Journal of Educational and Psychological Sciences (JEPS) • Vol 9, Sup Issue 7 (2025) • P: 22 - 1
https://journals.ajsrp.com/index.php/jeps
ISSN: 2522-3399 (Online) • ISSN: 2522-3399 (Print)

The Level of Cybersecurity Awareness among Graduate Female Students at King Saud University

Ms. Ahad Abdulkader Altayeb* ,Ms. Najla Turki Alwahbi, Ms. Noura Ahmed Almoqren
King Saud University | KSA

Received: 14/01/2025
Revised: 25/01/2025
Accepted: 17/03/2025
Published: 30/06/2025

* Corresponding author: tayeb.ahad@yahoo.com

Citation: Altayeb, A. A., Alwahbi, N. T., & Almoqren, N. A. (2025). The level of cybersecurity awareness among female graduate students at King Saud University. *Journal of Educational and Psychological Sciences, 9*(7S), 1 – 22. https://doi.org/10.26389/AJSRP.E160125

Abstract: The study aimed to identify the level of cybersecurity awareness among female graduate students in the Curriculum and Instruction Department at the College of Education, King Saud University. This was achieved by assessing their awareness of cybersecurity concepts, their awareness of cybersecurity applications, and the key strategies to enhance cybersecurity awareness from their perspective. To achieve the study's objectives, a descriptive survey methodology was employed, utilizing a questionnaire consisting of 30 statements distributed across three axes: awareness of cybersecurity concepts, awareness of cybersecurity applications, and strategies for enhancing cybersecurity awareness. The study's key findings revealed that the participants demonstrated a high level of awareness regarding cybersecurity concepts. Similarly, they exhibited a high level of awareness concerning cybersecurity applications. Additionally, the participants strongly agreed on the importance of strategies for enhancing cybersecurity awareness. Based on these findings, the study recommended the development of training programs aimed at increasing cybersecurity awareness among female graduate students in universities.

Keywords: Cybersecurity Awareness - Cybersecurity in Universities - Graduate Studies.

درجة وعي طالبات الدراسات العليا في جامعة الملك سعود بالأمن السيبراني

أ. عهد عبد القادر الطيب*، أ. نجلاء تركي الوهبي، أ. نوره أحمد المقرن
جامعة الملك سعود | المملكة العربية السعودية

المستخلص: هدفت الدراسة إلى التعرف على درجة وعي طالبات الدراسات العليا في كلية التربية قسم المناهج وطرق التدريس في جامعة الملك سعود بالأمن السيبراني، من خلال معرفة درجة الوعي بمفاهيم الأمن السيبراني، ودرجة الوعي بتطبيقات الأمن السيبراني، وأبرز سبل تعزيز الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج في جامعة الملك سعود من وجهة نظرهن، ولتحقيق أهداف الدراسة، استخدمت الباحثات المنهج الوصفي المسحي، والاستبانة كأداة تكونت من (30) عبارة موزعة على ثلاثة محاور: الوعي بمفاهيم الأمن السيبراني، الوعي بتطبيقات الأمن السيبراني، سبل تعزيز الوعي بالأمن السيبراني. ومن أهم النتائج التي توصلت إليها الدراسة، أن عينة الدراسة يمتلكن درجة (عالية) في محور الوعي بمفاهيم الأمن السيبراني، كما أن عينة الدراسة يمتلكن درجة وعي (عالية) أيضاً في محور الوعي بتطبيقات الأمن السيبراني، بالإضافة إلى أن العينة وافقن بتقييم (مهم جداً) على محور سبل تعزيز الوعي بالأمن السيبراني. وفي ضوء النتائج أوصت الدراسة بإعداد برامج تدريبية تساهم في رفع درجة الوعي لدى طالبات الدراسات العليا في الجامعات.

الكلمات المفتاحية: الوعي بالأمن السيبراني- الأمن السيبراني في الجامعات- الدراسات العليا.

1- المقدمة.

في العصر الرقمي الذي نعيشه اليوم، أصبحت تقنيات الاتصالات والمعلومات جزءًا لا يتجزأ من حياتنا اليومية، حيث أثرت بشكل ملحوظ على جميع المجالات الحياتية بما في ذلك مجال التعليم. ففي الماضي القريب، كان التعليم مقتصرًا على الطرق التقليدية التي تعتمد بشكل أساسي على التفاعل المباشر بين المعلم والطلاب داخل الفصول الدراسية. لكن مع تطور التكنولوجيا، أصبح من الممكن تبني بيئات تعليمية تفاعلية تعتمد على الأنظمة الإلكترونية الحديثة التي تُسهل عملية التعلم، وتسمح بالوصول إلى مصادر المعرفة من أي مكان وفي أي وقت. وبفضل هذه التقنيات، أصبح من الممكن للطلاب أن يتعلموا بطريقة أكثر مرونة وتفاعلية، مما يسهم في تحسين جودة التعليم وزيادة فاعليته.

ومع هذا التقدم قامت التقنيات الحديثة بتغيير ملامح العديد من المجالات والأنشطة الحياتية، ومن ضمن المجالات التي شهدها التغير ملامح البيئات التعليمية لتتحول تدريجياً من البيئات التقليدية إلى بيئات تعليمية إلكترونية تفاعلية. ويشهد العالم الرقمي المعاصر بروز العديد من المخاطر، والتهديدات، والهجمات لنظم الأمن التي يشهدها من حين إلى آخر الفضاء السيبراني Cyberspace والتي غالباً ما تعتمد بقوة على استغلال ضعف مستويات وجاهزية العنصر البشري للتعامل مع حالات اختراق نظم المعلومات .ويدعو الانتشار المتزايد للتقنية في القرن الحادي والعشرين إلى تغيرات مقابلة في طرق تعليم وتعلم الطلاب، فمع تقدم التقنية هناك حاجة لتكييف التعلم وفقاً للطبيعة المتطورة لاستخدامها في مجال التعليم، ويصاحب ذلك التقدم الفهم بأن الطلاب يجب أن يكونوا على دراية بعملية استخدام التقنية من خلال تعلم كيفية التعامل معها للاستفادة من الفرص التي يقدمها الابتكار في التقنية (عويس، ووالي، 2021)؛ ويشير إسماعيل (2022) إلى أن الرقمنة المعلوماتية فرضت على المعلمين والتربويين أن يعملوا بمختلف الطرق والأدوات الحديثة لإكساب المتعلمين المهارات والقدرات التي تؤهلهم لتلبية هذه المتطلبات، وأهم هذه المتطلبات الحصول على المعلومات من مصادر عديدة في ظل عصر مختلف تتزايد فيه المعرفة عامة، والمعرفة الرقمية خاصة، وأصبح اعتماد الطلاب على استخدام التقنيات الحديثة والاعتماد على شبكة الإنترنت للحصول على المعلومات أمراً ضرورياً.

الفضاء السيبراني هو حالياً ثورة تقنية تؤثر على جميع المجالات بما في ذلك التعليم، وأن استخدام أدوات التقنية الحديثة يعزز عمليتي التعليم والتعلم، ويساعد على إضفاء الطابع الشخصي على تجربة التعلم ومساعدة المتعلمين في مساعيهم وتخفيف العبء عنهم، فتقوم الأنظمة التعليمية الذكية والقائمة على استخدام تقنية المعلومات والاتصالات بتقديم أنشطة التعلم التي تلبي احتياجات الطلاب المعرفية، فاعتماد الطلاب على التقنيات الحديثة واستخدام الشبكة العنكبوتية (الانترنت) جعل الطلاب أكثر عرضة للهجوم السيبراني (Florea & Radu, 2019). ويستخدم مصطلح "الأمن السيبراني" لتلخيص الأنشطة المختلفة كجمع المعلومات، ووضع السياسات العامة والتدابير الأمنية والمبادئ التوجيهية وطرق إدارة المخاطر والحماية والتدريب، ودليل لأفضل الممارسات المهنية، ومختلف التقنيات التي يمكن استخدامها لحماية شبكة الإنترنت؛ وتشمل هذه السياسات المعلومات وأجهزة الحاسب، والأفراد، والبنية التحتية والخدمات، ومجمل المعلومات المنقولة أو المخزنة في الأجهزة الإلكترونية، ويهدف الأمن السيبراني إلى ضمان تحقيق سلامة المؤسسات والأفراد في مواجهة المخاطر الأمنية وكل ما يتعلق بشبكة الأنترنت (المقصودي، 2017). ويشير سينثيلكومار وإيسوارامورثي (Senthilkumar & Easwaramoorthy, 2017) إلى ضعف الأمن السيبراني بالمؤسسات التعليمية، حيث تواجه مخاطر فقدان بيانات وحقوق الملكية الفكرية للأبحاث مثل براءات الاختراع الممنوحة للأساتذة والطلاب، وكذلك المعلومات الشخصية عن الطلاب والموظفين وأعضاء هيئة التدريس بسبب التزايد المتصاعد للهجمات السيبرانية عليها، الأمر الذي يظهر الحاجة إلى تنمية الوعي السيبراني لدى هؤلاء الطلاب، من خلال تنفيذ بعض برامج التوعية المتعلقة بالأمن السيبراني.

وقد أبدت وزارة التعليم السعودية الاهتمام بالأمن السيبراني وتوفير أمن المعلومات ورفع الوعي بين أفراد المجتمع المدرسي بهدف تأمين المعلومات الشخصية والبيانية والحد من اختراقها من الهجمات الإلكتروني، وفي هذا الصدد استهدفت رؤية المملكة العربية السعودية 2030 تطوير البنية التحتية للخدمات الرقمية والمعالجة الحاسوبية في مواكبة التقدم العالمي، وذلك بتنظيم قطاع الاتصالات من خلال الضوابط الأساسية والفرعية للأمن السيبراني والتي تركز على الأشخاص والاستراتيجيات والإجراءات التقنية (رؤية المملكة 2033، 2016). وأطلقت الهيئة الوطنية للأمن السيبراني- ممثلة بالمركز الوطني للأمن السيبراني- بالتعاون مع وزارة التعليم حملة بعنوان (بأمان- نتعلم) في إطار جهود المركز لرفع الوعي والمعرفة بالأمن السيبراني لتجنب المخاطر السيبرانية وتقليل آثارها عن طريق إصدار التنبيهات بأخر الثغرات والمنشورات التوعوية وأخطرها، بهدف رفع الوعي الأمني السيبراني وتقليل المخاطر التي قد يتعرض لها الطلاب أثناء ممارسة العملية التعليمية باستخدام شبكة الإنترنت (إبراهيم، 2021). وفقاً لما ذكره يونس وزملاؤه (Yumos et al., 2016)، أصبح تعزيز الوعي بالأمن السيبراني هدفاً محورياً للعديد من المؤسسات، وخصوصاً المؤسسات التعليمية. يركز هذا الوعي على تغيير المواقف الفردية والتنظيمية لفهم أهمية الأمن السيبراني والآثار السلبية الناتجة عن غياب أو ضعف تدابير الحماية. يعتبر الوعي بالأمن السيبراني عاملاً بالغ الأهمية في هذا المجال، حيث يتعلق بشكل أساسي بنقل المعرفة والمعلومات حول الأمن السيبراني وآثاره على المؤسسات.

وقد أدت الثورة الرقمية والتطور الهائل في وسائل الاتصال وشبكاته، والنمو السريع في الحواسيب الشخصية والهواتف الذكية، إلى تحسين سبل الأحوال المعيشية في جميع ميادين، وأصبحت متطلبًا أساسيًا ولا سيما الطلبة من كافة المستويات. وتزداد أعداد الطلبة

مستخدمي الإنترنت سنويًا بشكل كبير لأغراض متعددة، منها: التعليم، الترفيه، شبكات التواصل الاجتماعي، وعلى الرغم من مزايا الإنترنت، إلا أنها أصبحت فرصا لوقوع الطلبة كضحايا للجرائم السيبرانية؛ لعدم امتلاكهم الوعي الكافي بتلك الجرائم وكيفية تجنبها؛ مما يترتب على ذلك أضرار مادية ونفسية ومعنوية قد تؤثر على المعلم والطالب والمؤسسة التربوية، الأمر الذي يزيد من أهمية الأمن السيبراني في مجال التعليم والتعلم (المنتشري، 2020). وتفتقر مؤسسات تربوية عديدة للبنية التحتية القوية للأمن السيبراني، والتي يجعلها غير قادرة على مواجهة التهديدات. ولتحقيق الأمن السيبراني الناجح في المؤسسة التربوية، يتطلب التعاون بين تقنية المعلومات، وقادة الإدارات في المؤسسة ليكونوا أكثر فاعلية لمنع الهجمات التي تُعرّض أنظمة تقنية المعلومات للضعف (Davis, 2018)، حيث إن تهديدات المؤسسة التربوية يمكن أن تضر بسمعتها، وتسبب مسؤولية قانونية وخسارة مالية (Schuesster,2013).

في الختام، يُعتبر تعزيز الوعي بالأمن السيبراني في البيئات التعليمية أمرًا بالغ الأهمية لمواجهة التحديات المتزايدة في العصر الرقمي. مع تزايد الاعتماد على التقنيات الحديثة في التعليم، يصبح الطلاب والمعلمون عرضة للتهديدات الإلكترونية التي قد تؤثر على معلوماتهم وبياناتهم الشخصية. لذا، من الضروري أن تستثمر المؤسسات التعليمية في بناء بنية تحتية قوية للأمن السيبراني، بالإضافة إلى دمج مفاهيم الأمن السيبراني في المناهج الدراسية. إن تعزيز هذه الثقافة يمكن أن يساعد في تقليل المخاطر وتحقيق بيئات تعليمية آمنة. ويجب أن يشمل ذلك التوعية المستمرة والتدريب العملي للطلاب والمعلمين لمواكبة التطورات السريعة في هذا المجال.

1-2-مشكلة الدراسة:

في ظل التزايد الملحوظ في التهديدات والجرائم الإلكترونية في المملكة العربية السعودية، لا يزال الوعي بالأمن السيبراني بين طلاب الجامعات لم يحظ بالاهتمام الكافي (Al Arifi at al., 2012). وأشار الحربي وتصدق (Alharbi & Tassaddig, 2021) إلى أن معظم المؤسسات الأكاديمية لا تتضمن برامج توعية تتعلق بالأمن السيبراني ضمن استراتيجياتها التعليمية. ومع تزايد الهجمات السيبرانية التي تستهدف الأنظمة التعليمية في المدارس والجامعات، أصبح من الضروري أن يكتسب الطلاب فهم أعمق لمشاكل الأمن السيبراني والجرائم الإلكترونية. لذا، ينبغي أن يكون الوعي بالأمن السيبراني جزءاً أساسياً من اهتمامات المؤسسات التعليمية، لضمان إعداد الخريجين بالمهارات والمعرفة اللازمة لمواجهة التهديدات السيبرانية (Khader et al., 2021).

وأثّرت جائحة كوفد-19 بشكل ملحوظ على الأمن السيبراني، حيث دفعت المجتمعات إلى الاعتماد الكامل على الشبكات الإلكترونية في مختلف المجالات، بما في ذلك مجال التعليم الإلكتروني والتعليم عن بعد (Hasweh & Hamed Al-Qudah, 2023). ومع تزايد الاعتماد على التعليم الإلكتروني، أصبح من الضروري الانتباه إلى المخاطر المرتبطة باستخدام الإنترنت، ومنها التعرض للفيروسات التي قد تؤدي إلى تلف البيانات المخزنة، بالإضافة إلى احتمالية اختراق الحسابات الشخصية وتسريب المعلومات الحساسة، وسرقة البيانات المالية (الصائغ وآخرون، 2020). وتُعتبر فئة طلاب التعليم العالي من بين الفئات الأكثر عرضة لتلك التهديدات السيبرانية ويُعزى ذلك إلى اعتمادهم على قواعد البيانات والمصادر الإلكترونية لإجراء أبحاثهم الأكاديمية واستكمال أنشطتهم اليومية (الحبيب، 2022). ويجمع العديد من طلاب الدراسات العليا في قسم المناهج وطرق التدريس بين متابعة دراستهم وممارسة التدريس في الميدان التعليمي، مما يعرضهم يومياً للتعامل مع كميات كبيرة من البيانات التعليمية والمعلومات الشخصية الحساسة. وهذا الأمر يتطلب منهم تطبيق تدابير حماية معززة لضمان أمن هذه البيانات وسريتها من أي تهديدات أمنية قد تواجهها. ونظراً لأن طلاب التعليم العالي يُمثلون المستقبل الأكاديمي والبحثي في المملكة العربية السعودية، فإن تعزيز وعيهم بالأمن السيبراني يمثل خطوة حيوية لحمايتهم وحماية بياناتهم في ظل التهديدات المتزايدة في الفضاء السيبراني (Aljohani et al., 2021).

ولقد أشار خضر وآخرون (Khader et al., 2021) إلى أنه لا يزال هناك حاجة إلى إجراء المزيد من الدراسات لمعرفة درجة الوعي بالأمن السيبراني لدى طلاب التعليم العالي، ومعرفة سلوكياتهم في هذا المجال، بالإضافة إلى تحديد العوامل المؤثرة التي قد تكون ذات صلة. ومن خلال مراجعة الأدبيات التي تناولت الوعي بالأمن السيبراني في التعليم العالي، بما في ذلك دراسة الحبيب (2022)، والقحطاني (2022)، والحربي وتصدق (Alharbi & Tassaddiq, 2021)، تبين ندرة الدراسات التي تركز على معرفة درجة الوعي بالأمن السيبراني لدى طلبة قسم المناهج وطرق التدريس في جامعة الملك سعود. بناءً على ما سبق، تهدف هذه الدراسة إلى سد هذه الفجوة من خلال التعرف على درجة الوعي بالأمن السيبراني لدى طالبات قسم المناهج في جامعة الملك سعود، وقياس مدى استعدادهن لمواجهة التهديدات والمخاطر السيبرانية، لاسيما في ظل التزايد المستمر للاعتماد على التقنية والموارد الإلكترونية في العملية التعليمية.

1-3-أسئلة الدراسة:

تتمحور إشكالية الدراسة في السؤال الرئيس: "ما درجة الوعي بالأمن السيبراني لدى طالبات الدراسات العليا قسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن؟"

ويندرج تحت هذا السؤال الأسئلة الفرعية التالية:

1- ما درجة الوعي بمفاهيم الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن؟
2- ما درجة الوعي بتطبيقات الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن؟
3- ما أبرز سبل تعزيز الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن؟

1-4-أهداف الدراسة:

1. التعرف على درجة الوعي بمفاهيم الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن.
2. التعرف على درجة الوعي بتطبيقات الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن.
3. التعرف على أبرز سبل تعزيز الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن.

1-5-أهمية الدراسة

- **الأهمية النظرية:**

- إثراء المحتوى المعرفي حول الأمن السيبراني :تساهم الدراسة في تعزيز الفهم النظري لمفهوم الأمن السيبراني وأبعاده المختلفة، مما يضيف إلى المكتبة العربية مرجعًا أكاديميًا يمكن الاستفادة منه في الدراسات المستقبلية.
- تسليط الضوء على المخاطر السيبرانية في البيئة التعليمية :تقدم الدراسة تحليلًا عميقًا لأهم التحديات والتهديدات التي تواجه طلاب الدراسات العليا عند استخدامهم للإنترنت، مما يعزز الإدراك بأهمية التصدي لهذه المخاطر.
- لفت انتباه أعضاء هيئة التدريس ومطوري المناهج :تشير الدراسة إلى ضرورة تضمين مفاهيم الأمن السيبراني في المناهج الدراسية، مما يعزز من وعي الطلاب ويساعدهم على التعامل مع التهديدات السيبرانية بفعالية.
- فتح آفاق بحثية جديدة :تتيح هذه الدراسة الفرصة للباحثين لاستكمال الجهود البحثية في مجال الأمن السيبراني، عبر استكشاف تأثير الوعي السيبراني على مختلف الفئات المجتمعية وليس فقط طلاب الدراسات العليا.

- **الأهمية التطبيقية:**

- حماية بيانات الطلاب من الجرائم السيبرانية :توضح الدراسة أهمية رفع الوعي الأمني لدى طلاب الدراسات العليا، مما يسهم في تقليل تعرضهم للاختراقات الإلكترونية والجرائم المعلوماتية.
- تشجيع المؤسسات التعليمية على تطوير برامج توعوية :تحث الدراسة الجامعات والمؤسسات الأكاديمية على تبني استراتيجيات توعية وتدريب في مجال الأمن السيبراني، لتعزيز ثقافة الحماية الإلكترونية بين الطلاب.
- تمكين صناع القرار من اتخاذ تدابير فعالة :تقدم نتائج الدراسة توصيات يمكن أن تساعد وزارة التعليم العالي والمؤسسات المعنية على تطوير سياسات وإجراءات تهدف إلى تعزيز الأمن السيبراني في بيئة التعلم الأكاديمي.
- تعزيز الاستخدام الآمن للإنترنت في العملية التعليمية :توفر الدراسة إرشادات عملية يمكن تطبيقها لضمان بيئة تعليمية رقمية آمنة، مما يسهم في دعم التعلم الإلكتروني وتقليل المخاطر الأمنية.

1-6-حدود الدراسة:

- الحدود الموضوعية: درجة الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس.
- الحدود البشرية: جميع طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود .
- الحدود المكانية: جامعة الملك سعود.
- الحدود الزمانية: تم تطبيق البحث خلال العام الدراسي 1446هـ

1-7-مصطلحات الدراسة

- **الوعي**: التعريف الاصطلاحي: يعرف الوعي بأنه الإدراك العقلي للحقيقة ومضامينها (أو سياقاتها) الجامعة، والوعي الكلي هو مجموع ما يدركه الإنسان من حقائق (المرهون،2016).
  - التعريف الإجرائي: يعرف الوعي إجرائياً بأنه التصور الفكري والصورة الذهنية التي تحملها طالبات الدراسات العليا في الجامعات، متمثلة بطالبات كلية التربية قسم المناهج وطرق التدريس في جامعة الملك سعود، في الجوانب المختلفة ذات الصلة بالوعي بمفاهيم الأمن السيبراني، وطرق الوقاية من جرائم الفضاء السيبراني.
- **الأمن السيبراني**: التعريف الاصطلاحي: يعرف الأمن السيبراني بأنه 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 (الهيئة الوطنية للأمن السيبراني، 2018).
  - التعريف الإجرائي: يعرف الأمن السيبراني بأنه الإجراءات والوسائل والتقنيات وسبل الوعي والتطبيقات التي تتبعها طالبات الدراسات العليا، بهدف حماية البيانات والمعلومات والأنظمة، وما تقدمه من خدمات من التدخل غير المشروع، الذي قد يؤدي إلى تعطيل الأجهزة أو اختراق البيانات والمعلومات والتلاعب بها أو سوء استخدامها مما يشكل خطراً على المصالح الشخصية والعامة.

2- الإطار النظري والدراسات السابقة

2-1-الإطار النظري.

2-1-1-الأمن السيبراني ومفهومه:

ظهر مصطلح الأمن السيبراني (Cybersecurity) منذ العقد المنصرم في بداية التسعينات، عندما كان العلماء والمتخصصين في الحاسب وتقنية المعلومات يبحثون عن الحلول والإجراءات الممكنة للحد من التهديدات والمخاطر التي تتعرض لها الحواسيب والشبكات وأنظمتها، تطلق كلمة سايبر (cyber) على أي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية تعني فضاء الانترنت (الربيعة،2017). كذلك يُعرف الأمن السيبراني Cybersecurity 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 (الظويفري،2021). كما عُرف الأمن السيبراني بأنه: التدابير المتخذة لحماية جهاز الحاسب أو الشبكة من الوصول غير المُصرَّح به؛ للحفاظ على سلامة المعلومات المخزنة وأمنها. ويتضمن الأمن السيبراني التدخلات الفنية التي تحمي البيانات ومعلومات الهوية والأجهزة من الوصول غير المُصرَّح به أو الضرر، بما في ذلك أمن الفضاء الإلكتروني (Richardson et al., 2020). كما عرّف الداوود وسكنر (Aldawood & Skinner ,2019) الوعي بأمن الإنترنت أو الوعي بالأمن السيبراني: إلى مدى معرفة مستخدمي الإنترنت بالتهديدات التي تواجهها شبكاتهم والمخاطر التي يقابلونها وأفضل الممارسات الأمنية لتوجيه سلوكهم. وفي ضوء ما سبق، يتضح الاتفاق بين الباحثين، في أن مفهوم الأمن السيبراني يقوم على حماية المعلومات والبيانات والتطبيقات والأجهزة، والشبكات من أي شكل من أشكال الوصول غير المصرح به، أو استخدامها بشكل سلبي بحيث يشكل خطرًا على الأفراد أو الجهة ذات الصلة بتلك المعلومات.

2-1-2-أهداف الأمن السيبراني:

تسعى الدول والمؤسسات المختلفة حول العالم إلى تعزيز الأمن السيبراني، وذلك لتحقيق العديد من الأهداف والتي يمكن إيجازها على النحو التالي(صائغ،2018): تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص، توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات، صمود البنى التحتية الحساسة للهجمات الإلكترونية، توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين، مقاومة البرمجيات الخبيثة وما تستهدفه من إحداث أضرار بالغة بالمستخدمين وأنظمة المعلومات، الحد من التجسس والتخريب الإلكتروني على مستوى الحكومات والأفراد، التخلص من نقاط الضعف في أنظمة الحاسب الآلي والشبكات والأجهزة المحمولة باختلاف أنواعها. ويتبين أن أهداف الأمن السيبراني تسعى بكل ما أوتيت من قوة لحماية المستخدم، مما يؤكد على أن تعزيز الحماية هو الهدف الأساس للأمن السيبراني، والذي من أجله أنشئ هذا النوع من العلم.

2-1-3-الوعي بالأمن السيبراني:

زادت تقنية المعلومات بشكل كبير في العقد الماضي، مع معدلات عالمية هائلة لاستخدام الإنترنت من قبل الأفراد والمؤسسات، بدءًا من الأوساط الأكاديمية والحكومية إلى القطاعات الصناعية (Jalali et al. , 2019). ومع تزايد الاستخدام للإنترنت لا يزال الكثير من مستخدمي الإنترنت يفتقرون إلى الوعي الكافي بتهديدات الإنترنت المختلفة والتي تعرف أيضا باسم "المخاطر الإلكترونية (lee et al. ,2017). وفي الواقع غالبًا ما يفشل مستخدمو الإنترنت في امتلاك الحد الأدنى المطلوب من الوعي لحماية أجهزتهم الحاسوبية، ففي أسوأ السيناريوهات يعاني الأفراد من نقص تام في الوعي بمخاطر الإنترنت؛ ومن ثم فإن استعدادهم لاستخدام تدابير الحماية الأمنية السيبرانية غير موجود (Zwilling et al. ,2020). لذلك فقد اهتم كثير من الباحثين في مجال الأمن السيبراني بضرورة توعية المستخدمين بشبكات الإنترنت، وأن يكونوا على دراية بالمخاطر المحتملة التي يتعرضون لها كالتنمر عبر الإنترنت أو الاستخدام الغير واعي لمواقع التواصل الاجتماعي، و الألعاب عبر الإنترنت، وغيرها من الممارسات السلبية؛ من أجل العمل على اتخاذ احتياطات السلامة وإكسابهم المهارات اللازمة للحفاظ على معلوماتهم وضمان حمايتها، وهنا يطلب من المؤسسة التعليمية تنفيذ برنامج توعية لجميع العاملين والطلبة، وهذا يساهم في تعزيز ثقافة أمنية إيجابية، وبالتالي زيادة حماية المعلومات والبيانات.

لذلك يجب أن نكون كأفراد على استعداد للاستجابة للهجمات السيبرانية، وقادرين على التصدي لها بأفضل الممارسات، ويتم ذلك من خلال الجمع بين الوعي بالأمن السيبراني، وطرق تطبيق تنمية الوعي للتقليل أو التصدي للهجمات؛ من خلال إجراء تقييمات للمخاطر السيبرانية من ثلاثة مجالات رئيسة: تحديد البيانات الأكثر أهمية والتي تتطلب الحماية، تحديد التهديدات والمخاطر التي تواجه البيانات، تحديد الضرر الذي يتعرض له الفرد أو المؤسسة في حالة التعرض لهجمة سيبرانية، والقيام بوضع خطط، وتنفيذ إجراءات وقائية للتخفيف من مخاطر الإنترنت، مثل: برامج مكافحة الفيروسات والجدران النارية، وأنظمة كشف الاختراقات وغيرها، ومن هنا فإنّ الأمن السيبراني يمثل مفهومًا مهم في عصر الثورة المعلوماتية لمواجهة الأخطار والانتهاكات عبر الفضاء المعلوماتي(هيئة الاعلام،2021).

وتوجد طرق عديدة يجب على مستخدم الإنترنت اتباعها لتقليل مخاطر التهديد الإلكتروني أو الحدّ منها (المنتشري، 2020): إعداد كلمات السر القوية وتحديثها باستمرار، وعمليات التحقق الأمنية لمواقع التواصل الاجتماعي، والبريد الإلكتروني على كافة الأجهزة، التحديث المستمر للجدار الناري (Firewall)، والتي تمثل أنظمة الدفاع عن البنية التحتية المعلوماتية، عدم فتح أي رسائل إلكترونية مجهولة المصدر عبر البريد الإلكتروني، استخدام برامج الحماية من الفيروسات وبرامج التجسس وتحديثها باستمرار، عمل نسخ احتياطية من البيانات والمعلومات والاحتفاظ بها خارج المؤسسة، عدم إرسال المعلومات الشخصية عبر البريد الإلكتروني، أو مواقع التواصل الاجتماعي، تحميل البرامج والملفات من مواقع موثوقة، عقد دورات تدريبية للأفراد حول الوعي بالأمن السيبراني، وكيفية التصرف في حال وقوعهم ضحية للمخاطر والتهديدات السيبرانية.

كما توفر نظريات الأخلاق إطارًا لاتخاذ القرارات الأخلاقية في علوم الحاسب بشكل عام. من خلال النظر في العواقب المحتملة، واتباع القواعد والمبادئ الراسخة، وإعطاء الأولية للقيم الشخصية، والتفكير في التأثير على الأفراد والمجتمعات، لخلق بيئة تقنية أكثر أخلاقية ومسؤولية (Singh,2023). و تلعب نظرية الفضيلة الأخلاقية دوراً مهماً في مجال الأمن السيبراني. حيث تشكل إطار عمل لتحديد وتطوير سمات الشخصية الأخلاقية التي تمكن الأفراد من التصرف وفقاً لمعايير الصواب والخطأ، إن القواعد الأخلاقية القوية، يمكن أن تساعد على اتخاذ قرارات أخلاقية دقيقة، لاسيما في الوعي بمفاهيم وتطبيقات الأمن السيبراني. من هذا المنطلق، تُعزز نظرية الفضيلة الأخلاقية الصدق والمسؤولية في صناعة التقنية كما تُعزز الثقة في المنتجات والخدمات المطورة.

كما تركز نظرية الحقوق على مبدأ الاعتراف بحق الفرد في اتخاذ خياراته الخاصة. وهو منظور يعطي الأفراد استقلالية الفرد وحريته، ويؤكد أن الأفراد لديهم الحق في اتخاذ خيارات تتوافق مع القيم والمعتقدات طالما أنها لا تضر الآخرين. مع احترام ودعم حقوق الأفراد في اتخاذ قراراتهم المستقلة، وتطبيقها بشكل حازم ومستدام، خاصة في علوم الحاسب والهندسة بشكل عام، والأمن السيبراني بشكل خاص. كما تلعب دور هام عند التعامل مع قضايا مثل خصوصية البيانات واستخدام الذكاء الاصطناعي، لذلك من الضروري إعطاء الأولوية لاستقلالية الأفراد وضمان أن تكون الاعتبارات الأخلاقية عالية في كل قرار يتخذونه. تؤسس هذه النظرية بيئة تقنية أخلاقية أكثر إنصافاً ووعي.

2-1-4-المخاطر والتهديدات السيبرانية:

عرفت الهيئة الوطنية للأمن السيبراني (2018، ص32) المخاطر والتهديدات السيبرانية بأنها: "المخاطر والتهديدات التي تمس عمليات أعمال الجهة بما في ذلك رؤية الجهة، أو رسالتها، أو إدارتها، أو صورتها، أو سمعتها، أو أصول الجهة، أو الأفراد، أو المؤسسات، أو الدولة، بسبب إمكانية الوصول غير المصرح به، أو استخدام، أو الإفصاح، أو التعطيل، أو التعديل، أو تدمير، المعلومات، أو نظم المعلومات". كما حددت الجبور (2015، ص50) مجموعة من العوامل التي تعد انتهاكاً للأمن السيبراني وتمثل اعتداء (جريمة) سيبرانية، تمثلت في: أولاً: التعرض لأمن المعلومات، أي مصداقيتها وتوافرها، وصحتها، واختراق الأنظمة، أو رسائل التصيّد (Phishing Email)، والتضليل والاحتيال، كتدمير البيانات

أو سرقتها، ثانياَ: التعرض إلى سلامة الأشخاص، من حيث الكيد لهم، والترصد للأطفال بغية الاعتداء عليهم، واستدراجهم، واستغلالهم جنسياً، أو الإتجار بالأعضاء، أو المواد الإباحية، أو تقديمها، ثالثاَ: الاعتداء على الأموال، وذلك من خلال عمليات الغش والاحتيال، والتزوير، واختراق الأنظمة، والابتزاز، وغسيل الأموال، وغيرها من الاعتداء على الممتلكات، رابعاً: أمن الدولة وسيادتها، والتجسس، وإفشاء المعلومات السرية (Confidentiality)، أو اختراق أنظمة الدفاع، والبيانات العسكرية، أو الأهداف اللوجستية، والحيوية.

ويمكن تقسيم الجرائم السيبرانية وفقاً لأهدافها على النحو التالي:

أولاً: الجرائم التي تستهدف الأفراد

إن الجرائم السيبرانية التي تمس الأفراد وحياتهم الخاصة من أكثر الجرائم السيبرانية انتشاراً، والأكثر تنوعاً فالجرائم التي تمس الأفراد، لها صور وأشكال عدة، ولكن أكثرها ذلك الذي يمس كرامة الفرد ويحط من مكانته الاجتماعية، وهي متمثلة بالذم والتهديد والتشهير عبر الإنترنت كمن ينشر صورًا تمس سمعته بهدف تشويه صورته والانتقاص منه، وقد يرقى إلى أكبر من ذلك التشويه والتهديد إلى القتل (المناعسة والزغبي، 1431هـ).

ثانياً: الجرائم السيبرانية تستهدف أصول الأموال والاتصالات

بيّن الواقع أن الجرائم الواقعة على الأصول والأموال والاتصالات من أخطر الجرائم السيبرانية الحديثة، كون هذه الجرائم توقع خسائر مادية ضخمة، فالجرائم المالية التقليدية تحتاج إلى تخطيط مسبق ومجهود جماعي، بخلاف الجرائم المالية الإلكترونية فهي تتم بطرق سهلة تحتاج فقط إلى شخص متخصص في برامج الحاسب الآلي، وهي لا تحتاج مجهود جماعي، كما أن الجرائم السيبرانية توقع خسائر أكبر بكثير من الجرائم التقليدية، وكذلك الأمر بالنسبة للجرائم المتعلقة بالاتصالات (العفيفي، 2013).

ثالثًا: الجرائم السيبرانية التي تستهدف نظم وشبكات المعلومات

يقصد بجرائم نظم ووسائل وشبكات المعلومات الجرائم التي تقع على المكونات غير المادية للحاسب الآلي من بيانات ومعلومات، مثل اختراق الحاسب الآلي أو الشبكة إما مجرداً أو بهدف جريمة أخرى مثل تخريب الأنظمة، أو خلق البرامج الضارة التي تنقل عبر الشيكات وغيرها من الجرائم الأخرى (غيطاس، 2007). وأكثر الجرائم التي تتعلق بالأنظمة والمعلومات جريمة الدخول غير المصرح به، ويقصد بها وجود هجمات على معلومات الحاسب أو خدماته بقصد المساس بالسرية، أو تعطيل قدرة وكفاءة الأنظمة للقيام بأعمالها، ومن الأساليب المستخدمة في الفضاء السيبراني والتي تشكل ضرراً على تقنية المعلومات، وتهديد لأمن الإنترنت بالذات: "التصيد" حيث يمكن توريط المستخدم في فضح معلومات سرية. وتتم عمليات التصيد مثلًا من خلال البريد الإلكتروني حيث يتم توجيه رسائل يطلب فيها من المرسل إليه إعطاء معلومات يساعد منفذي عمليات التصيد في استخدام هوية الشخص المستهدف للدخول إلى نظام مالي أو اقتصادي أو اجتماعي يعمل عليه. ولا تنحصر المحاولات في البريد الإلكتروني، بل تتعداه إلى التراسل المباشر، حيث يلجأ القراصنة إلى توجيه رسائل تقود إلى وصلات خارجية يكفي الضغط عليها لتحميل برامج تجسس أو فيروسات على الجهاز الذي يتم عبره الاتصال (Heartworm, 2006). لذا تتعرض البنوك والمؤسسات المالية إلى عمليات اقتحام تتمثل في الوصول إلى معلومات خاصة بالعملاء، وليس البنوك فحسب، بل إن الجامعات والمدارس تعد مصدرًا هامًا للبيانات والمعلومات الشخصية التي يستهدفها القراصنة.

2-1-5-إجراءات تعزيز الأمن السيبراني

هناك ستة عناصر أساسية للأمن السيبراني، تتطلب تعزيز الأمن السيبراني فيها متمثلة بالتالي:

1. أمن التطبيقات: أمن التطبيقات هو العنصر الرئيسي الأول للأمن السيبراني الذي يضيف ميزات الأمن داخل التطبيقات أو مواقع الويب خلال فترة التطوير لمنع التهديدات السيبرانية، فهو يحمي المواقع والتطبيقات على شبكة الإنترنت من التهديدات الأمنية السيبرانية المختلفة التي تستغل نقاط الضعف في التعليمات البرمجية للتطبيق. وهناك أنواع مختلفة من أدوات أمن التطبيق مثل جدران الحماية، وبرامج مكافحة الفيروسات، وجدار حماية تطبيق ويب وأجهزة الأمن الأخرى التي يمكن أن تساعد في منع الهجمات السيبرانية من الوصول غير المصرح به (Baruch, 2019).
2. أمن المعلومات: يشير أمن المعلومات إلى العملية والمنهجية المتبعة لمنع الوصول غير المصرح لهم أو الاستخدام، أو الإفصاح، أو التعطيل، أو التعديل، أو الفحص، أو التسجيل، أو إتلاف المعلومات المادية وغير المادية، أو التفاصيل الشخصية، وبيانات تسجيل الدخول، وتفاصيل الشبكة أو الملف الشخصي الخاص على وسائل الإعلام الاجتماعية، والمعلومات على الهاتف المحمول، والمقاييس الحيوية (Baruch, 2019). كما أن أمن المعلومات يشير إلى الوسائل والأدوات الواجب توافرها لضمان أمن المعلومات من الأخطار الداخلية والخارجية (أحمد، 2012، ص16)، ولتحقيق أمن المعلومات يوجد العديد من التقنيات المستخدمة لذلك منها: تحديد العاملين المصرح لهم وغير المصرح لهم باستخدام هذه المعلومات، عملية التشفير، وتمثل بعض الرموز أو الأرقام التي عن طريقها لا يمكن فتح المعلومات أو فهمها أو الاستفادة منها إلا بعد الحصول على هذه الأكواد.

3. أمن الشبكات: تشمل عملية المنع والحماية ضد الوصول غير المصرح به إلى شبكات الحاسوب. وهي مجموعة من القواعد والتشكيلات لمنع ومراقبة الوصول غير المصرح به، وسوء الاستخدام، وتعديل شبكة الحاسوب والموارد. ويشمل ذلك كل من الأجهزة والبرمجيات (Baruch, 2019). ويعرف أمن الشبكات بأنه: هو النشاط المصمم لحماية البيانات عبر الشبكة الإلكترونية، وهو يتضمن تقنيات الأجهزة، والبرمجيات، كما أنه يستهدف العناصر الفاعلة التي توقف التهديدات وتمنعها من الانتشار داخل الشبكة وغالباً ما يكون ذلك عن طريق برامج الحماية (Cisco, 2017).
4. التخطيط للتعافي من الكوارث: هي خطة استراتيجية استمرارية للأعمال والإجراءات المدارة، التي تصف كيف يمكن استئناف العمل بسرعة وفاعلية بعد وقوع الكارثة. هناك أربعة أنواع من خطط التعافي من الكوارث وفقاً لطبيعة العمل: أولا: مركز البيانات للتعافي من الكوارث، ثانياً: سحابة استرداد الكوارث، ثالثاً: استعادة الأعطال الافتراضية، رابعاً: التعافي من الكوارث كخدمة (Hodhod et al., 2019).
5. أمن التشغيل: هو عملية تحليلية وإدارة للمخاطر التي تحدد المعلومات المهمة للمنظمة وتطوير آلية حماية لضمان أمن المعلومات الحساسة. ويعرف أيضاً بالأمن الإجرائي الذي يشجع المدير على عرض العمليات من أجل حماية المعلومات الحساسة من الاختراق، وهناك خمس خطوات لمعالجة برنامج أمن التشغيل، وهي كما يلي: تعريف المعلومات الحساسة للمؤسسة، تحديد فئات التهديد، تحليل ثغرات الأمان ونقاط الضعف، تقييم المخاطر، تنفيذ التدابير المضادة المناسبة (Hodhod et al., 2019).
6. تعليم المستخدم النهائي: هو العنصر الأكثر أهمية في هذه المنظومة، فالمستخدمون النهائيون أكبر خطر أمني في المؤسسات لأنه يمكن أن يحدث في أي وقت؛ ومع ذلك، فإن المستخدم النهائي لا يرتكب الخطأ من تلقاء نفسه، ويرجع ذلك في الغالب إلى عدم وجود الوعي وسياسات الأمن، والإجراءات، والبروتوكولات. يمكن تصنيف تهديدات المستخدم النهائي وفقا للطرق التالية: استخدام وسائل التواصل الاجتماعي، المراسلة النصية، تحميل التطبيقات، استخدام البريد الإلكتروني.

ومن الأفضل ترتيب وتوفير برامج للتدريب على التوعية الأمنية على أساس منتظم، وينبغي أن تغطي الموضوعات التالية: الاحتيال والتدابير الاجتماعية، الوصول والاتصال، أمان الجهاز، الأمن المادي، إنشاء كلمة المرور والاستخدام (Rahim et al. , 2019). حدد الحانوتي (2014)، وتوري (Tiwari et al ,2016) إلى العديد من الإجراءات التي تعزز الأمن السيبراني منها: التحقق من هوية الأطراف الآخرين عن طريق التحقق من هوية الأطراف المعنية بعملية تبادل البيانات بوضع كلمة مرور والشهادات الرقمية التي تتيح لصاحب البيانات من معرفة اتجاه بياناته وتحديد موافقته أو عدمها، إضافة جدار الحماية وهو أحد أنظمة الحماية التي تعيق أو تمنع عمليات الانتهاك أو الاحتيال الإلكتروني، التأكد من إعدادات الحاسب وشبكة الإنترنت، اختيار كلمات مرور قوية، وعمليات تحقق أمنية لمواقع التواصل الاجتماعي والبريد الإلكتروني والحسابات الشخصية، عدم الاستجابة لأي رسائل مجهولة المصدر، تدريب وتأهيل المستخدمين وتوعيتهم لاستخدام شبكات الإنترنت والأجهزة الإلكترونية، عدم إرسال أي معلومات شخصية أو الإفصاح عنها لأي جهة إلا بعد التأكد منها ومدى حرصها على سلامة هذه المعلومات.

2-2-الدراسات السابقة:

- **هدفت دراسة سينثيلكومار و إيسوارامورثي (Senthilkumar & Easwaramoorthy, 2017)** إلى تقييم الوعي بالأمن السيبراني لدى طلاب الجامعات في ولاية تاميل نادو، من خلال التركيز على التهديدات السيبرانية المختلفة على الإنترنت، وتكونت عينة الدراسة من (379) طالب وطالبة، واستخدمت أداة الاستبانة لجمع البيانات وفق المنهج الوصفي (التحليلي). وأظهرت نتائج الدراسة أن مستوى وعي الطلاب فوق المتوسط بقضايا التهديدات السيبرانية، مما يساعدهم على اتخاذ الاحتياطات اللازمة لحماية أنفسهم من الهجمات.
- **أما دراسة المعلم (Moallem, 2019)** فهدفت إلى التعرف على مدى وعي الطلاب بالأمن السيبراني والمخاطر السيبرانية في جامعتين في ولاية كاليفورنيا، وركزت على منطقة وادي السيليكون. وتكونت عينة الدراسة من (247) طالب، واستخدمت أداة الاستبانة لجمع البيانات وفق المنهج الوصفي (المسحي). وأظهرت نتائج الدراسة وجود نقص في الوعي بالأمن السيبراني، خاصة فيما يتعلق باستخدام المصادقة الثنائية، واستخدام كلمات مرور معقدة للحسابات. وأوصت الدراسة بأهمية تنظيم الجامعات تدريبات دورية، تهدف إلى تعزيز سلوك الطلاب وزيادة الوعي بالأمن السيبراني.
- **وأجرى جبرة وآخرون (Gabra et al . , 2020)** دراسة هدفت إلى تقييم مستوى وعي الطلاب بالأمن السيبراني وكيفية إدراك الهجمات السيبرانية في الجامعات النيجيرية، وتكونت عينة الدراسة من (367) طالب، واستخدمت أداة الاستبانة لجمع البيانات وفق المنهج الوصفي (المسحي). وأظهرت نتائج الدراسة وجود قصور في المعرفة الأساسية بالأمن السيبراني، لاسيما في إدارة كلمة المرور والتعرف على الهجمات السيبرانية. كما أشارت إلى أن معظم الجامعات تفتقر إلى برامج توعية مخصصة للأمن السيبراني. وأوصت الدراسة بضرورة دمج دورات متخصصة في الأمن السيبراني ضمن المناهج الدراسية الجامعية.

- **كما هدفت دراسة الحربي وتصدق (Alharbi & Tassaddiq, 2021)** إلى تقييم مستوى الوعي بالأمن السيبراني لدى طلاب البكالوريوس في جامعة المجمعة بالمملكة العربية السعودية. وتكونت عينة الدراسة من (576) طالب، واستخدمت أداة الاستبانة لجمع البيانات وفق المنهج الوصفي (المسحي). وأظهرت نتائج الدراسة وجود نقص في وعي الطلاب بمفاهيم الأمن السيبراني وكيفية إدارة بياناتهم بشكل آمن. بالإضافة إلى قصور في إدراك عواقب الجرائم الإلكترونية. وأوصت الدراسة بضرورة تبني المؤسسات الأكاديمية برامج تدريبية شاملة في مجال التوعية بالأمن السيبراني، لضمان تعزيز وعي الطلاب بطرق التعرف على التهديدات السيبرانية والتعامل معها.
- **أما دراسة الجهني وآخرون (Aljohni et al., 2021)** فهدفت إلى قياس مستوى الوعي بالأمن السيبراني بين طلاب الجامعات في المملكة العربية السعودية. وتكونت عينة الدراسة من (136) طالب وطالبة، واستخدمت أداة الاستبانة لجمع البيانات وفق المنهج الوصفي (المسحي). وأظهرت نتائج الدراسة أنه لا يوجد فرق كبير في مستوى الوعي بالأمن السيبراني بين الطلاب والطالبات وفقاً لمتغير الجنس، لكن الإناث يظهرن اهتماماً أكبر بالأمن السيبراني. بالإضافة إلى أنه هناك وعي عالي لدى طلاب قسم الحاسوب وتقنية المعلومات مقارنة بالآخرين. وأوصت الدراسة بضرورة اتخاذ التدابير السياسية اللازمة من قبل الجامعات لضمان حصول الطلاب من جميع الأقسام على نفس مستوى الوعي بالأمن السيبراني.
- **وهدفت دراسة الشهري (2021)** إلى التعرف على دور إدارة الجامعة في تعزيز الوعي بالأمن السيبراني لدى طلاب كلية التربية بجامعة الإمام محمد بن سعود الإسلامية، وتقييم مستوى معرفة الطلاب بالأمن السيبراني، وتكونت عينة الدراسة من (188) طالب وطالبة، واستخدمت الاستبانة لجمع البيانات وفق المنهج الوصفي (المسحي). وأظهرت نتائج الدراسة أن كلاً من معرفة الطلاب بالأمن السيبراني، وجهود إدارة الجامعة في تعزيز الوعي بالأمن السيبراني جاءت بمستوى متوسط. وأوصت الدراسة بضرورة تنسيق الجهود بين إدارة الجامعة والجهات المعنية بالأمن السيبراني، مثل الهيئة الوطنية للأمن السيبراني لاتخاذ الإجراءات اللازمة لتعزيز الوعي بين الطلاب. بالإضافة إلى إقامة ورش عمل ودورات تدريبية.
- **وقد أجرت عزة وآخرون (Azzeh et al., 2022)** دراسة هدفت إلى تحليل أثر دمج مفاهيم الأمن السيبراني في مناهج تقنية المعلومات على مستوى معرفة الطلاب وممارساتهم المتعلقة بالأمن السيبراني، واستخدمت الدراسة المنهج التجريبي ذو المجموعتين التجريبية والضابطة، وتم تطوير برنامج تدريبي قائم على مفاهيم الأمن السيبراني، وتكونت عينة الدراسة من (42) طالب تم تقسيمهم بالتساوي إلى مجموعة تجريبية وضابطة، وتضمنت أدوات الدراسة اختباراً لقياس مستوى المعرفة بالأمن السيبراني تم تطبيقه قبليا وبعديا على كلا المجموعتين. وأظهرت نتائج الدراسة وجود فروق ذات دلالة إحصائية في مستوى المعرفة لصالح المجموعة التجريبية. وأوصت الدراسة بتضمين موضوعات الأمن السيبراني ضمن المقررات الأكاديمية لتعزيز استعداد الطلاب لمواجهة التهديدات السيبرانية.
- **وسعت دراسة القحطاني (Alqahtani, 2022)** إلى معرفة درجة الوعي بالأمن السيبراني بين طلاب جامعة الإمام عبد الرحمن بن فيصل بناءً على ثلاثة جوانب: أمان كلمة المرور، وأمان المتصفح، ووسائل التواصل الاجتماعي، وتكونت عينة الدراسة من (450) طالب من مرحلتي البكالوريوس والدراسات العليا، واستخدمت أداة الاستبانة لجمع البيانات وفق المنهج الوصفي (المسحي). وأظهرت نتائج الدراسة وجود ضعف في الوعي بالأمن السيبراني، خاصة فيما يتعلق بأمان كلمة المرور. بالإضافة إلى أن معرفة كيفية التعامل مع أمان كلمة المرور، وأمان المتصفح، وأنشطة التواصل الاجتماعية تؤثر بشكل ملحوظ على الوعي بالأمن السيبراني. وأوصت الدراسة بضرورة تعزيز الوعي لدى الطلاب من خلال التنشئة الاجتماعية، وحملات تثقيفية متعلقة بالأمن السيبراني.
- **بينما قدم الحبيب (2022)** دراسة للتعرف على درجة الوعي بمفاهيم الأمن السيبراني، وتطبيقات الأمن السيبراني، وأبرز سبل تعزيز الوعي بالأمن السيبراني لدى طلاب الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية، وتكونت عينة الدراسة من (269) طالب وطالبة، واستخدمت أداة الاستبانة لجمع البيانات وفق المنهج الوصفي (المسحي). وأظهرت نتائج الدراسة أن طلاب الدراسات العليا لديهم مستوى عالٍ من الوعي بمفاهيم وتطبيقات الأمن السيبراني، كما أنهم موافقون للسبل المقترحة لتعزيز هذا الوعي. وأوصت الدراسة بأن تتبنى كلية التربية مجموعة من التدابير الفعالة التي تسهم في تعزيز مستوى الوعي بالأمن السيبراني لدى طلاب الدراسات العليا.

2-2-2-التعقيب على الدراسات السابقة:

اتفقت هذه الدراسة مع معظم الدراسات السابقة في الهدف الأساسي المتمثل في معرفة درجة الوعي بالأمن السيبراني لدى طلبة التعليم العالي. كما اتفقت مع الدراسات السابقة في اعتمادها على المنهج الوصفي (المسحي) كمنهج أساسي لجمع البيانات، وهو ما يعكس مدى فاعلية هذا النهج في تقييم مستوى الوعي بالأمن السيبراني بين الطلاب. بالإضافة إلى ذلك، استخدمت الدراسة الحالية أداة الاستبانة لجمع البيانات، وهو الأسلوب الأكثر شيوعًا في الدراسات السابقة، مما يدل على أهميته في قياس المعرفة والوعي بالسلوكيات السيبرانية.

وقد استفادت الدراسة الحالية من النتائج التي توصلت إليها الدراسات السابقة، حيث أكدت دراسة سينثيلكومار وإيسوارامورثي (Senthilkumar & Easwaramoorthy, 2017)على أهمية تقييم مستوى وعي الطلاب بالتهديدات السيبرانية، وهو ما يعزز ضرورة التحقق من

مدى إدراك طالبات الدراسات العليا في جامعة الملك سعود لهذه المخاطر. كما أظهرت دراسة المعلم (Moallem, 2019) أن هناك نقصًا في استخدام المصادقة الثنائية وكلمات المرور المعقدة، مما يوجه الدراسة الحالية إلى فحص هذه الجوانب لدى الفئة المستهدفة.

إضافةً إلى ذلك، قدمت دراسة جبرة وآخرون (Gabra et al., 2020) دليلاً على أن العديد من الجامعات تفتقر إلى برامج توعية بالأمن السيبراني، وهو ما يدعم الحاجة إلى البحث في مدى توفر هذه البرامج في بيئة الدراسة الحالية. ومن ناحية أخرى، أكدت دراسة الحربي وتصدق (Alharbi & Tassaddiq, 2021)وجود نقص في معرفة الطلاب بمفاهيم الأمن السيبراني، مما يشير إلى أهمية تقييم مدى إدراك طالبات الدراسات العليا لهذه المفاهيم.

أما دراسة عزة وآخرون (Azzeh et al., 2022) فقد استفادت منها الدراسة الحالية في إبراز أهمية دمج مفاهيم الأمن السيبراني في المناهج الدراسية، حيث أثبتت الدراسة أن إدخال هذه المفاهيم في مناهج تقنية المعلومات أدى إلى تحسن ملحوظ في مستوى المعرفة بالأمن السيبراني. كما استفادت الدراسة من نتائج القحطاني (Alqahtani, 2022) التي أكدت على أهمية تعزيز الوعي بأمان كلمة المرور والمتصفح ووسائل التواصل الاجتماعي، مما يوجه البحث الحالي إلى فحص هذه الجوانب لدى طالبات الدراسات العليا.

وبالإضافة إلى ذلك، قدمت دراسة الشهري (2021) رؤية مهمة حول دور إدارة الجامعة في تعزيز الوعي بالأمن السيبراني، وهو ما يفتح المجال أمام الدراسة الحالية للنظر في مدى تأثير الإدارة الأكاديمية على وعي الطالبات بالأمن السيبراني. وأخيرًا، أشارت دراسة الحبيب (2022) إلى أن طلاب الدراسات العليا لديهم مستوى عالٍ من الوعي بمفاهيم وتطبيقات الأمن السيبراني، وهو ما سيساعد الدراسة الحالية في مقارنة نتائجها مع هذه الدراسة لاكتشاف الفروقات المحتملة في مستوى الوعي بين المجموعات الأكاديمية المختلفة.

وبذلك، تميزت الدراسة الحالية عن غيرها من الدراسات السابقة من خلال الفئة المستهدفة، حيث ركزت على طالبات الدراسات العليا في قسم المناهج وطرق التدريس بجامعة الملك سعود، مما يضيف بعدًا جديدًا وغير مستكشف في الدراسات السابقة حول الوعي بالأمن السيبراني.

3- منهجية الدراسة وإجراءاتها

3-1-منهج الدراسة:

تم استخدام المنهج الوصفي (المسحي)؛ لمناسبته للكشف عن درجة الوعي بالأمن السيبراني لدى طالبات الدراسات العليا قسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن. ويستخدم المنهج الوصفي المسحي للتعرف على الظاهرة وتحديد الوضع الحالي وجوانب القوة والضعف لها (عباس وآخرون، 2020).

3-2-مجتمع الدراسة وعينتها:

تكوّن مجتمع الدراسة من جميع طالبات الدراسات العليا في كلية التربية، قسم المناهج وطرق التدريس بجامعة الملك سعود، خلال الفترة من (2021) إلى (2024)، والبالغ عددهن (212) طالبة. تم تصميم أداة الاستبيان عبر موقع Google Driveوإرسالها إلكترونيًا إلى مجتمع الدراسة، وعادت منها (71) استبانة صالحة للتحليل الإحصائي، بنسبة استجابة بلغت (33.5%)، وهي نسبة مقبولة لمجتمع أفراده بالمئات (عبيد، 2003). وقد تم استخدام خصائص العينة، مثل المستوى الدراسي والتخصص وسنوات الخبرة، في تحليل الفروق الإحصائية لاختبار تأثير هذه المتغيرات على مستوى الوعي بالأمن السيبراني.

3-2-1-وصف العينة تبعا لمتغير الدرجة العلمية:

جدول (1): توزيع أفراد الدراسة وفقاً لمتغير الدرجة العلمية

الدرجة العلمية	التكرار	النسبة
ماجستير	37	52.1
دكتوراه	34	47.9
المجموع	71	%100

يوضح جدول (1) توزيع أفراد الدراسة من طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود وفقاً لمتغير الدرجة العلمية، وقد اتضح أن (52.1%) من إجمالي أفراد الدراسة من الطالبات درجتهن العلمية (ماجستير)، بينما اتضح أن (47.9 %) من إجمالي أفراد الدراسة من الطالبات درجتهن العلمية (دكتوراه).

3-2-2-وصف العينة تبعا لمتغير التخصص:

جدول (2): توزيع أفراد الدراسة وفقاً لمتغير التخصص

التخصص	التكرار	النسبة
مناهج وطرق تدريس- عامة	25	35.2
مناهج وطرق تدريس- تعليم حاسب	16	22.5
مناهج وطرق تدريس- لغة إنجليزية	10	14.1
مناهج وطرق تدريس- العلوم الشرعية	9	12.7
مناهج وطرق تدريس- الرياضيات والعلوم	8	11.3
مناهج وطرق تدريس- لغة عربية	1	1.4
مناهج وطرق تدريس- فنية	1	1.4
مناهج وطرق تدريس الدراسات الاجتماعية	1	1.4
المجموع	71	%100

يوضح جدول (2) توزيع أفراد الدراسة من طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود وفقاً لمتغير التخصص، وقد اتضح أن (35.2%) من إجمالي أفراد الدراسة من الطالبات تخصصاتهن(مناهج وطرق تدريس- عامة)، بينما اتضح أن (22.5 %) من إجمالي أفراد الدراسة من الطالبات تخصصاتهن(مناهج وطرق تدريس- تعليم حاسب)، في حين اتضح أن (14.1 %) من إجمالي أفراد الدراسة من الطالبات تخصصاتهن(مناهج وطرق تدريس- لغة إنجليزية)، في حين اتضح أن (12.7 %) من إجمالي أفراد الدراسة من الطالبات تخصصاتهن(مناهج وطرق تدريس- العلوم الشرعية)، في حين اتضح أن (11.3 %) من إجمالي أفراد الدراسة من الطالبات تخصصاتهن(مناهج وطرق تدريس- الرياضيات والعلوم)، في حين اتضح أن (1.4 %) من إجمالي أفراد الدراسة من الطالبات تخصصاتهن(مناهج وطرق تدريس- لغة عربية)، وبنفس النسبة كلا من مناهج وطرق تدريس- فنية، ومناهج وطرق تدريس الدراسات الاجتماعية.

3-2-3-وصف العينة تبعا لمتغير الحصول على دورات في الأمن السيبراني:

جدول (3): توزيع أفراد الدراسة وفقاً لمتغير هل سبق الحصول على دورات في الأمن السيبراني

هل سبق الحصول على دورات في الأمن السيبراني	التكرار	النسبة
لا	50	70.4
نعم	21	29.6
المجموع	71	%100

يوضح جدول (3) توزيع أفراد الدراسة من طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود وفقاً لمتغير هل سبق الحصول على دورات في الأمن السيبراني، وقد اتضح أن (70.4%) من اجمالي أفراد الدراسة من الطالبات لم يحصلن على دورات في الأمن السيبراني، بينما اتضح أن (29.6%) من اجمالي أفراد الدراسة من الطالبات حصلن على دورات في الأمن السيبراني.

3-3-أداة الدراسة

3-3-1-بناء أداة الدراسة:

لتحقيق أهداف الدراسة تم استخدام الاستبانة للكشف عن درجة الوعي بالأمن السيبراني لدى طالبات الدراسات العليا قسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن. وبالرجوع إلى الدراسات والبحوث المتصلة بموضوع الدراسة، مثل دراسة الحبيب (2022)، والقحطاني (2022)، والشهري (2021)، والجهني وآخرون (Aljohni et al., 2021)، والحربي وتصدق (Alharbi & Tassaddiq, 2021)، وجبرة وآخرون (Gabra et al., 2020)، والمعلم (Moallem, 2019)، تم اختيار الاستبانة الواردة في دراسة الحبيب (2022) لتكون أداة البحث في الدراسة الحالية. وقد استند هذا الاختيار إلى سهولة اللغة المستخدمة في صياغة العبارات، وملاءمة طول الاستبانة، وتوافقها مع الأسئلة البحثية للدراسة الحالية. وبعد التواصل مع الباحث الحبيب والحصول على موافقته لاستخدام الأداة، حيث إنه تأكد من صدقها وثباتها بما يضمن صلاحيتها للاستخدام في نفس هذا السياق.

وقد تكونت الاستبانة من جزأين:

- الجزء الأول: بيانات أولية عن أفراد مجتمع الدراسة من حيث الدرجة العلمية، والحصول على دورات في الأمن السيبراني.
- الجزء الثاني: تضمّن عبارات الاستبانة موزّعة على ثلاثة محاور، هي:

- المحور الأول: درجة وعي طالبات الدراسات العليا بكلية التربية قسم المناهج بجامعة الملك سعود بمفاهيم الأمن السيبراني من وجهة نظرهم، وقد تضمن ١٠ عبارات،
- المحور الثاني: درجة وعي طلاب وطالبات الدراسات العليا بكلية التربية قسم المناهج بجامعة الملك سعود بتطبيقات الأمن السيبراني من وجهة نظرهم، وقد تضمن 12 عبارة، وُيقَّابَل كل عبارة من عبارات هذين المحورين حسب مقياس ليكرت الخماسي قاَئمة تحمل العبَارات الَتالية: (منخفضة جداً- منخفضة - متوسطة - عالية – عالية جداً)، وقد تم إعطاء كل عبارة من العبارات السابقة درجات لتتم معالجتها إحصائياً على النحو الآتي: عالية جداً (5)- عالية (4)- متوسطة(3) – منخفضة (2)- منخفضة جداً (1) درجة واحدة.
- المحور الثالث: السُبل المقترحة لتعزيز الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بكلية التربية قسم المناهج بجامعة الملك سعود من وجهة نظرهم، وتضمن 8 عبارات، ويقابل كل عبارة خمسة بدائل؛ وفقا لمقياس ليكرت الخماسي: (منعدم الأهمية- قليل الأهمية- متوسط الأهمية - مهم– مهم جداً)، وقد تم إعطاء كل عبارة من العبارات السابقة درجات لتتم معالجتها إحصائيا على النحو الآتي: مهم جداً (5) - مهم (4) - متوسط الأهمية (3) – قليل الأهمية (2)- منعدم الأهمية (1).

3-3-2-الخصائص السيكومترية للأداة (الصدق والثبات)

في الدراسة الحالية تم استخدام أداة الاستبانة التي تم تطويرها في دراسات سابقة من قبل الباحثين الحبيب (2022) وآخرين. ولضمان ملاءمة الأداة للسياق الحالي، وعليه قد تم بتطبيق الاستبانة على عينة استطلاعية من طالبات الدراسات العليا في جامعة الملك سعود (من خارج العينة الرئيسية) مكونة من 40 طالبة، لتحديد صدق وثبات الأداة في الدراسة الحالية. بعد تطبيق الاستبانة على العينة الاستطلاعية، تم حساب معاملات صدق الاتساق الداخلي للأداة باستخدام معاملات ارتباط بيرسون بين كل عبارة من عبارات المحاور والدرجة الكلية لكل محور. كما تم حساب معامل الثبات باستخدام طريقة كرونباخ ألفا، مما أتاح التحقق من مدى تناسق الأداة مع الأهداف البحثية في السياق الحالي.

3-3-3-صدق أداة الدراسة:

للتحقق من الصدق الظاهري عرضت الاستبانة، في صورتها الأولية على مجموعة من المحكمين من أعضاء هيئة التدريس المتخصصين في التربية، وتم الاستجابة لآراء المحكمين حيث تم إجراء ما يلزم من حذف أو إضافة أو تعديل في ضوء مقترحاتهم. وللتحقق من مدى تماسك العبارات وصدق الاتساق الداخلي للأداة، تم قياس معاملات ارتباط بيرسون بين كل عبارة من عبارات المحور والدرجة الكلية للمحور الذي تنتمي إليه، وذلك استناداً إلى بيانات استجابات أفراد الدراسة. والجداول التالية توضح ذلك:

جدول (4) معاملات الارتباط بين درجة كل عبارة من عبارات محور" درجة الوعي بمفاهيم الأمن السيبر اني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود " بالدرجة الكلية للمحور

رقم العبارة	معامل الارتباط بالمحور	رقم العبارة	معامل الارتباط بالمحور
1	**0.530	6	**0.695
2	**0.380	7	**0.752
3	**0.669	8	**0.786
4	**0.681	9	**0.711
5	**0.444	10	**0.430

**** دالة عند مستوى الدلالة 0.01**

يتضح من الجدول (4) أن قيم معامل ارتباط كل عبارة من العبارات مع الدرجة الكلية لمحور " درجة الوعي بمفاهيم الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود " الذي تنتمي إليه العبارة، موجبة ودالة إحصائيا عند مستوى الدلالة (0.01) فأقل، وتتراوح ما بين (0.380 إلى 0.786) وهي ذات قيم مرتفعة، مما يشير إلى أن عبارات هذا المحور تتمتع بدرجة صدق مرتفعة وصلاحيتها للتطبيق الميداني.

جدول (5): معاملات الارتباط بين درجة كل عبارة من عبارات محور" درجة الوعي بتطبيقات الأمن السيبر اني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود " بالدرجة الكلية للمحور

رقم العبارة	معامل الارتباط بالمحور	رقم العبارة	معامل الارتباط بالمحور
1	**0.493	7	**0.701
2	**0.592	8	**0.727

رقم العبارة	معامل الارتباط بالمحور	رقم العبارة	معامل الارتباط بالمحور
3	**0.498	9	**0.698
4	**0.639	10	**0.775
5	**0.589	11	**0.680
6	**0.815	12	**0.722

** دالة عند مستوى الدلالة 0.01

يتضح من الجدول (5) أن قيم معامل ارتباط كل عبارة من العبارات مع الدرجة الكلية لمحور " درجة الوعي بتطبيقات الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود " الذي تنتمي إليه العبارة، موجبة ودالة إحصائيا عند مستوى الدلالة (0.01) فأقل، وتتراوح ما بين (0.493 إلى 0.815) وهي ذات قيم مرتفعة، مما يشير إلى أن عبارات هذا المحور تتمتع بدرجة صدق مرتفعة وصلاحيتها للتطبيق الميداني.

جدول (6): معاملات الارتباط بين درجة كل عبارة من عبارات محور" سبل تعزيز الوعي بالأمن السيبر اني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود " بالدرجة الكلية للمحور

رقم العبارة	معامل الارتباط بالمحور	رقم العبارة	معامل الارتباط بالمحور
1	**0.623	5	**0.768
2	**0.566	6	**0.645
3	**0.517	7	**0.719
4	**0.667	8	**0.691

** دالة عند مستوى الدلالة 0.01

يتضح من الجدول (6) أن قيم معامل ارتباط كل عبارة من العبارات مع الدرجة الكلية لمحور " سبل تعزيز الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود " الذي تنتمي إليه العبارة، موجبة ودالة إحصائيا عند مستوى الدلالة (0.01) فأقل، وتتراوح ما بين (0.517 إلى 0.768) وهي ذات قيم مرتفعة، مما يشير إلى أن عبارات هذا المحور تتمتع بدرجة صدق مرتفعة وصلاحيتها للتطبيق الميداني.

3-3-3-ثبات أداة الدراسة

تم حساب ثبات الأداة باستخدام معامل ألفا كرونباخ (Cronbach's Alpha)، والجدول (7) يوضح معامل الثبات لمحاور أداة الدراسة وهي:

جدول (7): معامل ألفا كرونباخ لقياس ثبات أداة الدراسة

المحاور	عدد العبارات	معامل الثبات
المحور الأول: درجة الوعي بمفاهيم الأمن السيبر اني	10	0.792
المحور الثاني: درجة الوعي بتطبيقات الأمن السيبر اني	12	0.878
المحور الثالث: سبل تعزيز الوعي بالأمن السيبر اني	8	0.803
الثبات الكلي للاستبانة	30	0.863

من خلال النتائج الموضحة أعلاه بالجدول (7) يتضح أن معامل الثبات لمحاور الدراسة عالي، حيث يتراوح ما بين (0.792) و (0.878)، وبلغت قيمة معامل الثبات العام للاستبانة (0.863)، وهي قيمة ثبات مرتفعة توضح صلاحية أداة الدراسة للتطبيق الميداني.

3-4-الوزن المعياري المحك للإجابات:

قامت الباحثات بحساب الوسط الحسابي لإجابات أفراد الدراسة. ولتحديد طول خلايا المقياس الخماسي (الحدود الدنيا والعليا) المستخدم في محاور الدراسة، تم حساب المدى (5-1=4)، ثم تقسيمه على عدد خلايا المقياس للحصول على طول الخلية الصحيح أي (5/4= 0.80) بعد ذلك تم إضافة هذه القيمة إلى أقل قيمة في المقياس وذلك لتحديد الحد الأعلى لهذه الخلية، وهكذا أصبح طول الخلايا كما يوضحها جدول (8) التالي:

جدول (8): مقياس ليكرت الخماسي لقياس درجة الموافقة ومدى الموافقة

الترميز عند إدخال البيانات	مديات المتوسطات	التقدير اللفظي/ درجة الوعي المحور الأول والثاني/ الثالث (الأهمية)	
1	1.80 - 1.00	منخفضة جداً	منعدم الأهمية
2	2.60 - 1.80	منخفضة	قليل الأهمية
3	3.40 - 2.61	متوسطة	متوسط الأهمية
4	4.20 - 3.41	عالية	مهم
5	5.0 - 4.21	عالية جداً	مهم جداً

3-5-أساليب المعالجة الإحصائية

لتحليل البيانات التي تم تجميعها تم استخدام الحزم الإحصائية للعلوم الاجتماعية، والتي يرمز لها اختصاراً بالرمز (SPSS)، وذلك باستخدام المعالجات الإحصائية التالية:

- حساب التكرارات والنسب المئوية لوصف عينة الدراسة.
- إيجاد معامل ارتباط بيرسون لقياس صدق الاتساق الداخلي بين عبارات الأداة وكل محور تنتمي إليه.
- إيجاد معادلة ألفا كرونباخ لحساب معامل ثبات أداة الدراسة.
- حساب المتوسط الحسابي لاستجابات العينة على كل عبارة، ولكل محور من محاور أداة الدراسة.
- حساب الانحراف المعياري لحساب مدى تباعد القيم عن متوسطها الحسابي.

4- نتائج الدراسة ومناقشتها

4-1-الإجابة عن السؤال الأول: "ما درجة الوعي بمفاهيم الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن؟"

وللإجابة عن هذا السؤال تم حساب التكرارات، والنسب المئوية والمتوسطات الحسابية، والانحرافات المعيارية، والرتب، لاستجابات أفراد الدراسة من طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود على محور " درجة الوعي بمفاهيم الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود "، وجاءت النتائج كما يبيّنها الجدول (9) التالي:

جدول (9) : درجة الوعي بمفاهيم الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة الوعي
1	أرى أن الأمن السيبراني يحمي نظم المعلومات من الاختراق ومن الهجمات الفيروسية.	4.65	0.51	1	عالية جداً
3	أدرك أهمية المحافظة على الأمن السيبراني.	4.56	0.73	2	عالية جداً
4	أدرك أهمية الأمن السيبراني.	4.54	0.71	3	عالية جداً
6	أدرك مخاطر التفريط بالأمن السيبراني.	4.45	0.75	4	عالية جداً
5	أخشى على بياناتي الشخصية من انتهاكات الأمن السيبراني.	4.32	0.92	5	عالية جداً
2	أحتاج إلى دورات تدريبية في الأمن السيبراني.	4.03	0.86	6	عالية
7	لدي إلمام بمفهوم الأمن السيبراني.	3.31	1.12	7	متوسطة
8	لدي اطلاع واسع على جرائم الأمن السيبراني.	3.06	1.00	8	متوسطة
9	لدي إلمام بطرق المحافظة على الأمن السيبراني.	2.83	1.06	9	متوسطة
10	لدى معوقات شخصية تحول بيني وبين تحقيق الوقاية من مخاطر الأمن السيبراني.	2.65	1.02	10	متوسطة
	المتوسط الحسابي العام	3.84	0.52		عالية

يتبين من النتائج الموضحة في جدول (9) أن جميع العبارات التي تقيس درجة الوعي بمفاهيم الأمن السيبراني لدى طالبات الدراسات العليا يتراوح متوسطها الحسابي بين (2,65 إلى 4,65)، وهذه المتوسطات تقع بين الفئات الثالثة من (2,61 إلى 3,40) و الرابعة من (3,41 إلى 4,20) والخامسة من (4,21 إلى 5)، من المقياس الخماسي وهذه الفئات تشير إلى خيار(عالية جداً-عالية -متوسطة). وعند ترتيب العبارات ومتوسطها الحسابي على التوالي من المتوسط الأكبر إلى المتوسط الأقل تكون كما يلي: أرى أن الأمن السيبراني يحمي نظم المعلومات من الاختراق ومن الهجمات الفيروسية (4.65)، أدرك أهمية المحافظة على الأمن السيبراني (4.56)، أدرك أهمية الأمن السيبراني (4.54)، أدرك مخاطر التفريط بالأمن السيبراني (4.45)،أخشى على بياناتي الشخصية من انتهاكات الأمن السيبراني (4.32)،أحتاج إلى دورات تدريبية في الأمن السيبراني (4.03)، لدي إلمام بمفهوم الأمن السيبراني (3.31)، لدي اطلاع واسع على جرائم الأمن السيبراني (3.06)،لدي إلمام بطرق المحافظة على الأمن السيبراني (2.83)، لدى معوقات شخصية تحول بيني وبين تحقيق الوقاية من مخاطر الأمن السيبراني(2.65). ونستخلص مما سبق أن المتوسط العام لاستجابة أفراد الدراسة من طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود نحو محور" درجة الوعي بمفاهيم الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود " جاءت بدرجة وعي (عالية) حيث بلغ المتوسط الحسابي (3.84) وهذا يدل على أن طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود لديهن وعي بدرجة عالية فيما يتعلق بمفاهيم الأمن السيبراني.

ومن خلال تحليل النتائج، يمكن تفسير المستوى العالي من الوعي لدى طالبات الدراسات العليا من وجهة نظر الباحثات بعدة عوامل، من أبرزها التطور المتسارع في التكنولوجيا والاعتماد المتزايد على الفضاء الإلكتروني في العملية التعليمية والبحثية، مما يعزز اهتمام الطالبات بالأمن السيبراني. كما أن ارتفاع مستوى الإدراك بمخاطر التفريط في الأمن السيبراني يعكس تنامي الوعي بأهمية الحماية الشخصية للبيانات، خاصة مع انتشار التهديدات الرقمية والجرائم الإلكترونية. وعلى الرغم من ذلك، فإن الحاجة الملحوظة إلى دورات تدريبية تشير إلى أن هناك فجوة بين المعرفة النظرية والتطبيق العملي، مما يستدعي تعزيز البرامج التوعوية والتدريبية بشكل أكثر تخصصًا وعمقًا، لضمان قدرة الطالبات على تطبيق ممارسات الأمن السيبراني بفعالية في بيئاتهن الأكاديمية والمهنية.

وتتفق هذه النتيجة مع دراسة الحبيب (2022) والتي توصلت إلى أن طلاب الدراسات العليا لديهم مستوى عالٍ من الوعي بمفاهيم الأمن السيبراني، كما تتفق هذه النتيجة أيضاً مع دراسة الشهري (2021) والتي أظهرت أن من معرفة الطلاب بالأمن السيبراني جاءت بمستوى متوسط. في حين تختلف هذه النتيجة مع جبرة وآخرون (Gabra et al., 2020) والتي توصلت الى وجود قصور في المعرفة الأساسية بالأمن السيبراني، لاسيما بالتعرف على الهجمات السيبرانية، كما تختلف مع الحربي وتصدق (Alharbi& Tassaddiq, 2021) والتي أظهرت وجود نقص في وعي الطلاب بمفاهيم الأمن السيبراني وكيفية إدارة بياناتهم بشكل آمن.

4-2-الإجابة عن السؤال الثاني: ما درجة الوعي بتطبيقات الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن؟

للإجابة عن هذا السؤال تم حساب التكرارات، والنسب المئوية والمتوسطات الحسابية، والانحرافات المعيارية، والرتب، لاستجابات أفراد الدراسة من طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود على محور " درجة الوعي بتطبيقات الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود، وجاءت النتائج كما يبينها الجدول (10).

جدول(10): درجة الوعي بتطبيقات الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود

م	العبارات	المتوسط	الانحراف	الرتبة	درجة الوعي
1	أتجنب فتح أي رابط مرفق في رسالة مجهولة المصدر.	4.66	0.61	1	عالية جداً
3	أتجنب نشر صوري الشخصية والعائلية من خلال تطبيقات التواصل الاجتماعي.	4.32	1.05	2	عالية جداً
2	أتجنب إرسال معلوماتي الشخصية عبر الرسائل النصية أو البريد الإلكتروني.	4.20	0.94	3	عالية
4	أعي خطورة الاتصال بالشبكات في الأماكن العامة.	4.14	1.09	4	عالية
5	أستخدم في جهازي تقنية التحقيق الثنائي (كلمة المرور- البصمة).	3.92	1.27	5	عالية
6	أُعطل خدمات الوصول لموقعي في التطبيقات المحملة على جهازي.	3.58	1.24	6	عالية
7	اهتم بتحديث جهازي بصفة مستمرة حفاظاً عليه.	3.51	1.14	7	عالية

م	العبارات	المتوسط	الانحراف	الرتبة	درجة الوعي
9	أهتم بتحميل برامج آمنة لمكافحة الفيروسات.	3.41	1.26	8	عالية
10	أختار كلمة مرور قوية، وأهتم بتغييرها كل فترة.	3.37	1.14	9	متوسطة
8	أستطيع رفع بلاغ عن الإساءات التي قد أتعرض لها في مو اقع التواصل.	3.35	1.22	10	متوسطة
11	أعد نسخة احتياطية للبيانات المخزنة في جهازي على الخدمة السحابية	3.18	1.19	11	متوسطة
12	أُغير إعدادات جهازي بشكل مستمر لكي لا تخترق شبكة Wi-Fi.	2.56	1.18	12	منخفضة
	المتوسط الحسابي العام	3.68	0.73		عالية

يتبين من النتائج الموضحة في جدول (10) أن هناك تفاوت في درجة وعي عينة الدراسة على عبارات محور (درجة الوعي بتطبيقات الأمن السيبراني)، حيث يشمل المحور على (12) عبارة، وتراوحت متوسطاتهم الحسابية من (2.56 إلى 4.66). وهذه المتوسطات تقع بين الفئات الثانية من (1.80 إلى 2.60)و الثالثة من(2,61 إلى 3,40) و الرابعة من(3,41 إلى 4,20) والخامسة من(4,21 إلى 5)، من المقياس الخماسي وهذه الفئات تشير إلى خيار(عالية جداً-عالية -متوسطة- منخفضة).وعند ترتيب العبارات ومتوسطها الحسابي على التوالي من المتوسط الأكبر إلى المتوسط الأقل تكون كما يلي: أتجنب فتح أي رابط مرفق في رسالة مجهولة المصدر (4.66)،أتجنب نشر صوري الشخصية والعائلية من خلال تطبيقات التواصل الاجتماعي (4.32)،أتجنب إرسال معلوماتي الشخصية عبر الرسائل النصية أو البريد الإلكتروني (4.20)،أعي خطورة الاتصال بالشبكات في الأماكن العامة(4.14)،أستخدم في جهازي تقنية التحقيق الثنائي (كلمة المرور- البصمة) (3.92)،أُعطل خدمات الوصول لموقعي في التطبيقات المحملة على جهازي(3.58)،اهتم بتحديث جهازي بصفة مستمرة حفاظاً عليه (3.51)، أهتم بتحميل برامج آمنة لمكافحة الفيروسات (3.41)،أختار كلمة مرور قوية، وأهتم بتغييرها كل فترة (3.37)،أستطيع رفع بلاغ عن الإساءات التي قد أتعرض لها في مواقع التواصل الاجتماعي (3.35)، أقوم بإعداد نسخة احتياطية للبيانات المخزنة في جهازي على الخدمة السحابية (3.18)،أُغير إعدادات جهازي بشكل مستمر لكي لا تخترق شبكة Wi-Fi (2.56).

أظهرت النتائج أن المتوسط العام لاستجابة عينة الدراسة نحو محور "درجة الوعي بتطبيقات الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود" جاءت بدرجة وعي (عالية) حيث بلغ المتوسط الحسابي (3.68). وهذا يدل على أن طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود لديهن وعي بدرجة عالية فيما يتعلق بتطبيقات الأمن السيبراني ويتضح ذلك من خلال سلوكياتهن المسؤولة، مثل تجنب فتح الروابط المرفقة في الرسائل مجهولة المصدر، والامتناع عن نشر الصور الشخصية والعائلية عبر تطبيقات التواصل الاجتماعي، وتجنب إرسال المعلومات الشخصية عبر الرسائل النصية أو البريد الإلكتروني. بالإضافة إلى ذلك، يظهر هذا الوعي في الحذر عند الاتصال بالشبكات في الأماكن العامة، واستخدام تقنيات التحقيق الثنائي (كلمة المرور- البصمة).

وتتفق هذه النتائج مع دراسة الحبيب (2022) والتي توصلت إلى أن طلاب الدراسات العليا لديهم مستوى عالٍ من الوعي بتطبيقات الأمن السيبراني. ومع ذلك، تختلف هذه النتائج مع دراسة القحطاني (Alqahtani, 2022) التي أشارت إلى وجود ضعف في الوعي بالأمن السيبراني، خاصة فيما يتعلق بأمان كلمة المرور، وأمان المتصفح، وأنشطة وسائل التواصل الاجتماعي، مما يؤثر بشكل ملحوظ على الوعي بتطبيقات الأمن السيبراني. كما تختلف النتائج مع دراسة المعلم (Moallem, 2019) ودراسة جبرة وآخرون (Gebra et al., 2020) التي أظهرت وجود نقص في الوعي باستخدام المصادقة الثنائية وإدارة وتعقيد كلمات المرور للحسابات.

ويمكن تفسير النتائج التي أظهرت درجة عالية من الوعي بتطبيقات الأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود من خلال عدة عوامل. أولاً، يمكن أن يكون للبيئة الأكاديمية تأثير كبير على هذا الوعي، حيث إن الطالبات في هذه الدراسة ينتمين إلى مرحلة دراسات عليا، مما يعزز من تفاعلهن مع التكنولوجيا بشكل أكبر مقارنة بالمراحل الدراسية الأخرى، وهو ما قد يساعدهن في زيادة وعيهن بالمخاطر السيبرانية وطرق الحماية. ثانيًا، قد تكون الخبرات السابقة لهن مع الإنترنت قد ساهمت في اكتساب سلوكيات وقائية، مثل تجنب فتح الروابط المشبوهة أو نشر المعلومات الشخصية. بالإضافة إلى ذلك، قد يكون الطالبات قد تلقين تدريبات أو ورش عمل متعلقة بالأمن السيبراني من قبل الجامعة أو من خلال مصادر أخرى، مما عزز من معرفتهن بهذه المسائل. كما أن الوعي العام الذي أصبح سائدًا في المجتمع، من خلال وسائل الإعلام والبرامج التوعوية حول أهمية حماية البيانات الشخصية، قد يكون ساهم في زيادة وعيهن بهذه المواضيع. في ضوء هذه العوامل، يمكن أن يكون هذا الوعي الملاحظ نتيجة لتفاعل الطالبات مع التكنولوجيا بشكل مستمر ووجود بيئة تعليمية تدعم هذا الوعي.

تشير هذه النتائج من وجهة نظر الباحثات إلى أن وعي طالبات الدراسات العليا بتطبيقات الأمن السيبراني لا يأتي فقط من التعرض المباشر للمخاطر، بل يتشكل نتيجة تفاعل متكامل بين التعليم الأكاديمي، والتوعية المجتمعية، والتجارب الشخصية. وقد حرصت الباحثات على استكشاف هذا التفاعل من خلال ربط سلوكيات الطالبات بالمتغيرات البيئية والتقنية التي تؤثر على إدراكهن للمخاطر السيبرانية. ويدل هذا التحليل على أهمية استمرار الجهود التوعوية التي تستهدف هذه الفئة، حيث إن تعزيز الأمن السيبراني لا يقتصر على المعرفة النظرية فقط، بل يتطلب بناء ثقافة رقمية مسؤولة تدمج بين المعرفة والممارسة الفعلية.

وعند مقارنة هذه النتائج بالدراسات السابقة، يمكن ملاحظة أن النتائج تتوافق مع دراسة الحبيب (2022)، التي أظهرت أيضًا أن طلاب الدراسات العليا لديهم مستوى عالٍ من الوعي بتطبيقات الأمن السيبراني. وفي المقابل، تختلف هذه النتائج مع دراسة القحطاني (2022) التي أشارت إلى وجود ضعف في الوعي، خاصة في مجالات مثل أمان كلمات المرور وأمان المتصفح، وهو ما قد يعود إلى اختلاف البيئة الأكاديمية أو الفئة المستهدفة في تلك الدراسة. كما أن نتائج الدراسة تختلف مع دراسات أخرى مثل دراسة المعلم (2019) ودراسة جبرة وآخرون (2020)، التي أظهرت نقصًا في الوعي باستخدام المصادقة الثنائية أو إدارة كلمات المرور، مما يعكس اختلاف الظروف التعليمية أو التوعوية بين العينات المختلفةFormularende.

4-3-الإجابة عن السؤال الثالث: "ما أبرزسبل تعزيز الوعي بالأمن السيبر اني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود من وجهة نظرهن؟"

للإجابة عن هذا السؤال تم حساب التكرارات، والنسب المئوية والمتوسطات الحسابية، والانحرافات المعيارية، والرتب، لاستجابات أفراد الدراسة من طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود على محور " سبل تعزيز الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود، وجاءت نتائج الاستجابات كما يبينها الجدول (11).

جدول (11): سبل تعزيز الوعي بالأمن السيبر اني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود

م	العبارة	المتوسط	الانحراف	الرتبة	درجة الأهمية
1	الشراء عبر الإنترنت من مو اقع موثوقة.	4.66	0.63	1	مهم جداً
3	تجنب وضع البيانات والصور الشخصية على مو اقع التواصل الاجتماعي إلا لضرورة.	4.59	0.67	2	مهم جداً
4	تقديم دورات تدريبية لطلاب وطالبات الدراسات العليا بكلية التربية عن الأمن السيبر اني بشكل دوري.	4.55	0.58	3	مهم جداً
2	استخدام حسابات المصارف والفيزا ووسائل الدفع الأخرى في المو اقع الموثوق فيها.	4.51	0.67	4	مهم جداً
5	إنشاء كلية التربية لبرنامج "الدبلوم العالي في الأمن السيبر اني.	4.49	0.69	5	مهم جداً
6	قيام كلية التربية بتوصيف مقررعن الأمن السيبر اني يقوم أعضاء هيئة التدريس بالكلية بتدريسه للطلاب والطالبات.	4.37	0.78	6	مهم جداً
7	حضور دورات في الأمن السيبر اني بشكل دوري.	4.32	0.71	7	مهم جداً
8	القراءة الدورية عن مشكلات الأمن السيبر اني.	4.32	0.71	8	مهم جداً
	المتوسط الحسابي العام	4.48	0.44	مهم جداً	

يتبين من النتائج الموضحة في الجدول (11) أن هناك تقارب في درجة موافقة أفراد الدراسة من طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود على عبارات محور (سبل تعزيز الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود) حيث يشمل المحور (8) عبارات، وجاءت استجابات أفراد الدراسة على جميع عبارات المحور بدرجة (مهم جداً) على أداة الدراسة، حيث تراوحت متوسطاتهم الحسابية من (4.32 إلى 4.66) وهذه المتوسطات تقع بالفئة الخامسة (4,21 إلى 5.0)من فئات المقياس الخماسي، والتي تشير الى درجة (مهم جداً). وعند ترتيب العبارات ومتوسطها الحسابي على التوالي من المتوسط الأكبر إلى المتوسط الأقل تكون كما يلي: الشراء عبر الإنترنت من مواقع (4.66)، تجنب وضع البيانات والصور الشخصية على مواقع التواصل الاجتماعي إلا لضرورة (4.59)، تقديم دورات تدريبية لطلاب وطالبات الدراسات العليا بكلية التربية عن الأمن السيبراني بشكل دوري (4.55)، استخدام حسابات المصارف والفيزا ووسائل الدفع الأخرى في المواقع الموثوق فيها (4.51)، إنشاء كلية التربية لبرنامج "الدبلوم العالي في الأمن

السيبراني " (4.49)، قيام كلية التربية بتوصيف مقرر عن الأمن السيبراني يقوم أعضاء هيئة التدريس بالكلية بتدريسه للطلاب والطالبات (4.37)، حضور دورات في الأمن السيبراني بشكل دوري (4.32)، القراءة الدورية عن مشكلات الأمن السيبراني (4.32).

وأظهرت النتائج أن المتوسط العام لاستجابة أفراد الدراسة من طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود نحو محور " سبل تعزيز الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود" جاءت بدرجة موافقة (مهم جداً) حيث بلغ المتوسط الحسابي (4.48)، وقد اتضح أن أبرز سبل تعزيز الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود تتمثل (الشراء عبر الإنترنت من مواقع موثوقة، تجنب وضع البيانات والصور الشخصية على مواقع التواصل الاجتماعي إلا لضرورة، تقديم دورات تدريبية لطلاب وطالبات الدراسات العليا بكلية التربية عن الأمن السيبراني بشكل دوري، استخدام حسابات المصارف والفيزا ووسائل الدفع الأخرى في المواقع الموثوق فيها، إنشاء كلية التربية لبرنامج "الدبلوم العالي في الأمن السيبراني... إلخ). وتتفق هذه النتائج مع دراسة كلا من دراسة الجهني وآخرون (Aljohni et al., 2021)، الحبيب (2022) والتي توصلت إلى أن طلاب الدراسات العليا موافقون للسبل المقترحة لتعزيز هذا الوعي.

كما يمكن تفسير النتائج التي أظهرت أبرز سبل تعزيز الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود من خلال مجموعة من العوامل التي تعكس وعي الطالبات وحاجتهن إلى حماية أنفسهن من المخاطر السيبرانية. أوضحت النتائج أن الطالبات يوافقن بشدة على عدة سبل لتعزيز الوعي، مثل الشراء عبر الإنترنت من مواقع موثوقة، تجنب وضع البيانات والصور الشخصية على مواقع التواصل الاجتماعي إلا لضرورة، وتقديم دورات تدريبية لطلاب وطالبات الدراسات العليا في مجال الأمن السيبراني بشكل دوري. هذه النتائج تشير إلى أن الطالبات يدركن أهمية الأمن السيبراني في حياتهن اليومية، ويشعرن بالحاجة إلى تعزيز هذا الوعي من خلال التعليم المستمر والتمكين المهني.

وعليه يعد اهتمام الطالبات بتعزيز الوعي بالأمن السيبراني من خلال وسائل مثل الدورات التدريبية وحضور ورش العمل المتعلقة بالأمن السيبراني خطوة مهمة نحو تزويدهن بالمعرفة والمهارات الضرورية لحماية بياناتهن الشخصية والعملية. ويعكس التأييد الكبير لفكرة "الشراء من مواقع موثوقة" و"استخدام حسابات المصارف والفيزا في المواقع الموثوق فيها" مستوى عالٍ من الإدراك للمخاطر المالية عبر الإنترنت، مما يشير إلى أن الطالبات يبدين حذرًا كبيرًا فيما يتعلق بالتعامل مع المعلومات المالية.

كما ترى الباحثات في سياق النتائج الواردة وتفسيرها يوضح أن الطالبات ليس فقط يوافقن على سبل تعزيز هذا الوعي، بل يقدّرن أهمية التعليم والتدريب المستمر في حماية بياناتهن الشخصية والمهنية. وهذا يؤكد على أهمية التعليم المستمر يعكس رأهمية توفير بيئة أكاديمية آمنة تتيح للطالبات التعامل مع المخاطر السيبرانية بثقة ومعرفة.

كما عند مقارنة هذه النتائج بالدراسات السابقة، نجد أن هذه النتائج تتفق مع دراسة الجهني وآخرون (2021) والحبيب (2022)، حيث أظهرت تلك الدراسات أن الطلاب في مرحلة الدراسات العليا يتفقون مع سبل تعزيز الوعي بالأمن السيبراني، مثل تقديم الدورات التدريبية المتخصصة. وهذا يتماشى مع النتائج الحالية التي تؤكد على أهمية تقديم برامج تعليمية مستمرة لتحسين الوعي بالأمن السيبراني. من ناحية أخرى، قد تكون هذه النتائج أكثر توافقًا مع الدراسات التي توصي بتطوير برامج تدريبية ودورات دراسية مختصة بالأمن السيبراني للطلاب بشكل دوري، مما يعكس اتجاهًا موحدًا في الدراسات الحديثة حول أهمية تزويد الطلاب بالمعرفة اللازمة لحماية أنفسهم من التهديدات السيبرانية.

4-4-ملخص النتائج

أجريت هذه الدراسة على طالبات الدراسات العليا في قسم المناهج بكلية التربية في جامعة الملك سعود، ويتضح من النتائج المتعلقة بالبيانات الأولية لأفراد الدراسة، أن (52.1%) من إجمالي أفراد الدراسة من الطالبات درجاتهن العلمية (ماجستير)، بينما اتضح أن (47.9 %) من إجمالي أفراد الدراسة من الطالبات درجاتهن العلمية (دكتوراه)، كما أن غالبية عينة الدراسة لم يحصلن على دورات في الأمن السيبراني، وذلك بنسبة بلغت (70.4%)، أما (29.6%) من إجمالي عينة الدراسة حصلن على دورات في الأمن السيبراني.

وقد أظهرت نتائج الدراسة أن طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود لديهم درجة وعى عالية بالأمن السيبراني، وأن المتوسط العام لاستجابة أفراد الدراسة نحو محور" درجة الوعي بمفاهيم الأمن السيبراني "، جاءت بدرجة موافقة (عالية) حيث بلغ المتوسط الحسابي (3.84) وهذا يدل على أن طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود لديهن وعي بدرجة عالية فيما يتعلق بمفاهيم الأمن السيبراني. بينما ظهرت بعض العبارات التي لم تصل إلى (عالية جداً)، وهي مرتبة على التوالي من المتوسط الأعلى إلى الأقل: أحتاج إلى دورات تدريبية في الأمن السيبراني (4.03)، لدي إلمام بمفهوم الأمن السيبراني (3.31)، لدي اطلاع واسع على جرائم الأمن السيبراني (3.06)، لدى معوقات شخصية تحول بيني وبين تحقيق الوقاية من مخاطر الأمن السيبراني (2,65).

كما اتضح من النتائج أن المتوسط العام لاستجابة أفراد الدراسة لمحور" درجة الوعي بتطبيقات الأمن السيبراني "، جاءت بدرجة موافقة (عالية) حيث بلغ المتوسط الحسابي(3.68)، وهذا يدل على أن طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود لديهن وعي بدرجة عالية فيما يتعلق بتطبيقات الأمن السيبراني، إلا أن هناك بعض العبارات لم تصل إلى (عالية جداً)، وهي مرتبة على التوالي من المتوسط الأعلى إلى الأقل: أتجنب إرسال معلوماتي الشخصية عبر الرسائل النصية أو البريد الإلكتروني (4,20)، أعي خطورة الاتصال بالشبكات في الأماكن العامة (4,14)، استخدام تقنية التحقق الثنائي باستخدام كلمات المرور والبصمة(3,92)، أُعطل خدمات الوصول لموقعي في التطبيقات المحملة على جهازي (3,58)،اهتم بتحديث جهازي بصفة مستمرة حفاظاً عليه(3,51)، أهتم بتحميل برامج آمنة لمكافحة الفيروسات(3,41)،أختار كلمة مرور قوية، وأهتم بتغييرها كل فترة(3,37)، أستطيع رفع بلاغ عن الإساءات التي قد أتعرض لها في مواقع التواصل الاجتماعي(3,35)، أقوم بإعداد نسخة احتياطية للبيانات المخزنة في جهازي على الخدمة السحابية(3,18)، أُغير إعدادات جهازي بشكل مستمر لكي لا تخترق شبكة Wi-Fi (2,56).

أما بالنسبة للنتائج المتعلقة بمحور " سبل تعزيز الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بقسم المناهج وطرق التدريس في جامعة الملك سعود"، فقد تبين أن المتوسط العام لاستجابة أفراد الدراسة جاءت بدرجة موافقة (مهم جداً) حيث بلغ المتوسط الحسابي (4.48)، والذي يدل على موافقتهم بشدة على سبل تعزيز الوعي بالأمن السيبراني، ومن أبرز سبل تعزيز الوعي بالأمن السيبراني لدى عينة الدراسة، وهي مرتبة حسب الأكثر تكرار إلى الأقل:(الشراء عبر الإنترنت من مواقع موثوقة، تجنب وضع البيانات والصور الشخصية على مواقع التواصل الاجتماعي إلا لضرورة، تقديم دورات تدريبية لطلاب وطالبات الدراسات العليا بكلية التربية عن الأمن السيبراني بشكل دوري، استخدام حسابات المصارف والفيزا ووسائل الدفع الأخرى في المواقع الموثوق فيها، إنشاء كلية التربية لبرنامج الدبلوم العالي في الأمن السيبراني، قيام كلية التربية بتوصيف مقرر عن الأمن السيبراني يقوم أعضاء هيئة التدريس بالكلية بتدريسه للطلاب والطالبات، حضور دورات في الأمن السيبراني بشكل دوري، القراءة الدورية عن مشكلات الأمن السيبراني.

التوصيات والمقترحات

في ضوء النتائج التي توصلت اليها الدراسة، توصي الباحثات ويقترحن ما يلي:

1- ضرورة تعزيز الوعي لدى الطلاب من خلال التنشئة الاجتماعية، وحملات تثقيفية متعلقة بالأمن السيبراني.
2- ضرورة تعزيز المناهج الدراسية بموضوعات تتعلق بمجال الأمن السيبراني.
3- تنظيم دورات تدريبية منتظمة حول الأمن السيبراني في كل فصل دراسي لتعزيز الوعي بالمخاطر السيبرانية.
4- نشر ثقافة الأمن السيبراني بين طلبة قسم المناهج وطرق التدريس في جامعة الملك سعود.
5- إلزام طلبة قسم المناهج وطرق التدريس بحضور دورة تدريبية واحدة على الأقل في الأمن السيبراني خلال مسيرتهم الأكاديمية.
6- ضمان عدم ربط أجهزة الطلبة بأجهزة العرض في القاعات الدراسية إلا بعد التحقق من خلوها من الفيروسات والبرامج الضارة.
7- إعداد دليل رقمي إرشادي للطلبة يوضح كيفية استخدام البيئة الرقمية بشكل آمن، وتقديم الدعم التقني والفني اللازم.
8- المقترحات: ونظرا لوجود فجوة بحثية في الموضوع؛ تقترح الباحثات إجراء الدراسات المستقبلية الآتية:

1. إجراء دراسات مماثلة على طلبة جامعات سعودية أخرى لتوسيع نطاق النتائج والاستفادة منها.
2. إجراء دراسات مماثلة تعتمد على أدوات بحثية أخرى، مثل: المقابلات.
3. دراسة معوقات تحقيق الأمن السيبراني في الجامعات السعودية.
4. إجراء أبحاث حول متطلبات تحقيق الأمن السيبراني في الجامعات السعودية لتطوير استراتيجيات فعالة.

قائمة المراجع.

أولاً-المراجع بالعربية:

- إبراهيم، منال محمد. (2021). الوعي بجوانب الأمن السيبراني في التعليم عن بعد. *المجلة العلمية لجامعة الملك فيصل للعلوم الإدارية، 22*(2)، 307-299.
- إسماعيل، ناريمان. (2022). فاعلية مقرر إلكتروني في طرق تدريس العلوم قائم على الرحلات المعرفية عبر الويب على تنمية بعض مهارات التعلم الذاتي واليقظة العقلية لدى طلاب الشعب العلمية بكلية التربية .*مجلة جامعة الفيوم للعلوم التربوية والنفسية، 16* (1)، 624-721.
- جبور، منى الأشقر .(2015) .*السيبرانية هاجس العصر* .المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية.

- الحانوتي، تيسير. (2014). أمن المعلومات: هاجس العالم الرقمي. في *المؤتمر الدولي الأول، جمعية المكتبات والمعلومات الأردنية* (ص. 189-207). عمان، الأردن.
- الحبيب، ماجد. (2022). درجة وعي بالأمن السيبراني لدى طالب وطالبات الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية وسبل تعزيزه من وجهة نظرهم. *مجلة العلوم التربوية، 30*.
- الربيعة، صالح علي. (2017). *الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت*. الرياض: هيئة الاتصالات وتقنية المعلومات.
- 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*.
- الصائغ، نورة، عسران، عواطف، السواط، حمد، منصور، إيناس، &أبو عيشة، زاهدة. (2020). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. *مجلة كلية التربية، 36*(6)، 90-41.
- صائغ، وفاء حسن عبد الوهاب. (2018). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية. *المجلة العربية للعلوم الاجتماعية، 14* (3)، 18-70.
- الظويفري، مشاعل شيب. (2021). واقع الأمن السيبراني وزيادة فاعليته في التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية. *المجلة الدولية للدراسات التربوية والنفسية، 10* (3)، 635-655.
- عباس، محمد خليل، نوفل، محمد بكر، العبسي، محمد مصطفى، &أبو عواد، فريال محمد. (2020). *مدخل إلى مناهج البحث في التربية وعلم النفس*. دار المسيرة للنشر والتوزيع والطباعة.
- عبيد، مصطفى فؤاد. (2003). *مهارات البحث العلمي*. أكاديمية الدراسات العالمية.
- العفيفي، يوسف خليل. (2013). *الجرائم الإلكترونية في التشريع الفلسطيني* (رسالة ماجستير). كلية الشريعة والقانون، الجامعة الإسلامية، غزة، فلسطين.
- عويس، حسنية حسين عبد الرحمن، &والي، محمد فوزي رياض. (2021). المتطلبات التربوية لتدريس مقرر التفكير الحاسوبي في مناهج مرحلة التعليم الأساسي في كل من إنجلترا وفنلندا وإمكانية الإفادة منها في مصر لتنمية مهارات القرن الحادي والعشرين. *المجلة التربوية، 91*، 5051-5161.
- غيطاس، جمال محمد. (2007). *أمن المعلومات والأمن القومي*. نهضة مصر للطباعة والنشر، القاهرة.
- القحطاني، نوره ناصر. (2019). مدى توافر الوعي بالأمن السيبراني لدي طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. *مجلة جمعية الاجتماعيين في الشارقة، 36*.(144)
- المقصودي، محمد احمد. (2017). *الأمن السيبراني والجهود الدولية لمكافحة الجرائم عابرة القارات*. جامعة نايف العربية للعلوم الأمنية، 37(427)، 7-102.
- المناعسة، أسامة أحمد، &الزعبي، جلال محمد. (1431هـ). *جرائم تقنية نظم المعلومات الإلكترونية: دراسة مقارنة*. دار الثقافة، الأردن.
- المنتشري، فاطمة، &حريري، رندة. (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للتربية النوعية*.
- هيئة الإعلام. (2021). الأمن السيبراني. قسم الدراسات والاتصال والعلاقات العامة. https://2u.pw/htAedOdN. تاريخ الاسترجاع: 20 أكتوبر 2024.
- الهيئة الوطنية للأمن السيبراني. (2018). الضوابط الأساسية للأمن السيبرانيhttps://nca.gov.sa ..

ثانياً-المراجع بالإنجليزية:

- Alarifi, A., Tootell, H., & Hyland, P. (2012). Information security awareness in Saudi Arabia. *Proceedings of the CONF-IRM*, Vienna, Austria, 21–23 May 2012, 57, 1–11.
- Aldawood, H., & Skinner, G. (2019). Reviewing cybersecurity social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet, 11*(3), 73. https://doi.org/10.3390/fi11030073
- Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(23). https://doi.org/10.3390/bdcc5020023
- Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cybersecurity awareness in educational environments in the Middle East. *Information and Knowledge Management, 15*, 1650007. https://doi.org/10.1142/S0219649216500076

- Aljohni, W., Elfadil, N., Jarajreh, M., & Gasmelsied, M. (2021). Cybersecurity awareness level: The case of Saudi Arabia university students. *International Journal of Advanced Computer Science and Applications, 12*(3), 47–53. https://doi.org/10.14569/IJACSA.2021.0120307
- Alqahtani, M. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences, 12*(1), 123. https://doi.org/10.3390/app12010123
- Altamimi, A., Azzeh, M., & Mahmood, B. (2022). Adopting the cybersecurity concepts into curriculum: The potential effects on students' cybersecurity knowledge. *Indonesian Journal of Electrical Engineering and Computer Science, 25*, 1451–1461. https://doi.org/10.11591/ijeecs.v25.i3.1451-1461
- Azzeh, M., Altamimi, A., Albashayreh, M., & Al-Oudat, M. (2022). Adopting the cybersecurity concepts into curriculum: The potential effects on students' cybersecurity knowledge. *Indonesian Journal of Electrical Engineering and Computer Science, 25*, 1462–1472. https://doi.org/10.11591/ijeecs.v25.i3.1462-1472
- Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *Emerging cyber threats & cognitive vulnerabilities* (pp. 73–92). Academic Press.
- Baruch, D. W., Wollenberg, J. M., & Kaplan, K. S. (2019). Cybersecurity compliance and the False Claims Act. *Journal of Internet Law, 23*(1), 3–8.
- Cisco. (2017). What is network security? Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-network-security.html
- Davis, D. (2018). Best practices for balancing technology use and safety in a modern school. In *Society for Information Technology & Teacher Education International Conference* (pp. 1026–1030). Washington, DC: Association for the Advancement of Computing in Education (AACE).
- Emm, D. (2021). Gamification—Can it be applied to security awareness training? *Network Security, 4*, 16–18. https://doi.org/10.1016/j.netse.2021.03.002
- Florea, A. M., & Radu, S. (2019). Artificial intelligence and education. In *22nd International Conference on Control Systems and Computer Science (CSCS)* (pp. 1–6). IEEE. https://doi.org/10.1109/CSCS.2019.00069
- Gabra, A., Sirat, M., Hajar, S., & Dauda, I. (2020). Cybersecurity awareness among university students: A case study. *International Journal of Advanced Science and Technology, 29*(10), 2297–2312.
- Hasweh, R., & Al-Qudah, M. H. (2023). The role of secondary school teachers in developing cybersecurity awareness among students from the perspective of teachers in private schools in Amman. *Dirasat: Educational Sciences, 50*(3), 61–75. https://doi.org/10.35516/edu.v50i3.222
- Hodhod, R., Khan, S., & Shuangbao, W. (2019). CyberMaster: An expert system to guide the development of cybersecurity curricula. *International Journal of Online Engineering, 15*(3), 70–81. https://doi.org/10.3991/ijoe.v15i03.9890
- Jabbour, M. (2016). Cyber obsession of the times. Lebanon: League of Arab States, Arab Centre for Legal and Judicial Research.
- Jalali, M., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems, 28*(1), 66–82. https://doi.org/10.1016/j.jsis.2018.10.003
- Kamara, S., & Lauter, K. (2010). Cryptographic cloud storage. In *International Conference on Financial Cryptography and Data Security* (pp. 136–149). Springer. https://doi.org/10.1007/978-3-642-14411-9_10
- Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information, 12*(10), 323. https://doi.org/10.3390/info12100323
- Lee, K. G., Chong, C. W., & Ramayah, T. (2017). Website characteristics and web users' satisfaction in a higher learning institution. *International Journal of Management in Education, 11*(3), 266–283.
- Moallem, A. (2019). Cybersecurity awareness among college students. In *Advances in Intelligent Systems and Computing* (Vol. 782, pp. 79–87). Springer. https://doi.org/10.1007/978-3-319-97438-9_9

- Odemis, M., Yucel, C., & Koltuksuz, A. (2022). Detecting user behavior in cyber threat intelligence: Development of Honeypsy system. *Security & Communication Networks*. https://doi.org/10.1155/2022/4979842
- Rahim, N. H. A., Hamid, S., & Kiah, L. M. (2019). Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An assessment. *Malaysian Journal of Computer Science, 32*(3), 221–245. https://doi.org/10.22452/mjcs.vol32no3.4
- Raineri, E. M., & Resig, J. (2020). Evaluating self-efficacy pertaining to cybersecurity for small businesses. *Journal of Applied Business & Economics, 22*(12), 74–85.
- Richardson, M., Lemoine, P., Stephens, W., & Waller, R. (2020). Planning for cybersecurity in schools: The human factor. *Educational Planning, 2*(2), 23–39.
- Schuesster, J. H. (2013). Contemporary threats and countermeasures. *Journal of Information Privacy & Security, 9*(2), 3–20.
- Seigfried-Spellar, K. C., Flores, B. M., & Griffin, D. J. (2015). Explanatory case study of the Arthur Pendragon cyber threat: Socio-psychological & communication perspectives. In *International Conference on Digital Forensics & Cyber Crime* (pp. 143–175).
- Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cybersecurity awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering, 263*(4), 1–10. https://doi.org/10.1088/1757-899X/263/4/042038
- Shaw, L. M., Vanderstichele, H., Knapik-Czajka, M., Clark, C. M., Aisen, P. S., Petersen, R. C.,... & Alzheimer's Disease Neuroimaging Initiative. (2009). Cerebrospinal fluid biomarker signature in Alzheimer's disease neuroimaging initiative subjects. *Annals of Neurology, 65*(4), 403–413. https://doi.org/10.1002/ana.21600
- Singh, S. (2023). Approaches, theories, and the role of ethics in computer science and engineering. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)* (pp. 1–8). IEEE. https://doi.org/10.1109/CSCE57857.2023.00006
- Tiwari, S., Bhalla, A., & Rawat, R. (2016). Cyber-crime and security. *International Journal of Advanced Research in Computer Science and Software Engineering, 6*(4), 46–52.
- Yumos, Z., Ab amid, R. S., & Almud, M. (2016). Development of a cybersecurity awareness strategy using focus group discussion. In *2016 SAI Computing Conference (SAT)* (pp. 1063–1067). IEEE. https://doi.org/10.5281/zenodo.1131053
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cybersecurity awareness, knowledge, and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2021.1897803