مجلة الباحث
موقع المجلة: https://journals.uokerbala.edu.iq/index.php/bjh/

تحليل مستوى وعي وممارسات الأمن السيبراني المتبعة لدى طلبة الدراسات العليا في كلية التربية في جامعة دمشق

محمود اسماعيل الفارس

محاضر في كلية التربية في جامعة دمشق

التخصص العام للبحث: أصول التربية	التخصص الدقيق للبحث: علم الاجتماع التربوي

معلومات الورقة البحثية

تاريخ الاستلام 2025/1/1
تاريخ القبول 2025/2/1
تاريخ النشر 2025/3/1

الكلمات الرئيسية:

الوعي، الممارسات، الأمن السيبراني، طلبة الدراسات العليا

المستخلص باللغة العربية:

هدف البحث إلى دراسة مستوى وعي طلبة الدراسات العليا في كلية التربية بجامعة دمشق بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية، وتحليل ممارساتهم الفعلية عند استخدام التقنيات الرقمية، إضافة إلى الكشف عن أبرز التحديات التي تواجههم في الالتزام بإجراءات الأمن السيبراني. كما سعى إلى استقصاء العلاقة بين مستوى الوعي ومستوى الممارسة من وجهة نظر الطلبة أنفسهم.اعتمد الباحث المنهج الوصفي التحليلي، حيث أُعدّت استبانة لقياس واقع الأمن السيبراني، وطُبقت على عينة عشوائية طبقية بلغت (205) طالباً وطالبة من طلبة الدراسات العليا في كلية التربية بجامعة دمشق. أظهرت النتائج أن مستوى وعي الطلبة بإجراءات الأمن السيبراني كان مرتفعاً، في حين جاءت ممارساتهم الفعلية جيدة بشكل عام، لكنها تركزت في الإجراءات الفردية الأساسية مثل استخدام كلمات مرور قوية، النسخ الاحتياطي، وضبط إعدادات الخصوصية، بينما تراجعت الممارسات التشغيلية والمؤسسية كإجراءات تسجيل الخروج والإبلاغ عن الحوادث الأمنية. كما بينت النتائج وجود تحديات كبيرة تواجه الطلبة، أبرزها ارتفاع تكلفة أدوات الحماية، نقص التدريب والدعم الفني، وصعوبة تفعيل المصادقة الثنائية. وكشفت التحليلات الإحصائية عن فروق دالة لصالح طلبة الدكتوراه في مستوى الوعي، وفروق لصالح ذوي الخبرة التقنية المتوسطة والمتقدمة في مستوى الممارسة، إضافة إلى وجود علاقة ارتباطية قوية بين الوعي والممارسة، مما يؤكد أن تعزيز المعرفة يسهم في تحسين السلوكيات الأمنية لدى الطلبة.

doi: https://doi.org/10.63797/bjh.

1. مقدمة:

مع التطور السريع في تكنولوجيا المعلومات والانتشار الواسع لأنظمة الشبكات، أصبح الإنترنت جزءًا لا يتجزأ من الحياة اليومية للطلبة الجامعيين وأنشطتهم الأكاديمية، بما في ذلك منصات التعلم الإلكتروني، وقواعد البيانات، ومستودعات الدورات، ومقاطع الفيديو التعليمية، ومنصات التواصل الاجتماعي. ورغم ما توفره هذه الأدوات من فرص للتعلم والتواصل والتعاون، فإن الاعتماد المتزايد عليها يرافقه مخاطر حقيقية قد تؤثر سلباً على مستخدميها وسلامة بياناتهم في حال إساءة الاستخدام أو غياب ممارسات الحماية المناسبة.

لذا باتت الحاجة إلى الحماية الرقمية ملحة، لاسيما عند طلبة الدراسات العليا، الذين يعتمدون بشكل كبير على المنصات الإلكترونية في إنجاز البحوث، وإدارة المشاريع العلمية، والتواصل مع المشرفين والزملاء، فقد تغيرت طرق التفاعل مع الموارد التعليمية، وأصبح إدخال المعلومات الشخصية والبحثية عبر الإنترنت للانضمام إلى موقع تعليمي أو دروس أو فصول دراسية عبر الإنترنت أمراً معتاداً، مما أدى إلى تراكم كميات كبيرة من البيانات الحساسة على منصات رقمية متعددة، هذا التعرض المتزايد يجعل الطلبة عرضة لمجموعة من الأنشطة غير المشروعة التي تنتهك الخصوصية وتسبب أضراراً مادية ونفسية، مثل هجمات الفيروسات، والاختراق، والاحتيال المصرفي، والبرمجيات الخبيثة، وتسريب المعلومات الشخصية.

في هذا السياق، برز الأمن السيبراني كأحد أهم القضايا التي تشغل المؤسسات التعليمية والبحثية على حد سواء. حيث يشير الأمن السيبراني إلى "التدابير المتخذة لحماية الحواسيب والشبكات من الوصول غير المصرح به، بما يضمن سلامة المعلومات وأمنها، ويشمل التدخلات التقنية التي تحمي البيانات ومعلومات الهوية والأجهزة من الاختراق أو الضرر" (Richardson et al., 2020).

غير أن الأمن السيبراني لا يقتصر على الجانب التقني فحسب، بل يشمل أيضاً مستوى الوعي والسلوكيات التي يتبناها المستخدمون عند تعاملهم مع التقنيات الرقمية. فقد أكدت العديد من الدراسات أن ضعف الوعي الأمني يعد من أبرز أسباب نجاح الهجمات الإلكترونية، الأمر الذي يفرض على المؤسسات التعليمية مسؤولية مضاعفة لتعزيز ثقافة الأمن الرقمي بين طلبتها من خلال برامج توعوية وتدريبية فعّالة. مثل دراسة العودة (2025) التي أشارت إلى أن نقص الوعي وسوء التطبيق العملي لإجراءات الحماية يزيدان من تعرض الأفراد والمؤسسات للاختراقات وسرقة البيانات، داعيةً إلى تعزيز التشريعات والبنية التحتية والتوعية كجزء من منظومة الأمن القومي.

من هنا تأتي أهمية هذا البحث، الذي يسعى إلى تحليل مستوى وعي طلبة الدراسات العليا في كلية التربية بمفهوم الأمن السيبراني وممارساتهم المتعلقة به، والكشف عن التحديات والمعوقات التي تواجههم في هذا المجال، بما يسهم في وضع توصيات عملية لتعزيز ثقافة الأمن الرقمي في البيئة الأكاديمية مما يساعد في ضمان حماية البيانات والمعلومات الحساسة والحفاظ على سلامة أنظمة وشبكات التعليم.

2. مشكلة البحث:

أصبحت الجرائم والتهديدات الإلكترونية في ظل التطور المتسارع لتكنولوجيا المعلومات والاتصالات من أبرز التحديات التي تواجه مؤسسات التعليم العالي، التي تعتمد بشكل متزايد على التقنيات الرقمية في إدارة عملياتها الأكاديمية والبحثية. ومع هذا الاعتماد الكبير، تبرز قضية وعي الطلبة الجامعيين، ولا سيما طلبة الدراسات العليا، بإجراءات الأمن السيبراني، ومدى التزامهم بها أثناء استخدامهم للتقنيات الرقمية في أنشطتهم العلمية. وتزداد خطورة هذه القضية بالنظر إلى طبيعة البيانات التي يتعامل معها هؤلاء الطلبة، مثل الأبحاث العلمية، والمراسلات الأكاديمية، والمعلومات الشخصية، والتي تجعلهم أكثر عرضة لمخاطر متعددة في حال ضعف الممارسات الأمنية. فضعف الثقافة الأمنية الرقمية وسلوكيات الاستخدام غير الآمنة لدى طلبة الدراسات العليا يعدان من أبرز أسباب الاختراقات والهجمات الإلكترونية، حيث إن كثيراً من الانتهاكات لا تعود إلى قصور في الأنظمة التقنية بقدر ما ترتبط بسلوكيات المستخدمين أنفسهم. وفي بيئة التعليم العالي، قد يؤدي هذا القصور إلى تسريب معلومات بحثية، أو فقدان بيانات مهمة، أو حتى الإضرار بسمعة المؤسسة الأكاديمية. وبالتالي يمكن تجنب الاحتيال إذا كان الطلبة على دراية بالمخاطر الإلكترونية التي قد يواجهونها، ويعرفون كيفية استخدام الإنترنت بأمان. وهذا ما أكدته دراسة مشعل والشناوي (2024) أن تعزيز الوعي بالأمن السيبراني في كليات التربية يُعد أمراً بالغ الأهمية لتحقيق تكامل تكنولوجيا التعليم وبناء بيئة تعليمية آمنة وموثوقة، وأن المؤسسات والطلبة معاً بحاجة إلى الاستعداد لمواجهة التحديات السيبرانية المتنامية.

ورغم أهمية هذا الموضوع، لا يزال الوعي بالأمن السيبراني بين طلبة الدراسات العليا في الجامعات العربية لم يحظ بالاهتمام الكافي. فقد أشار خضر وآخرون (Khader et al.، 2021) إلى الحاجة المستمرة لإجراء المزيد من الدراسات لقياس درجة الوعي بالأمن السيبراني لدى طلبة التعليم العالي، والكشف عن سلوكياتهم في هذا المجال، بالإضافة إلى تحديد العوامل المؤثرة ذات الصلة. كما أوضح الحربي والصديق (Alharbi & Tassaddig، 2021) أن معظم المؤسسات الأكاديمية لا تتضمن برامج توعية ممنهجة بالأمن السيبراني ضمن

استراتيجياتها التعليمية، الأمر الذي يبرز الحاجة إلى إدماج هذا الجانب كجزء أساسي من اهتمامات المؤسسات التعليمية لضمان إعداد الخريجين بالمهارات والمعرفة اللازمة لمواجهة التهديدات السيبرانية.
يتضح مما سبق أن العديد من الانتهاكات السيبرانية تعود في جوهرها إلى سلوكيات المستخدمين أكثر من كونها قصورًا تقنيًا، ومع ذلك تندر الدراسات الميدانية التي تستكشف مستوى الوعي الأمني وممارسات الطلبة في كليات التربية، لا سيما بين طلبة الدراسات العليا الذين يمثلون نواة التطوير العلمي والتربوي. وتزداد حدة المشكلة في ظل غياب برامج توعية منهجية ومتكاملة داخل كثير من المؤسسات التعليمية. لذا تبرز الحاجة إلى سد هذه الفجوة من خلال تقييم مفصل لمستويات وعي طلبة الدراسات العليا في كلية التربية بالتهديدات السيبرانية المحتملة وسبل حماية أنفسهم منها، وتحديد المجالات التي يفتقرون فيها إلى الفهم، بما يسهم في توفير بيانات محلية دقيقة تساعد صانعي القرار في الجامعات على تصميم برامج توعوية مستهدفة، وتطوير سياسات حماية معلوماتية تضمن سلامة البيانات البحثية والشخصية، وتعزيز جاهزية المجتمع الأكاديمي لمواجهة التهديدات السيبرانية المتجددة.
وانطلاقاً مما سبق يمكن تحديد مشكلة البحث بالسؤال التالي: ما مستوى وعي طلبة الدراسات العليا في كلية التربية بجامعة دمشق بإجراءات الأمن السيبراني وما الممارسات الفعلية المتبعة عند استخدامهم للتقنيات الرقمية في أنشطتهم الأكاديمية والبحثية من وجهة نظرهم؟

3. أهمية البحث:

تنبع أهمية هذا البحث من عدة جوانب نظرية وتطبيقية، يمكن توضيحها بالأتي:

1. **الأهمية النظرية:**
   - يسهم البحث في إثراء الأدبيات التربوية المتعلقة بالأمن السيبراني في التعليم العالي، من خلال التركيز على فئة طلبة الدراسات العليا في كليات التربية، وهي فئة غالباً ما تكون أقل تناولاً في الدراسات السابقة مقارنة بالطلبة الجامعيين أو الكادر الأكاديمي.
   - يسهم في بناء إطار معرفي يساعد الباحثين في فهم العلاقة بين الوعي بالأمم السيبراني والممارسات الفعلية في البيئة الأكاديمية.
   - قد يفتح المجال أمام دراسات مستقبلية تتناول جوانب أخرى.
2. **الأهمية التطبيقية:**
   - يقدم البحث بيانات واقعية يمكن أن تستفيد منها إدارات كليات التربية في وضع سياسات وبرامج تدريبية لتعزيز ثقافة الأمن السيبراني لدى طلبة الدراسات العليا.
   - يساعد في تحديد الثغرات السلوكية والتقنية التي قد تعرض الطلبة لمخاطر أمنية، مما يمكّن المؤسسات التعليمية من تطوير إجراءات وقائية فعالة.
   - يسهم في رفع مستوى الأمان الرقمي في بيئة التعليم العالي، بما ينعكس إيجاباً على جودة البحث العلمي وحماية الملكية الفكرية.
   - يمكن أن يشكل أساساً لتصميم حملات توعية أو مقررات دراسية تدمج مفاهيم الأمن السيبراني في برامج الدراسات العليا.

4. أهداف البحث:

يهدف هذا البحث إلى تحقيق مجموعة من الأهداف التي تسعى إلى فهم وتحليل واقع ممارسات طلبة الدراسات العليا في كلية التربية لإجراءات الأمن السيبراني، ويمكن تحديدها فيما يأتي:

1. تعرف مستوى وعي طلبة الدراسات العليا في كلية التربية في جامعة دمشق بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية.
2. تحليل الممارسات الفعلية التي يقوم بها طلبة الدراسات العليا عند استخدامهم للتقنيات الرقمية في ضوء إجراءات الأمن السيبراني.
3. الكشف عن أبرز التحديات والصعوبات التي تواجه الطلبة في الالتزام بإجراءات الأمن السيبراني.
4. دراسة الفروق في مستوى وعي طلبة الدراسات العليا بالأمن السيبراني وممارساتهم الفعلية لهذه الممارسات وفقاً لمتغيري المرحلة الدراسية، والخبرة التقنية.
5. تقديم توصيات عملية تسهم في تعزيز ثقافة الأمن السيبراني لدى طلبة الدراسات العليا في كليات التربية.

5. أسئلة البحث:

ينطلق هذا البحث من السؤال الرئيس الآتي:
ما مستوى وعي طلبة الدراسات العليا في كلية التربية بجامعة دمشق بإجراءات الأمن السيبراني وما الممارسات الفعلية المتبعة عند استخدامهم للتقنيات الرقمية من وجهة نظر الطلبة أنفسهم؟

ويتفرع عنه الأسئلة الفرعية التالية:

1. ما مستوى وعي طلبة الدراسات العليا في كلية التربية في جامعة دمشق بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية؟
2. ما أبرز إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية؟
3. ما التحديات والصعوبات التي تواجه طلبة الدراسات العليا في كلية التربية في جامعة دمشق في الالتزام بإجراءات الأمن السيبراني؟
4. ما المقترحات التي يمكن أن تسهم في تعزيز ثقافة الأمن السيبراني لدى طلبة الدراسات العليا في كليات التربية؟

6. فرضيات البحث:

يتحقق البحث من صحة الفرضيات الآتية:

1. لا توجد فروق ذات دلالة إحصائية عند مستوى 0.05 فيما يتعلق بمستوى وعي طلبة الدراسات العليا بإجراءات الأمن السيبراني تعزى لمتغير المرحلة الدراسية (ماجستير/ دكتوراه).
2. لا توجد فروق ذات دلالة إحصائية عند مستوى 0.05 فيما يتعلق بمستوى إجراءات الأمن السيبراني التي يتبعها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية تعزى لمتغير الخبرة التقنية (مبتدئ- متوسط- متقدم).
3. لا توجد علاقة ذات دلالة إحصائية عند مستوى دلالة (0.05) بين مستوى وعي طلبة الدراسات العليا بالأمن السيبراني ومستوى ممارساتهم الفعلية لهذه الإجراءات عند استخدامهم للتقنيات الرقمية في كلية التربية في جامعة دمشق من وجهة نظر الطلبة أنفسهم.

7. حدود البحث:

لتحديد نطاق الدراسة وضبط متغيراتها، يلتزم هذا البحث بالحدود الآتية:

1. **الحدود البشرية والمكانية**: يشمل البحث طلبة الدراسات العليا (ماجستير ودكتوراه) المسجلين في كلية التربية في جامعة دمشق خلال الفصل الدراسي.
2. **الحدود الزمانية**: تم تنفيذ البحث خلال العام الدراسي 2026/2025م.
3. **الحدود العلمية**: يركز البحث على تعرف مستوى الوعي بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية، وتحليل الممارسات الفعلية التي يقوم بها طلبة الدراسات العليا عند استخدامهم للتقنيات الرقمية في ضوء إجراءات الأمن السيبراني، والكشف عن أبرز التحديات والصعوبات التي تواجه الطلبة في الالتزام بإجراءات الأمن السيبراني.

8. مصطلحات البحث وتعريفاته الإجرائية:

الأمن السيبراني (Cybersecurity): "مجموعة من الوسائل والأساليب التقنية، والعمليات، والإجراءات الإلكترونية، والتنظيمية والإدارية، والآليات والبرامج والتطبيقات الرقمية، التي توفر الحماية والسلامة لأنظمة المعلومات والبيانات، والشبكات، والمنصات، وأجهزة الحواسيب والأجهزة الذكية، من التهديدات والأخطار والجرائم الإلكترونية، وتأمينها من الدخول غير المصرح به، وسوء الاستخدام، وتهديد سريتها وخصوصيتها في الفضاء السيبراني الواسع" (حنتولي والزبون، 2025، 18).

ويعرف الباحث الأمن السيبراني إجرائياً: بأنه مجموعة الإجراءات والممارسات التقنية التي يتبعها طلبة الدراسات العليا لحماية أجهزتهم، وحساباتهم، وبياناتهم الرقمية من الاختراق أو التهديدات الإلكترونية أثناء استخدامهم للتقنيات الرقمية في البيئة الأكاديمية.

الوعي بالأمن السيبراني: التصور الفكري والصورة الذهنية التي يحملها طلاب الجامعات، في الجوانب المختلفة ذات الصلة بالوعي بمفاهيم الأمن السيبراني، وطرق الوقاية من جرائم الفضاء السيبراني (الطيب وأخرون، 2025، 5).

ويعرف الباحث الوعي الأمني السيبراني إجرائياً: بأنه مستوى إدراك طلبة الدراسات العليا في كلية التربية لأهمية الأمن السيبراني، ومعرفتهم بالمخاطر المحتملة، والإجراءات الوقائية اللازمة لحماية المعلومات والبيانات في الفضاء الرقمي.

ويعرف الباحث ممارسات الأمن السيبراني إجرائياً: بأنها السلوكيات والإجراءات العملية التي يقوم بها الدراسات العليا في كلية التربية عند التعامل مع الأجهزة والبرمجيات والشبكات، مثل استخدام كلمات مرور قوية، تحديث البرامج، تجنب الروابط المشبوهة، وتفعيل أدوات الحماية.

ويعرف الباحث طلبة الدراسات العليا (graduate students) إجرائياً بأنهم: الطلبة المسجلين في برامج الماجستير والدكتوراه الأكاديمية في كلية التربية في جامعة دمشق بموجب مفاضلة الدراسات العليا.

9. الإطار النظري والدراسات السابقة:

أولاً-الإطار النظري:

ظهر مصطلح الأمن السيبراني (Cybersecurity) في مطلع تسعينيات القرن الماضي، حين بدأ الباحثون والمتخصصون في علوم الحاسوب وتقنية المعلومات بالبحث عن حلول وإجراءات تحد من المخاطر والتهديدات التي تواجه الحواسيب والشبكات وأنظمتها. ويعود أصل المصطلح إلى مفهوم "السيبرانية"، المشتق من كلمة *Cyber* المرتبطة بمصطلح *Cybernetics* ذي الجذور اليونانية، والذي يعني "التوجيه والتحكم". وقد استخدم نوربرت وينر الكلمة اليونانية القديمة *Kybernetes* التي تعني "الربان"، أي الشخص الذي يقود دفة السفينة، لوصف مبدأ إدارة وتوجيه الأنظمة والآلات، وهو ما تُرجم لاحقًا إلى الإنجليزية بمصطلح *Cybernetics* (Beer, 2002).

وقد تناولت الأدبيات العلمية مفهوم الأمن السيبراني بتعريفات متعددة. فقد عرّفته المفوضية الأوروبية بأنه "الأنشطة اللازمة لحماية الشبكات وأنظمة المعلومات ومستخدميها، وغيرهم من الأشخاص المتأثرين بالتهديدات السيبرانية، من خلال حماية البيانات .(European Commission, 2020, p.15) "كما يُعرف بأنه التدابير المتخذة لحماية الحواسيب والشبكات من الوصول غير المصرح به، بما يضمن سلامة المعلومات وأمنها، ويشمل التدخلات التقنية التي تحمي البيانات ومعلومات الهوية والأجهزة من الاختراق أو الضرر.(Richardson et al., 2020)

وقد عرّفه السعادات والتميمي (2022) بأنه "الوعي بالممارسات غير المشروعة التي تستهدف الاختراق أو التعطيل أو التعديل أو الاستغلال غير المصرح به للبيانات والمعلومات، بهدف الوقاية منها" (ص. 249). بينما يرى أبو حسين (2021) أن الأمن السيبراني هو "مجال يتعلق بإجراءات ومعايير الحماية المفروض الالتزام بها لمواجهة التهديدات والحد من آثارها في أسوأ الأحوال" (ص. 18). أما حنتولي والزبون (2025) فقد وسّعا المفهوم ليشمل "مجموعة من الوسائل والأساليب التقنية، والعمليات، والإجراءات الإلكترونية، والتنظيمية والإدارية، والآليات والبرامج والتطبيقات الرقمية، التي توفر الحماية والسلامة لأنظمة المعلومات والبيانات، والشبكات، والمنصات، وأجهزة الحواسيب والأجهزة الذكية، من التهديدات والأخطار والجرائم الإلكترونية، وتأمينها من الدخول غير المصرح به، وسوء الاستخدام، وتهديد سريتها وخصوصيتها في الفضاء السيبراني الواسع" (ص. 18). ويضيف حصوة والقضاة (2023) أن الأمن السيبراني يتضمن "الإجراءات والتقنيات التي تهدف إلى حماية البيانات والأنظمة من أي تدخل غير مشروع قد يؤدي إلى تعطيل الأجهزة أو التلاعب بالمعلومات" (ص. 64).

مما سبق نجد أن الأمن السيبراني هو مجموعة من الإجراءات والتدابير التقنية والتنظيمية والإدارية التي تهدف إلى حماية أنظمة المعلومات، والشبكات، والأجهزة الرقمية، والبيانات المخزنة أو المتبادلة عبر الفضاء الإلكتروني، من أي وصول غير مصرح به أو استغلال غير مشروع، وذلك من خلال ضمان سرية المعلومات، وسلامتها، وتوا، وسلامتها، وتوافرها، والحد من المخاطر والتهديدات السيبرانية التي قد تؤدي إلى تعطيل الخدمات أو الإضرار بالمصالح الفردية والمؤسسية.

وهناك أربعة أنواع شائعة من تهديدات الأمن السيبراني.

- التصيد الاحتيالي: هو إرسال رسائل بريد إلكتروني مزيفة تبدو وكأنها واردة من مصدر موثوق. يهدف التصيد الاحتيالي إلى سرقة معلومات سرية مثل أرقام بطاقات الائتمان وبيانات تسجيل الدخول. وهو أكثر أنواع التهديدات السيبرانية شيوعًا. يمكن حماية النفس من هذا النوع من التهديدات بالتعامل السليم مع رسائل البريد الإلكتروني من مصادر مجهولة أو باستخدام حلول تقنية لتصفية الرسائل الإلكترونية الضارة.
- البرمجيات الخبيثة: هي نوع من البرامج المصممة للوصول غير المصرح به إلى جهاز الكمبيوتر أو إلحاق الضرر به.
- برامج الفدية: هي نوع من البرمجيات الخبيثة. تهدف إلى ابتزاز الأموال عن طريق منع الوصول إلى الملفات أو نظام الكمبيوتر قبل دفع الفدية. دفع الفدية لا يضمن استعادة الملفات أو الجهاز.
- الهندسة الاجتماعية: هي أسلوب يستخدمه المهاجمون لتوجيه المستخدمين نحو كشف معلوماتهم الخاصة. قد يتصلون بشأن رسوم مالية أو للوصول إلى معلوماتهم الشخصية. قد يتم دمج الهندسة الاجتماعية مع أي من التهديدات المذكورة أعلاه لجعل المستخدمين أكثر عرضة للنقر على الروابط أو تنزيل البرامج الضارة أو الاعتقاد بأن المصدر الخبيث حقيقي (CISCO, 2020).

تتفق معظم الدراسات على أن الأمن السيبراني يمثل عنصراً جوهرياً في العصر الرقمي، خاصة في المؤسسات الأكاديمية التي تعتمد بشكل واسع على التكنولوجيا والاتصالات الإلكترونية. وقد أبرزت الأدبيات (Alhaif, 2023؛ Matyokurehwa et al., 2021؛ Wangen, 2021؛ العتيبي، 2022؛ الخضري وآخرون، 2020؛ سراج، 2022) أهمية الأمن السيبراني في الجامعات من خلال النقاط التالية:

- حماية البيانات الحساسة :مثل السجلات الطبية والمالية والأكاديمية، وضمان سريتها وعدم وصول غير المخولين إليها.
- الحفاظ على سلامة الأنظمة الأكاديمية :حماية الأنظمة الحاسوبية المعقدة من الهجمات التي قد تعطل العملية التعليمية.
- الحفاظ على سمعة المؤسسة :منع تسريب المعلومات الحساسة الذي قد يؤثر سلبًا على سمعة الجامعة واعتماديتها.
- حماية الأبحاث العلمية :صون البيانات البحثية والنتائج العلمية من الاختراقات التي تهدد مصداقيتها.
- تعزيز الثقة والاعتمادية :بناء ثقة أكبر لدى الطلاب وأعضاء الهيئة التدريسية من خلال الالتزام بإجراءات الحماية.
- الحد من التكاليف والخسائر :تقليل الأضرار المالية الناتجة عن الهجمات السيبرانية أو تسريب البيانات.
- حماية الخصوصية الشخصية :ضمان أمن المعلومات الشخصية للأفراد في بيئة التواصل الرقمي.
- مواجهة الهجمات المتطورة :التصدي للتطور المستمر في تقنيات القرصنة والبرمجيات الخبيثة.

وهناك مجموعة من الإجراءات التي ينبغي على مستخدمي الإنترنت الالتزام بها لتعزيز الأمن السيبراني أشارت إليها دراسة تيواري وأخرون (Tiwari, et al, 2016)، منها:

- تحديث جدران الحماية بشكل دوري لضمان حماية البنية التحتية المعلوماتية.
- ضبط إعدادات الحاسوب وشبكة الإنترنت بما يتوافق مع معايير الأمان.
- اختيار كلمات مرور قوية وتحديثها بانتظام (مرة أو مرتين شهريًا على الأقل).
- تفعيل آليات التحقق الأمني في البريد الإلكتروني ومواقع التواصل الاجتماعي.
- تجنب الاستجابة للرسائل مجهولة المصدر.
- استخدام برامج الحماية ومضادات الفيروسات وتحديثها باستمرار.
- حماية المعلومات الشخصية ومنع مشاركتها عبر البريد الإلكتروني أو المنصات العامة.

ثانياً- دراسات سابقة:

دراسة (حنتولي والزبون، 2025) بعنوان: واقع وعي الطلبة في الجامعات الأردنية بثقافة الأمن السيبراني ومفاهيمه ومجالاته من وجهة نظر الطلبة أنفسهم.

هدفت الدراسة إلى التعرف على واقع وعي الطلبة في الجامعات الأردنية بثقافة الأمن السيبراني ومفاهيمه ومجالاته من وجهة نظر الطلبة أنفسهم. استخدمت الدراسة المنهج الوصفي المسحي، وطبقت على عينة مكونة من (361) طالباً وطالبة من طلبة الجامعات الأردنية، تم اختيارهم بالطريقة الطبقية العشوائية. واستخدمت الاستبانة كأداة لجمع البيانات، حيث تكونت من (26) فقرة، وتم التأكد من صدقها وثباتها. أشارت النتائج إلى أن واقع وعي الطلبة في الجامعات الأردنية بثقافة الأمن السيبراني ومفاهيمه ومجالاته من وجهة نظر الطلبة أنفسهم جاء متوسطاً، وعدم وجود فروق ذات دلالة إحصائية عند مستوى ($a<0.05$) تعزى لأثر متغيرات الجنس المستوى الدراسي الكلية على تقديرات عينة الدراسة لواقع وعي الطلبة في الجامعات الأردنية بثقافة الأمن السيبراني ومفاهيمه ومجالاته.

دراسة ديوري (Deuri, 2025) بعنوان: تعزيز الوعي السيبراني: دور مؤسسات التعليم العالي في بناء جيل يتمتع بالأمن الرقمي

هدفت الدراسة إلى تقييم الوضع الحالي لتعليم الأمن السيبراني في مؤسسات التعليم العالي، واستكشاف مواقف الطلاب وتصوراتهم فيما يتعلق بمخاطر الأمن السيبراني والسلامة على الإنترنت، واقتراح استراتيجيات لتعزيز تعليم الأمن السيبراني والتوعية به في الجامعات، وباستخدام منهج البحث الوصفي، تم تصميم استبانة لتقييم وعي الطلاب بالأمن السيبراني، وتصوراتهم، وممارساتهم في مجال السلامة على الإنترنت، كما أُجريت مقابلات شبه مُهيكلة مع أعضاء هيئة التدريس وموظفي تكنولوجيا المعلومات والإداريين لفهم دور المؤسسات في التوعية بالأمن السيبراني وسياسات الأمن الرقمي، حيث بلغت العينة 300 طالب دراسات عليا، وأعضاء هيئة تدريس، وموظفي تقنية المعلومات، وإداريين في سبع كليات في مقاطعة ديماجي. أشارت النتائج إلى انخفاض مستوى الوعي بالأمن السيبراني وضعف عادات الأمان لدى الطلاب، 52٪ فقط يُدركون عمليات الاحتيال الإلكتروني، و60٪ يُشاركون كلمات المرور، وهو أمرٌ مُقلق، مما يزيد من خطر تعرضهم للهجمات السيبرانية. كما أشارت إلى ثغراتٍ جوهرية في تعليم الأمن السيبراني في مؤسسات التعليم العالي. فبينما تُقدم (42.86٪) من الكليات دوراتٍ في الأمن السيبراني، تفتقر الغالبية العظمى (57.14٪) إلى برامج تدريبية رسمية، مما يجعل الطلاب عرضةً للتهديدات السيبرانية مثل التصيد الاحتيالي، واختراقات البيانات، وسرقة الهوية. كما كشفت الدراسة عن التحديات المؤسسية، وهي محدودية دمج الأمن السيبراني في المناهج الدراسية، وعدم كفاية الموارد، وعدم كفاية سياسات الأمن السيبراني. وبناءً على هذه النتائج، تتضمن التوصيات دمج دورات الأمن السيبراني في المناهج الدراسية، وتنظيم

برامج توعية، وتعزيز السياسات المؤسسية، وتحسين البنية التحتية للأمن السيبراني. ستساهم هذه المبادرات في بناء مجتمع طلابي واعٍ بالأمن السيبراني وضمان بيئة أكاديمية أكثر أماناً.

دراسة (الطيب وأخرون، 2025) بعنوان: درجة وعي طالبات الدراسات العليا في جامعة الملك سعود بالأمن السيبراني.

هدفت الدراسة إلى تعرف 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.

دراسة يغيت (Yiğit, 2025) بعنوان: دور الوعي الذهني كعامل مُؤثر في سلوكيات الأمن السيبراني لدى طلاب المرحلة الجامعية الأولى

هدفت الدراسة إلى بحث الأثر التنبؤي للوعي الذهني على سلوكيات الأمن السيبراني لدى طلاب المرحلة الجامعية الأولى، أُجريت الدراسة باستخدام المنهج الوصفي، وشملت 179 طالباً جامعياً مسجلين في جامعة حكومية، جُمعت بيانات الدراسة من خلال استمارة إلكترونية باستخدام "مقياس توفير الأمن السيبراني الشخصي" و"مقياس الوعي الذهني". وأظهرت النتائج عدم وجود فروق ذات دلالة إحصائية في سلوكيات الأمن السيبراني بين الطلاب والطالبات. لوحظت اختلافات بين الأقسام في سلوكيات الأمن السيبراني فقط بين قسمي إعداد معلمي الرياضيات للمرحلة الابتدائية وإعداد معلمي اللغة التركية، حيث أظهر طلاب القسم الأول سلوكيات أفضل. ولم تُلاحظ أي اختلافات في سلوكيات الأمن السيبراني بين المراحل الدراسية المختلفة. كما وُجد ارتباط إيجابي متوسط بين الوعي الذهني وسلوكيات الأمن السيبراني، حيث يُفسر الوعي الذهني 9.4% من التباين في سلوكيات الأمن السيبراني. وأخيرًا، كشف تحليل العوامل المُعدِّلة أن الجنس والقسم والمرحلة الدراسية لم تؤثر بشكلٍ كبير على هذا التأثير.

دراسة بوك وأخرون (Booc,et al, 2024) بعنوان: الوعي بالأمن السيبراني وسلوكيات الأمن السيبراني لدى طلاب المدارس الثانوية في مدينة دافاو: دور وسيط للتحكم السلوكي المُدرك

هدفت الدراسة إلى تحديد الدور الوسيط للتحكم السلوكي المُدرَك في العلاقة بين الوعي بالأمن السيبراني وسلوكيات الأمن السيبراني لدى طلاب المرحلة الثانوية في مدينة دافاو، الفلبين، وذلك بالاستناد إلى نظرية السلوك المخطط. وباستخدام منهج كمي، جُمعت البيانات من خلال استبيان وُزِّع على 100 طالب وطالبة في مدرسة ثانوية خاصة بمدينة دافاو. واستُخدمت مقاييس معتمدة لتقييم الوعي بالأمن السيبراني، والتحكم السلوكي المُدرَك، وسلوكيات الأمن السيبراني، مع الالتزام التام بالاعتبارات الأخلاقية وسرية البيانات. وكشفت الدراسة أن طلاب المرحلة الثانوية يُظهرون عموماً مستوى عالياً من الوعي بالأمن السيبراني، والتحكم السلوكي المُدرك، والسلوكيات المسؤولة في مجال الأمن السيبراني. ومع ذلك، لا يزال هناك مجال للتحسين، لا سيما في تعزيز السلوكيات المسؤولة في هذا المجال. علاوة على ذلك، تكشف الدراسة عن وجود علاقة إيجابية متوسطة وذات دلالة إحصائية بين الوعي بالأمن السيبراني والسلوكيات المسؤولة في هذا المجال، مما يشير إلى أنه كلما زاد الوعي، زاد السلوك المسؤول في مجال الأمن السيبراني. بالإضافة إلى ذلك، توجد علاقة ذات دلالة إحصائية بين التحكم السلوكي المُدرك والسلوكيات المسؤولة في هذا المجال، مما يوحي بأن الطلاب الذين يشعرون بمزيد من التحكم في تصرفاتهم المتعلقة بالأمن السيبراني يميلون إلى إظهار سلوكيات أفضل في هذا المجال. كما تُبرز النتائج الدور الوسيط للتحكم السلوكي المُدرك في العلاقة بين الوعي بالأمن السيبراني والسلوكيات المسؤولة في هذا المجال. وهذا يُشير إلى أن التحكم السلوكي المُدرك يلعب دوراً حاسماً في التأثير على كيفية ترجمة الوعي بالأمن السيبراني إلى سلوكيات فعلية لدى طلاب المرحلة الثانوية.

دراسة (زيدان، 2024) بعنوان: تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية (تصور مقترح)

هدفت الدراسة إلى الوقوف على الإطار المفاهيمي للتربية الاعلامية الرقمية بالجامعات، وتحديد أهم كفايات التربية الإعلامية الرقمية اللازمة لطلاب الجامعات لتنمية ثقافة الأمن السيبراني، والكشف عن الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية، وأساليب تنميتها ووضع تصور مقترح لتنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية. اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات. تكونت عينة الدراسة من (347) طالباً من كليات التربية،

التجارة وإدارة الأعمال، السياحة والفنادق في جامعة حلوان، وتوصلت الدراسة إلى عدة نتائج من أهمها: ضعف تركيز اللوائح والقوانين الجامعية على قضايا وممارسات الأمن السيبراني بالجامعات، ونقص المتخصصين في مجال الأمن السيبراني في الجامعات، مما يصعب تنفيذ استراتيجيات الأمن السيبراني بشكل فعال، وضعف وعي الطلاب بكيفية استخدام شبكات الإنترنت العامة بشكل آمن ومشفر لحماية بياناتهم الحساسة من الاختراق والسرقة، ونقص البرامج التعليمية والتدريبية المتخصصة في مجال الأمن السيبراني، وضعف وعي الطلاب بأهمية استخدام كلمات مرور قوية وتغييرها بشكل منتظم لتأمين حساباتهم الشخصية والبيانات الحساسة من التهديدات السيبرانية والاختراقات، وإغفال بعض الطلاب إجراءات تحديث البرامج والتطبيقات الضرورية لمعالجة الثغرات الأمنية.

دراسة أونيما وأخرون (Onyema,et al, 2021) بعنوان: الوعي بالأمن السيبراني بين طلاب المرحلة الجامعية الأولى في إنوغو، نيجيريا.

هدفت الدراسة إلى الوقوف على مستوى الوعي بالأمن السيبراني بين طلاب المرحلة الجامعية الأولى من أربع مؤسسات جامعية مختارة في إينوجو، نيجيريا. اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات من خلال توزيعها على 200 من طلاب المرحلة الجامعية الأولى في أربع مؤسسات تعليمية عليا مختلفة في إينوجو، نيجيريا (جامعة كول سيتي إينوجو؛ جامعة ولاية إينوجو للعلوم والتكنولوجيا؛ كلية ولاية إينوجو التقنية للتربية؛ ومعهد الإدارة والتكنولوجيا، إينوجو). أظهرت النتائج أن معظم المشاركين لديهم معرفة أساسية بالتهديدات السيبرانية مثل الفيروسات، والبريد العشوائي، والتصيّد الاحتيالي، وهجمات حجب الخدمة، وسرقة الهوية، وحقن SQL، وانتحال الهوية، والاختراق غير القانوني، لكنهم يجهلون كيفية حماية أنفسهم من التهديدات والهجمات الإلكترونية. كما تم إثبات وجود علاقة إحصائية دالة بين معرفة المشاركين بالأمن السيبراني وتصوراتهم تجاه تعليم الأمن السيبراني، وبين معرفتهم بالأمن السيبراني واهتمامهم بتعليمه. وقد تم تحديد نقص الكفاءات في مجال الأمن السيبراني، وضيق الوقت، واستبعاد الأمن السيبراني من المقررات الدراسية غير الحاسوبية، وضعف المعرفة بأساسيات الحوسبة، وقلة الموجهين ذوي الخبرة العملية في الأمن السيبراني، ونقص البنية التحتية الداعمة، والجهل، كبعض العوائق التي تعرقل تعليم الأمن السيبراني. نخلص إلى ضرورة دمج الأمن السيبراني في المناهج الدراسية لإعداد الطلاب لمواجهة واقع الأمن السيبراني المعاصر، وتعزيز قدراتهم على حماية أنفسهم والآخرين من الجرائم والتجسس في الفضاء السيبراني.

التعليق على الدراسات السابقة:

يتفق البحث الحالي مع غالبية الدراسات السابقة في تركيزه على موضوع الوعي بالأمن السيبراني لدى الفئات التعليمية، كما يشترك معها في اعتماد المنهج الوصفي المسحي كإطار منهجي، وفي استخدام الاستبانة كأداة رئيسية لجمع البيانات، وهو ما يعكس انسجاماً في التوجهات البحثية في هذا المجال.

وفي المقابل، يختلف البحث الحالي عن الدراسات السابقة من حيث الفئة المستهدفة؛ إذ ركزت بعض الدراسات مثل دراسة بوك وأخرون (Booc,et al, 2024) على طلبة المرحلة الثانوية، بينما تناولت دراسات أخرى مثل (حنتولي والزبون، 2025)، ويغيت (Yiğit, 2025)، و(زيدان، 2024)، وأونيما وأخرون (Onyema,et al, 2021) طلبة المرحلة الجامعية الأولى، في حين اهتمت دراسة كل من (الطيب وآخرون، 2025)، (ديوري، 2025) بطلبة الدراسات العليا وأعضاء هيئة التدريس والإداريين بشكل عام. أما البحث الحالي فيتميز بتركيزه على طلبة الدراسات العليا (الماجستير والدكتوراه) في كلية التربية بجامعة دمشق، وهو نطاق جغرافي وأكاديمي محدد لم يُتناول سابقاً في الأدبيات، إضافة إلى أن معظم الدراسات السابقة أجريت في بيئات تعليمية خارج سورية.

كما أن غالبية الدراسات السابقة انحصرت في قياس مستوى الوعي أو التصورات النظرية، دون التطرق بشكل متكامل إلى العلاقة بين الوعي والممارسات الفعلية للأمن السيبراني، وهو ما يسعى البحث الحالي إلى معالجته من خلال تحليل مستوى الوعي والممارسات المتبعة لدى طلبة الدراسات العليا، بما يسد فجوة بحثية مهمة في السياق السوري، ويضيف بعداً عملياً لم يتم التركيز عليه في معظم الدراسات السابقة.

وقد استفاد الباحث من الدراسات السابقة في تصميم أداة البحث، وصياغة الإطار النظري، إضافة إلى الاستفادة من التوصيات والمقترحات الواردة فيها لربطها بنتائج البحث الحالي.

10. منهجية البحث:

أولاً- منهج البحث:

اعتمد الباحث على المنهج الوصفي المسحي؛ لكونه الأنسب لدراسة واقع ممارسات طلبة الدراسات العليا في كلية التربية لإجراءات الأمن السيبراني، حيث يتيح جمع بيانات كمية من عينة كبيرة وتحليلها إحصائياً للوصول إلى استنتاجات دقيقة. حيث قام الباحث من خلال هذا المنهج بإعداد استبانة لتقويم واقع الأمن السيبراني في كلية التربية في جامعة دمشق متمثلة بثلاثة محاور هي: (المحور الأول: يشخص مستوى وعي طلبة الدراسات العليا بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية، والمحور الثاني: يشخص أبرز إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية، والمحور الثالث: يشخص

التحديات والصعوبات التي تواجه طلبة الدراسات العليا في كلية التربية في جامعة دمشق في الالتزام بإجراءات الأمن السيبراني)، ثم طبقت هذه الاستبانة على أفراد عينة البحث وجمعت البيانات منهم وتمَّ وصفها وتحليلها من خلال العمليات الإحصائية المناسبة ثم نوقشت وفسّرت في ضوء الأدب السابق والواقع الميداني.

ثانياً- مجتمع البحث وعينته:

- **المجتمع الأصلي:** تكوّن المجتمع الأصلي للبحث من جميع طلبة الدراسات العليا (ماجستير ودكتوراه) في كلية التربية في جامعة دمشق خلال العام الدراسي 2025-2026، والبالغ عددهم حسب إحصائيات كلية التربية في جامعة دمشق 450 طالباً وطالبة.
- **العينة:** اختيرت عينة البحث بالطريقة العشوائية الطبقية، حيث تم تقسيم مجتمع البحث إلى طبقتين: الطبقة الأولى تشمل طلبة الماجستير، والطبقة الثانية تشمل طلبة الدكتوراه، وقد تم سحب عينة عشوائية ضمن كل طبقة بحيث تتناسب مع حجم المجتمع الأصلي. فبلغت عينة البحث 205 طالباً وطالبة أي ما نسبته 45% تقريباً من حجم المجتمع الأصلي.

ثالثاً- أداة البحث:

تطلب تحقيق أهداف البحث والتحقق من فرضياته استخدام أداة الاستبانة من (إعداد الباحث)، وقد تم إعداد الاستبانة في صورتها الأولية بعد الاطلاع على الأدب النظري والدراسات السابقة والاطلاع على بعض أدوات البحث المتعلقة بالأمن السيبراني. وفي ضوء ذلك تم إعداد الاستبانة في صورتها الأولية مكونة من ثلاثة محاور: المحور الأول: يشخص مستوى وعي طلبة الدراسات العليا بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية، والمحور الثاني: يشخص أبرز إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية، والمحور الثالث: يشخص التحديات والصعوبات التي تواجه طلبة الدراسات العليا في كلية التربية في جامعة دمشق في الالتزام بإجراءات الأمن السيبراني. وتحديد بدائل الإجابة بـ (دائماً، عالباً، أحياناً، نادراً، أبداً). بعد ذلك عُرضت الاستبانة على مجموعة من السادة المحكمين من أصحاب الخبرة والاختصاص، وذلك للتأكد من صلاحية الاستبانة علمياً وتمثيلها للغرض الذي وضعت من أجله، والاستفادة من ملاحظتهم وآرائهم ومقترحاتهم في تعديل بعض العبارات الموجودة في الاستبانة، وقدم المحكّمون ملاحظاتهم التي بيّنوا فيها ضرورة إعادة النظر في صياغة بعض العبارات من حيث المعنى واللغة، وحذف بعض العبارات التي وجد أنها تتشابه مع عبارات أخرى، ولا تتناسب تماماً مع أهداف البحث، حيث تم تعديل عدد من عبارات الاستبانة وحذف 4 عبارات، والجدول (1) يوضّح العبارات التي تم حذفها في استبانة واقع الأمن السيبراني وفقاً لآراء السادة المحكّمين.

جدول (1) العبارات التي تم حذفها في استبانة واقع الأمن السيبراني وفقاً لآراء السادة المحكّمين.

أشارك أقل قدر ممكن من البيانات الشخصية عبر الإنترنت
أقيّم مخاطر مشاركة الملفات عبر روابط عامة قبل المشاركة
أشعر بالثقة في قدرتي على اتخاذ قرارات رقمية آمنة
أستوعب مفهوم المصادقة متعددة العوامل وأين يجب تفعيلها

بعد الأخذ بملاحظات السادة المحكمين بلغ المجموع الكلي لعبارات الاستبانة 38 عبارة. وبعد تحكيم الاستبانة طُبقت على عينة استطلاعية قوامها 20 طالباً وطالبة من طلبة الدراسات العليا في كلية التربية في جامعة دمشق وهم من خارج عينة البحث الأساسية، وذلك للتحقق من الخصائص السيكومترية للاستبانة. فقد جرى التأكد من الصدق البنيوي بإيجاد معاملات الارتباط بين محاور الاستبانة بعضها ببعض وكذلك بين محاور الاستبانة والدرجة الكلية للاستبانة. والجدول الآتي يوضح نتائج معاملات الارتباط.

جدول (2) معاملات الارتباط بين درجة كل محور من محاور استبانة واقع الأمن السيبراني مع المحاور الأخرى ومع الدرجة الكلية للاستبانة

الاستبانة ومحاورها	الوعي بالأمن السيبراني	ممارسات الأمن السيبراني	تحديات الأمن السيبراني	الدرجة الكلية
الوعي بالأمن السيبراني	1	.868**	.946**	.978**
ممارسات الأمن السيبراني	-	1	.805**	.934**
تحديات الأمن السيبراني	-	-	1	.957**

(**) دال عند مستوى دلالة 0,01

يلاحظ من الجدول (2) أن جميع معاملات الارتباط بين محاور الاستبانة بعضها مع بعض وبين المحاور والدرجة الكلية للاستبانة دالة إحصائياً عند مستوى دلالة (0.01) مما يشير إلى أن هذه المحاور مرتبطة مع بعضها بعضاً ومرتبطة أيضاً مع الدرجة الكلية، وأنها تقيس ما وضعت لقياسه وهذا يؤكد الصدق البنيوي لهذه المحاور والاستبانة ككل.

كما تم دراسة ثبات الاستبانة بطريقتين اثنتين من خلال حساب معامل الاتساق الداخلي للعينة الاستطلاعية نفسها في التطبيق الأول باستخدام معادلة ألفا كرونباخ، كما في الجدول (3)، ومن خلال استخراج معامل الثبات بطريقة الإعادة لاستبانة واقع الأمن السيبراني على (20) من العينة الاستطلاعية السابقة من خلال إعادة تطبيق الاستبانة للمرة الثانية عليهم بعد مضي أسبوعين من التطبيق الأول، كما في الجدول (3).

جدول(3) معاملات ثبات ألفا كرونباخ ومعاملات ارتباط الثبات بالإعادة لاستبانة واقع الأمن السيبراني

استبانة واقع الأمن السيبراني ومحاورها	عدد بنود الاستبانة	ألفا كرونباخ	معامل ارتباط الثبات بالإعادة
الوعي بالأمن السيبراني	12	.854	0.862**
ممارسات الأمن السيبراني	16	.891	0.871**
تحديات الأمن السيبراني	10	.914	0.880**
الاستبانة ككل	38	.958	0.874**

(**) دال عند مستوى دلالة 0.01

يتضح من الجدول (3) أن معامل الاتساق الداخلي بمعادلة ألفا كرونباخ لبنود استبانة واقع الأمن السيبراني على الدرجة الكلية بلغت (958.) وهو معامل ثبات مناسب لأغراض الدراسة الحالية، أما معامل ارتباط الثبات بالإعادة للدرجة الكلية للاستبانة بلغ (874.) وهو معامل مناسب لأغراض الدراسة الحالية. يتضح مما سبق أن استبانة واقع الأمن السيبراني مناسبة من الصدق والثبات تجعلها صالحاً للاستخدام كأداة للدراسة الحالية.

وتكونت الاستبانة بصورتها النهائية من جزأين:

الجزء الأول: البيانات الأولية لأفراد عينة البحث ويمثل متغيرات البحث المستقلة وهي (المرحلة الدراسية، الخبرة التقنية).

الجزء الثاني: يتكون من ثلاثة محاور: المحور الأول: يشخص مستوى وعي طلبة الدراسات العليا بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية، والمحور الثاني: يشخص أبرز إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية، والمحور الثالث: يشخص التحديات والصعوبات التي تواجه طلبة الدراسات العليا في كلية التربية في جامعة دمشق في الالتزام بإجراءات الأمن السيبراني. وتحديد بدائل الإجابة بـ (دائماً، عالباً، أحياناً، نادراً، أبداً).

ولوضع معيار يبين مستويات كل من وعي وممارسة طلبة الدراسات العليا في كلية التربية في جامعة دمشق لإجراءات الأمن السيبراني، تم إجراء الخطوات الآتية:

حساب المدى وذلك بطرح أكبر قيمة في الاستبانة من أصغر قيمة (5-1=4).

حساب طول الفئة وذلك بتقسيم المدى وهو (4) على أكبر قيمة في الاستبانة وهي (5).

4 ÷ 5 = 0.8 (طول الفئة)

جدول (4) معيار مستويات كل من كل وعي وممارسة طلبة الدراسات العليا في كلية التربية في جامعة دمشق لإجراءات الأمن السيبراني وفقاً للمتوسطات الحسابية على كل عبارة في الاستبانة وعلى الدرجة الكلية

فئات المتوسط الحسابي للعبارة الواحدة	مستويات كل من كل وعي وممارسة طلبة الدراسات العليا في كلية التربية في جامعة دمشق لإجراءات الأمن السيبراني
5 – 4.21	مرتفع جداً
4.20 – 3.41	مرتفع
3.40 – 2.61	متوسط
2.60 – 1.81	منخفض
1.8 – 1	منخفض جداً

رابعاً- الأساليب الإحصائية المستخدمة:

- **الإحصاءات الوصفية:** المتوسطات، الانحراف المعياري، التكرارات، النسب المئوية.
- **اختبارات الفروق:** اختبار (t) لفحص الفروق بين الجنسين، واختبار (ANOVA) للفروق حسب المرحلة الدراسية والخبرة التقنية.
- **الارتباط:** معامل بيرسون لدراسة العلاقة بين مستوى الوعي والممارسات الفعلية.
- **برامج التحليل:** تم استخدام برنامج SPSS للتحليل الإحصائي.

11. عرض النتائج وتحليلها ومناقشتها:

أولاً- النتائج المتعلقة بالإجابة عن السؤال الأول: ما مستوى وعي طلبة الدراسات العليا في كلية التربية في جامعة دمشق بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية؟

للإجابة عن هذا السؤال قام الباحث بحساب المتوسطات الحسابية، والانحرافات المعيارية، وتحديد مستوى وعي طلبة الدراسات العليا في كلية التربية في جامعة دمشق بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية من

وجهة نظر الطلبة أنفسهم على الدرجة الكلية من خلال الرجوع إلى المعيار الذي وضع في الجدول (4)، ثم ترتيب العبارات من مستوى الوعي الأعلى إلى الأقل، والجدول الآتي يوضح النتائج التي تم التوصل إليها.

جدول (5) المتوسطات الحسابية والانحرافات المعيارية وترتيب مستويات وعي طلبة الدراسات العليا في كلية التربية في جامعة دمشق بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية من وجهة نظر الطلبة أنفسهم من الأعلى مستوى إلى الأقل

عبارات محور مستوى الوعي بالأمن السيبراني	المتوسط الحسابي	الانحراف المعياري	مستوى الوعي	الترتيب
1-أمتلك معرفة كافية بأنماط التهديدات السيبرانية الشائعة في البيئة الأكاديمية.	3.94	.755	مرتفع	9
2-أدرك أهمية استخدام وسائل حماية الحسابات مثل كلمات مرور قوية والتحقق بخطوتين.	4.02	.822	مرتفع	7
3-أدرك أن ضعف الإجراءات الأمنية أو استخدام أجهزة غير محمية يزيد من خطر الاختراق.	4.20	.848	مرتفع	3
4-أعلم أن الروابط المشبوهة قد تحتوي على برمجيات خبيثة.	4.01	1.026	مرتفع	8
5-أعرف مؤشرات رسائل التصيّد الاحتيالي في البريد الإلكتروني والمنصات التعليمية.	4.22	.671	مرتفع جداً	1
6-أميّز مواقع الويب الآمنة من خلال بروتوكولات HTTPS والشهادات الموثوقة.	4.21	.966	مرتفع جداً	2
7-أدرك أن الأمن السيبراني يشمل حماية الأجهزة والبرمجيات والبيانات معًا.	4.06	1.268	مرتفع	6
8-أعرف الإجراءات الأولية الواجب اتخاذها عند الاشتباه باختراق حسابي.	4.19	.957	مرتفع	4
9-أنتبه لعدم تخزين معلوماتي الشخصية على أجهزة غير جهازي الشخصي.	3.40	1.050	متوسط	12
10-أعي أن تسريب البيانات البحثية يشكل خطرًا على الملكية الفكرية.	4.10	1.017	مرتفع	5
11-أعرف أن تحديث البرامج بشكل دوري يقلل من المخاطر الأمنية.	3.53	1.215	مرتفع	11
12-أدرك أن مشاركة البيانات عبر شبكات عامة غير آمنة يعرضها للاختراق.	3.56	1.218	مرتفع	10
الدرجة الكلية	3.95	.984	مرتفع	-

يلاحظ من الجدول (5) أن مستوى وعي طلبة الدراسات العليا في كلية التربية بجامعة دمشق بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية جاء مرتفعاً، حيث بلغ المتوسط الحسابي الكلي (3.95)، مع انحراف معياري (.984). هذا يعني أن الطلبة يمتلكون إدراكاً جيداً لمخاطر الأمن السيبراني وطرق الحماية، لكن هناك بعض الجوانب التي تحتاج إلى تعزيز. وقد تبيّن أن أعلى مظاهر الوعي تمثلت في إدراك مؤشرات رسائل التصيّد الاحتيالي وتمييز المواقع الآمنة عبر بروتوكولاتHTTPS، إذ حققت هذه العبارات متوسطات تجاوزت (4.20) بمستوى مرتفع جداً، مما يعكس قوة الوعي المعرفي المتين لدى الطلبة بمفاهيم أمنية أساسية ترتبط بالسلوك اليومي في البيئة الأكاديمية (البريد، المنصات التعليمية، التصفح الآمن). ويمكن تفسير ذلك بأن هذه المهارات ترتبط ارتباطاً مباشراً بالتجارب الرقمية اليومية للطلبة في البيئة الأكاديمية، حيث يعتمدون بشكل كبير على البريد الإلكتروني والمنصات التعليمية للتواصل وتبادل الملفات، مما يجعلهم أكثر تعرضاً لمحاولات التصيّد والروابط غير الآمنة. هذا الاحتكاك العملي يولّد لديهم وعياً متزايداً بأهمية التحقق من الرسائل والمواقع قبل التفاعل معها، خاصة في ظل انتشار التحذيرات المؤسسية والدورات التوعوية التي تركز على هذه الجوانب الأساسية للأمن السيبراني.

في المقابل، ظهرت فجوات في السلوكيات الأمنية العملية، أبرزها ضعف الالتزام بعدم تخزين البيانات الشخصية على أجهزة غير شخصية، وتحديث البرامج بشكل دوري، وتجنب مشاركة البيانات عبر الشبكات العامة، حيث تراوحت متوسطاتها بين (3.40–3.56) بمستوى متوسط إلى مرتفع حدّي، مما يشير إلى عادات رقمية غير صائبة لدى شريحة معتبرة من الطلبة، ويمكن تفسير ذلك بأن هذه الممارسات ترتبط بسلوكيات وقائية تتطلب جهداً إضافياً واستمرارية من جانب الطالب، وليست مجرد معرفة نظرية. غالباً ما ينظر الطلبة إلى هذه الإجراءات على أنها ثانوية أو غير عاجلة مقارنة بمهامهم الأكاديمية، مما يؤدي إلى ضعف الالتزام بها. كما أن غياب سياسات جامعية صارمة أو أدوات تقنية مساعدة (مثل التنبيهات التلقائية للتحديث أو توفير شبكات آمنة) يساهم في انخفاض مستوى الوعي العملي بهذه الجوانب، مما يستدعي تصميم برامج تدريبية تطبيقية، وتضمين هذه المهارات في المناهج، إلى جانب توفير بيئة مؤسسية داعمة تعزز الالتزام بالسلوكيات الآمنة.

تتوافق هذه النتيجة مع ما أفادته دراسات تناولت فئاتٍ متقدّمة أكاديمياً كدراسة الطيب وآخرون (2025)، بينما تختلف عن نتائج بيئات أخرى أشارت إلى وعي متوسط أو منخفض (حنتولي والزبون، 2025؛Deuri, 2025)، ويُعزى ذلك إلى خصائص الفئة المدروسة واحتكاكها العملي بالأدوات الرقمية الأكاديمية. وفي المقابل، أظهرت النتائج فجوات في السلوكيات الوقائية الروتينية (التحديثات، الشبكات العامة، التخزين على أجهزة غير شخصية)، وهي فجوات واسعة الانتشار في الأدبيات (زيدان، 2024؛ Onyema et al, 2021)، وتتطلب معالجة مؤسسية تتجاوز المعرفة النظرية إلى التدريب التطبيقي وسياسات داعمة.

ثانياً- النتائج المتعلقة بالإجابة عن السؤال الثاني: ما أبرز إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية؟

للإجابة عن هذا السؤال قام الباحث بحساب المتوسطات الحسابية، والانحرافات المعيارية، وتحديد أبرز إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية من وجهة نظر الطلبة أنفسهم على الدرجة الكلية من خلال الرجوع إلى المعيار الذي وضع في الجدول (4)، ثم ترتيب العبارات من الأعلى درجة ممارسة إلى الأقل، والجدول الآتي يوضح النتائج التي تم التوصل إليها.

جدول (6) المتوسطات الحسابية والانحرافات المعيارية وترتيب إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية من وجهة نظر الطلبة أنفسهم من الأعلى درجة ممارسة إلى الأقل

عبارات محور الممارسات الفعلية للأمن السيبراني	المتوسط الحسابي	الانحراف المعياري	مستوى الممارسة	الترتيب
13-أستخدم كلمات مرور قوية وفريدة لكل حساب أكاديمي أو بحثي وأغيرها باستمرار.	4.24	.855	مرتفع جداً	1
14-أفعّل خاصية المصادقة الثنائية أو المتعددة عند توفرها.	3.73	1.284	مرتفع	8
15-أتجنب تنزيل الملفات أو تثبيت الإضافات من مصادر غير موثوقة وأفحصها قبل الاستخدام.	3.05	.778	متوسط	15
16-لا أقدم معلوماتي الشخصية إلا لجهات موثوقة ومعروفة.	3.84	1.400	مرتفع	7
17-أنفّذ نسخاً احتياطياً منتظماً لملفات الدراسة والبيانات البحثية.	4.18	.858	مرتفع	2
18-أحرص على تسجيل الخروج من الحسابات بعد استخدامها.	3.12	.792	متوسط	14
19-أحدّث الأنظمة والبرمجيات بصورة دورية.	3.20	.837	متوسط	12
20-أبلغ الجهات المختصة عند اكتشاف أي محاولة اختراق أو رسالة مشبوهة.	2.97	.776	متوسط	16
21-ألتزم باستخدام البريد الجامعي والمنصات الرسمية وفق البروتوكولات المعتمدة.	3.24	.720	متوسط	9
22-أقفل أجهزتي وأفعّل خاصية القفل التلقائي عند الابتعاد عنها.	3.18	.797	متوسط	13
23-أدير أجهزة التخزين الخارجية بحذر وأفحصها قبل الاستخدام.	3.23	.745	متوسط	10
24-أتحقق من صلاحيات التطبيقات والمنصات التعليمية قبل منح الأذونات.	3.97	.727	مرتفع	6
25-أستخدم برامج مكافحة الفيروسات/الحماية وأحدّثها بانتظام.	4.02	.819	مرتفع	4
26-أتجنب استخدام شبكات الواي فاي العامة غير المحمية عند رفع أو تنزيل الملفات.	3.22	.727	متوسط	11
27-أتحقق من صحة عناوين المواقع قبل إدخال بياناتي أو تسجيل الدخول إلى المنصات التعليمية.	3.99	1.029	مرتفع	5
28-أضبط إعدادات الخصوصية وصلاحيات الوصول للملفات المشتركة.	4.16	.675	مرتفع	3
الدرجة الكلية	3.58	.863	مرتفع	-

يلاحظ من الجدول (6) أن مستوى ممارسة طلبة الدراسات العليا لإجراءات الأمن السيبراني عند استخدامهم للتقنيات الرقمية جاء بدرجة مرتفعة على المستوى الكلي، حيث بلغ المتوسط الحسابي (3.58)، مما يشير إلى وجود وعي تطبيقي جيد. وقد تصدّرت قائمة الممارسات استخدام كلمات مرور قوية وفريدة مع تغييرها المنتظم، تلاه النسخ الاحتياطي الدوري للبيانات، ثم ضبط إعدادات الخصوصية وصلاحيات الوصول، والاستخدام المنتظم لبرامج الحماية، وهي جميعاً إجراءات ذات طابع فردي مباشر وبكلفة منخفضة نسبياً. يمكن تفسير إنّ هذه البنود تمثل ممارسات أساسية وسهلة التطبيق ترتبط مباشرة بوعي الفرد ومسؤوليته الشخصية تجاه حماية بياناته. كما يمكن إرجاع ذلك إلى طبيعة التكوين الأكاديمي لطلبة الدراسات العليا في كلية التربية؛ إذ يتميز هؤلاء الطلبة بامتلاكهم مستوى مرتفعاً من الكفايات الرقمية الأساسية نتيجة خبراتهم السابقة في البحث والدراسة، إضافة إلى إدراكهم لأهمية حماية البيانات البحثية التي تمثل جهداً علمياً كبيراً. كما أن هذه الممارسات لا تتطلب موارد خارجية أو إجراءات مؤسسية معقدة، بل تعتمد على التحكم الذاتي، وهو ما يتوافق مع خصائص المتعلم البالغ الذي يميل إلى الاستقلالية وتحمل المسؤولية. علاوة على ذلك، فإن البيئة الأكاديمية التي تركز على النزاهة العلمية وحماية المعلومات الشخصية تعزز لدى الطلبة الالتزام بهذه الإجراءات، خاصة تلك التي ترتبط مباشرة بسلامة أعمالهم البحثية وحماية خصوصيتهم. وبالتالي، فإن ارتفاع تقييم هذه العبارات يعكس تأثير الوعي التربوي والمهني في تشكيل سلوكيات أمنية رقمية متقدمة لدى هذه الفئة.

في المقابل، انخفضت درجات بعض الممارسات التشغيلية اليومية مثل تسجيل الخروج وقفل الأجهزة وفحص التنزيلات وتجنّب الشبكات العامة، كما برز ضعفٌ في ثقافة الإبلاغ عن الحوادث الأمنية، ويمكن تفسير ذلك إنّ هذه الممارسات ترتبط بسلوكيات وقائية مؤسسية أو روتينية أكثر من ارتباطها بالتحكم الفردي المباشر، مما يجعلها أقل ممارسة لدى الطلبة. كما يمكن إرجاع ذلك إلى عدة عوامل: أولاً، ضعف الوعي الإجرائي لدى الطلبة حول أهمية هذه الخطوات في منظومة الأمن السيبراني، إذ غالباً ما يُنظر إليها على أنها إجراءات ثانوية أو غير ضرورية مقارنة بالممارسات الشخصية مثل كلمات المرور والنسخ الاحتياطي. ثانياً، غياب ثقافة الإبلاغ في البيئة الأكاديمية، حيث لا توجد قنوات واضحة أو سياسات معلنة تشجع على الإبلاغ عن الحوادث، مما يؤدي إلى شعور الطلبة بعدم

جدوى هذه الخطوة أو الخوف من تبعاتها. ثالثاً، الميل الطبيعي لدى المتعلم البالغ إلى تجنب الإجراءات التي تتطلب وقتًا إضافياً أو جهداً متكرراً مثل تسجيل الخروج أو فحص الملفات قبل التنزيل، خاصة في ظل ضغط المهام الأكاديمية. وأخيراً، يمكن أن يعكس هذا الضعف فجوة في برامج التوعية الرقمية التي تركز غالباً على الجوانب التقنية الأساسية دون تعزيز السلوكيات الوقائية اليومية. وبالتالي، فإن انخفاض تقييم هذه العبارات يشير إلى حاجة تربوية لتصميم برامج تدريبية قصيرة وموجهة تبرز أثر هذه الممارسات في حماية البيانات الشخصية والمؤسسية، وتربطها بمسؤولية أكاديمية وأخلاقيات البحث العلمي.

تُظهر النتائج مستوى ممارسة مرتفعاً لإجراءات أمنية شخصية مباشرة وعالية الأثر (كلمات المرور القوية، النسخ الاحتياطي، إعدادات الخصوصية، برامج الحماية)، وهو ما يتقاطع مع الأدبيات التي تربط الوعي بالممارسة المسؤولة (Booc et al, 2024 ؛ Yiğit, 2025). وفي المقابل، ينخفض الالتزام بالممارسات التشغيلية الروتينية (تسجيل الخروج، قفل الأجهزة، فحص التنزيلات، تجنّب الشبكات العامة، الإبلاغ عن الحوادث)، وهي جوانب معروفة بالقصور في الأوساط الأكاديمية وتستدعي تدخّلاً مؤسسياً يرفع التحكم السلوكي المُدرَك ويبسّط الإجراءات ويجعلها افتراضية/مؤتمتة قدر الإمكان (زيدان، 2024؛ Onyema et al, 2021).

ثالثاً- النتائج المتعلقة بالإجابة عن السؤال الثالث: ما التحديات والصعوبات التي تواجه طلبة الدراسات العليا في كلية التربية في جامعة دمشق في الالتزام بإجراءات الأمن السيبراني؟

للإجابة عن هذا السؤال قام الباحث بحساب المتوسطات الحسابية، والانحرافات المعيارية، وتحديد أبرز التحديات والصعوبات التي تواجه طلبة الدراسات العليا في كلية التربية في جامعة دمشق في الالتزام بإجراءات الأمن السيبراني من وجهة نظر الطلبة أنفسهم على الدرجة الكلية من خلال الرجوع إلى المعيار الذي وضع في الجدول (4)، ثم ترتيب العبارات من الأعلى درجة إلى الأقل، والجدول الآتي يوضح النتائج التي تم التوصل إليها.

جدول (7) المتوسطات الحسابية والانحرافات المعيارية وترتيب التحديات والصعوبات التي تواجه طلبة الدراسات العليا في كلية التربية في جامعة دمشق في الالتزام بإجراءات الأمن السيبراني من وجهة نظر الطلبة أنفسهم من الأعلى درجة إلى الأقل

عبارات محور تحديات وصعوبات الالتزام بإجراءات الأمن السيبراني	المتوسط الحسابي	الانحراف المعياري	مستوى الصعوبة	الترتيب
29-أجد صعوبة في تذكر كلمات المرور المعقدة.	4.06	1.023	مرتفع	4
30-أواجه مشكلة في تفعيل خاصية التحقق بخطوتين.	4.04	1.277	مرتفع	5
31-أعتبر تحديث البرامج أمراً مزعجاً ويستهلك الوقت.	3.51	1.211	مرتفع	9
32-أفتقر إلى التدريب الكافي حول إجراءات الأمن السيبراني.	4.18	.976	مرتفع	2
33-أعتقد أن الالتزام بإجراءات الأمن السيبراني يعيق سرعة إنجاز المهام.	3.38	1.053	متوسط	10
34-أواجه نقصاً في الدعم الفني من المؤسسة التعليمية.	4.16	.974	مرتفع	3
35-أجد أن بعض المنصات التعليمية لا توفر خيارات أمان كافية.	3.55	1.210	مرتفع	8
36-أواجه صعوبة في استخدام برامج التشفير أو النسخ الاحتياطي.	3.71	1.280	مرتفع	7
37-أرى أن تكلفة بعض أدوات الحماية مرتفعة.	4.19	.864	مرتفع	1
38-أعتقد أن الوقت المطلوب لتطبيق الإجراءات الأمنية غير متاح دائماً.	3.78	1.374	مرتفع	6
الدرجة الكلية	3.85	1.124	مرتفع	-

يلاحظ من الجدول (7) أن الدرجة الكلية للتحديات والصعوبات التي تواجه طلبة الدراسات العليا في الالتزام بإجراءات الأمن السيبراني جاءت مرتفعة بمتوسط حسابي قدره (3.85)، مما يدل على وجود عقبات حقيقية تحول دون التطبيق الأمثل لهذه الإجراءات. وقد تصدرت قائمة التحديات ارتفاع تكلفة أدوات الحماية، يليه نقص التدريب الكافي حول إجراءات الأمن السيبراني، ثم غياب الدعم الفني من المؤسسة التعليمية، إضافة إلى صعوبة تذكر كلمات المرور المعقدة، ومشكلة تفعيل خاصية التحقق بخطوتين. في المقابل، جاءت أقل التحديات في الاعتقاد بأن الالتزام بالإجراءات يعيق سرعة إنجاز المهام، وتحديث البرامج باعتباره أمراً مزعجاً.

ويمكن تفسير هذه النتائج بأن التحديات الأعلى ترتبط بعوامل بنية تحتية ومعرفية أكثر من كونها سلوكيات فردية؛ فارتفاع تكلفة أدوات الحماية يعكس فجوة اقتصادية لدى الطلبة، خاصة في بيئة تعليمية لا توفر بدائل مجانية أو تراخيص مؤسسية. أما نقص التدريب والدعم الفني فيشير إلى قصور في التمكين الرقمي المؤسسي؛ إذ لم يتم إدماج الأمن السيبراني بشكل كافٍ في برامج الإعداد الأكاديمي، مما يترك الطلبة أمام إجراءات معقدة دون إرشاد عملي. كذلك، صعوبة تذكر كلمات المرور وتفعيل المصادقة الثنائية تعكس الحاجة إلى تصميم بيئات تعليمية سهلة الاستخدام وتبني حلول تقنية مثل إدارة كلمات المرور أو المصادقة الموحدة.أما التحديات الأقل مثل تحديث البرامج أو الاعتقاد بأن الإجراءات تعيق الإنجاز، فترتبط بضعف الوعي بأهمية هذه الخطوات في حماية البيانات، إضافة إلى ضغط الوقت الأكاديمي الذي يجعل الطلبة يفضلون السرعة على الأمان.

بشكل عام، تشير النتائج إلى أن الالتزام بالأمن السيبراني ليس مجرد مسألة تقنية، بل قضية تربوية تتطلب إدماج الأمن الرقمي في ثقافة التعلم، وتوفير تدريب عملي، ودعم فني مستمر، وحلول اقتصادية وتقنية تقلل من العبء على الطالب، مع تعزيز القيم الأكاديمية المرتبطة بالمسؤولية الرقمية.

تتسم التحديات بطابع مؤسسي (تكلفة الأدوات، نقص التدريب، ضعف الدعم الفني) أكثر من كونها عادات فردية؛ ما ينسجم مع ما وثقته الأدبيات حول فجوة التمكين الرقمي المؤسسي في التعليم العالي (Deuri, 2025 ؛ زيدان، 2024؛ Onyema et al, 2021).

12. النتائج المتعلقة بالتحقق من فرضيات البحث:

أولاً- مناقشة النتائج المتعلقة بالفرضية الأولى وتفسيرها: لا توجد فروق ذات دلالة إحصائية عند مستوى 0.05 فيما يتعلق بمستوى وعي طلبة الدراسات العليا بإجراءات الأمن السيبراني تعزى لمتغير المرحلة الدراسية (ماجستير/ دكتوراه).

للتحقق من صحة هذه الفرضية قام الباحث بحساب المتوسطات الحسابية والانحرافات المعيارية لإجابات أفراد عينة البحث على الدرجة الكلية لمحور مستوى وعي طلبة الدراسات العليا بإجراءات الأمن السيبراني وفقاً لمتغير المرحلة الدراسية، ومن ثم استخدام اختبار ت ستودينت للعينات المستقلة للتحقق من دلالة الفروق بين المتوسطات وفقاً لمتغير المرحلة الدراسية، وجاءت نتائج البحث كما هو موضح في الجدول (8).

جدول (8) نتائج اختبار ت ستودينت لدلالة الفروق بين متوسطات درجات أفراد عينة البحث على الدرجة الكلية لمحور مستوى وعي طلبة الدراسات العليا بإجراءات الأمن السيبراني وفقاً لمتغير المرحلة الدراسية (ماجستير، دكتوراه).

الدرجة الكلية لمحور مستوى وعي طلبة الدراسات العليا بإجراءات الأمن السيبراني	المرحلة الدراسية	العدد	المتوسط الحسابي	الانحراف المعياري	ت	درجة الحرية	القيمة الاحتمالية	القرار
	ماجستير	138	46.362	7.109	-3.116-	203	0.002	دال
	دكتوراه	67	49.746	7.662				

يُلاحظ من الجدول (8) بأن نتائج اختبار ت ستودينت تشير إلى وجود فروق ذات دلالة إحصائية عند مستوى (0.05) بين متوسطات درجات طلبة الدراسات العليا في مستوى وعيهم بإجراءات الأمن السيبراني وفقًا لمتغير المرحلة الدراسية (ماجستير/دكتوراه)، حيث بلغت القيمة الاحتمالية (Sig = 0.002) وهي أقل من 0.05، مما يعني رفض الفرضية الصفرية وقبول الفرضية البديلة بوجود فروق دالة لصالح إحدى المجموعتين. وهذا يدل على أن المرحلة الدراسية تؤثر في مستوى الوعي بالأمن السيبراني، حيث أظهرت النتائج أن طلبة الدكتوراه يمتلكون متوسطًا أعلى في الوعي مقارنة بطلبة الماجستير، وهو ما يعكس اختلافاً في الخبرة الأكاديمية والتعامل مع البيانات البحثية الحساسة. ويمكن تفسير هذه النتيجة بأن طلبة الدكتوراه غالباً يمتلكون خبرة أكاديمية أطول، ويتعاملون مع بيانات بحثية أكثر حساسية، مما يعزز إدراكهم لأهمية إجراءات الأمن السيبراني، إضافة إلى أن طبيعة الدراسات العليا في مرحلة الدكتوراه تتطلب استخدام منصات رقمية متقدمة وإدارة بيانات ضخمة، ما يفرض عليهم التزاماً أكبر بالإجراءات الأمنية. في المقابل، قد يكون طلبة الماجستير أقل تعرضاً لمخاطر أمنية معقدة، وبالتالي أقل وعياً ببعض الإجراءات المتقدمة. هذه النتيجة تؤكد الحاجة إلى تصميم برامج تدريبية متخصصة في الأمن السيبراني تستهدف جميع طلبة الدراسات العليا، مع التركيز على رفع مستوى الوعي لدى طلبة الماجستير لتقليص الفجوة بين المرحلتين وضمان بيئة بحثية آمنة.

ثانياً- مناقشة النتائج المتعلقة بالفرضية الثانية وتفسيرها: لا توجد فروق ذات دلالة إحصائية عند مستوى 0.05 فيما يتعلق بمستوى إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية تعزى لمتغير الخبرة التقنية (مبتدئ- متوسط- متقدم).

للتحقق من صحة هذه الفرضية تم حساب المتوسطات الحسابية والانحرافات المعيارية لإجابات أفراد عينة البحث باختلاف مستوى الخبرة التقنية على الدرجة الكلية لمحور إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية وفقاً لمتغير الخبرة التقنية . كما هو موضح في الجدول (9).

جدول (9) المتوسطات الحسابية والانحرافات المعيارية لإجابات أفراد عينة البحث باختلاف مستوى الخبرة التقنية على الدرجة الكلية لمحور إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية

الدرجة الكلية لمحور إجراءات الأمن السيبراني	الخبرة التقنية لأفراد عينة الدراسة	العدد	المتوسط الحسابي	الانحراف المعياري
	مبتدئ	62	54.0645	8.10357
	متوسط	101	57.9703	9.51468

التي يطبقها طلبة الدراسات العليا	متقدم	42	60.7143	5.58869
	المجموع	205	57.3512	8.72306

يلاحظ من خلال الجدول (9) وجود فروق بين إجابات أفراد عينة الدراسة وفقاً لمستوى الخبرة التقنية على الدرجة الكلية لمحور إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية، وللكشف عن الدلالة الإحصائية لهذه الفروق، تمَّ استخدام تحليل التباين الأحادي، كما هو موضَّح في الجدول (10).

جدول (10) نتائج تحليل التباين الأحادي لأثر متغير الخبرة التقنية لاستجابات أفراد عينة الدراسة على الدرجة الكلية لمحور إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية

	مصدر التباين	مجموع المربعات	د ح	متوسط المربعات	(ف)	الدلالة	القرار
ممارسات الأمن السيبراني	بين المجموعات	1183.488	2	591.744	8.336	.000	دال
	داخل المجموعات	14339.224	202	70.986			
	الكلي	15522.712	204				

يبين الجدول (10) وجود فروق ذات دلالة إحصائية في إجابات أفراد عينة الدراسة تعزى لمستوى الخبرة التقنية على الدرجة الكلية لمحور إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية، وللكشف عن جهة هذه الفروق (لصالح من) تمَّ استخراج نتائج اختبار (شيفيه) للمقارنات البعدية للعينات المتجانسة على الدرجة الكلية للمحور كما موضح في الجدول (11).

جدول (11) نتائج اختبار شيفيه للمقارنات البعدية لدى أفراد عينة الدراسة تبعاً لمستوى الخبرة التقنية على الدرجة الكلية لمحور إجراءات الأمن السيبراني التي يطبقها طلبة الدراسات العليا في كلية التربية في جامعة دمشق عند استخدامهم للتقنيات الرقمية

	الخبرة التقنية لأفراد عينة الدراسة		الفرق بين المتوسطات	الدلالة	القرار
إجراءات الأمن السيبراني المتبعة	مبتدئ	متوسط	-3.90578-*	.017	دال
		متقدم	-6.64977-*	.001	دال
	متوسط	متقدم	-2.74399-	.210	غير دال

أظهرت نتائج اختبار شيفيه للمقارنات البعدية ما يلي:

وجود فروق ذات دلالة إحصائية عند مستوى (0.05) وفقاً لمتغير الخبرة التقنية بين الطلبة ذوي الخبرة المبتدئة، والطلبة ذوي الخبرة المتوسطة في مستوى إجراءات الأمن السيبراني التي يطبقونها، لصالح الطلبة ذوي الخبرة المتوسطة.

وجود فروق ذات دلالة إحصائية عند مستوى (0.05) وفقاً لمتغير الخبرة التقنية بين الطلبة ذوي الخبرة المبتدئة، والطلبة ذوي الخبرة المتقدمة في مستوى إجراءات الأمن السيبراني التي يطبقونها، لصالح الطلبة ذوي الخبرة المتقدمة.

عدم وجود فروق ذات دلالة إحصائية عند مستوى (0.05) وفقاً لمتغير الخبرة التقنية بين الطلبة ذوي الخبرة المتوسطة، والطلبة ذوي الخبرة المتقدمة في مستوى إجراءات الأمن السيبراني التي يطبقونها.

يشير ذلك إلى أن مستوى الخبرة التقنية يؤثر في درجة الالتزام بإجراءات الأمن السيبراني، حيث يميل الطلبة ذوو الخبرة المتقدمة أو المتوسطة إلى تطبيق إجراءات أكثر مقارنة بالمبتدئين، بينما لا يوجد فرق جوهري بين الفئتين المتوسطة والمتقدمة، مما يعكس تقارباً في مستوى الممارسة عند تجاوز المرحلة الأساسية من الخبرة. ويمكن تفسير هذه النتيجة بأن الطلبة المبتدئين يفتقرون إلى المهارات الرقمية اللازمة لفهم وتطبيق الإجراءات الأمنية، في حين أن اكتساب خبرة تقنية متوسطة يرفع مستوى الوعي والممارسة بشكل ملحوظ، وهو ما يتوافق مع نظريات التعلم التي تؤكد أن الممارسة والخبرة العملية تعزز الكفايات الرقمية. أما تقارب الفئتين المتوسطة والمتقدمة فقد يعود إلى أن الإجراءات الأمنية الأساسية لا تتطلب مهارات تقنية عالية، بل تعتمد على وعي المستخدم أكثر من اعتماده على التخصص التقني العميق. وتبرز هذه النتيجة أهمية إدماج برامج تدريبية عملية في الأمن السيبراني تستهدف الطلبة المبتدئين بشكل خاص، لضمان رفع مستوى الممارسة وتقليص الفجوة بين الفئات المختلفة من حيث الخبرة التقنية.

ثالثاً- مناقشة النتائج المتعلقة بالفرضية الثالثة وتفسيرها: لا توجد علاقة ذات دلالة إحصائية عند مستوى دلالة (0.05) بين مستوى وعي طلبة الدراسات العليا بالأمن السيبراني ومستوى ممارساتهم الفعلية لهذه الإجراءات عند استخدامهم للتقنيات الرقمية في كلية التربية في جامعة دمشق من وجهة نظر الطلبة أنفسهم.

للتحقق من صحة هذه الفرضية قام الباحث بحساب معامل ارتباط بيرسون بين درجات طلبة الدراسات العليا أفراد عينة البحث على محور الوعي بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية ودرجاتهم على محور إجراءات الأمن السيبراني التي يطبقونها عند استخدامهم للتقنيات الرقمية، وكانت النتائج كالآتي:

الجدول (12) معامل ارتباط بيرسون بين درجات طلبة الدراسات العليا أفراد عينة البحث على محور الوعي بمفهوم الأمن السيبراني وأهميته في البيئة الأكاديمية ودرجاتهم على محور إجراءات الأمن السيبراني التي يطبقونها عند استخدامهم للتقنيات الرقمية

الوعي بمفهوم الأمن السيبراني * إجراءات الأمن السيبراني المتبعة	ارتباط بيرسون	مستوى الدلالة	القرار
ارتباط بيرسون	0.868**	0.00	دالة
العدد	205		

(**) دالة عند مستوى دلالة (0.01)

أظهرت النتائج وجود علاقة ارتباطية قوية ودالة إحصائياً بين مستوى وعي طلبة الدراسات العليا بالأمن السيبراني ومستوى ممارساتهم الفعلية لهذه الإجراءات عند استخدامهم للتقنيات الرقمية، حيث بلغ معامل ارتباط بيرسون (0.868) عند مستوى دلالة (0.01)، مما يشير إلى أن ارتفاع مستوى الوعي يرتبط ارتباطاً مباشراً بزيادة مستوى الممارسة. ويمكن تفسير هذه النتيجة في ضوء نظريات التعلم البنائي والسلوكي التي تؤكد أن المعرفة تشكل أساس السلوك؛ فكلما امتلك الطالب فهماً أعمق لمفهوم الأمن السيبراني وأهميته في حماية البيانات وضمان النزاهة العلمية، زادت دافعيته لتطبيق الإجراءات الأمنية بشكل عملي. كما أن البيئة الأكاديمية التي تعزز الوعي من خلال التوجيهات والسياسات المؤسسية تسهم في تحويل المعرفة النظرية إلى ممارسة فعلية، وهو ما ينسجم مع مبدأ "التعلم من أجل التطبيق" في التربية الحديثة. هذه النتيجة تؤكد أن برامج التوعية ليست مجرد إضافة معرفية، بل هي مدخل أساسي لتغيير السلوكيات الرقمية، مما يستدعي إدماج الأمن السيبراني في المناهج والأنشطة التدريبية لضمان استدامة الممارسات الآمنة لدى طلبة الدراسات العليا.

وتدعم هذه النتيجة نماذج نظرية السلوك المخطّط التي تُبرز دور التحكم السلوكي المُدرَك في ترجمة الوعي إلى ممارسة (Booc et al, 2024)، كما تتقاطع مع أدلة تربط الوعي الذهني بالسلوكيات الآمنة (Yiğit, 2025).

13. مقترحات البحث:

استنادًا إلى النتائج التي توصل إليها البحث، يمكن تقديم مجموعة من المقترحات والتوصيات التي تهدف إلى تعزيز الوعي والممارسات الأمنية الرقمية لدى طلبة الدراسات العليا في كلية التربية، وهي كما يأتي:

- إدماج الأمن السيبراني في المناهج الدراسية من خلال تضمين وحدات تعليمية متخصصة ضمن مقررات البحث العلمي وأخلاقياته، بحيث تركز على حماية البيانات الشخصية والبحثية.
- تنظيم برامج تدريبية عملية تستهدف جميع طلبة الدراسات العليا، مع التركيز على الفئات ذات الخبرة التقنية المحدودة، لتزويدهم بالمهارات اللازمة لتطبيق إجراءات الأمن السيبراني بشكل فعّال.
- توفير دعم فني مؤسسي دائم عبر إنشاء وحدة مختصة بالأمن السيبراني في الكلية، تقدم الإرشاد الفوري وحلول المشكلات التقنية التي تواجه الطلبة في أثناء استخدام المنصات الرقمية.
- تفعيل سياسات إلزامية للأمان الرقمي مثل المصادقة متعددة العوامل على البريد الجامعي والمنصات التعليمية، وضبط إعدادات القفل التلقائي للأجهزة المستخدمة في البيئة الأكاديمية.
- إتاحة أدوات الحماية بشكل مجاني أو منخفض التكلفة من خلال توفير تراخيص مؤسسية لبرامج مكافحة الفيروسات وأدوات التشفير، بما يخفف العبء المالي على الطلبة.
- إطلاق حملات توعية دورية عبر البريد الجامعي والمنصات الرسمية، تتضمن إرشادات مختصرة وفيديوهات تعليمية تبرز أهمية الإجراءات الأمنية في حماية البيانات وضمان النزاهة العلمية.
- إعداد دليل إجرائي موحد للأمن السيبراني يوضح الخطوات العملية لتطبيق الإجراءات الأمنية، ويكون متاحاً لجميع الطلبة بشكل رقمي ومطبوع.
- تشجيع ثقافة الإبلاغ عن الحوادث الأمنية من خلال توفير قنوات واضحة وسرية للإبلاغ، وضمان سرعة الاستجابة، مع تعزيز الثقة لدى الطلبة في فعالية هذه القنوات.
- تطوير استراتيجية مؤسسية للأمن السيبراني في التعليم العالي، تشمل التدريب الإلزامي، الدعم الفني، وتقييم دوري لمستوى الالتزام.
- إجراء دراسات مستقبلية لقياس أثر البرامج التدريبية على تحسين الممارسات الأمنية، ومقارنة الفروق بين التخصصات المختلفة.

المراجع:

المراجع العربية:

- أبو حسين، حنين. (2021). *الإطار القانوني لخدمات الأمن السيبراني: دراسة مقارنة*. رسالة ماجستير غير منشورة، كلية الحقوق، جامعة الشرق الأوسط، الأردن.
- حصوة، رنا والقضاة، محمد أمين. (2023). دور معلمي المدرسة الثانوية في تنمية الوعي بالأمن السيبراني لدى طلابها من وجهة نظر المعلمين في مدارس التعليم الخاص في مدينة عمان، *مجلة دراسات، العلوم التربوية*، 50 (3)، ص ص 61- 75.
- حنتولي، أماني، والزبون، محمد. (2025). واقع وعي الطلبة في الجامعات الأردنية بقافة الأمن السيبراني ومفاهيمه ومجالاته من وجهة نظر الطلبة أنفسهم، *سلسلة العلوم التربوية والنفسية، المنارة*، 4 (1)، ص ص 9-38.
- الخضري، جيهان وسلامي، هدي وكليبي، نعمه. (2020). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية دراسة مقارنة. *مجلة تطوير الأداء الجامعي، جامعة المنصورة*، 12 (1)، ص ص 217-233.
- زيدان، أسماء. (2024). تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية (تصور مقترح)، *مجلة دراسات تربوية واجتماعية، كلية التربية، جامعة حلوان*، 30 (يوليو)، ص ص 11- 129.
- سراج، شيماء. (2022). التحليل البعدي لدراسات الأمن السيبراني في المجال التربوي. *العربية للعلوم التربوية والنفسية، المؤسسة العربية للتربية والعلوم والآداب*، 6 (26)، ص ص 199-212.
- السعادات، خليل والتميمي، ندى. (2022). رفع الوعي بالأمن السيبراني لدى المعلمين في ضوء مبادئ تعليم الكبار. *آفاق جديدة في تعليم الكبار*، 1 (32)، ص ص. 255-280.
- الطيب، عهد والوهبي، نجلاء والمقرن، نوره. (2025). درجة وعي طالبات الدراسات العليا في جامعة الملك سعود بالأمن السيبراني، *مجلة العلوم التربوية والنفسية*، 9 (7)، ص ص 1- 22.
- العتيبي، سعود. (2022). مدى توفر الوعي بالأمن السيبراني لدى أفراد الأسر في المجتمع السعودي (دراسة استطلاعية على عينة من الأسر بمحافظة جدة. *المجلة الدولية لنشر البحوث والدراسات*، 3 (27)، ص ص 575 - 613.
- العودة، هيله. (2025). التحديات التي تواجه الأمن السيبراني. *مجلة العلوم الإنسانية والطبيعية*، 6 (7)، ص ص 720 - 734.
- مشعل، مروه والشناوي، مروه. (2024). واقع الوعي بإجراءات الأمن السيبراني كما يدركها طلبة كليات التربية بجامعة مطروح. *مجلة بحوث ودراسات الطفولة، جامعة الفيوم*، العدد العشرون، ص ص 1-48.

المراجع الأجنبية:

- Alhaif, A. M. (2023). Training Needs of Information Specialists at Saudi Universities Libraries to Achieve Cybersecurity Requirements. *International Journal of Education and Information Technologies*, 17, 38-50.
- Beer, S. (2002). "What is cybernetics?", *Kybernetes*, 31(2),209-219, [Online]. Available: https://doi.org/10.1108/03684920210417283.
- Booc, N. B. B., Budiongan, K., & Carballo, R. (2024). Cybersecurity Awareness, and Cybersecurity Behavior of High School Students in Davao City: A Mediation Role of Perceived Behavioral Control. *European Journal of Applied Science, Engineering and Technology*, 2(3), 4-9.
- CISCO. What is cybersecurity? (2020) [Online]. Available: https://www.cisco.com/c/en_ae/products/security/what-is-cybersecurity.html.

- Deuri, R. (2025). Enhancing Cyber Awarenesse: The Role of Higher Education Institutions in Building a Digitally Secure Generation. *International Journal for Multidisciplinary Research*, 7(2), 1-8.
- Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Mlambo, C. (2021). Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. *Security and privacy*, 4(2), e141.
- Onyema, E. M., Edeh, C. D., Gregory, U. S., Edmond, V. U., Charles, A. C., & Richard-Nnabu, N. E. (2021). Cybersecurity Awareness Among Undergraduate Students in Enugu Nigeria. *International Journal of Information Security, Privacy and Digital Forensic*, 5(1), 34-42.
- Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, 27(2), 23-39.
- 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.
- Wang, P. (2021). Cybersecurity student talent recruitment and development: A case study. *Issues Inf. Syst*, 22(2), 210-222.
- Yiğit, M. F. (2025). Investigating the Role of Mindful Awareness as an Antecedent of University Students' Cyber Security Behaviors. *Journal of Learning and Teaching in Digital Age*, 10(2), 156-169.
- Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(23), 15-1. https://doi.org/10.3390/bdcc5020023.
- Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, *12*(10), 417- 437. https://doi.org/10.3390/info12100323

المستخلص باللغة الانكليزية

Analysis of Cybersecurity Awareness and Practices Among Graduate Students at the Faculty of Education, Damascus University

Mahmoud Esmaeel Al-Fares
Lecturer at the Faculty of Education, Damascus University

abstract
This research aimed to examine the level of awareness among postgraduate students at the Faculty of Education, Damascus University, regarding the concept of cybersecurity and its importance in the academic environment. It also analyzed their

actual practices when using digital technologies and identified the most significant challenges they face in adhering to cybersecurity procedures. Furthermore, the study sought to investigate the relationship between awareness and practice from the students' own perspective. A descriptive-analytical approach was adopted, and a questionnaire was developed to assess the current state of cybersecurity awareness. This instrument was administered to a stratified random sample of 205 postgraduate students at the Faculty of Education, Damascus University.The findings revealed that students demonstrated a high level of awareness of cybersecurity procedures, while their actual practices were generally satisfactory. However, these practices were primarily limited to basic individual measures, such as using strong passwords, performing backups, and adjusting privacy settings, whereas operational and institutional practices—such as logging out and reporting security incidents—were less frequently observed. The study also highlighted significant challenges faced by students, including the high cost of security tools, insufficient training and technical support, and difficulties in enabling two-factor authentication. Statistical analysis indicated significant differences in awareness favoring PhD students, and differences in practice favoring those with intermediate and advanced technical experience. Additionally, a strong positive correlation was found between awareness and practice, confirming that enhancing knowledge contributes to improving security behaviors among students.