Digital security awareness levels among graduate students in the faculty of education in Latakia university

Hazem Shafek Trraf*
Dr. Mutieah Ahmad**
Dr. Khodor Ali***

(Received 4 / 3 / 2026 . Accepted 25 / 3 / 2026)

□ ABSTRACT □

This research aims to determine the level of digital security awareness among graduate students at the Faculty of Education, University of Lattakia, amid rapid digital transformation. A questionnaire was developed comprising three dimensions: knowledge of digital concepts and threats, preventive behaviors, and awareness of educational and ethical responsibility.

The study adopted a descriptive methodology. The instrument's validity and reliability were verified and administered to 105 graduate students. Results revealed high digital awareness levels, with educational and ethical responsibility ranking first, followed by ethical behaviors and practices second, and knowledge of digital concepts and threats third. Findings indicated significant differences attributed to specialization, but no significant differences related to degree level (master's/doctoral) or exposure to digital security incidents.

In light of the research findings, the researcher recommends:

- dedicating an independent module for humanities students on participants' data protection.
- tasking the educational technology department with developing training materials including practical phishing examples and fraudulent link identification.
- conducting quasi-experimental studies to measure the effectiveness of a short awareness program across the three survey dimensions.

Keywords: Digital security - graduate students – faculty of education.

Copyright **:**Latakia University journal (formerly tishreen) -Syria, The authors retain the copyright under a CC BY-NC-SA 04

* **PhD student, Faculty of Education, Department of Curricula and Teaching Methods, Latakia University, syria, Email: hazem.taraf@latakia-univ.edu.sy.**

** **Professor, Department of Curricula and Teaching methods, Faculty of education, Latakia University, syria.**

*** **Professor, Department of Curricula and Teaching methods, Faculty of education, Latakia University, syria.**

مستوى الوعي بالأمن الرقمي لدى طلبة الدراسات العليا في كلية التربية بجامعة اللاذقية

حازم شفيق طراف *

د.مطيعة أحمد**

د.خضر علي***

(تاريخ الإيداع 4 / 3 / 2026. قُبِل للنشر في 25 / 3 / 2026)

□ ملخّص □

هدف البحث إلى تحديد مستوى الوعي بالأمن الرقمي لدى طلبة الدراسات العليا في كلية التربية بجامعة اللاذقية في ظل التحول الرقمي المتسارع الذي يشهده العالم وذلك من خلال بناء استبانة مكونة من ثلاثة محاور: أولاً: المعرفة بالمفاهيم والتهديدات الرقمية، ثانياً: السلوكيات الوقائية، ثالثاً: الوعي بالمسؤولية التربوية والأخلاقية.

اعتمد البحث المنهج الوصفي، جرى التأكد من صدق وثبات الأداة، وتم تطبيقها على عينة مكونة من 105 طالباً وطالبة من طلبة الدراسات العليا. أظهرت النتائج أن مستوى الوعي الرقمي لدى طلبة الدراسات كان مرتفعاً، حيث كان بالمرتبة الأولى محور المسؤولية التربوية والأخلاقية، وفي المرتبة الثانية محور السلوكيات والممارسات الأخلاقية، وفي المرتبة الثالثة محور المعرفة بالمفاهيم والتهديدات الرقمية، كما بينت النتائج وجود فروق دالة تُعزى للاختصاص، وعدم وجود فرق جوهري يعزى للمرحلة (ماجستير/دكتوراه) أو للتعرض لحوادث أمنية رقمية.

يقترح الباحث في ضوء نتائج البحث:

- تخصيص وحدة مستقلة لطلاب التخصصات الإنسانية حول حماية بيانات المبحوثين في الأبحاث التربوية والنفسية.
- تكليف قسم تقنيات التعليم في الكلية بتصميم مواد تدريبية تتضمن أمثلة واقعية على رسائل التصيد الإلكتروني وأساليب التعرف على الروابط الاحتيالية الشائعة.
- تنفيذ دراسات شبه تجريبية لقياس فاعلية برنامج توعوي قصير على محاور الاستبانة الثلاثة.

الكلمات المفتاحية: الأمن الرقمي– طلبة الدراسات العليا – كلية التربية.

حقوق النشر : مجلة جامعة اللاذقية (تشرين سابقاً)– سوريا، يحتفظ المؤلفون بحقوق النشر بموجب الترخيص CC BY-NC-SA 04

* **طالب دراسات عليا (دكتوراه)، قسم المناهج وطرائق التدريس، كلية التربية، جامعة اللاذقية، سوريا.**
hazem.taraf@latakia-univ.edu.sy.

** **أستاذ ، قسم المناهج وطرائق التدريس، كلية التربية، جامعة اللاذقية، سوريا .**

*** **أستاذ ، قسم المناهج وطرائق التدريس، كلية التربية، جامعة اللاذقية، سوريا .**

مقدمة

استراتيجية التحول الرقمي هي الخطة الشاملة التي تضعها المؤسسة لتحقيق تحولها بشكل استراتيجي نحو استخدام التكنولوجيا والرقمنة بشكل استراتيجي حيث أصبح الاعتماد على البيئة الرقمية في التعليم العالي والبحث العلمي واقعًا يوميًا يتداخل مع جميع مراحل إنتاج المعرفة: من الوصول إلى قواعد البيانات، وتبادل الملفات، وإدارة الأدوات الإحصائية، وصولًا إلى استخدام المنصات السحابية وخدمات المراسلة الأكاديمية. هذا التحول رفع كفاءة العمل البحثي، لكنه في المقابل زاد من تعرض الباحثين لمخاطر رقمية متنوعة تمس سرية البيانات وسلامتها وتوافرها، وتنعكس آثارها على جودة البحث ومصداقيته وحقوق المشاركين فيه. وتؤكد الأدبيات التربوية أن الوعي بالأمن الرقمي لم يعد مهارة تقنية هامشية، بل أصبح جزءًا من الكفايات البحثية والأخلاقية التي ينبغي توافرها لدى طلبة الدراسات العليا الذين يتعاملون مع بيانات حساسة وأدوات رقمية متعددة في سياقات تعليمية وبحثية متغيرة، حيث يشير مصطلح الأمن الرقمي إلى كل الطرق المختلفة والمتعددة التي تكون غايتها هي حماية حسابات الإنترنت المتعلقة في الحاسب الألي وحماية الملفات من التسلل أو التدخل من قبل مستخدمين خارجيين أخرين . فهو مجموعة من الممارسات ، الأدوات، والتقنيات،(ككلمات المرور، التشفير، برامج مكافحة الفيروسات.....).

حيث تُظهر الدراسات العربية والأجنبية أن الوعي الأمني يتكون عادةً من مكونات معرفية وسلوكية وقيمية: معرفة المفاهيم والتهديدات الرقمية، وترجمة هذه المعرفة إلى ممارسات وقائية قابلة للتطبيق، ثم استيعاب البعد المسؤول تربويًا وأخلاقيًا في التعامل مع البيانات والمصادر الرقمية والأدوات الحديثة. ففي سياق الجامعات العربية مثلًا، توصلت دراسة عداد إلى رصد مستوى الوعي بالأمن السيبراني لدى عينة من طلبة جامعة حماة، وأبرزت أهمية التنظيم المعرفي للتهديدات وتحويله إلى سلوكيات داخل البيئة الجامعية [3,pp160]. وفي سياق ليبي، ناقشت دراسة الفقهي مدى توافر الوعي بالأمن السيبراني لدى طلبة قسم الحاسوب بكليات التربية بجامعة طرابلس، بما يعكس اهتمامًا بحثيًا متزايدًا بفئات الطلبة المرتبطة بالتربية والتكنولوجيا في آن واحد [4,pp77].

قدمت دراسة الطيب والوهبي والمقرن مؤشرًا على ارتفاع وعي طالبات الدراسات العليا بالأمن السيبراني في جامعة الملك سعود، وربطت ذلك بالحاجة إلى برامج تدريبية جامعية منظمة[2,pp1]. كما تشير أعمال في بيئات جامعية آسيوية إلى أن التدريب والانتظام في التعلم المنظم يرتبطان عادة بتحسن الوعي وإجراءات الحماية الرقمية لدى الطلبة الجامعيين [6,pp747]. وضمن مسار منهجي مكمل، اهتمت بحوث حديثة بإعادة فحص صلاحية مقاييس الوعي الأمني للتحقق من دقة قياسه لدى فئة طلبة التعليم ما بعد الثانوي، بما يؤكد أن قياس الوعي يحتاج أدوات متينة ومناسبة للسياق [5,pp149]، وعلى المستوى المحلي أكدت دراسة ضعضع التي أجريت عام 2024 في سوريا على تطوير نماذج تدريبية لزيادة الوعي بالحرب السيبرانية لدى طلاب التعليم العالي[1,pp99].

وتزداد أهمية هذا الموضوع في الدراسات العليا التربوية تحديدًا؛ لأن الباحث التربوي لا يتعامل مع بياناته بوصفها معلومات شخصية فحسب، بل يتعامل معها بوصفها أمانة علمية تتصل بحقوق المشاركين وبالنزاهة الأكاديمية وبالسلامة المنهجية.

مشكلة البحث:

على الرغم من تزايد الاهتمام بدراسة الوعي بالأمن الرقمي في الجامعات، فإن مراجعة الأدبيات تُظهر أن كثيرًا من الدراسات ركزت إما على قياس الوعي بصورة عامة لدى طلبة الجامعات أو لدى تخصصات تقنية محددة، أو

اتجهت إلى موضوعات قريبة مثل بناء مقاييس مرتبطة بالحرب السيبرانية [1,pp100]، أو دراسة الوعي لدى عينات جامعية في مدن/جامعات محددة داخل سورية [3,pp160]، أو داخل بيئات عربية أخرى [2, PP77 ,2,pp1]. وتبرز الحاجة إلى دراسة الوعي بالأمن الرقمي لدى طلبة الدراسات العليا في كليات التربية، نظرًا لما يجمع هذه الفئة من تقاطع بين متطلبات البحث العلمي ومقتضيات المسؤولية التربوية، فضلًا عن كونهم مرشحين لأداء أدوار بحثية وتدريسية تُسهم في نقل هذا الوعي إلى الميدان التربوي.

ومن خلال انخراط الباحث في البيئة الأكاديمية لكلية التربية بجامعة اللاذقية، رصد تصاعدًا ملحوظًا في توظيف طلبة الدراسات العليا للأدوات والمنصات الرقمية في سياقات البحث العلمي والتواصل الأكاديمي، مما أثار تساؤلًا بحثيًا محددًا حول المستوى الفعلي لوعيهم بالأمن الرقمي المرتبط بهذا التوظيف، وللتحقق من هذا التساؤل الأولي أجرى الباحث دراسة استطلاعية على عينة مؤلفة من (21) طالبًا وطالبة من طلبة الدراسات العليا في الكلية ذاتها لمعرفة مستوى الوعي بالأمن الرقمي لديهم، استخدم الباحث استبانة مؤلفة من (10) بنود تغطي جوانب أساسية من الوعي بالأمن الرقمي في السياق الأكاديمي، وفق مقياس ثلاثي المستويات: (دائماً – أحياناً – نادراً). وقد صُممت البنود لتعكس سلوكيات يومية مرتبطة بالأمن الرقمي في بيئة البحث العلمي والتواصل الأكاديمي(إدارة كلمات المرور، والوعي بالتصيد الإلكتروني، والنسخ الاحتياطي للبيانات، وإعدادات الخصوصية، وتحديث البرمجيات، وأمن الشبكات، والاستجابة للحوادث الأمنية، والمصادقة الثنائية، والوعي بمخاطر مشاركة البيانات، والتمييز بين المواقع الآمنة وغير الآمنة)، والملحق رقم(1) يوضح التكرارات والنسب المئوية ومستوى الوعي لكل بند من بنود الاستبانة الاستطلاعية.

كشفت نتائج الدراسة الاستطلاعية عن عدة مؤشرات يمكن إجمالها فيما يأتي:

1. جاء في المستوى المرتفع (أكثر من 50%): البند المتعلق باستخدام كلمات مرور قوية ومختلفة حيث أجاب (61.9%) من أفراد العينة بـ (دائماً)، والبند المتعلق بإدراك مخاطر مشاركة البيانات بنسبة (57.1%). ويُلاحظ أن هاذين البندين يرتبطان بسلوكيات أساسية يتعرض لها الطلبة بشكل يومي ومتكرر، مما يرفع مستوى ممارستهم لها.

2. جاء في المستوى المتوسط (من 25% إلى 50%): البند المتعلق بالتحقق من مصداقية الروابط بنسبة (42.9%)، والبند المتعلق بالتمييز بين المواقع الآمنة وغير الآمنة بنسبة (38.1%)، والبند المتعلق بضبط إعدادات الخصوصية بنسبة (33.3%)، والبند المتعلق بالنسخ الاحتياطي بنسبة (28.6%). وتشير هذه النسب إلى أن أقل من نصف أفراد العينة يمارسون هذه السلوكيات بشكل دائم، في حين أن البقية يمارسونها أحياناً أو نادراً فقط، وهو ما يستدعي التحقق منه على مستوى المجتمع الأصلي.

3. جاء في المستوى المنخفض (أقل من 25%): البند المتعلق بتحديث البرمجيات بنسبة (23.8%)، والبند المتعلق بتجنب شبكات Fi–Wi العامة بنسبة (23.8%)، والبند المتعلق بمعرفة كيفية التصرف عند الاختراق بنسبة (19%)، والبند المتعلق باستخدام المصادقة الثنائية بنسبة (14.3%). وهذا يعني أن أقل من ربع أفراد العينة يمارسون هذه الإجراءات الأمنية بشكل دائم، وهي نسبة منخفضة تُثير القلق لا سيما أن بعض هذه الإجراءات (كالمصادقة الثنائية والاستجابة للاختراق) تُعدّ ضرورية لحماية البيانات البحثية والحسابات الأكاديمية.

4. نسبة من أجابوا بـ (نادراً) بلغت أعلى قيمها في البند المتعلق باستخدام المصادقة الثنائية بنسبة (57.1%) والبند المتعلق بمعرفة كيفية التصرف عند اختراق الحسابات الرقمية بنسبة (47.6%)، مما يعني أن أكثر

من نصف العينة لا يستخدم المصادقة الثنائية إلا نادراً، وأن ما يقارب نصفها لا يعرف كيف يتصرف عند تعرض حسابه الرقمي للاختراق إلا نادراً.

وعليه، فإن هذه المؤشرات تؤكد الحاجة الفعلية إلى إجراء البحث الحالي بوصفه استجابة منهجية لما كشفت عنه الدراسة الاستطلاعية من نتائج تستدعي التعمق والتوثيق العلمي الدقيق والتحليل الشامل على مستوى المجتمع الأصلي.

ويمكن صياغة مشكلة البحث بالسؤال الرئيس الآتي:

ما مستوى الوعي بالأمن الرقمي لدى طلبة الدراسات العليا في كلية التربية بجامعة اللاذقية؟

أهمية البحث:

تنطلق أهمية البحث من أن الأمن الرقمي لم يعد وظيفة تقنية مساندة، بل أصبح شرطًا مرتبطًا بسلامة إجراءات البحث العلمي وجودة بياناته وحقوق المشاركين فيه. وفي سياق كليات التربية، يتعزز هذا المعنى لأن الباحث التربوي يُنتظر منه أن يجمع بين الكفاية البحثية والمسؤولية المهنية والأخلاقية في التعامل مع البيانات والموارد الرقمية. وعليه تتجسد أهمية الدراسة في :

1- إثراء الأدبيات المتعلقة بالوعي بالأمن الرقمي لدى طلبة الدراسات العليا في كليات التربية ضمن سياق جامعي سوري، بما يدعم سد فجوة معرفية في الدراسات المتاحة.

2- قد تفيد نتائج البحث وزارة التعليم العالي والبحث العلمي في بناء صورة واقعية عن مستوى الوعي بالأمن الرقمي لدى طلبة الدراسات العليا، مما يمكّن صانعي القرار من تصميم سياسات وقائية هادفة تدعم حماية البيانات البحثية وتُقلّل من مخاطر فقدانها أو تسريبها أو الإخلال بسلامتها عبر الحسابات والملفات والشبكات والمنصات الرقمية.

3- فتح آفاق بحثية جديدة أمام الباحثين لاستقصاء أبعاد ومتغيرات أخرى ذات صلة بمنظومة الأمن الرقمي لم يتناولها البحث الحالي، بما يسهم في بناء تراكم معرفي شامل حول هذا الموضوع.

أهداف البحث:

يسعى البحث الحالي إلى:

- قياس مستوى الوعي بالأمن الرقمي لدى طلبة الدراسات العليا في كلية التربية بجامعة اللاذقية في ضوء أبعاده الثلاثة (المعرفة بالمفاهيم والتهديدات الرقمية، السلوكيات والممارسات الوقائية، الوعي بالمسؤولية التربوية والأخلاقية).

أسئلة البحث:

يتناول البحث السؤال الرئيسي الآتي:

ما مستوى الوعي بالأمن الرقمي لدى طلبة الدراسات العليا في كلية التربية بجامعة اللاذقية؟ ويتفرع عنه:

1. ما مستوى الوعي بالمفاهيم والتهديدات الرقمية لدى طلبة الدراسات العليا في كلية التربية (جامعة اللاذقية)؟
2. ما مستوى الوعي بالسلوكيات والممارسات الوقائية الرقمية لدى طلبة الدراسات العليا في كلية التربية (جامعة اللاذقية)؟
3. ما مستوى الوعي بالمسؤولية التربوية والأخلاقية الرقمية لدى طلبة الدراسات العليا في كلية التربية (جامعة اللاذقية)؟

فرضيات البحث:

اختبرت فرضيات البحث عند مستوى الدلالة (0.05):

- لا يوجد فرق ذو دلالة إحصائية بين متوسطي درجات طلبة الدراسات العليا في مستوى الوعي بالأمن الرقمي تبعًا لمتغير المرحلة الدراسية(ماجستير/ دكتوراة).
- لا توجد فروق ذات دلالة إحصائية بين متوسطات درجات طلبة الدراسات العليا على مقياس الوعي بالأمن الرقمي تبعًا لمتغير الأختصاص(رياض أطفال – تقنيات التعليم – طرائق التدريس – أصول التربية – ارشاد نفسي).
- لا يوجد فرق ذو دلالة إحصائية بين متوسطات درجات طلبة الدراسات العليا على مقياس الوعي بالأمن الرقمي تبعًا لمتغير التعرض لحوادث أمنية رقمية (تعرض لحوادث أمنية رقمية/ لم يتعرض لحوادث أمنية رقمية).

منهج البحث:

استخدم الباحث المنهج الوصفي، وهو منهج علمي يهدف إلى تصوير الظاهرة التعليمية كما هي في الواقع عبر جمع بيانات عنها ثم تنظيمها وتحليلها لتحديد ملامحها الأساسية وإبراز أنماطها واتجاهاتها ودرجة التباين داخلها. ويركّز هذا المنهج على تقديم إجابات دقيقة لأسئلة من نوع: من؟ ماذا؟ أين؟ متى؟ وإلى أي مدى؟ بما يوفّر قاعدة معرفية واضحة تساعد على فهم الظاهرة وتحديد احتياجاتها الفعلية، وقد يُستخدم كبحث مستقل عندما نحتاج إلى استكشاف ظواهر غير موثقة أو أنماط خفية في البيانات، كما يمكن أن يكمّل الدراسات التي تسعى لاحقًا لاختبار العلاقات أو تفسير الأسباب. [8,pp1].وقد اعتمد على هذا المنهج في جمع البيانات الإحصائية عن مستوى وعي طلبة الدراسات العليا بالأمن الرقمي من خلال استبانة وجهت إليهم، ومن ثم تحليل هذه البيانات، واستخلاص النتائج لتقديم المقترحات.

حدود البحث ومحدداته:

تم الاقتصار في البحث الحالي على الحدود الآتية:

- الحدود البشرية: عينة من طلبة الدراسات العليا في كلية التربية في جامعة اللاذقية.
- الحدود الزمانية: تم تطبيق الأستبانة في الفترة الممتدة من (20 كانون الأول 2025م) لغاية (8 كانون الثاني 2026م).
- الحدود المكانية: كلية التربية في جامعة اللاذقية.
- الحدود الموضوعية: تمثلت في تعرف مستوى الوعي بالأمن الرقمي لدى طلبة الدراسات العليا(ماجستير/دكتوراه).

المصطلحات والتعريفات الإجرائية:

1. الأمن الرقمي:

الأمن الرقمي هو منظومة من الضوابط والإجراءات التنظيمية والتقنية والسلوكية التي تهدف إلى حماية المعلومات والأنظمة والشبكات في البيئة الرقمية من الوصول غير المصرّح به أو سوء الاستخدام أو الكشف أو

التعطيل أو التغيير أو الإتلاف، بما يضمن تحقيق متطلبات الحماية الأساسية مثل السرية والسلامة والتوافر. [25,pp13].

التعريف الإجرائي للأمن الرقمي:

يُقصد بالأمن الرقمي إجرائيًا مجموعة من المفاهيم والسلوكيات المتعلقة بالمعرفة بالمفاهيم والتهديدات الرقمية والسلوكيات والممارسات الوقائية والوعي بالمسؤولية التربوية والأخلاقية التي تضمن تحقيق السلامة الرقمية.

الوعي بالأمن الرقمي:

الوعي بالأمن الرقمي هو مستوى إدراك الفرد للمخاطر والتهديدات الرقمية وفهمه لطرق الحماية الملائمة، مع قابلية ترجمة هذا الإدراك إلى سلوكيات عملية تقلل احتمال التعرض للحوادث في أثناء استخدام التقنيات والخدمات الرقمية. [3,pp160].

التعريف الإجرائي للوعي بالأمن الرقمي:

يُقاس الوعي بالأمن الرقمي إجرائيًا بالدرجة التي يحصل عليها طالب الدراسات العليا على الاستبانة المخصصة للدراسة، والتي تتكون من (25) بندًا وفق مقياس ليكرت الخماسي.

الأسس النظرية والدراسات السابقة للبحث:

1) الأمن الرقمي في التعليم العالي: من المخاطر التقنية إلى القرارات اليومية

تتسم مؤسسات التعليم العالي بكثافة استخدام الخدمات الرقمية في التعلم والبحث والإدارة (منصات تعليم، بريد جامعي، قواعد بيانات، تخزين سحابي، أنظمة هوية رقمية). ومع هذا الاتساع، لا تُفهم المخاطر الرقمية بوصفها "حوادث اختراق" منفصلة فقط، بل بوصفها نتيجة تفاعل بين بنية المؤسسة من جهة، وسلوك المستخدمين وقراراتهم المتكررة أثناء الاستخدام من جهة أخرى؛ لذلك يصبح الوعي بالأمن الرقمي عاملًا مفسِّرًا مهمًا في الوقاية داخل الجامعة.[12,pp151–11,pp1]. كما يبرز منظور "الأمن المتمركز حول الإنسان" الذي يؤكد أن تقليل المخاطر لا يعتمد على الأدوات والسياسات وحدها، بل على تصميم بيئة رقمية تدعم المستخدم وتراعي حدود الانتباه والضغط الزمني، بما يساعد على تثبيت السلوك الآمن في الممارسة الفعلية. [13,pp169].

2) الوعي بالأمن الرقمي في سياق تربوي

يتداخل الأمن الرقمي مع مجالات متقاربة تشمل حماية الأنظمة والشبكات، وأمن المعلومات (سرية/سلامة/توافر)، وحماية الخصوصية والبيانات الشخصية. وتزداد حساسية هذا المجال في الجامعة لأن البيانات لا تقتصر على حسابات فردية، بل تمتد إلى بيانات تعلم ومراسلات أكاديمية وملفات بحثية قد تكون حساسة أو محكومة بأخلاقيات البحث. [11,pp1].

أما الوعي بالأمن الرقمي فيُفهم على أنه بناء مركّب لا يقتصر على معرفة "القواعد"، بل يضم فهمًا لأسبابها وتقديرًا لأهميتها وقدرة على تحويلها إلى ممارسة، بحيث تتداخل المعرفة مع الاتجاهات والسلوك. [12,pp151, 14,pp40].

3) أبعاد الوعي بالأمن الرقمي

3.1 المعرفة بالمفاهيم والتهديدات الرقمية

تشير المعرفة الأمنية الرقمية إلى امتلاك مفاهيم أساسية تُعين الطالب على تفسير المواقف الرقمية وفهمها بصورة صحيحة، ومن أبرز هذه المفاهيم: المصادقة متعددة العوامل التي تضيف طبقات حماية إضافية تتجاوز كلمة المرور وحدها، وإدارة كلمات المرور التي تشمل معرفة كيفية إنشاء كلمات مرور قوية وفريدة لكل حساب وتجنب إعادة استخدامها عبر المنصات المختلفة. وتمتد هذه المفاهيم لتشمل التصيد الاحتيالي والهندسة الاجتماعية، وهي أساليب يلجأ إليها المهاجمون للتلاعب بالضحية نفسياً واستدراجها للكشف عن معلومات حساسة أو النقر على روابط ضارة، فضلاً عن برمجيات الفدية التي تُشفّر بيانات الضحية وتطالبها بدفع مبالغ مالية مقابل استعادتها، وخصوصية البيانات التي تعني إدراك الطالب لحقوقه الرقمية وآليات جمع بياناته واستخدامها من قِبل التطبيقات والمنصات، وأخيراً النسخ الاحتياطي بوصفه خط دفاع أخير يكفل استمرارية الوصول إلى البيانات في حال تعرضها للفقدان أو التلف. وتعمل هذه المعرفة كشرط تمهيدي للسلوك الوقائي، لأن الطالب الذي يفتقر إليها يكون عُرضةً لاتخاذ قرارات مبنية على سوء فهم أو تقدير خاطئ للمخاطر، كأن يظن أن كلمة مرور بسيطة كافية لتأمين حساباته، أو أن الروابط الواردة من جهات تبدو موثوقة لا تستدعي التحقق. وبعبارة أخرى، فإن المعرفة الأمنية لا تُكسب الطالب مهارات تقنية متقدمة بالضرورة، بل تمنحه القدرة على قراءة المشهد الرقمي بوعي نقدي يُمكّنه من التمييز بين الآمن والمشبوه قبل أن يقع الضرر.[12,pp151] .

ويزداد أهمية هذه المعرفة حين يُؤخذ بعين الاعتبار الطابع الخاص للبيئة الجامعية، إذ تقوم هذه البيئة على اعتماد مكثف على البريد الإلكتروني المؤسسي الذي كثيراً ما يُستهدف بحملات تصيد موجَّهة تنتحل صفة الجهات الأكاديمية الرسمية كالجامعة أو الأستاذ أو المكتبة. يُضاف إلى ذلك أن الطلاب يتبادلون الملفات والروابط بشكل يومي في سياق التعاون الأكاديمي، مما يُوسّع نطاق التهديد ويجعل اكتشافه أصعب، نظراً لأن المحتوى الضار قد يصل مُغلَّفاً في سياق طبيعي ومألوف كمشاركة ورقة بحثية أو تكليف دراسي. وهذا ما يجعل المعرفة الأمنية المطلوبة في هذا السياق ليست مجرد معرفة عامة، بل معرفةً سياقيةً مرتبطة تحديداً بنمط الاستخدام الأكاديمي وطبيعة التفاعل الرقمي داخل المؤسسة التعليمية، بحيث يستطيع الطالب التعرف على التهديدات التي تتبثق من داخل بيئته اليومية وليس فقط تلك القادمة من مصادر غريبة أو مجهولة.[11,pp1] .

3.2 السلوكيات والممارسات الوقائية

يمثل هذا البعد ترجمة المعرفة إلى إجراءات قابلة للرصد: كلمات مرور قوية، تفعيل المصادقة، التحقق من الروابط والمرفقات، التحديثات، حماية الأجهزة، ضبط الخصوصية، وتقييد مشاركة الملفات وفق الصلاحيات. وتدعم المقاييس المعيارية فكرة قياس الوعي عبر دمج المعرفة والاتجاه والسلوك في مجالات ممارسة متكررة، مثل HAIS-Q، وكذلك قياس نوايا السلوك الأمني عبر SeBIS [15,pp2873–14,pp40]. وتشير الأدبيات إلى أن امتلاك المعرفة لا يضمن تلقائيًا سلوكًا وقائيًا مرتفعًا؛ إذ قد تظهر فجوة بين الإدراك والتطبيق إذا غابت تقنيات تغيير السلوك أو كانت التوعية عامة وغير موجهة. [16,pp1].

3.3 الوعي بالمسؤولية التربوية والأخلاقية

في كلية التربية، لا يرتبط الأمن الرقمي بحماية الفرد فقط، بل يمتد إلى مسؤولية مهنية تجاه المتعلمين والمشاركين في البحث والزملاء، ويظهر ذلك في حماية بيانات المشاركين وسرية الوثائق، واحترام الخصوصية، والالتزام

بالنزاهة الأكاديمية الرقمية، واعتماد سلوك مهني على المنصات. ويُقرأ هذا البعد ضمن إطار المواطنة الرقمية بوصفها مفهومًا يدمج الحقوق والواجبات والأخلاق والمشاركة في الفضاء الرقمي. [18,pp100–17,pp565].

4) الأسس النظرية المفسِّرة للوعي والسلوك الأمني

4.1 نموذج المعرفة–الاتجاه–السلوك

يساعد هذا النموذج على فهم الوعي الأمني بوصفه علاقة بين ما يعرفه الفرد وما يتبناه من تقييمات ومعايير، وما يقوم به فعليًا. وتظهر أهمية هذا الإطار عند بناء أدوات تقيس الوعي بوصفه بنية متعددة المكونات لا مجرد معرفة نظرية. [12,pp151,14,pp40].

4.2 نظرية السلوك المخطط والدافعية للحماية

تفسر نظرية السلوك المخطط السلوك المتعمد عبر اتجاهات الفرد، والمعايير الاجتماعية، والتحكم السلوكي المدرك، وهو ما يفسر اختلاف الالتزام بالممارسات الوقائية داخل البيئة الجامعية تبعًا لثقافة المؤسسة وتوقعات المحيط وسهولة التطبيق. [19,pp179].

أما نظرية الدافعية للحماية فتركز على تقييم التهديد (الشدة/القابلية) وتقييم المواجهة (فاعلية الاستجابة/الكفاءة الذاتية/تكلفة الاستجابة)، وهي مفيدة لتفسير لماذا يتبنى بعض الطلبة ممارسات وقائية بينما يتردد آخرون رغم إدراكهم للمخاطر. [20,pp93].

وقد دعمت أعمال بحثية دمج هذين الإطارين في تفسير الامتثال لسياسات أمن المعلومات في السياقات المؤسسية. [21,pp83].

4.3 نموذج المعتقدات الصحية وتفسير الاستجابات للتهديدات

ينظر نموذج المعتقدات الصحية إلى السلوك الوقائي بوصفه نتاج إدراك الشدة والقابلية والفوائد والعوائق وإشارات الفعل والكفاءة الذاتية. وقد طُبق هذا المنطق لتفسير سلوكيات أمن الحاسوب، كما استخدم في تفسير سلوك الطلبة تجاه التصيد بالبريد الإلكتروني باعتباره تهديدًا شائعًا في البيئات التعليمية. [22,pp815–23,pp1]. وتشير دراسات مناشدات الخوف إلى أن الرسائل التي ترفع إدراك التهديد تكون أكثر فاعلية عندما تُقرن بمسار واضح يعزز الفاعلية والكفاءة الذاتية بدل الاقتصار على التخويف. [24,pp549].

5) سياق التعليم العالي بوصفه إطارًا لتشكل المخاطر والوعي

يتكون سياق التعليم العالي من تداخل أنظمة رسمية وأجهزة شخصية وتطبيقات طرف ثالث وشبكات عامة وتعاون بحثي يتطلب مشاركة ملفات ومصادر. وقد بينت مراجعات المخاطر في التعليم العالي أن هذا التنوع يزيد احتمالات التعرض لحوادث مثل اختراق الحسابات وتسريب البيانات والبرمجيات الخبيثة، ما يجعل الوعي جزءًا من الحوكمة الرقمية اليومية داخل الجامعة. [11,pp160]. كما توفر وثائق معيارية حديثة إطارًا عامًا يمكن الاستناد إليه لفهم الأمن الرقمي بوصفه نتائج ومخرجات قابلة للتطبيق مؤسسيًا، ويُسهم ذلك في ربط تعلم الأمن الرقمي بالسياسات والأدوار داخل المؤسسة. [10,pp7, 25,pp1].

الدراسات السابقة:

- دراسة Chintakovid التي أجريت عام 2023[6] (الصين)، هدفت الدراسة إلى استقصاء مستوى الوعي بالأمن السيبراني لدى طلبة البكالوريوس وتحليل مكونات مثل المعرفة وإدارة كلمات المرور والخصوصية والثقة/إدراك المخاطر، وكذلك أثر التعلم الرسمي وغير الرسمي، وقد استخدمت منهجًا وصفيًا مسحيًا، وتألفت العينة من (384) مشاركًا (184 ذكرًا و200 أنثى)، وقد أظهرت النتائج انخفاضًا نسبيًا في الوعي العام مع تفاوت بين المحاور، حيث ارتفعت المعرفة والخصوصية عبر الإنترنت مقارنةً بضعف إدارة كلمات المرور، كما أشارت النتائج إلى علاقة بين التعلم الرسمي ومستوى الوعي بالأمن السيبراني.
- دراسة GOLIATH التي أجريت عام 2024[26] (جنوب أفريقيا)، هدفت الدراسة إلى تقييم اتجاهات الطلبة وسلوكياتهم المرتبطة بالأمن السيبراني ومقارنة طلبة البكالوريوس (UG) بطلبة الدراسات العليا (PG) للكشف عن "فجوة مرونة" بين المعرفة/الاتجاهات والسلوك الفعلي وتحديد مجالات التدخل، وقد اعتمدت منهجًا كميًا مقطعيًا قائمًا على نظرية السلوك المخطط (TPB) مع استخدام أداة Q–HAIS بعد تعديلها، وبلغت العينة النهائية (266) طالبًا وطالبة بعد تنظيف البيانات، وقد أظهرت النتائج تفوق طلبة الدراسات العليا على طلبة البكالوريوس في بعض المجالات (خصوصًا كلمات المرور والبريد الإلكتروني) مع فروق دالة في عدد من المتغيرات، وأكدت وجود فجوة تستدعي تدخلات توعوية وتدريبًا عمليًا مبكرًا لطلبة البكالوريوس.
- دراسة ضعضع التي أجريت عام 2024[1] في سورية، هدفت الدراسة إلى بناء مقياس لقياس مستوى الوعي بالحرب السيبرانية لدى طلبة الجامعة والتحقق من خصائصه السيكومترية، وقد استخدمت المنهج الوصفي المسحي مع إجراءات بناء وتقنين المقياس، وكانت أداة الدراسة مقياسًا متعدد الأبعاد شمل مجالات مثل معرفة المخاطر السيبرانية واستراتيجيات الحماية وفهم المسؤوليات والوعي بالأدوات والاستجابة للطوارئ، وتألفت عينة الدراسة من (176) طالبًا وطالبة من جامعة حلب، وقد أظهرت النتائج ارتفاع مستوى الوعي العام بالحرب السيبرانية وأبعادها (وزن نسبي 80.04%)، ووجود فروق دالة حسب الجنس لصالح الذكور في معظم الأبعاد مع عدم وجود فروق في بعد "التأثيرات الاجتماعية"، وعدم وجود فروق في معظم الأبعاد حسب التخصص مع وجود فروق في "معرفة المخاطر" والدرجة الكلية لصالح طلبة العلوم التطبيقية.
- دراسة عداد التي أجريت عام 2024 [3] في سورية، هدفت الدراسة إلى التعرف إلى درجة الوعي بالأمن السيبراني لدى طلبة جامعة حماة والكشف عن الفروق تبعًا لمتغيري السنة الدراسية (الأولى/الرابعة) والتخصص (علمي/نظري)، وقد استخدمت الدراسة المنهج الوصفي التحليلي، وكانت أداة الدراسة استبانة وفق مقياس ليكرت الخماسي (24 فقرة بعد التحكيم)، وتألفت العينة من (273) طالبًا وطالبة (حوالي 10% من المجتمع)، وقد أظهرت النتائج أن مستوى الوعي بالأمن السيبراني كان مرتفعًا، مع وجود فروق دالة لصالح طلبة السنة الرابعة، وفروق دالة لصالح طلبة الكليات العلمية.
- دراسة الفقهي التي أجريت عام 2024 [4] في ليبيا، هدفت الدراسة إلى تحديد مدى توافر الوعي بالأمن السيبراني لدى طلبة قسم الحاسوب في كليات التربية والكشف عن الفروق تبعًا لكلية الانتماء، وقد اعتمدت المنهج الوصفي، وكانت أداتها استبانة لقياس الوعي وترتيب فقراته وفق متوسطات الاستجابات، وتألفت العينة من (40) طالبًا

وطالبة، وقد أظهرت النتائج أن نسبة كبيرة من الطلبة يدركون أهمية حماية الأصول المعلوماتية الرقمية والحذر عند التعامل مع البيانات الحساسة، كما لم تُظهر النتائج فروقًا ذات دلالة إحصائية تُعزى لكلية الانتماء.

- دراسة الطيب التي أجريت عام 2025 [2] في السعودية، هدفت الدراسة إلى تحديد مستوى الوعي بالأمن السيبراني لدى طالبات الدراسات العليا في كلية التربية (قسم المناهج وطرق التدريس) عبر ثلاثة مجالات: مفاهيم الأمن السيبراني وتطبيقاته واستراتيجيات تعزيز الوعي، وقد استخدمت الدراسة المنهج الوصفي المسحي، وكانت أداة الدراسة استبانة مكوّنة من (30) عبارة موزعة على ثلاثة محاور، وتألفت العينة من (71) استبانة صالحة للتحليل، وقد أظهرت النتائج ارتفاع مستوى الوعي بمفاهيم الأمن السيبراني وارتفاع الوعي بتطبيقاته، مع اتفاق قوي على أهمية استراتيجيات تعزيز الوعي وتوصية بتقديم برامج تدريبية منظمة لرفع الوعي.
- دراسة BROMALL التي أجريت عام 2025[5] (أجنبية)، هدفت الدراسة إلى قياس مستوى الوعي بالأمن السيبراني لدى طلبة ما بعد الثانوي باستخدام أداة Q-HAIS/HAIS-Q، وفحص الفروق بين طلبة تخصصات تقنية المعلومات (IT) وغير IT، وقد استخدمت منهجًا وصفيًا مسحيًا مع اختبارات فروق، وتألفت العينة من نحو (100) مشارك مع تمثيل محدود لطلبة الدراسات العليا، وقد أظهرت النتائج مستويات مرتفعة نسبيًا في معظم المجالات (قريبة من 80% فأعلى)، وأن أقل المجالات كان مرتبطًا باستخدام وسائل التواصل الاجتماعي، كما ظهرت فروق صغيرة لكنها دالة لصالح مجموعة IT في غالبية المجالات، مع ارتباطات قوية بين المعرفة والاتجاه والسلوك.

التعقيب على الدراسات السابقة:

من خلال عرض الدراسات السابقة يتضح أن البحث الحالي يتقاطع معها في المنهج؛ إذ إن غالبية الدراسات اعتمدت المنهج الوصفي (مسحي/تحليلي) مثل دراسة عداد التي أجريت عام 2024 [3] ودراسة الفقهي التي أجريت عام 2024 [4] ودراسة الطيب التي أجريت عام 2025 [2] ودراسة BROMALL التي أجريت عام 2025[5] ودراسة Chintakovid التي أجريت عام 2023[6]، كما يلتقي معها في اعتماد الاستبانة أداةً رئيسة لجمع البيانات وقياس مستوى الوعي. ويتشابه البحث الحالي مع دراسة الطيب التي أجريت عام 2025 [2] في مجال الدراسة (كلية التربية) وفي التركيز على فئة الدراسات العليا، كما يتقاطع مع دراسة عداد التي أجريت عام 2024 [3] و دراسة الفقهي التي أجريت عام 2024 [4] في كونه يقيس الوعي في سياق جامعي عربي وبناءً على استجابات الطلبة. في المقابل، يختلف البحث الحالي عن بعض الدراسات من حيث الفئة المستهدفة؛ إذ ركزت دراسة Chintakovid التي أجريت عام 2023 [6] على طلبة البكالوريوس، بينما قارنت دراسة Chintakovid التي أجريت عام 2023 [26] بين طلبة البكالوريوس والدراسات العليا، كما تميزت دراسة ضعضع التي أجريت عام 2024 [1] بكونها دراسة بنائية هدفت إلى بناء مقياس وتقنينه وليس قياسًا وصفيًا مباشرًا فقط.

وما يميز البحث الحالي عن الدراسات السابقة أنه يُطبق على طلبة الدراسات العليا في كلية التربية بجامعة اللاذقية تحديدًا، ويعالج الوعي بوصفه بناءً ثلاثي الأبعاد يجمع بين المعرفة بالمفاهيم والتهديدات الرقمية والسلوكيات والممارسات الوقائية والوعي بالمسؤولية التربوية والأخلاقية، وهو بعد يظهر في أغلب الدراسات السابقة بصورة ضمنية أكثر منه محورًا مستقلًا واضحًا. كذلك استفاد الباحث من الدراسات السابقة في صياغة مشكلة البحث وأسئلته وفرضياته، وفي تحديد المتغيرات المقارنة (كالاختصاص وخصائص العينة)، وفي بناء أداة الاستبانة وتحديد محاورها، وفي دعم الإطار النظري وربط نتائج الدراسة بالمناقشات العلمية المرتبطة بالأمن الرقمي في التعليم العالي.

منهجيّة البحث وإجراءاته:

أولاً– منهج البحث:

أُستخدم المنهج الوصفي لملاءمته لطبيعة البحث، بهدف الكشف عن مستوى الوعي بالأمن الرقمي لدى طلبة الدراسات العليا، والكشف عن الفروق في الاستجابات تبعاً لمتغيرات المرحلة والاختصاص والتعرض لحوادث أمنية رقمية.

ثانياً– مجتمع البحث وعينته

بلغ عدد أفراد مجتمع البحث 180 طالباً وطالبة من طلبة الدراسات العليا في كلية التربية في جامعة اللاذقية، تم سحب عينة عشوائية بلغت 105 طالباً وطالبة. ويبين الجدول 1 توزع أفراد عينة البحث وفقاً لمتغيرات المرحلة والاختصاص والتعرض لحوادث أمنية رقمية

الجدول 1. توزع أفراد عينة البحث وفقاً لمتغيرات المرحلة والاختصاص والتعرض لحوادث أمنية رقمية

المتغير	الفئة	العدد	النسبة المئوية
المرحلة	ماجستير	82	78.1%
	دكتوراه	23	21.9%
الاختصاص	طرائق التدريس	36	34.3%
	رياض أطفال	27	25.7%
	أصول التربية	18	17.1%
	ارشاد نفسي	16	15.2%
	تقنيات التعليم	8	7.6%
التعرض لحوادث أمنية	لا	86	81.9%
	نعم	19	18.1%

ثالثاً– أداة البحث

تم إعداد استبانة لقياس مستوى الوعي بالأمن الرقمي لدى طلبة الدراسات العليا بعد الاطلاع على الأدب النظري والدراسات السابقة كدراسة ضعضع التي أجريت عام 2024[1] ودراسة عداد التي أجريت عام 2024 [3] ودراسة الفقهي التي أجريت عام 2024 [4] ودراسة الطيب التي أجريت عام 2025 [2] ودراسة GOLIATH التي أجريت عام 2024[26] (جنوب أفريقيا)، وتكوّنت من (25) بنداً موزعة على ثلاثة محاور:

1) المعرفة بالمفاهيم والتهديدات الرقمية: (9) بنود (1–9).
2) السلوكيات والممارسات الوقائية: (9) بنود (10–18).
3) الوعي بالمسؤولية التربوية والأخلاقية: (7) بنود (19–25).

وقد تم اعتماد مقياس ليكرت الخماسي للاستجابة (أوافق بشدة=5، أوافق=4، محايد=3، لا أوافق=2، لا أوافق بشدة=1).

تم حساب المدى (5–1=4) وتقسيمه على عدد الفئات (5) للحصول على طول الفئة (0.8)، وبناءً عليه تم تحديد مستويات التقدير كما في الجدول 2.

الجدول 2. مستويات التقدير للإجابة على الإستبانة

المدى	الوزن النسبي المقابل	درجة التقدير
من 1 إلى1.80	من 20% إلى36%	منخفضة جداً
أكبر من 1.80 إلى2.60	أكبر من 36% إلى52%	منخفضة
أكبر من 2.60 إلى3.40	أكبر من 52% إلى68%	متوسطة

أكبر من 3.40 إلى4.20	أكبر من 68% إلى84%	مرتفعة
أكبر من 4.20 إلى5.00	أكبر من 84% إلى100%	مرتفعة جداً

رابعاً –صدق وثبات الأداة

تم التحقق من صدق وثبات الأداة بتطبيق الأداة على عينة سيكومترية مكونة من (31) طالباً/طالبة من خارج عينة البحث.

أ– صدق الأداة:

1) صدق المحكّمين: تم عرض الاستبانة بصيغتها الأولية (26 بنداً) على مجموعة من المحكّمين ذوي الاختصاص وعددهم(6) محكمين، للتأكد من وضوح البنود وملاءمتها للمحاور، وتم إجراء التعديلات اللازمة كما في الجدول 3.

الجدول 3. التعديلات على بنود الاستبانة بعد عرضها على المحكمين

رقم البند	الصيغة الأولية (قبل التعديل)	الصيغة النهائية (بعد التعديل)
1	أفهم ماهية الأمن الرقمي	أعرف مفهوم الأمن الرقمي وأهميته في البحث العلمي
5	لدي معرفة بالهجمات الإلكترونية	أعرف مفهوم الهجمات السيبرانية وتأثيرها على الجامعات
11	أستخدم المصادقة الثنائية لحماية حساباتي	أفعّل المصادقة الثنائية في بريدي الإلكتروني ومنصات البحث
14	أحفظ نسخاً احتياطية من بياناتي البحثية	أحتفظ بنسخ احتياطية آمنة لبيانات بحثي باستخدام تقنيات التخزين السحابي
23	يجب على الجامعة توفير دورات عن الأمن الرقمي	أعتقد أن الجامعة يجب أن تقدم دورات إلزامية عن الأمن الرقمي لطلبة الدراسات العليا
_	حذف البند	أتابع دورات تدريبية في مجال الاختراق الأخلاقي (Ethical Hacking) لتنمية مهاراتي في الأمن الرقمي

2) صدق الاتساق الداخلي: تم حساب معاملات ارتباط بيرسون لكل محور بالدرجة الكلية للأستبانة كما في الجدول4.

الجدول 4. معاملات ارتباط المحاور بالدرجة الكلية للاستبانة

المحور	معامل الارتباط(r)	P	الدلالة
المعرفة بالمفاهيم والتهديدات الرقمية	0.806	0.000	**
السلوكيات والممارسات الوقائية	0.801	0.000	**
الوعي بالمسؤولية التربوية والأخلاقية	0.792	0.000	**

** دال عند (0.01)، * دال عند (0.05).

نلاحظ من الجدول 4 أن معاملات الارتباط موجبة ودالة إحصائياً، بما يدعم صدق الاستبانة وهي قابلة للتطبيق النهائي.

ب– ثبات الأداة:

1) الثبات بالتجزئة النصفية Split Half: تم تقسيم البنود إلى فردية وزوجية وفق ترتيبها، ثم حساب معامل الارتباط بين النصفين وتصحيحه بمعادلة سبيرمان–براون كما في الجدول 5.

الجدول 5. معاملات ثبات التجزئة النصفية المصححة بمعادلة سبيرمان–براون

المحور	سبيرمان–براون
المعرفة بالمفاهيم والتهديدات الرقمية	0.891
السلوكيات والممارسات الوقائية	0.768
الوعي بالمسؤولية التربوية والأخلاقية	0.544
الاستبانة	0.903

نلاحظ من الجدول 5 أن قيم معامل سبيرمان–براون تدل على درجة ثبات تراوحت بين متوسطة إلى عالية بحسب المحور وهي قابلة للتطبيق النهائي.

2) الثبات عن طريق معامل ألفا كرونباخ :

الجدول 6. معاملات الثبات باستخدام ألفا كرونباخ

المحور	ألفا كرونباخ
المعرفة بالمفاهيم والتهديدات الرقمية	0.846
السلوكيات والممارسات الوقائية	0.775
الوعي بالمسؤولية التربوية والأخلاقية	0.558
الاستبانة	0.864

نلاحظ من الجدول 6 أن معاملات ألفا كرونباخ تراوحت بين (0.558) و(0.864) وبالتالي تتمتع الاستبانة بدرجة ثبات جيدة.

خامساً– نتائج البحث:

أولاً: الإجابة عن أسئلة البحث:

السؤال الرئيسي: ما مستوى الوعي بالأمن الرقمي لدى طلبة الدراسات العليا في كلية التربية (جامعة اللاذقية)؟

للإجابة عن السؤال تم حساب المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لكل محور وللدرجة الكلية كما في الجدول 7.

الجدول 7. المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لمستوى الوعي بالأمن الرقمي

المحور	عدد البنود	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي%	درجة التقدير	الترتيب
الوعي بالمسؤولية التربوية والأخلاقية	7	4.050	0.571	81.0	مرتفعة	1
السلوكيات والممارسات الوقائية	9	3.884	0.713	77.7	مرتفعة	2
المعرفة بالمفاهيم والتهديدات الرقمية	9	3.545	0.736	70.9	مرتفعة	3
الدرجة الكلية	25	3.808	0.580	76.2	مرتفعة	

تشير نتائج الجدول 7 إلى أن الدرجة الكلية لمستوى الوعي بالأمن الرقمي لدى أفراد العينة جاءت مرتفعة بصورة عامة؛ إذ بلغ المتوسط الحسابي (3.808) وبوزن نسبي (76.2%). ويعني ذلك أن غالبية طلبة الدراسات العليا يمتلكون أساسًا معرفيًا وسلوكيًا وتقييمًا أخلاقيًا إيجابيًا تجاه قضايا الأمن الرقمي المرتبطة بالعمل الأكاديمي.

كما حل محور الوعي بالمسؤولية التربوية والأخلاقية في المرتبة الأولى، تلاه محور السلوكيات والممارسات الوقائية، ثم محور المعرفة بالمفاهيم والتهديدات الرقمية.

ويمكن تفسير هذا الارتفاع في مستوى الوعي بالأمن الرقمي استناداً إلى طبيعة البيئة الأكاديمية التي يعيشها طلبة الدراسات العليا يومياً، فهم بحكم مرحلتهم البحثية يتعاملون بصورة مستمرة مع منصات رقمية متعددة

كقواعد البيانات الأكاديمية وأنظمة إدارة التعلم والبريد الجامعي المؤسسي، وهذه المنصات بطبيعة تصميمها لا تكتفي بتقديم خدماتها بل تُصدر تنبيهات أمنية دورية وتلقائية للمستخدم كتنبيهات تغيير كلمات المرور وإشعارات محاولات الدخول غير المصرح به واشتراطات التحقق الثنائي وسياسات الخصوصية، مما يعني أن الطالب يتلقى تنبيهات أمنية رقمية متكررة حتى وهو يمارس نشاطه البحثي الاعتيادي دون أن يقصد التعلم الأمني الرقمي تحديداً. وبتراكم هذه التنبيهات عبر الزمن يتشكّل لدى الطالب رصيد معرفي ووعي أمني رقمي تدريجي.

علاوةً على ذلك، فإن التحول الواسع والمتسارع نحو الرقمنة في التعليم العالي خلال السنوات الأخيرة لم يكن مجرد تحول أدواتي، بل فرض على الطالب الباحث مواجهة تحديات أمنية حقيقية تمس صميم عمله الأكاديمي، كحماية بيانات المبحوثين من التسريب، وصون النزاهة الأكاديمية من الانتهاك، وضمان موثوقية المصادر الرقمية التي يبني عليها بحثه، مما دفع طالب الدراسات العليا تدريجياً إلى تبني ممارسات وقائية وتطوير حساسية أمنية رقمية نابعة من الحاجة الفعلية لا من التلقين النظري، وهو ما يُفسّر ارتفاع مستوى الوعي لديهم بصورة طبيعية ومنطقية تتسق مع طبيعة المرحلة التي يمرون بها.

وتتسق هذه النتيجة مع ما توصلت إليه دراسة الطيب التي أجريت عام 2025 [2] التي أشارت إلى مستوى مرتفع من الوعي بالأمن السيبراني لدى طالبات الدراسات العليا بجامعة الملك سعود، كما تتقاطع مع نتائج دراسة عداد التي أجريت عام 2024 [3] لدى طلبة جامعة حماة التي انتهت إلى ارتفاع درجة الوعي بالأمن السيبراني من وجهة نظر الطلبة.

الجدول 8. المتوسطات والانحرافات المعيارية لبنود الاستبانة

رقم	المحور	البند	المتوسط	الانحراف المعياري	درجة التقدير
1	المعرفة بالمفاهيم والتهديدات الرقمية	أعرف مفهوم الأمن الرقمي وأهميته في البحث العلمي	3.533	1.075	مرتفعة
2		أدرك مخاطر التصيد الإلكتروني على بياناتي البحثية	3.886	1.077	مرتفعة
3		أعرف كيفية عمل البرمجيات الضارة وتأثيرها على الأجهزة	3.152	1.142	متوسطة
4		أدرك مخاطر استخدام شبكة الواي فاي العامة أثناء البحث عبر الإنترنت	3.333	1.190	متوسطة
5		أعرف مفهوم الهجمات السيبرانية وتأثيرها على الجامعات	2.905	1.156	متوسطة
6		أعرف القوانين المحلية المتعلقة بالجرائم الإلكترونية وحماية البيانات	3.105	1.176	متوسطة
7		أدرك أهمية التشفير لحماية الملفات البحثية	3.743	1.110	مرتفعة
8		أعرف مخاطر مشاركة البيانات الشخصية في قواعد البيانات العالمية	4.057	0.979	مرتفعة
9		أدرك تأثير الجرائم الرقمية على النزاهة الأكاديمية)مثل السرقة الفكرية(	4.190	0.833	مرتفعة
10	السلوكيات والممارسات الوقائية	أستخدم كلمات مرور قوية وأقوم بتغييرها بانتظام لحماية حساباتي الأكاديمية	3.971	1.078	مرتفعة
11		أفعل المصادقة الثنائية في بريدي الإلكتروني ومنصات البحث	3.476	1.210	مرتفعة
12		أقوم بتحديث برامج مضادات الفيروسات بانتظام على أجهزتي	3.352	1.135	متوسطة
13		أتجنب فتح روابط أو ملفات من مصادر مجهولة أثناء البحث	4.352	0.961	مرتفعة جداً
14		أحتفظ بنسخ احتياطية آمنة لبيانات بحثي باستخدام تقنيات التخزين السحابي	3.771	1.112	مرتفعة
15		أتحقق من أمان المواقع العلمية قبل الدخول إليها	3.800	1.069	مرتفعة
16		أتجنب مشاركة معلومات بحثية حساسة عبر وسائل التواصل غير الآمنة	4.143	0.882	مرتفعة
17		أتحقق من مصداقية المصادر الرقمية قبل استخدامها في بحثي	4.133	0.856	مرتفعة
18		أتجنب استخدام أجهزة مشتركة للوصول الى بياناتي البحثية	3.952	0.892	مرتفعة
19	الوعي بالمسؤولية التربوية والأخلاقية	أعتقد أن الوعي بالأمن الرقمي جزء أساسي من مسؤوليتي كباحث تربوي	4.257	0.797	مرتفعة جداً
20		أدرك أهمية دمج التوعية الرقمية في رسائل الماجستير والدكتوراه	4.324	0.791	مرتفعة جداً
21		أدرك تأثير الجرائم الرقمية على الطلاب في المدارس والجامعات	4.076	0.874	مرتفعة
22		أسعى لتعلم المزيد عن الأمن الرقمي لتطبيقه في أبحاثي الأكاديمية	4.133	0.867	مرتفعة

23		أعتقد أن الجامعة يجب أن تقدم دورات إلزامية عن الأمن الرقمي لطلبة الدراسات العليا	4.495	0.761	مرتفعة جداً
24		أشارك في مناقشات أكاديمية حول الخصوصية الرقمية والأمن الرقمي	3.029	0.985	متوسطة
25		أتجنب استخدام أدوات ذكاء اصطناعي غير آمنة أثناء إعداد الأبحاث العلمية	4.038	0.940	مرتفعة

السؤال الفرعي(1): ما مستوى الوعي بالمفاهيم والتهديدات الرقمية لدى طلبة الدراسات العليا في كلية التربية (جامعة اللاذقية)؟

حقق محور المعرفة متوسطًا حسابيًا بلغ (3.545) وبوزن نسبي (70.9%)، وهو مستوى مرتفع، لكنه جاء الأدنى مقارنة ببقية المحاور. ويشير ذلك إلى توافر معرفة عامة بالمفاهيم والتهديدات الرقمية لدى الطلبة، مع وجود فجوات في بعض الجوانب المتخصصة.

وتبرز الفجوات المعرفية في البنود التي حصلت على تقدير متوسط، مثل: المعرفة بمفهوم الهجمات السيبرانية (المتوسط=2.905)، والإلمام بالقوانين المحلية المتعلقة بالجرائم الإلكترونية وحماية البيانات (المتوسط=3.105)، وفهم آلية عمل البرمجيات الضارة (المتوسط=3.152).

ويرتبط هذا النمط بطبيعة ما يتعرض له طلبة كلية التربية، إذ إن المفاهيم التقنية الدقيقة والجوانب القانونية غالبًا لا تُدرّس ضمن المساقات التربوية بصورة منهجية، كما تتطلب تدريبًا تطبيقيًا ومتابعة مستمرة للمستجدات. وفي المقابل، ارتفعت المعرفة المرتبطة بالنزاهة الأكاديمية والسرقة الفكرية (مثل بند تأثير الجرائم الرقمية على النزاهة الأكاديمية، المتوسط=4.190)، وهو أمر منطقي لارتباطه المباشر بمتطلبات البحث العلمي ومعايير الجامعة.

وعند المقارنة، جاءت نتائج هذا المحور منسجمة مع دراسة Chintakovid التي أجريت عام 2023 [6] التي رصدت وجود مستوى جيد من الوعي المعرفي مع استمرار مناطق ضعف تتطلب تعليمًا موجهًا، كما تدعمها نتائج دراسة BROMALL التي أجريت عام 2025 [5] التي أوضحت أن الوعي العام قد يكون مرتفعًا لدى طلبة التعليم ما بعد الثانوي مع بقاء مجالات محددة تحتاج إلى تعزيز.

السؤال الفرعي(2): ما مستوى الوعي بالسلوكيات والممارسات الوقائية الرقمية لدى طلبة الدراسات العليا في كلية التربية (جامعة اللاذقية)؟

حقق محور السلوكيات والممارسات الوقائية متوسطًا (3.884) وبوزن نسبي (77.7%)، وهو مستوى مرتفع يعكس ميلًا واضحًا لدى الطلبة إلى تبني إجراءات عملية تقلل من احتمالات التعرض للمخاطر أثناء البحث عبر الإنترنت أو التعامل مع الملفات والحسابات الأكاديمية.

وتتمثل أبرز الممارسات المرتفعة جدًا في تجنب فتح الروابط أو الملفات من مصادر مجهولة (المتوسط=4.352)، وهو سلوك يرتبط بوعي مباشر بمخاطر التصيد والبرمجيات الخبيثة. كما برزت ممارسات التحقق من مصداقية المصادر الرقمية وتجنب مشاركة المعلومات البحثية الحساسة عبر قنوات غير آمنة بدرجات مرتفعة، ما يشير إلى أن الطلبة يربطون بين الأمن الرقمي وجودة العمل الأكاديمي.

في المقابل، ظهرت بعض الممارسات بدرجة متوسطة، وعلى رأسها تحديث برامج مضادات الفيروسات بانتظام (المتوسط=3.352). ويمكن تفسير ذلك بأن التحديثات الدورية قد تُؤجل بسبب ضعف البنية التقنية للأجهزة الشخصية، أو الاعتماد على أنظمة تشغيل غير محدثة، أو بسبب تصور خاطئ بأن الحماية الافتراضية كافية. كما أن تفعيل المصادقة الثنائية جاء أقل نسبيًا من بقية الممارسات، وقد يرتبط ذلك بمحدودية الثقافة الأمنية الإجرائية أو الاعتقاد بأن الإجراء معقد أو غير ضروري.

وتتفق هذه النتائج مع ما طرحته دراسة الفقهي التي أجريت عام 2024 [4] حول ارتفاع الوعي الأمني العام لدى الطلبة مع بقاء بعض السلوكيات الإجرائية متفاوتة، كما أشارت دراسة BROMALL التي أجريت عام 2025 [5] إلى وجود "نقاط ضعف بؤرية" داخل مستوى الوعي المرتفع، غالبًا ما ترتبط بممارسات تشغيلية مثل التحديثات وإدارة الحسابات وكلمات المرور.

السؤال الفرعي(3): ما مستوى الوعي بالمسؤولية التربوية والأخلاقية الرقمية لدى طلبة الدراسات العليا في كلية التربية (جامعة اللاذقية)؟

جاء محور الوعي بالمسؤولية التربوية والأخلاقية في المرتبة الأولى بمتوسط (4.050) وبوزن نسبي (81.0%)، وهو ما يعكس أن الطلبة ينظرون إلى الأمن الرقمي بوصفه جزءًا من هوية الباحث التربوي ومتطلبات النزاهة العلمية، وليس مجرد مهارات تقنية مساندة.

ويتضح ذلك في ارتفاع البنود التي تؤكد ضرورة تقديم دورات إلزامية في الأمن الرقمي لطلبة الدراسات العليا (المتوسط=4.495)، وكذلك إدماج التوعية الرقمية في رسائل الماجستير والدكتوراه (المتوسط=4.324). ويمكن تفسير ذلك بأن الطلبة يدركون أن الممارسات غير الآمنة قد تنعكس مباشرة على مصداقية البيانات البحثية وسرية المشاركين وحقوق الملكية الفكرية.

غير أن مشاركة الطلبة في مناقشات أكاديمية حول الخصوصية والأمن الرقمي جاءت بدرجة متوسطة (المتوسط=3.029). ويمكن تفسير ذلك بقلة الفعاليات والندوات المتخصصة أو محدودية المساحات المؤسسية التي تتيح نقاشًا معمقًا حول القضايا الأخلاقية المرتبطة بالبيانات والذكاء الاصطناعي وأمن المنصات البحثية.

وتتوافق هذه الصورة مع ما أظهرته دراسة الطيب التي أجريت عام 2025 [2] من نزعة إيجابية لدى طلبة الدراسات العليا نحو استراتيجيات تعزيز الأمن السيبراني (مثل التدريب والتوعية المؤسسية)، وهو ما يدعم فكرة أن البعد القيمي والأخلاقي قد يكون أعلى من بعض الممارسات التقنية التفصيلية.

ثانياً: نتائج اختبار فرضيات البحث:

الفرضية الأولى: لا يوجد فرق ذو دلالة إحصائية عند مستوى دلالة (0.05) بين متوسطات درجات أفراد العينة على محاور الوعي بالأمن الرقمي والدرجة الكلية تُعزى لمتغير المرحلة (ماجستير/دكتوراه).

الجدول 9. المتوسطات والانحرافات المعيارية حسب متغير المرحلة

المحور	المرحلة	العينة	المتوسط	الانحراف المعياري
المعرفة	ماجستير	82	3.524	0.763
	دكتوراه	23	3.618	0.641
الممارسات	ماجستير	82	3.881	0.742
	دكتوراه	23	3.894	0.614
المسؤولية	ماجستير	82	4.049	0.610
	دكتوراه	23	4.056	0.417
الدرجة الكلية	ماجستير	82	3.800	0.614
	دكتوراه	23	3.840	0.450

الجدول 10. نتائج اختبار (t) للفروق حسب متغير المرحلة.

المحور	قيمة اختبار(t)	درجات الحرية(Df)	مستوى الدلالة الإحصائية(p)	اختبار تجانس التباين(Levene p)	القرار

المعرفة	-0.539	103.0	0.591	0.336	غير دال
الممارسات	-0.077	103.0	0.939	0.740	غير دال
المسؤولية	-0.053	103.0	0.958	0.221	غير دال
الدرجة الكلية	-0.295	103.0	0.769	0.117	غير دال

تُظهر نتائج الجدول 10 عدم وجود فروق ذات دلالة إحصائية تبعاً لمتغير المرحلة على المحاور والدرجة الكلية عند مستوى (0.05)، وبذلك تُقبل الفرضية الصفرية.

حيث لم تُظهر اختبارات (t) فروقًا ذات دلالة إحصائية بين طلبة الماجستير والدكتوراه في أي من المحاور أو في الدرجة الكلية (جميع قيم $p>0.05$). ويمكن تفسير ذلك بتقارب متطلبات البحث والاعتماد على المنصات الرقمية بين المرحلتين، إضافة إلى أن مصادر التعلم الذاتي الرقمية قد تقلص الفروق بين المجموعتين.

الفرضية الثانية: لا توجد فروق ذات دلالة إحصائية بين متوسطات درجات أفراد العينة على محاور الوعي بالأمن الرقمي والدرجة الكلية تُعزى لمتغير الاختصاص، عند مستوى دلالة (0.05).

الجدول 11. المتوسطات والانحرافات المعيارية حسب متغير الاختصاص

الاختصاص	العينة	المعرفة		الممارسات		المسؤولية		الدرجة الكلية	
		المتوسط الحسابي	الانحراف المعياري	المتوسط الحسابي	الانحراف المعياري	المتوسط الحسابي	الانحراف المعياري	المتوسط الحسابي	الانحراف المعياري
أصول التربية	18	3.747	0.468	4.062	0.513	4.103	0.356	3.960	0.287
ارشاد نفسي	16	3.222	0.747	3.472	0.583	3.634	0.475	3.428	0.525
تقنيات التعليم	8	3.764	0.633	3.931	0.661	4.268	0.503	3.965	0.574
رياض أطفال	27	3.457	0.828	3.745	0.939	3.995	0.791	3.711	0.775
طرائق التدريس	36	3.605	0.765	4.071	0.591	4.202	0.423	3.940	0.47

الجدول 12. نتائج تحليل التباين الأحادي (ANOVA/Welch) للفروق حسب متغير الاختصاص

المحور	نوع الاختبار	قيمة(f) اختبار الفروق بين المتوسطات	مستوى الدلالة الإحصائية(p)	اختبار تجانس التباين(Levene p)
المعرفة	ANOVA	1.468	0.218	0.246
الممارسات	ANOVA	2.657	0.037	0.479
المسؤولية	ANOVA	3.451	0.011	0.155
الدرجة الكلية	Welch	3.605	0.015	0.041

للكشف عن اتجاه الفروق عند دلالة النتائج، تم استخدام اختبار توكي (Tukey) للمحاور ذات تجانس تباين، واختبار جيمز–هويل (Games–Howell) للدرجة الكلية عند عدم تجانس التباين، كما في الجدول 13.

الجدول 13. المقارنات البعدية (Post Hoc) حسب الاختصاص

المقارنة	المحور	فرق المتوسطات	مستوى الدلالة الإحصائية(p)
ارشاد نفسي × طرائق التدريس	الممارسات	0.599	0.038
ارشاد نفسي × طرائق التدريس	المسؤولية	0.569	0.007
أصول التربية × ارشاد نفسي	الدرجة الكلية	0.532	0.012
ارشاد نفسي × طرائق التدريس	الدرجة الكلية	-0.512	0.019

تشير نتائج الجدولين 12 و13 إلى وجود فروق دالة إحصائياً تبعاً لمتغير الاختصاص في محور السلوكيات والممارسات الوقائية، ومحور الوعي بالمسؤولية التربوية والأخلاقية، وكذلك في الدرجة الكلية. وقد كانت الفروق الدالة لصالح اختصاص طرائق التدريس مقارنة باختصاص الإرشاد النفسي في محوري الممارسات والمسؤولية،

ولصالح اختصاص أصول التربية وطرائق التدريس مقارنة باختصاص الإرشاد النفسي في الدرجة الكلية. وبذلك تُرفض الفرضية الصفرية جزئياً وفق هذه النتائج.

ظهرت فروق دالة إحصائيًا تبعًا للاختصاص في محور السلوكيات والممارسات الوقائية (p=0.037)، ومحور المسؤولية التربوية والأخلاقية (p=0.011)، وكذلك في الدرجة الكلية (p=0.015). وتشير المتوسطات إلى أن اختصاص الإرشاد النفسي سجل أدنى القيم في الممارسات والدرجة الكلية مقارنة ببقية الاختصاصات، بينما حققت اختصاصات مثل تقنيات التعليم وطرائق التدريس وأصول التربية متوسطات أعلى. ويُفسَّر ذلك بأن طبيعة البيئة الأكاديمية في بعض الاختصاصات تتطلب استخدامًا أوسع للأدوات الرقمية، بما يراكم خبرات عملية في إدارة الحسابات والمنصات والملفات، بينما قد يكون الاستخدام التقني لدى بعض التخصصات أكثر محدودية أو أقل تركيزًا على الجوانب الإجرائية للأمن.

وتتفق هذه النتيجة جزئيًا مع دراسة BROMALL التي أجريت عام 2025 [5] التي أشارت إلى ميزة نسبية لفئات مرتبطة بالتخصصات التقنية في بعض مجالات الوعي والسلوك، بينما تختلف جزئيًا مع دراسة Chintakovid التي أجريت عام 2023 [6] التي لم تُبرز فروقًا واضحة في الوعي وفق بعض التخصصات، وهو ما قد يعود لاختلاف السياق المؤسسي وطبيعة البرامج.

الفرضية الثالثة: لا يوجد فرق ذو دلالة إحصائية عند مستوى دلالة (0.05) بين متوسطات درجات أفراد العينة على محاور الوعي بالأمن الرقمي والدرجة الكلية تُعزى لمتغير التعرض لحوادث أمنية رقمية (نعم/لا).

الجدول 14. المتوسطات والانحرافات المعيارية حسب التعرض لحوادث أمنية رقمية

المحور	التعرض	العينة	المتوسط	الانحراف المعياري
المعرفة	نعم	19	3.474	0.807
	لا	86	3.561	0.723
الممارسات	نعم	19	3.784	0.638
	لا	86	3.906	0.730
المسؤولية	نعم	19	3.940	0.520
	لا	86	4.075	0.582
الدرجة الكلية	نعم	19	3.716	0.553
	لا	86	3.829	0.587

الجدول 15. نتائج اختبار (t) للفروق حسب التعرض لحوادث أمنية رقمية

المحور	قيمة اختبار(t)	درجات الحرية(Df)	مستوى الدلالة الإحصائية (p)	اختبار تجانس التباين(Levene p)	القرار
المعرفة	−0.465	103.0	0.643	0.554	غير دال
الممارسات	−0.674	103.0	0.502	0.791	غير دال
المسؤولية	−0.931	103.0	0.354	0.825	غير دال
الدرجة الكلية	−0.768	103.0	0.445	0.767	غير دال

تشير نتائج الجدول 15 إلى عدم وجود فروق ذات دلالة إحصائية تبعاً لمتغير التعرض لحوادث أمنية رقمية على المحاور والدرجة الكلية عند مستوى (0.05)، وبذلك تُقبل الفرضية الصفرية.

لم يظهر فرق دال إحصائيًا بين من تعرضوا لحوادث أمنية رقمية ومن لم يتعرضوا لها على المحاور أو الدرجة الكلية (جميع قيم p>0.05). ويفسر ذلك بأن الخبرة المكتسبة من الحادثة تظل خبرة ظرفية محدودة النطاق

مرتبطة بالموقف الذي وقع فيه الحادث الأمني الرقمي تحديداً، ولا تتحول إلى وعي أمني شامل أو سلوك وقائي مستدام ما لم تُعزَّز بتدريب مؤسسي منظم، اذ يستجيب الفرد للحادثة الأمنية الرقمية التي وقعت له تحديداً دون أن تتشكل لديه قاعدة معرفية وقائية شاملة.

الاستنتاجات:

توصلت نتائج البحث إلى أن مستوى الوعي بالأمن الرقمي لدى طلبة الدراسات العليا في كلية التربية بجامعة اللاذقية جاء مرتفع، مع تفوق محور المسؤولية التربوية والأخلاقية .كما لم يظهر فرق دال تبعاً للمرحلة أو التعرض لحوادث أمنية رقمية، بينما ظهرت فروق دالة تبعاً للاختصاص في محور الممارسات ومحور المسؤولية والدرجة الكلية.

مقترحات البحث:

بناءً على النّتائج المُستخلصة من البحث قُدّمت المقترحات الآتية:

- تخصيص وحدة مستقلة لطلاب التخصصات الإنسانية حول حماية بيانات المبحوثين في الأبحاث التربوية والنفسية.
- تكليف قسم تقنيات التعليم في الكلية بتصميم مواد تدريبية تتضمن أمثلة واقعية على رسائل التصيد الإلكتروني وأساليب التعرف على الروابط الاحتيالية الشائعة في البيئة الأكاديمية.
- تنفيذ دراسات شبه تجريبية لقياس فاعلية برنامج توعوي قصير على محاور الاستبانة الثلاثة.

المراجع (REFRENCES):

[1] **ضعضع، هبة عبد اللطيف.** *بناء مقياس الوعي بالحرب السيبرانية لدى طلاب الجامعة في الجمهورية العربية السورية*. (مجلة جامعة بابل للعلوم الإنسانية)، مج 32، / ع 11/ 99-121، 2024.

[1] H. Doudouh, "Developing a Cyber Warfare Awareness Scale among University Students in the Syrian Arab Republic," *Journal of the University of Babylon for Humanities*, vol. 32, no. 11, pp. 99-121, 2024.

[2] **الطيب، عهد عبدالقادر؛ الوهبي، نجلاء تركي؛ والمقرن، نورة أحمد.** *درجة وعي طالبات الدراسات العليا في جامعة الملك سعود بالأمن السيبراني*. (مجلة العلوم التربوية والنفسية)، مج 9، / ع 7/ 1-22، 2025.

[2] A. Altayeb, N. Alwahbi, and N. Almoqren, "The Level of Cybersecurity Awareness among Graduate Female Students at King Saud University," *Journal of Educational and Psychological Sciences*, vol. 9, suppl. no. 7, pp. 1-22, 2025.

[3] **عداد، علي.** *درجة الوعي بالأمن السيبراني لدى عينة من طلبة جامعة حماة من وجهة نظرهم*. (مجلة جامعة حماة)، مج 7، / ع 16/ 160-174، 2024.

[3] A. Addad, "The Degree of Cybersecurity Awareness among a Sample of Hama University Students from Their Perspective," *Hama University Journal*, vol. 7, no. 16, pp. 160-174, 2024.

[4] **الفقهي، فتحي علاق.** *مدى توافر الوعي بالأمن السيبراني لدى طلبة قسم الحاسوب بكليات التربية جامعة طرابلس* . (مجلة القلعة)، / ع 23/ 77-89، 2024.

[4] F. Al-Fiqhi, "The Availability of Cybersecurity Awareness among Computer Department Students in Colleges of Education at the University of Tripoli," *Al-Qala'a Journal*, no. 23, pp. 77-89, 2024.

[5] N. Bromall, P. Draus, S. Mishra, K. Slonka, and J. Trunkos, "Cybersecurity Awareness among Post-Secondary Students," *Issues in Information Systems*, vol. 26, no. 3, pp. 149-157, 2025.

[6] Y. Du and T. Chintakovid, "A Survey of Cybersecurity Awareness among Undergraduate Students in *Proceedings of the 12th* International Conference on Economics, Management and Knowledge Innovation (ICEKIM 2023)", pp. 747-754, 2023.

[7] S. Thaba and J. Mtsweni, *Analysing Cyberwarfare Capabilities and Impact in *Proceedings of the 22nd European Conference on Cyber Warfare and Security* (ECCWS 2023)*. Athens, Greece, 2023.

[8] S. Loeb, S. Dynarski, D. McFarland, P. Morris, S. Reardon, and S. Reber, *Descriptive Analysis in Education: A Guide for Researchers*. NCEE 2017-4023, U.S. Department of Education, Institute of Education Sciences, National Center for Education Evaluation and Regional Assistance, 2017.

[9] C. Paulsen, J. Boyens, N. Bartol, and K. Winkler, *Glossary of Key Information Security Terms*. NISTIR 7298 Rev. 3, National Institute of Standards and Technology, 2019.

[10] M. Merritt, S. Hansche, B. Ellis, K. Sanchez-Cherry, J. Nethery Snyder, and D. Walden, *Building a Cybersecurity and Privacy Learning Program*. NIST Special Publication 800-50 Rev. 1, National Institute of Standards and Technology, 2024.

[11] J. Ulven and G. Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education," *Future Internet*, vol. 13, no. 2, Art. no. 39, 2021.

[12] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual Differences and Information Security Awareness," *Computers in Human Behavior*, vol. 69, pp. 151-156, 2017.

[13] V. Zimmermann and K. Renaud, "Moving from a 'Human-as-Problem' to a 'Human-as-Solution' Cybersecurity Mindset," **International Journal of Human-Computer* Studies*, vol. 131, pp. 169-187, 2019.

[14] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies," *Computers & Security*, vol. 66, pp. 40-51, 2017.

[15] S. Egelman and E. Peer, "Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)," *in Proceedings of CHI '15*, ACM, pp. 2873-2882, 2015.

[16] T. van Steen, E. Norris, K. Atha, A. Joinson, and L. Coventry, "What (If Any) Behaviour Change Techniques Do Government-Led Cybersecurity Awareness Campaigns Use?," *Journal of Cybersecurity*, vol. 6, no. 1, Art. no. tyaa019, 2020.

[17] M. Choi, "A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age," *Theory & Research in Social Education*, vol. 44, no. 4, pp. 565-607, 2016.

[18] M. Choi, M. Glassman, and D. Cristol, "What It Means to Be a Citizen in the Internet Age: Development of a Reliable and Valid Digital Citizenship Scale," *Computers & Education*, vol. 107, pp. 100-112, 2017.

[19] I. Ajzen, "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179-211, 1991.

[20] R. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology*, vol. 91, no. 1, pp. 93-114, 1975.

[21] P. Ifinedo, "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security*, vol. 31, no. 1, pp. 83-95, 2012.

[22] B.-Y. Ng, A. Kankanhalli, and Y. Xu, "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems*, vol. 46, no. 4, pp. 815-825, 2009.

[23] A. Gwenhure, "University Students' Security Behavior Against Email Phishing Attacks: Insights from the Health Belief Model," *Journal of Cybersecurity*, vol. 11, no. 1, Art. no. tyaf034, 2025.

[24] A. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," * MIS Quarterly*, vol. 34, no. 3, pp. 549-566, 2010.

[25] C. Pascoe, S. Quinn, and K. Scarfone, *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper 29, National Institute of Standards and Technology, 2024.

[26] S. Goliath, P. Tsibolane, and D. Snyman, "Exploring the Cybersecurity-Resilience Gap: An Analysis of Student Attitudes and Behaviors in Higher Education," *arXiv preprint*, arXiv:2411.03219, 2024. [Online]. Available: https://arxiv.org/abs

الملاحق:

الملحق 1. التكرارات والنسب المئوية ومستوى الوعي لكل عبارة من عبارات الاستبانة الاستطلاعية

م	العبارة	دائماً (التكرارات)	النسبة المئوية	أحياناً (التكرارات)	النسبة المئوية	نادراً ((التكرارات)	النسبة المئوية	المستوى
1	أستخدم كلمات مرور قوية ومختلفة لحساباتي الأكاديمية والشخصية على الإنترنت.	13	% 61.9	6	%28.6	2	%9.5	مرتفع
2	أتحقق من مصداقية الروابط والمرفقات في رسائل البريد الإلكتروني قبل فتحها.	9	%42.9	8	%38.1	4	%19.0	متوسط
3	أحتفظ بنسخ احتياطية من بياناتي البحثية وملفاتي الأكاديمية بشكل دوري.	6	%28.6	8	%38.1	7	%33.3	متوسط
4	أضبط إعدادات الخصوصية في حساباتي على منصات التواصل الاجتماعي والمنصات الأكاديمية.	7	%33.3	9	%42.9	5	%23.8	متوسط
5	أحرص على تحديث أنظمة التشغيل والتطبيقات والبرامج المضادة للفيروسات على أجهزتي.	5	%23.8	8	%38.1	8	%38.1	منخفض
6	أتجنب استخدام شبكات Fi–Wi العامة غير المحمية عند الوصول إلى بياناتي الأكاديمية.	5	%23.8	9	%42.9	7	%33.3	منخفض
7	أعرف كيف أتصرف في حال تعرض أحد حساباتي الرقمية للاختراق أو الاستخدام غير المصرح به.	4	%19.0	7	%33.3	10	%47.6	منخفض
8	أستخدم ميزة التحقق بخطوتين (المصادقة الثنائية) لحماية حساباتي المهمة.	3	%14.3	6	%28.6	12	%57.1	منخفض
9	أدرك المخاطر المرتبطة بمشاركة البيانات الشخصية والبحثية عبر المنصات الرقمية.	12	%57.1	7	%33.3	2	%9.5	مرتفع
10	أميّز بين المواقع الإلكترونية الآمنة وغير الآمنة عند تحميل المراجع والمصادر البحثية.	8	%38.1	10	%47.6	3	%14.3	متوسط