعرف أهمية استخدام كلمات مرور قوية." بمتوسط: 2.08 وهذا المستوى من المعرفة يعد مستوى متوسط؛ يُظهر أن المفهوم معروف لكنه غير مطبق دائمًا؛ ربما يعرفون القاعدة ولكن يفتقرون إلى الفهم العملي لصنع كلمة مرور قوية.

المرتبة السادسة: العبارة رقم 6 والتي تنص على "أعرف أن هناك قوانين تحمي من الجرائم الإلكترونية." بمتوسط حسابي: 2.04 وتعد هذه المعرفة محدودة بالقوانين الوطنية أو اللوائح التنظيمية للأمن السيبراني؛ وهذا يشير إلى ضعف الوعي القانوني رغم تكرار القضايا الإعلامية.

المرتبة السابعة: العبارة رقم 2 والتي تنص على "أفهم مخاطر مشاركة المعلومات الشخصية على الإنترنت." بمتوسط حسابي: 2.00 وهو إدراك متوسط؛ يدل على معرفة بالمبدأ دون تصور لتبعاته الأمنية، وقد يكون هذا الفهم غالبًا نابع من تحذيرات عامة، لا من معرفة تحليلية للمخاطر التقنية؛ مما يستوجب معه التركيز على التدريب التحليلي حول سيناريوهات الاختراق أو التسريب.

المرتبة الثامنة: العبارة رقم 1 والتي تنص على "أعرف معنى مصطلح الأمن السيبراني." بمتوسط حسابي: 1.96 وهذ المستوى يعد ضعفا نسبيا في الفهم النظري للمفهوم الأساس للمجال، وغياب

المفهوم المجرد يحدّ من عمق الوعي العام؛ فالطلبة يتعاملون مع الأمن السيبراني كسلوك لا كمجال معرفي متكامل؛ مما يفرض تعزيز التعريف بالمصطلح ضمن المحتوى التعليمي وربطه بالأمن الوطني والرقمي.

المرتبة التاسعة: العبارة رقم 7 والتي تنص على "أفهم أسباب خطورة النقر على روابط غير معروفة." بمتوسط حسابي: 1.95 وهو مستوى وعي ضعيف نسبيًا؛ يدل على وجود ثغرات في فهم طرق الاختراق عبر الروابط، وهذه النتيجة تشكل فجوة معرفية خطيرة نظرًا لارتباطها بالتصيد الإلكتروني؛ مما يفرض دمج تجارب تفاعلية توضح كيف يتم استغلال الروابط في سرقة البيانات.

المرتبة العاشرة: العبارة رقم 8 والتي تنص على "أعرف أن حفظ كلمة المرور في مكان آمن مهم." بمتوسط حسابي: 1.91 الأدنى في المحور؛ وهذا يعكس ضعفا معرفيًا أو عدم قناعة بأهمية التخزين الآمن، فالطلبة يفتقرون لمهارات إدارة كلمات المرور (حفظ، تحديث، تشفير) مما يحتم تصميم برامج توعوية عملية حول استخدام أدوات إدارة كلمات المرور الآمنة.

2. نتائج الإجابة على السؤال الثاني

نص السؤال الثاني على ما درجة وعي طلبة المرحلة المتوسطة بالقصيم بالأساليب الاحترازية السيبرانية؟

وللإجابة عن هذا السؤال؛ استخدمت الباحثة التكرارات، والنسب المئويَّة، والمتوسِّط الحسابي، والانحراف المعياري وجدول (4) يوضح الاستجابات على هذا المحور.

جدول (4) المتوسِّط الحسابي، والانحراف المعياري لوعي الطلبة بالأساليب الاحترازية السيبرانية

الرتبة	رقم العبارة	نص العبارة	الانحراف المعياري	المتوسط الحسابي
1	15	لا أشارك معلوماتي الخاصة مثل الرقم السري مع أي شخص.	0.537	2.311
2	11	لا أضغط على الروابط غير الموثوقة في الرسائل أو المواقع.	0.570	2.272
3	17	لا أستخدم شبكات Wi-Fi العامة غير المحمية.	0.582	2.238
4	20	أتحقق دائمًا من أن الموقع الذي أستخدمه آمن.(https)	0.658	2.180
5	14	لا أفتح الرسائل أو المرفقات من مرسلين غير معروفين.	0.677	2.157
6	18	لا أشارك حساباتي الإلكترونية مع الآخرين.	0.789	2.000
7	19	أحرص على تحديث التطبيقات والبرامج بانتظام.	0.803	1.996
8	16	أستخدم خاصية القفل أو كلمة مرور للجهاز دائمًا.	0.819	1.973

الرتبة	رقم العبارة	نص العبارة	الانحراف المعياري	المتوسط الحسابي
9	12	أستخدم برامج الحماية (مثل الجدران النارية) على أجهزتي.	0.822	1.973
10	13	أستخدم برامج مكافحة الفيروسات بشكل منتظم.	0.826	1.970

بلغ المتوسط الحسابي العام لهذا المحور (2.11) بانحراف معياري قدره (0.69)، وهو ما يعكس مستوى وعي سلوكي جيد نسبيًا لدى الطلبة فيما يتعلق بالممارسات اليومية الآمنة أثناء استخدام الإنترنت والأجهزة الذكية، وقد أظهرت النتائج ارتفاعاً واضحاً في المتوسطات الخاصة بالبندين "عدم مشاركة المعلومات الشخصية أو كلمات المرور" و"عدم النقر على الروابط غير الموثوقة"، وهو ما يعكس وجود حذر عالي لدى الطلبة تجاه أبرز التهديدات الإلكترونية شيوعًا.

كما سجلت البنود المتعلقة باستخدام برامج الحماية ومكافحة الفيروسات، والتحقق من المواقع الآمنة (https) متوسطات جيدة، مما يدل على سلوك تقني واعٍ نسبيًا لدى شريحة واسعة منهم.

في المقابل، جاءت المتوسطات الأدنى في البنود التي تتعلق بـ استخدام شبكات Wi-Fi العامة وتحديث التطبيقات والبرامج بانتظام، مما قد يشير إلى قصور في الممارسات الوقائية المرتبطة بالجانب التقني الدقيق، وهو ما يستدعي تعزيز التوعية العملية من خلال الأنشطة التطبيقية في المدارس، وربط السلوك اليومي بالمعرفة المكتسبة.

ويمكن تفسير هذه النتائج بأن الطلبة يطبقون السلوكيات الأساسية للأمن السيبراني عندما تكون واضحة ومباشرة (مثل عدم مشاركة كلمات المرور)، لكنهم أقل التزاماً بالسلوكيات التي تتطلب فهماً تقنياً متقدماً أو متابعة مستمرة (مثل التحديثات أو ضبط إعدادات الحماية)؛ وهذا يؤكد الحاجة إلى تنمية الوعي العملي التطبيقي وليس الاكتفاء بالجانب التوجيهي أو التحذيري.

وقد تمَّ ترتيب العبارات حسب درجة الاستجابة على النحو التالي:

المرتبة الأولى: عبارة رقم 15 والتي تنص على "لا أشارك معلوماتي الخاصة مثل الرقم السري مع أي شخص." بمتوسط حسابي 2.31 وهو الأعلى بين العبارات؛ مما يدل على وعي عالٍ بمفهوم السرية الرقمية وحماية البيانات الشخصية، فالطلبة يمتلكون وعياً متجذرًا تجاه خطورة مشاركة المعلومات، نتيجة الرسائل التحذيرية المتكررة في التطبيقات البنكية والمنصات الإلكترونية؛ وهذا السلوك يمثل حجر الأساس في الوعي السيبراني السلوكي، ويمكن استثمار هذا

الوعي كنقطة انطلاق لتعزيز سلوكيات أكثر تخصصًا (مثل إدارة كلمات المرور المتعددة أو التحقق الثنائي).

المرتبة الثانية: عبارة رقم 11 والتي تنص على "لا أضغط على الروابط غير الموثوقة في الرسائل أو المواقع." بمتوسط حسابي: 2.27 وهو مستوى مرتفع يشير إلى حذر متقدم رغم عدم الفهم الكافي للمخاطر كما أوضح الجانب المفاهيمي؛ وقد يكون هذا الحذر ناتج عن توجيهات وتحذيرات تلقاها الطلبة من نحو "افعل ولا تفعل" بشكل مبسط وجذاب دون تبريرات عميقة؛ مما أظهر سلوكا مرتفعا دون التعمق في فهم الأسباب المفاهيمية التي قد تكون معقدة على طلبة في هذا السن.

المرتبة الثالثة: عبارة رقم 17 والتي تنص على "لا أستخدم شبكات Wi-Fi العامة غير المحمية." بمتوسط حسابي: 2.24 وهذا يشير إلى إدراك واضح لمخاطر الاتصال بالشبكات المفتوحة.

المرتبة الرابعة: عبارة رقم 20 والتي تنص على "أتحقق دائمًا من أن الموقع الذي أستخدمه آمن (https)." بمتوسط حسابي: 2.18 وهو يدل على وعي جيد نسبياً بعناصر الأمان في المواقع الإلكترونية؛ مما يظهر أن مفهوم "القفل الأخضر" أصبح مألوفاً، لكنه لا يصاحبه غالباً فهم متعمق لتشفير البيانات.

المرتبة الخامسة: عبارة رقم 14 والتي تنص على "لا أفتح الرسائل أو المرفقات من مرسلين غير معروفين." بمتوسط حسابي:2.16 وهذه الدرجة من الالتزام جيدة نسبيًا تدل على وعي بخطر الهندسة الاجتماعية؛ ويعد سلوكا وقائيا جيدا، مع الحاجة إلى مزيد من التعزيز عبر تجارب محاكاة للبريد الاحتيالي لزيادة وعي الطلبة.

المرتبة السادسة: عبارة رقم 18 والتي تنص على "لا أشارك حساباتي الإلكترونية مع الآخرين." بمتوسط حسابي: 2.00 وهذا يدل على وعي متوسط؛ مما يشير إلى وجود نسبة من الطلبة تشارك الحسابات (خاصة الحسابات الأسرية أو التعليمية). وهذا السلوك ناتج غالبًا عن ممارسات اجتماعية لا تُدرك مخاطرها التقنية؛ وهذا يستلزم تدريب الطلبة على أمثلة واقعية عن الأضرار المترتبة على مشاركة الحسابات مثل الاختراقات، حذف بيانات، وسرقة الهوية الرقمية.

المرتبة السابعة: عبارة رقم 19 والتي تنص على "أحرص على تحديث التطبيقات والبرامج بانتظام." بمتوسط حسابي: 1.99 وهو سلوك ضعيف نسبيًا؛ يعكس قلة إدراك لأهمية التحديثات الأمنية؛ فقد يكون الطلبة يتجاهلون التحديثات لاعتقادهم أنها شكلية، لا تتعلق بالأمن؛ مما يحتم توعيتهم بأن التحديثات تتضمن إصلاحات أمنية ضرورية وليست تحسينات شكلية.

المرتبة الثامنة: عبارة رقم 16 والتي تنص على "أستخدم خاصية القفل أو كلمة مرور للجهاز دائمًا." بمتوسط: 1.97 وهو مستوى منخفض، يشير إلى إهمال بسيط لعادات الأمان اليومية؛ قد يرتبط ذلك باعتقاد الطلبة أن القفل غير ضروري دائما مما يستوجب التأكيد على أن فقدان الجهاز أو دخوله في أيدٍ خاطئة أخطر من التهديدات الإلكترونية البعيدة.

المرتبة التاسعة: عبارة رقم 12 والتي تنص على "أستخدم برامج الحماية (مثل الجدران النارية) على أجهزتي." بمتوسط حسابي: 1.97 وهذا يشير لضعف واضح في الجانب التقني للسلوك الأمني؛ قد يعكس جهلًا بوجود هذه الأدوات أو صعوبة في إعدادها، وهذا الأمر يفرض على مؤسسات التعليم تقديم ورش تطبيقية حول تفعيل إعدادات الجدار الناري واستخدام أدوات النظام الافتراضية.

المرتبة العاشرة: عبارة رقم 13 والتي تنص على "أستخدم برامج مكافحة الفيروسات بشكل منتظم." بمتوسط حسابي: 1.97 وهو الأدنى في المحور؛ مما يدل على تهاون في صيانة الحماية الرقمية؛ ربما يعتقد الطلبة أن برامج النظام المدمجة كافية، أو لعدم الإدراك الكافي بخطر الفيروسات وهذا يتطلب إعادة نشر الوعي بمفهوم الوقاية المستمرة، وربط الاستخدام المنتظم بمفاهيم الصيانة الوقائية للأمن السيبراني.

تفسير إجمالي عام لنتائج الوعي السيبراني الكلي

عند النظر إلى نتائج المحورين معًا، يتضح أن المتوسط العام للاستبانة الكاملة بلغ (2.11) بانحراف معياري مقداره (0.68)، وهو ما يدل على أن مستوى الوعي السيبراني العام لدى طلبة المرحلة المتوسطة بالقصيم متوسط يميل إلى الجيد، كما أظهر معامل الثبات الكلي (كرونباخ ألفا) قيمة (0.91)، مما يدل على ارتفاع الاتساق الداخلي لمفردات المقياس وموثوقية نتائجه.

وتشير هذه النتائج إلى أن الطلبة يمتلكون وعياً معرفياً وسلوكياً متقارباً في المستوى، حيث تظهر ملامح فهمهم النظري متوازنة تقريباً مع ممارساتهم الواقعية، وإن كانت الأخيرة بحاجة إلى تعزيز

تربوي متواصل، كما تكشف النتائج أن لدى الطلبة أسس مقبولة للوعي السيبراني، لكنها في الوقت نفسه تُبرز الحاجة إلى مزيد من تعزيز الوعي ودمج مهارات الأمن السيبراني في المناهج الدراسية بشكل عملي ومنهجي لترسيخ السلوك الآمن وتطوير التفكير النقدي لدى الطلبة أثناء استخدام التقنية.

ثانيًا: التوصيات

استنادًا إلى النتائج السابقة، تُوصي الدراسة بما يلي:

- تصميم أنشطة تعليمية تطبيقية وتفاعلية (مثل المحاكاة والمواقف الافتراضية) تُسهم في ترسيخ الممارسات الآمنة لدى الطلبة، وتربط المفاهيم النظرية بالتجربة الواقعية.
- تطوير برامج تدريبية للمعلمين والمرشدين الطلابيين حول أساليب توعية الطلبة بالأمن السيبراني، بحيث يستخدمون لغة مبسطة تربط بين السلوك الأخلاقي والاستخدام التقني الآمن.
- تعزيز دور الأسرة في مراقبة السلوك الرقمي لأبنائها، من خلال نشر أدلة مختصرة للأهالي توضح أساسيات الحماية الرقمية وطرق المتابعة التربوية الإيجابية.
- تضمين وحدات تدريبية حول التهديدات التقنية الشائعة، بأسلوب مبسط يناسب الطلبة ويحول المفاهيم التقنية إلى مواقف حياتية ملموسة.

ثالثًا: اقتراحات لدراسات مستقبلية

-دراسة العلاقة بين مستوى الوعي السيبراني والتحصيل الدراسي أو استخدام التقنية التعليمية.

-تحليل دور المعلم والبيئة المدرسية في تشكيل ثقافة الأمان الرقمي لدى المراهقين.

المراجع

المراجع العربية:

- أبو منصور، حسين يوسف. (2017). توظيف تقنية التصنيف الربطي للكشف عن مواقع التصيد الإلكتروني. المجلة العربية الدولية للمعلوماتية، 5(9)، 32–40.
- البقمي، ناصر حمد. (2007). فاعلية التشريعات العقابية في مكافحة الجرائم المعلوماتية. مكتبة الملك فهد الوطنية.
- جبور، منى. (2012). الأمن السيبراني: التحديات ومستلزمات المواجهة [ورقة علمية]. اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية.
- الحباشنة، عبير. (2023). درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك. مجلة الزرقاء للبحوث والدراسات الإنسانية، 23(3)، 662–679.
- الربيعة، صالح بن علي. (2018، 27 أبريل). الأمن الرقمي وحماية المستخدم من مخاطر الانترنت [ورقة علمية]. الملتقى الأول بالإدارة العامة لتعليم بمحافظة جدة، جدة، المملكة العربية السعودية.
- الزبيدي، محمد، وعسيري، محمد، والبقمي، سعود، والمناخرة، الحسن. (2021). العلاقة بين الوعي بالأمن السيبراني وقيم الانتماء الوطني لدى طلبة المرحلة الثانوية بمنطقة مكة المكرمة. مجلة جامعة الملك عبد العزيز: الآداب والعلوم الإنسانية، 28(2)، 61–92.
- الشايع، خالد. (2019). الأمن السيبراني: مفهومه وخصائصه وسياساته. دار العالمية.
- الشهري، مريم محمد. (2021). دور إدارة الجامعة في تعزيز الوعي بالأمن السيبراني لدى طلبة كلية التربية بجامعة الإمام محمد بن سعود الإسلامية. مجلة العلوم الإنسانية والإدارية، (25)، 83–104.
- شعبان، رشا عبد القادر محمد الهندي. (2021). تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول. مجلة جامعة الفيوم للعلوم التربوية والنفسية، 15(11)، 338–383.

- عبد الصادق، عادل. (2014). الفضاء الإلكتروني والثورة في شؤون أجهزة الاستخبارات الدولية. مركز الأهرام للدراسات السياسية والاستراتيجية.
- القحطاني، ذيب بن عايض. (2015). أمن المعلومات. مكتبة الملك فهد الوطنية.
- القحطاني، نورة بنت ناصر. (2019). مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. شؤون اجتماعية، 36(144)، 85–120.
- المنتشري، فاطمة، وحريري، رندة. (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية، 4(13)، 95–140.
ا- لمنيع، الجوهرة بنت عبد الرحمن. (2022). متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030. مجلة كلية التربية، 38(1)، 155–194.
- متولي، أحمد حسني. (2015). الجريبات المعلوماتية: رؤية مقترحة من منظور تربوي لدور أعضاء هيئة التدريس بكليات التربية لزيادة الوعي بمكافحة الجرائم المعلوماتية [ورقة علمية]. المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسوب والمعلومات، 184–194.
- مركز الأمن الإلكتروني. (2019). التقرير السنوي. من http://bit.ly/32x6Dif
- الهيئة الوطنية للأمن السيبراني. (2025). الاستراتيجية الوطنية للأمن السيبراني. من https://nca.gov.sa/ar/national-cybersecurity-strategy/
- وزارة التعليم. (2024). إحصاءات التعليم – التقرير الإحصائي السنوي. من https://departments.moe.gov.sa/Statistics/Educationstatistics/Pages/gestats.aspx
- وكالة الأنباء السعودية (واس). (2023، 15 نوفمبر). اقتصادي / هيئة الاتصالات تصدر تقرير إنترنت السعودية. من https://www.spa.gov.sa/w1866543

المراجع الأجنبية:

- Alghamdi, A. A. (2022). Cyberthreats facing high school students and methods of addressing them. Journal of Information Security and Cybercrimes Research, 5(2), 116–123.
- Al-Mohannadi, H., Al-Kuwari,M., & Al-Maadeed, S. (2023). Cybersecurity awareness in educational settings: A Gulf cooperation council perspective. Journal of Educational Technology & Society, 26(4), 110–125.
- Alrashed, T., & Alharbi, F. (2024). Compliance with Saudi cybersecurity framework: A case study of public universities. International Journal of Cybersecurity and Digital Forensics, 13(1), 85–102.
- Coughlin, T. (2017). Cybersecurity education for adolescents and non-technical adults. Journal of Information Security, 11(1). https://www.scirp.org/reference/referencespapers?referenceid=2641657
- Saeed, S. (2023). Education, online presence and cybersecurity implications: A study of information security practices of computing students in Saudi Arabia. Sustainability, 15(12), 9426. https://doi.org/10.3390/su15129426
- Scholl, M. (2021). NIST cybersecurity framework: A guide for educational leaders. Routledge.
- Smith, P., & Jones, L. (2022). Data encryption and privacy in the digital school. Computers & Security, 115, 70–85.