Comprehensive Journal of Science
Volume (10), Issue (39), (March, 2026)
ISSN: 3014-6266

مجلة العلوم الشاملة
المجلد (10) ملحق العدد 39 مارس 2026
ردمد: 3014-6266

تأثير الأمن السيبراني على جودة التعليم الالكتروني في الجامعات الليبية

دعاء ضؤ اللالي
قسم تحليل البيانات، كلية الاقتصاد ,جامعة الزاوية , العجيلات ,ليبيا

The impact of cybersecurity on the quality of e-learning in Libyan universities

Daua Allali
Department of Data Analysis, Facility of Economics , Al-Ajilat, University of Zawia , Libya
d.allali@zu.edu.ly

تاريخ الاستلام:2026/02/15 –تاريخ المراجعة:2026/03/12– تاريخ القبول: 2026/03/13– تاريخ للنشر2026/04/25

الملخص
يواجه التحول الرقمي في الجامعات الليبية تحدياً جوهرياً يتمثل في الفجوة بين الوعي النظري بالأمن السيبراني والممارسة الفعلية لتدابير الحماية الرقمية، وهو ما يهدد استدامة جودة التعليم الإلكتروني. تهدف هذه الدراسة إلى تشخيص حجم هذه الفجوة لدى أعضاء هيئة التدريس والطلاب، وقياس أثر الأمن السيبراني على جودة التعليم الإلكتروني. واعتمدت الدراسة المنهج الوصفي التحليلي، وطُبقت على عينة عشوائية طبقية من كلية الاقتصاد بجامعة الزاوية، باستخدام استبانة إلكترونية تم التحقق من صدقها وثباتها. أُجري التحليل الإحصائي عبر برنامج (SPSS) باستخدام معاملات الارتباط والانحدار المتعدد واختبارات الفروق. كشفت النتائج عن مستوى وعي نظري مرتفع مقترناً بممارسة أمنية متوسطة، مما يؤكد وجود فجوة سلوكية. كما أثبتت نتائج الانحدار وجود أثر دال إحصائياً للأمن السيبراني على تعزيز الثقة في جودة التعليم. وفي ضوء ذلك، توصي الدراسة بضرورة الانتقال من التوعية النظرية إلى برامج تدريبية سلوكية، وتفعيل المصادقة المتعددة العوامل، ودمج مؤشرات الأمن السيبراني ضمن معايير ضمان الجودة الأكاديمي لتعزيز التحول الرقمي الآمن في التعليم العالي.
الكلمات المفتاحية: الأمن السيبراني، جودة التعليم الإلكتروني، الثقة الرقمية، الفجوة المعرفية، التحول الرقمي.

Abstract
The digital transformation in Libyan universities faces a fundamental challenge: the gap between theoretical cyber security awareness and the actual practice of digital protection measures, which threatens the sustainability of e-learning quality. This study aims to diagnose the size of this gap among faculty members and students, and to measure the impact of cyber security on e-learning quality, considering "trust" as a mediating variable. The study adopted a descriptive-analytical approach, applied to a stratified random sample from the Faculty of Economics at Zawia University, using an electronic questionnaire whose validity and reliability were verified. Statistical analysis was conducted using SPSS through correlation coefficients, multiple regression, and difference tests. The results revealed a high level of theoretical awareness coupled with weak security practices, confirming a behavioral gap. Regression results also proved a statistically significant impact of cyber security on enhancing trust, educational quality, and beneficiary satisfaction. Consequently, the study recommends shifting from theoretical awareness to behavioral training programs, activating multifactor authentication, and integrating cyber security indicators into academic quality assurance standards to support a secure digital transformation in higher education.
Keywords: Cyber security, E-learning Quality, Digital Trust, Cognitive Gap, Digital Transformation.

اولا: المقدمة

شهد قطاع التعليم العالي، عالمياً ومحلياً، تحولاً جذرياً نحو الرقمية نتيجة التطورات التكنولوجية المتسارعة، حيث أصبحت المنصات التعليمية الإلكترونية أحد الأعمدة الرئيسة في تقديم المعرفة وتبادل الخبرات. وقد اكتسب هذا التحول زخماً استثنائياً في أعقاب الأزمات العالمية كجائحة كوفيد-19، التي فرضت اعتماداً شبه كامل على الوسائط الرقمية في استمرارية العملية التعليمية(Almaiah et al., 2020).

وفي السياق الليبي، تطلب هذا التحول المستعجل -الذي رافقته ظروف استثنائية- اعتماداً مكثفاً على أدوات التعلم عن بعد، مما أتاح فرصاً لتوسيع نطاق الوصول التعليمي، لكنه في الوقت ذاته كشف عن هشاشة في البنية التحتية الرقمية وثغرات أمنية جوهرية. إن الاعتماد المتزايد على الشبكات والمنصات الرقمية في الجامعات قد حوّل هذه المؤسسات إلى

أهداف مرغوبة للهجمات السيبرانية، مما يهدد سلامة البيانات الأكاديمية والشخصية للطلاب وأعضاء هيئة التدريس (González-Zamar et al., 2020). فاختراق هذه المنصات أو تسريب بياناتها لا يقتصر أثره على الخسائر التقنية، بل يمتد ليمس جوهر العملية التعليمية؛ إذ أن جودة التعليم الإلكتروني وفقاً للمعايير الأكاديمية الحديثة لم تعد تُقاس فقط بجودة المحتوى العلمي أو كفاءة أساليب التدريس، بل باتت ترتبط ارتباطا جوهرياً بمدى أمان وسلامة البيئة الرقمية التي تُدار فيها هذه العملية (Ifinedo, 2021).

تزداد أهمية الأمن السيبراني كمتغير مؤثر في جودة التعليم عندما نأخذ بعين الاعتبار النموذج السيكولوجي للمتعلم, فالطالب الذي يدرك أن بياناته أو تقييماته عرضة للاختراق، سيعاني من انخفاض في مستوى الثقة (Trust)، مما ينعكس سلباً على تفاعله الإيجابي ومشاركته الفاعلة، وهو ما يشكل انتقاصاً مباشراً من مؤشرات جودة المخرجات التعليمية. من هنا، يبرز الأمن السيبراني ليس مجرد مفهوم تقني ثانوي، بل كركيزة استراتيجية (Strategic Pillar), لضمان استدامة وموثوقية التعليم الجامعي في صورته الحديثة. ورغم الاتفاق الأكاديمي على هذه العلاقة، إلا أن الواقع التطبيقي في المؤسسات التعليمية -وخاصة في سياقات الدول التي تشهد تحولاً رقمياً غير مدروس كلياً مثل ليبيا- يشير إلى وجود فجوة واضحة بين "الإدراك النظري" لأهمية الأمن السيبراني، و"الممارسة الفعلية" للإجراءات الأمنية (AlHogail, 2018). وهذه الفجوة تشكل إشكالية علمية تستدعي التوقف؛ لأن استمرارها يعني بناء منظومة تعليمية رقمية هشة التأسيس. من هذا المنطلق، جاءت هذه الدراسة لسد الفجوة المعرفية في الأدبيات العربية التي ربطت بين المتغيرين، من خلال دراسة وتحليل العلاقة بين الوعي والممارسة الأمنية وقياس انعكاساتهما على ثقة المستفيدين وجودة التعليم الإلكتروني في الجامعات الليبية. وتهدف إلى تقديم استجابة علمية لتساؤل جوهري: "إلى أي مدى يمكن اعتبار الأمن السيبراني عاملاً حاسماً في تحديد مستوى جودة التعليم الرقمي في المؤسسات الأكاديمية الليبية؟". وما لم تسبر هذه الدراسة أغوار هذه العلاقة وتقدم توصيات تطبيقية مبنية على بيانات ميدانية، ستظل الجامعات الليبية تعمل في بيئة رقمية تكتنفها مخاطر قد تقوض جهود التحول نحو جودة التعليم (Miranda et al., 2021).

ثانيا: مشكلة الدراسة

تتجسد مشكلة الدراسة في الفجوة القائمة بين التوجه المتسارع نحو تبني التعليم الإلكتروني في الجامعات الليبية، وبين القصور الملحوظ في تفعيل الممارسات والسياسات الفعلية للأمن السيبراني لحماية هذه البيئات الرقمية. فرغم إدراك المؤسسات الأكاديمية لأهمية التحول الرقمي، إلا أن اعتماد كلا الطرفين الرئيسيين في العملية التعليمية (أعضاء هيئة التدريس والطلاب) على منصات التعلم الإلكتروني، في غياب وعي السيبراني تطبيقي كافٍ وبنية تحتية أمنية راسخة، قد خلق حالة من الهشاشة التقنية. هذه الهشاشة تهدد سرية البيانات الأكاديمية والشخصية، وتخلق حالة من الشك والقلق تنال من "ثقة" المستفيدين في هذه المنصات، وهو ما ينعكس سلباً -في المحصلة- على "جودة" العملية التعليمية واستدامتها. وعليه، تتمحور إشكالية هذا البحث في ضرورة تشخيص حجم هذه الفجوة بين (الإدراك النظري والممارسة الفعلية) لدى الطلاب وأعضاء هيئة التدريس، وقياس مدى انعكاس مستوى الأمن السيبراني على المعايير الجوهرية لجودة التعليم الإلكتروني في السياق الليبي.

ثالثا: أسئلة الدراسة

بناءً على الإشكالية المطروحة، تسعى هذه الدراسة للإجابة عن السؤال الرئيسي التالي:

- ما أثر الأمن السيبراني (بمكوناته: الوعي والممارسة والثقة) على جودة التعليم الإلكتروني في الجامعات الليبية من وجهة نظر كل من أعضاء هيئة التدريس والطلاب؟

ويتفرع من هذا السؤال الرئيسي الأسئلة الفرعية التالية:

- ما مستوى الوعي بالمخاطر السيبرانية ومتطلبات الحماية الرقمية لدى أعضاء هيئة التدريس والطلاب في بيئة التعليم الإلكتروني؟
- ما طبيعة العلاقة الارتباطية بين تطبيق ممارسات الأمن السيبراني (مثل: التشفير، المصادقة المتعددة، حماية الخصوصية) وبناء الثقة في منصات التعليم الإلكتروني لدى عينة الدراسة؟
- ما حجم التأثير الذي تتركه ممارسات الأمن السيبراني على مستوى رضا المستفيدين (الطلاب وأعضاء هيئة التدريس) وجودة تجربتهم التعليمية الرقمية؟
- هل توجد فروق ذات دلالة إحصائية في مستوى الوعي أو الممارسة الأمنية لدى عينة الدراسة تعزى للمتغيرات الديموغرافية (الفئة: طالب/أستاذ، الجنس، العمر، المستوى الأكاديمي)؟

رابعا: أهداف الدراسة

سعت هذه الدراسة إلى تحقيق الأهداف التالية، والتي تتسق بشكل مباشر مع إشكالية وأسئلة البحث:

- قياس مستوى الوعي بالمخاطر السيبرانية ومتطلبات الحماية الرقمية لدى عينة الدراسة (أعضاء هيئة التدريس والطلاب) في بيئة التعليم الإلكتروني.
- تحديد طبيعة العلاقة الارتباطية بين تطبيق ممارسات الأمن السيبراني ودرجة الثقة في منصات التعليم الإلكتروني.

- قياس حجم الأثر الذي تتركه ممارسات الأمن السيبراني على مستوى رضا المستفيدين وجودة تجربتهم التعليمية الرقمية.
- التعرف على الفروق في مستوى الوعي أو الممارسة الأمنية لدى عينة الدراسة تبعاً للمتغيرات الديموغرافية (الفئة، الجنس، العمر، المستوى الأكاديمي).
- تقديم توصيات استراتيجية لتعزيز البنية الأمنية في الجامعات الليبية بما يضمن استدامة جودة التعليم الإلكتروني.

خامسا: فرضيات الدراسة

للإجابة عن أسئلة الدراسة، تم صياغة الفرضية الرئيسية التالية، والتي تفرعت منها الفرضيات الجزئية، جميعها صيغت بصيغة إحصائية فارغة (Null Hypotheses) لاختبارها لاحقاً عبر برنامج (SPSS):

الفرضية الرئيسية:

لا يوجد أثر ذو دلالة إحصائية للأمن السيبراني (بمكوناته: الوعي والممارسة والثقة) على جودة التعليم الإلكتروني في الجامعات الليبية من وجهة نظر عينة الدراسة.

الفرضيات الفرعية:

- لا يوجد أثر ذو دلالة إحصائية لمستوى الوعي الأمني السيبراني في جودة التعليم الإلكتروني لدى أعضاء هيئة التدريس والطلاب.
- لا يوجد أثر ذو دلالة إحصائية لتطبيق ممارسات الأمن السيبراني في جودة التعليم الإلكتروني.
- لا يوجد أثر ذو دلالة إحصائية بين الثقة بالأمن السيبراني وجودة التعليم الإلكتروني.
- لا توجد فروق ذات دلالة إحصائية في مستوى الوعي والممارسة الأمنية لدى عينة الدراسة تعزى للمتغيرات الديموغرافية (الفئة، الجنس، العمر، المستوى الأكاديمي).

سادسا: منهجية الدراسة

لتحقيق أهداف الدراسة والإجابة عن أسئلتها واختبار فرضياتها، اعتمدت هذه الدراسة على المنهج الوصفي التحليلي (Descriptive Analytical Approach). وقد تم اختيار هذا المنهج لملاءمته الطبيعة الكمية للدراسة، حيث يُمكّن الباحثة من وصف الواقع الفعلي لمتغيرات الدراسة (الوعي السيبراني، مستوى الثقة، جودة التعليم) لدى عينة البحث، ثم تحليل العلاقات الارتباطية وتقدير حجم التأثير بين هذه المتغيرات بدقة.

سابعا: مجتمع وعينة الدراسة

المجتمع الأصلي: يتكون مجتمع الدراسة من جميع أعضاء هيئة التدريس والطلبة المسجلين والمتفاعلين مع منصات التعليم الإلكتروني في كلية الاقتصاد بجامعة الزاوية.

العينة: تم اختيار عينة عشوائية طبقية (Stratified Random Sample) من مجتمع الدراسة، حيث جُمعت الاستجابات عبر الاستبيان الإلكتروني (Google Forms)، وتم الاحتفاظ بالاستجابات الصالحة للتحليل الإحصائي لتمثيل العينة النهائية , حيت بلغ حجم العينة (240) فردا موزعين كالتالي : (100) عضو هيئة التدريس, (140) طالبا.

ثامنا: أداة الدراسة

تمثل أداة الدراسة في استبانة إلكترونية مغلقة، تم تصميم فقراتها بناءً على الأدبيات السابقة والمقاييس المعتمدة علمياً، وتألفت من خمسة محاور هي: (البيانات الديموغرافية، مستوى الوعي السيبراني، دور الأمن في بناء الثقة، أثر الأمن على الجودة، والتحديات الأمنية.

وتم تقسيم الاستبانة الى محورين رئيسيين، بالإضافة للبيانات الشخصية والوظيفية وهي:

1- المحور الاول (المعلومات العامة) : وهو يتمثل في مجموعة من العبارات المتعلقة : الصفة، الجنس ، العمر.
2- المحور الثاني وهو يتمثل في مجموعة من العبارات المتعلقة بـ (الوعي بالأمن السيبراني).
3- المحور الثالث وهو يتمثل في مجموعة من العبارات المتعلقة بـــ (**ممارسات الأمن السيبراني**).
4- المحور الرابع وهو يتمثل في مجموعة من العبارات المتعلقة بـــ (**الثقة بالأمن السيبراني**).
5- المحور الخامس وهو يتمثل في مجموعة من العبارات المتعلقة بـــ (**جودة التعليم الإلكتروني**).

بدت عملية توزيع الاستبانة على عينة الدراسة خلال شهر اكتوبر 2025م والجدول التالي يوضح عدد الاستبانة التي تم توزيعها على عينة الدراسة: -

جدول رقم (1) يوضح عدد الاستبانة التي تم توزيعها عينة عي الدراسة

عدد الاستبانة	عدد الاستبانة الموزعة	الاستبانات المسترجعة	الفاقد	عدد الاستبانة الصالحة للتحليل
240	240	228	20	220

تاسعا: حدود الدراسة

يُفهم من نتائج هذه الدراسة في إطار الحدود التالية التي يجب مراعاتها عند التعميم:

- **الحدود المكانية**: اقتصرت الدراسة على كلية الاقتصاد بجامعة الزاوية (العجيلات).
- **الحدود الزمنية**: تم إجراء هذه الدراسة وتطبيق أداتها خلال الفصل الدراسي خريف 2025 للعام الجامعي 2026/2025م.
- **الحدود البشرية**: تقتصر نتائج الدراسة وتعميماتها على فئتي (أعضاء هيئة التدريس والطلبة) المستخدمين للمنصات التعليمية الإلكترونية داخل مجتمع العينة المحدد.
- **الحدود الموضوعية**: تقتصر الدراسة على المتغيرات المدروسة فقط (الوعي، الممارسة، الثقة، الجودة) دون التطرق لمتغيرات أخرى قد تؤثر في جودة التعليم كالبنية التحتية التقنية العامة للجامعة أو الكفاءة التدريسية التقليدية.

الإطار النظري والمفاهيم للدراسة

يهدف هذا الإطار إلى تأسيس قاعدة مفاهيمية وعلمية تُفسر العلاقة بين متغيرات الدراسة، بعيداً عن التناول الموسوعي العام للأمن السيبراني، ومركّزاً على النماذج النظرية التي تشرح كيفية تأثير البيئة الرقمية الآمنة على مخرجات التعليم العالي.

1- المفهوم الإجرائي للأمن السيبراني في السياق التعليمي

في سياق هذه الدراسة، لا يُنظر إلى الأمن السيبراني باعتباره مجرد حماية لأجهزة الخوادم (Servers)، بل يُعرّف إجرائياً على أنه: "مجموعة من السياسات التقنية والسلوكية (الوعي والممارسة) التي تتبناها المؤسسة الأكاديمية ومستخدموها (طلاب وأساتذة)، بهدف حماية المنصات التعليمية، والبيانات الأكاديمية والشخصية، لضمان استمرارية تقديم الخدمة التعليمية دون توقفات أو اختراقات".

وينبثق من هذا المفهوم ثلاثة ابعاد رئيسية هم محور بحثنا:

- الوعي السيبراني (Cognitive Dimension): مدى معرفة المستفيدين بالمخاطر الرقمية (التصيد، كلمات المرور الضعيفة) وسلوكيات الحماية الذاتية.

- الممارسة الأمنية التقنية (Technical Dimension): مدى تطبيق الإجراءات الفعلية من قبل إدارة الجامعة والمستخدمين (التشفير، المصادقة الثنائية FA2، التحديثات).

- الثقة بالأمن السيبراني تعني مدى شعور الأفراد بالاطمئنان والاعتماد على الأنظمة الرقمية (مثل منصات التعليم الإلكتروني) في حماية بياناتهم وخصوصيتهم ومنع الاختراق أو سوء الاستخدام.

2- جودة التعليم الإلكتروني (المتغير التابع)

وفقاً للنماذج المعيارية لجودة التعليم الإلكتروني (مثل نموذج DeLone & McLean لأنظمة المعلومات)، فإن تقييم جودة التعليم الرقمي يختلف عن التعليم التقليدي. في هذه الدراسة، تُقيّم الجودة إجرائياً من خلال ثلاثة مؤشرات رئيسية:

جودة النظام (System Quality): وتشمل استقرار المنصة، سرعة التحميل، والأهم من ذلك: أمانها وخلوه من الثغرات.

جودة المحتوى والتفاعل (Information Quality): وتشمل دقة المحتوى وسلامته من التلاعب أو التغيير غير المصرح به. وتُعد جودة المحتوى والتفاعل من أهم أبعاد جودة التعليم الإلكتروني، حيث يسهم المحتوى المنظم والواضح في تسهيل عملية التعلم، بينما يعزز التفاعل من مشاركة المتعلمين ويزيد من فاعلية العملية التعليمية. .

جودة الخدمة/الرضا (Service Quality): وتتمثل في مدى سهولة الوصول للمنصة وتلبية احتياجات المتعلم دون قلق أو عوائق تقنية.

3- الآلية النظرية لربط المتغيرات (كيف يؤثر الأمن على الجودة؟)

لا يوجد تأثير مباشر سحري للأمن السيبراني على "جودة" المحتوى العلمي للمحاضر. بل يحدث التأثير عبر آلية نظرية يمكن تفسيرها كالتالي:

الأمن كشرط مسبق للاستمرارية (Continuity): وفق نموذج (Business Continuity Planning)، أي اختراق أو هجوم حجب خدمة (DDoS) يؤدي إلى توقف المنصة. التوقف يعني انقطاع التعليم، والانقطاع يعني انهيار جودة العملية التعليمية (صفر جودة).

الأمن كمنتج للثقة (Trust Generation): وفقاً لنظرية "المخاطرة المدركة" (Perceived Risk Theory)، عندما يقل الأمن، ترتفع المخاطر المدركة لدى الطالب. الطالب الذي يخشى على بياناته الشخصية أو درجاته سيفقد الثقة في النظام. وبدون ثقة، يحدث ما يُسمى بـ "المقاومة التكنولوجية" (Technology Resistance)، مما يقلل من تفاعله وتقييمه لجودة المنصة.

الأمن وحماية النزاهة الأكاديمية: الاختراقات لا تسرق البيانات فحسب، بل قد تؤدي لتسريب الامتحانات أو التلاعب بالدرجات، مما يمس جوهر "نزاهة المخرجات التعليمية" وهي أعمدة الجودة.

4- الإطار المفاهيمي المقترح للدراسة (Conceptual Framework)

بناءً على ما سبق، تم بناء النموذج المفاهيمي التالي الذي يوجه فرضيات الدراسة ويوضح مسار التأثير:

المتغير المستقل: الأمن السيبراني (يتكون من: الوعي السيبراني ، الممارسات الأمنية، الثقة).

المتغير التابع: جودة التعليم الإلكتروني (تُقاس بـ: جودة المحتوى والتفاعل معه، فاعلية الاستخدام ، رضا المستفيدين ، حماية البيانات).
مسار التأثير المفترض:
تؤدي الممارسات الأمنية الجيدة والوعي المرتفع (المستقل) إلى خفض المخاطر المدركة، مما يُعزز "الثقة" لدى الطلاب والأساتذة، وبالتالي ينعكس إيجاباً على تفاعلهم وتقييمهم لـ "جودة التعليم الإلكتروني" (التابع). وإذا غاب الأمن، تسقط الثقة، ويتحول التقييم إلى سلبية بغض النظر عن جودة المحتوى التعليمي نفسه.

الدراسات السابقة:

تناولت الأدبيات العلمية السابقة موضوع الأمن السيبراني في البيئات التعليمية من زوايا متعددة، ولغرض التحليل العلمي الدقيق، تم تقسيم هذه الدراسات إلى ثلاثة محاور رئيسية تتقاطع مع متغيرات الدراسة الحالية، على النحو التالي:

المحور الأول: دراسات تناولت (الوعي والممارسات الأمنية في التعليم العالي)

ركزت هذه المحاور على قياس مدى إدراك المستفيدين للمخاطر السيبرانية، حيث أشارت دراسة (Aldawood & Skinner, 2019) إلى أن الوعي السيبراني لدى الطلاب يُعد عاملاً حاسماً لتقليل المخاطر، لكنه أشارت إلى فجوة بين المعرفة النظرية والتطبيق. وفي السياق نفسه، قدمت دراسة (AlHogail, 2018) إطاراً مفاهيمياً لتحسين الوعي الأمني في الجامعات، مؤكدة أن الوعي وحده لا يكفي ما لم يترجم إلى سلوكيات مؤسسية يومية. وتتفق معها دراسة (الحربي، 2019) التي أكدت على ضرورة بناء استراتيجيات مؤسسية لتحويل الوعي إلى ممارسات فعلية.

المحور الثاني: دراسات تناولت (دور الأمن السيبراني في بناء الثقة بالمنصات التعليمية)

لأن الثقة تمثل المتغير الوسيط في هذا البحث، فقد تناولت دراسة (Almaiah et al., 2020) أهمية الاعتبارات الأمنية خلال جائحة كوفيد-19، وخلصت إلى أن غياب السياسات الأمنية يؤدي حتماً إلى انهيار ثقة المستخدمين. ويتقاطع معها دراسة (Ifinedo, 2021) التي فحصت إدراك الطلاب لثقة الأنظمة الإلكترونية، مؤكدة أن الشعور بعدم الأمان يقلل من التفاعل. وعربياً، أثبتت دراسة (العتيبي، 2021) في الجامعات السعودية وجود علاقة إيجابية ذات دلالة إحصائية بين تطبيق سياسات الأمن السيبراني ورفع مستوى ثقة الطلاب.

المحور الثالث: دراسات تناولت (الأثر المباشر للأمن على جودة التعليم الإلكتروني)

بحثت هذه الدراسات في المخرج النهائي (الجودة)، حيث بينت دراسة (González-Zamar et al., 2020). أن دمج الأمن السيبراني يُعد عنصراً محورياً لرفع جودة مخرجات التعليم. كما أوضحت دراسة (الموسوي، 2018). أن تطبيق التدابير الأمنية يساهم بشكل مباشر في رفع مستوى رضا الطلبة. بينما ركزت دراسة (عياد، 2020) و(Alharthi et al., 2017). على البنية التحتية، مؤكدين أن ضعف الجاهزية الأمنية يشكل عائقاً حقيقياً يحول دون تحقيق جودة الخدمات التعليمية الرقمية.

التعقيب النقدي على الدراسات السابقة (موقع الدراسة الحالية):

من خلال المراجعة النقدية للمحاور الثلاثة، يمكن توصل إلى عدة ملاحظات علمية تحدد موقف وقيمة الدراسة الحالية:
الاتفاق: تتفق جميع الدراسات السابقة (عربية و أجنبية) على أن الأمن السيبراني ليس ترفاً تقنياً، بل هو متطلب حتمي لجودة التعليم الإلكتروني وثقة المستفيدين.
الاختلاف والقصور (الفجوة البحثية): رغم غزارة الدراسات، إلا أن أغلبها (مثل العتيبي، والموسوي) تناولت الأمن والجودة كمتغيرين منفصلين، وقليل منها من ربطهما عبر "نموذج مفاهيمي متكامل" يدرس الآلية (كيف يحدث التأثير عبر الثقة؟).
السياق الميداني: معظم الدراسات أجريت في بيئات مستقرة تقنياً (السعودية، الغرب)، ولم تُجر دراسات تكشف عن طبيعة "الفجوة بين الإدراك والممارسة" في بيئات هشة تشهد تحولاً رقمياً قسرياً ومتسرعاً كالجامعات الليبية.
محددية العينة: العديد من الدراسات اكتفت بقياس وجهة نظر الطلاب فقط، متناسية أن أعضاء هيئة التدريس هم طرف أساسي في إدارة المنصة وتقييم جودتها.

وبذلك، تتميز هذه الدراسة عن سابقاتها بأنها: لا تكتفي بقياس الوعي، بل تدرس "الفجوة بين الوعي والممارسة" لدى (الطلاب والأساتذة معاً) في السياق الليبي، وتختبر نموذجاً يفترض أن الأمن يؤثر على الجودة عبر تعزيز الثقة (كمتغير وسيط)، مما يمنح البحث إضافة علمية تطبيقية جديدة.

الأساليب الإحصائية المستخدمة في تحليل البيانات:

تم استخدام البرنامج الإحصائي SPSS (الحزم الإحصائية للعلوم الاجتماعية) في تفريغ وتحليل البيانات الواردة في استمارة الاستبيان وذلك من خلال عدد من الأساليب الإحصائية التالية:

1. معامل ألفا كرونباخ: لقياس ثبات الاستبانة.
2. معامل الارتباط بيرسون: لحساب معامل الارتباط وقياس صدق الاتساق الداخلي، وكذلك تحديد طبيعة العلاقة بين المتغيرين المستقل والتابع.
3. النسب المئوية والتكرارات والمتوسط الحسابي: وتستخدم بشكل أساسي لأغراض معرفة تكرار فئات متغير ما ويتم الاستفادة منها في وصف عينة الدراسة.
4. الانحراف المعياري: لقياس الانحرافات في إجابات مفردات عينة الدراسة على فقرات الاستبانة.
5. نحليل الانحدار الخطي البسيط : (الوعي + الممارسة + الثقة) جودة التعليم◄

الصدق والثبات:

الصدق :(Validity) تم التحقق من صدق المحتوى الظاهري من خلال عرض الاستبانة على مجموعة من المحكمين المتخصصين في تكنولوجيا التعليم والأمن المعلوماتي، وتم تعديل الفقرات بناءً على ملاحظاتهم.

الثبات :(Reliability) يعتبر عامل ألفا كرونباخ هو مقياس الاتساق الداخلي للاختبارات الاحصائية مثل الاستبيانات والمقاييس المشابهة، والاتساق الداخلي أو الموثوقية هو مدى ارتباط مجموعة من العناصر ببعضها البعض كمجموعة متسقة.

تم استخدام طريقة معامل طريقة معامل الفا كرونباخ لقياس ثبات الاستبانة لكل محور من محاورها، وكانت معاملات الثبات تتمتع بدلالات ثبات مقبولة لغايات البحث العلمي، حيث وجد ان قيمة معامل الفا كرونباخ للبنود، تقترب من الواحد الصحيح، وبذلك يكون قد تأكد من صدق وثبات الاستبانة، وتكون الاستبانة في صورتها النهائية قابلة للتحليل والنتيجة موضحة في الجدول (2).

ت	البند	عدد الفقرات	معامل الثبات
1	الوعي بالأمن السيبراني	8	0.771
2	ممارسات الأمن السيبراني	8	0.721
3	الثقة بالأمن السيبراني	7	0.735
4	جودة التعليم الإلكتروني	15	0.711
متوسط معامل الثبات			0.734

الجدول (2) يبين معاملات الثبات للاستبانة باستخدام طريقة الفا كرونباخ

تم حساب معامل ثبات الاتساق الداخلي باستخدام معادلة (كرونباخ ألفا(Cronbach's Alpha) ، وبلغت القيمة المحسوبة (0.734) وهي قيمة تدل على ثبات عالٍ للأداة.

معامل ارتباط بيرسون :(Pearson Correlation) :

1- مقياس واقع الوعي بالأمن السيبراني

جدول رقم (3) معاملات الارتباط بين فقرات مقياس واقع الوعي بالأمن السيبراني والدرجة الكلية للمقياس.

	واقع الوعي بالأمن السيبراني	معامل الارتباط	مستوى الدلالة
1	**توجد معرفة بمخاطر الأمن السيبراني في التعليم الإلكتروني**	**0.458****	**0.000**
2	**يمكن التمييز بين المواقع الآمنة وغير الآمنة**	**0.496****	**0.000**
3	**توجد الية لحماية البيانات الشخصية أثناء التعلم الإلكتروني**	**0.541****	**0.000**
4	**هناك ادراك بأهمية حماية البيانات الشخصية أثناء استخدام المنصات التعليمية**	**0.483****	**0.000**
5	**هناك وعي بأساليب الاحتيال الإلكتروني مثل الروابط المزيفة**	**0.558****	**0.000**
6	**هناك وعي مخاطر مشاركة المعلومات الشخصية عبر الإنترنت**	**0.683****	**0.000**
7	**هناك وعي أهمية تحديث البرامج لحماية الأجهزة**	**0.691****	**0.000**
8	**توجد معرفة بأساسيات حماية الخصوصية الرقمية**	**0.543****	**0.000**

يوضح الجدول رقم (3) والذي يضم (8) فقرات أن معامل الارتباط بين كل فقرة من فقرات المحور الاول في الاستبيان والدرجة الكلية للمحور وهي واقع الوعي بالأمن السيبراني ، حيث جاءت كل نتائج فقرات المحور الاول موجبة وهذا يبين ان معاملات الارتباط المبينة بالجدول السابق دالة احصائية عند مستوى (0.05) هي علاقات طردية، وهذا يعني انه كلما توافرت فقرات المتغير الفرعي الاول زاد الوعي بالأمن السبراني.

2- مقياس ممارسات الأمن السيبراني

جدول رقم (4) معاملات الارتباط بين فقرات مقياس ممارسات الأمن السيبراني والدرجة الكلية للمقياس.

	ممارسات الأمن السيبراني	معامل الارتباط	مستوى الدلالة
1	**هناك استخدام كلمات مرور قوية ومختلفة لكل حساب**	**0.456****	**0.000**
2	**هناك بتحديث البرامج والتطبيقات بشكل دوري**	**0.488****	**0.000**
3	**تميل الى تجنب فتح الروابط المشبوهة.**	**0.612****	**0.000**
4	**توجد برامج الحماية.(Antivirus)**	**0.462****	**0.000**
5	**هناك حرص على تسجيل الخروج من الحسابات بعد الاستخدام**	**0.615****	**0.000**
6	**لا تشارك بياناتي مع أشخاص غير موثوقين**	**0.541****	**0.000**
7	**شبكات إنترنت المستخدمة آمنة أثناء التعلم**	**0.468****	**0.000**
8	**تتلقى الدعم الكافي من الإدارة فيما يتعلق بالأمن السيبراني**	**0.572****	**0.000**

يوضح الجدول رقم (4) والذي يضم (8) فقرات أن معامل الارتباط بين كل فقرة من فقرات المحور الثاني في الاستبيان والدرجة الكلية للمحور وهي ممارسات الأمن السيبراني ، حيث جاءت كل نتائج فقرات المحور الثاني موجبة وهذا يبين ان

معاملات الارتباط المبينة بالجدول السابق دالة احصائية عند مستوى (0.05) هي علاقات طردية، وهذا يعني انه كلما توافرت فقرات المتغير الفرعي الاول زاد ممارسات الأمن السبراني.

3- **مقياس الثقة بالأمن السيبراني**

الجدول رقم (5) معاملات الارتباط بين فقرات مقياس الثقة بالأمن السيبراني والدرجة الكلية للمقياس.

	الثقة بالأمن السيبراني	معامل الارتباط	مستوى الدلالة
1	توجد ثقة في أن المنصات التعليمية تحمي بياناتي الشخصية.	0.511**	0.000
2	يوجد شعور بالأمان أثناء استخدام أنظمة التعليم الإلكتروني.	0.458**	0.000
3	أن المؤسسات التعليمية توفر حماية كافية للمعلومات.	0.542**	0.000
4	أرى أن سياسات الخصوصية واضحة في المنصات التعليمية.	0.459**	0.000
5	أثق في قدرة الأنظمة على منع الاختراقات.	0.502**	0.000
6	أشعر بالاطمئنان عند إدخال بياناتي الشخصية.	0.452**	0.000
7	أعتقد أن الجهات المسؤولة تستجيب بسرعة للمخاطر الأمنية.	0.399**	0.000

يوضح الجدول رقم (5) والذي يضم (7) فقرات أن معامل الارتباط بين كل فقرة من فقرات المحور الثالث في الاستبيان والدرجة الكلية للمحور وهي الثقة بالأمن السيبراني ، حيث جاءت كل نتائج فقرات المحور الثالث موجبة وهذا يبين ان معاملات الارتباط المبينة بالجدول السابق دالة احصائية عند مستوى (0.05) هي علاقات طردية، وهذا يعني انه كلما توافرت فقرات المتغير الفرعي الثالث زاد الثقة بالأمن السيبراني .

4- **جودة التعليم الإلكتروني**

الجدول رقم (6) معاملات الارتباط بين فقرات مقياس جودة التعليم الإلكتروني والدرجة الكلية للمقياس.

	جودة التعليم الإلكتروني	معامل الارتباط	مستوى الدلالة
1	المحتوى التعليمي المقدم عبر الإنترنت واضح ومنظم	0.618**	0.000
2	المواد التعليمية متاحة بسهولة وفي الوقت المناسب	0.561**	0.000
3	يتم تحديث المحتوى بشكل مستمر	0.451**	0.000
4	يوجد تفاعل فعال بين الطلاب والمعلمين	0.435**	0.000
5	توفر المنصات التعليمية وسائل تواصل متعددة .	0.511**	0.000
6	أشعر بالمشاركة أثناء التعلم الإلكتروني	0.541**	0.000
7	المنصات التعليمية سهلة الاستخدام	0.499**	0.000
8	يمكنني الوصول إلى المحتوى بسهولة	0.563**	0.000
9	لا أواجه صعوبات تقنية أثناء الاستخدام	0.511**	0.000
10	أشعر بالأمان أثناء استخدام منصات التعليم الإلكتروني	0.526**	0.000
11	أثق في حماية بياناتي داخل المنصات التعليمية	0.458**	0.000
12	توفر المنصات سياسات واضحة لحماية الخصوصية	0.547**	0.000
13	أنا راضٍ عن تجربة التعليم الإلكتروني بشكل عام	0.512**	0.000
14	أفضل استخدام التعليم الإلكتروني في المستقبل	0.514**	0.000
15	أرى أن التعليم الإلكتروني يحقق أهداف التعلم بكفاءة	0.651**	0.000

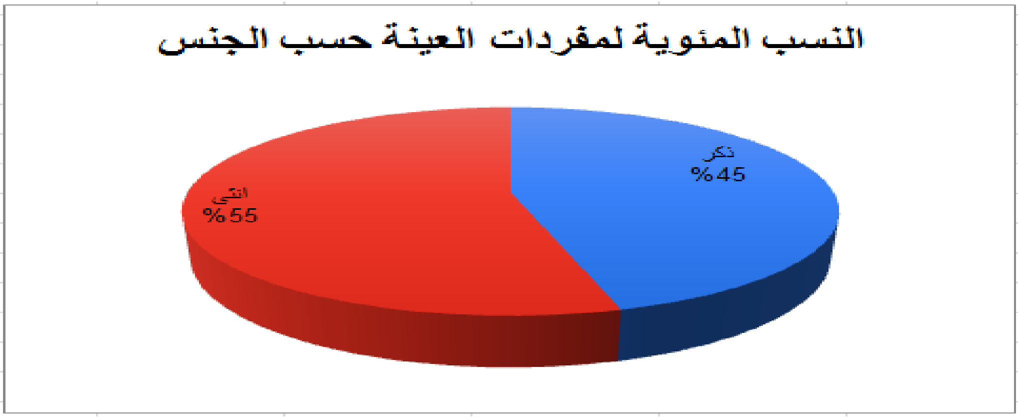
يوضح الجدول رقم (6) والذي يضم (15) فقرات أن معامل الارتباط بين كل فقرة من فقرات المحور الرابع في الاستبيان والدرجة الكلية للمحور وهو جودة التعليم الإلكتروني ، حيث جاءت كل نتائج فقرات المحور الرابع موجبة وهذا يبين ان معاملات الارتباط المبينة بالجدول السابق دالة احصائية عند مستوى (0.05) هي علاقات طردية، وهذا يعني انه كلما توافرت فقرات المتغير الفرعي الرابع زاد جودة التعليم الإلكتروني.

الإحصاء الوصفي: (المتوسطات الحسابية، الانحرافات المعيارية، التكرارات، والنسب المئوية)

1- خصائص عينة الدراسة

الجدول (7) يبين التوزيع التكراري لمفردات مجتمع الدراسة حسب الجنس

الرقم	الجنس	التكرار	النسبة %
1	ذكر	100	%45
2	انثى	120	%55
المجموع		220	%100

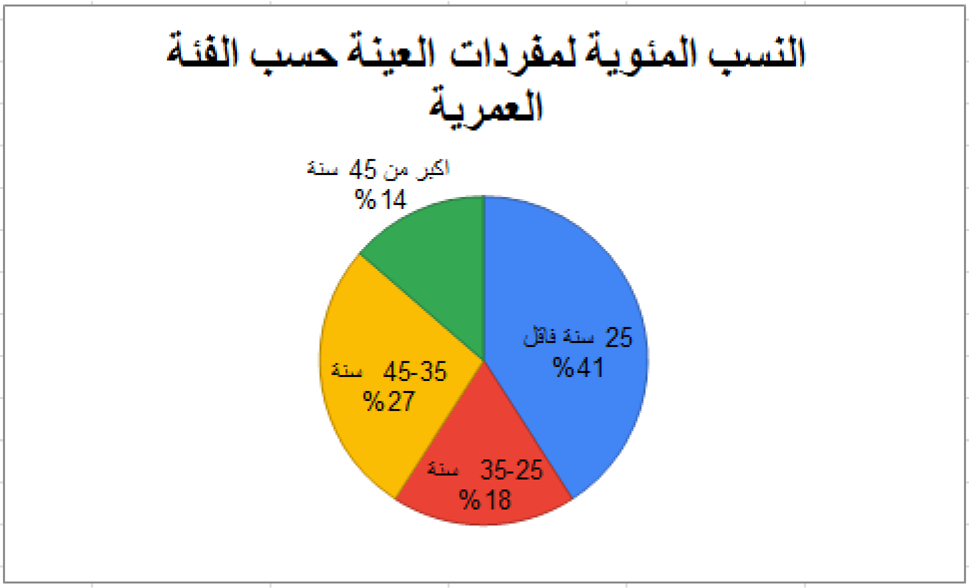


الشكل البياني رقم (1) يبين النسب المئوية لمفردات عينة الدراسة حسب الجنس

تبين من خلال البيانات الواردة في الجدول والاشكال البيانية السابقة، ان اغلب مفردات عينة الدراسة هم فئة الاناث بنسبة (55%) بينما يشكل فئة الذكور نسبة كانت (45%).

الجدول (8) يبين التوزيع التكراري والنسب المئوية لمفردات مجتمع الدراسة حسب الفئة العمرية

الرقم	الفئة العمرية	التكرار	النسبة %
1	25 سنة فاقل	90	%41
2	25-35 سنة	40	%18
	35-45 سنة	60	%27
3	اكبر من 45 سنة	30	%14
المجموع		220	%100



الشكل البياني رقم (2) يبين التوزيع التكراري لمجتمع الدراسة حسب الفئة العمرية

تبين من خلال البيانات الواردة في الجدول والاشكال البيانية السابقة، ان نسبة (14%) كانت للفئة العمرية اكبر من 45 سنة، بينما جاءت نسبة (27%) للفئة العمرية 35-45 سنة واما نسبة (41%) كانت للفئة العمرية اقل من 25 سنة. وكانت نسبة (18%) للفئة العمرية (25-35 سنة).

2- اساليب الاحصاء الوصفي (المتوسط الحسابي، الانحراف المعياري)

التحليل الوصفي (واقع الوعي بالأمن السبراني)

تم احتساب المتوسط الحسابي لكل فقرات المحور الاول معا وكذلك الانحراف المعياري حيث جاءت النتائج على النحو الموضح بالجدول التالي:

الجدول رقم (9) يبين المتوسط الحسابي والانحراف المعياري لمتغير واقع الوعي بالأمن السبراني

ت	العبارة	المتوسط الحسابي	الانحراف المعياري	مدى التوفر
1	توجد معرفة بمخاطر الأمن السيبراني في التعليم الإلكتروني	4.35	0.286	مرتفع
2	يمكن التميز بين المواقع الآمنة وغير الآمنة	4.33	0.421	مرتفع
3	توجد الية لحماية البيانات الشخصية أثناء التعلم الإلكتروني	4.68	0.257	مرتفع
4	هناك ادراك بأهمية حماية البيانات الشخصية أثناء استخدام المنصات التعليمية	4.19	0.361	مرتفع
5	هناك وعي بأساليب الاحتيال الإلكتروني مثل الروابط المزيفة	3.89	0.247	مرتفع
6	هناك وعي مخاطر مشاركة المعلومات الشخصية عبر الإنترنت	3.65	0.324	مرتفع
7	هناك وعي أهمية تحديث البرامج لحماية الأجهزة	3.87	0.289	مرتفع
8	توجد معرفة بأساسيات حماية الخصوصية الرقمية	3.44	0.379	مرتفع
المتوسط الحسابي ككل لمتغير واقع الوعي بالأمن السبراني		4.05	0.320	مرتفع

يتضح من جدول السابق ان المتوسطات الحسابية لمتغير واقع الوعي الامن السبراني جاءت مرتفعة حسب المقياس المعتمد في الدراسة، حيث بلغ المتوسط الحسابي العام لمتغير واقع الامن السبراني (4.05) وانحراف معياري (0.320)، ويشير ذلك الى وجود وعي بالأمن السبراني لدى الطلاب واعضاء هيئة التدريس بالجامعات.

التحليل الوصفي (ممارسات الامن السبراني)

تم ايجاد المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات متغير ممارسات الامن السبراني.

الجدول رقم (10) يبين المتوسط الحسابي والانحراف المعياري لمتغير ممارسات الامن السبراني

ت	العبارة	المتوسط الحسابي	الانحراف المعياري	مدى التوفر
1	هناك استخدام كلمات مرور قوية ومختلفة لكل حساب	3.41	0.352	مرتفع
2	هناك تحديث البرامج والتطبيقات بشكل دوري	3.32	0.483	متوسط
3	تميل الى تجنب فتح الروابط المشبوهة.	3.40	0.361	مرتفع
4	توجد برامج الحماية.(Antivirus)	3.42	0.312	مرتفع
5	هناك حرص على تسجيل الخروج من الحسابات بعد الاستخدام	4.01	0.278	مرتفع
6	لا تشارك بياناتي مع أشخاص غير موثوقين	3.21	0.397	متوسط
7	شبكات إنترنت المستخدمة آمنة أثناء التعلم	3.16	0.612	متوسط
8	تتلقى الدعم الكافي من الإدارة فيما يتعلق بالأمن السيبراني	3.20	0.597	متوسط
المتوسط الحسابي ككل لمتغير ممارسات الامن السبراني		3.39	0.424	مرتفع

يتضح من جدول السابق ان المتوسطات الحسابية لمتغير ممارسات الامن السبراني جاءت متوسطة حسب المقياس المعتمد في الدراسة وحيث بلغ المتوسط الحسابي العام لمتغير ممارسات الامن السبراني (3.39) وانحراف معياري (0.42)، ويشير ذلك الى توفر نظم حماية للمواقع المستخدمة في التعليم الالكتروني.

التحليل الوصفي (الثقة بالأمن السيبراني)

لقد تم ايجاد المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات متغير الثقة بالأمن السيبراني.

الجدول رقم (11) يبين المتوسط الحسابي والانحراف المعياري لمتغير الثقة بالأمن السيبراني

ت	العبارة	المتوسط الحسابي	الانحراف المعياري	مدى التوفر
1	توجد ثقة في أن المنصات التعليمية تحمي بياناتي الشخصية.	4.22	0.397	مرتفع
2	يوجد شعور بالأمان أثناء استخدام أنظمة التعليم الإلكتروني.	4.17	0.481	مرتفع
3	أن المؤسسات التعليمية توفر حماية كافية للمعلومات.	4.23	0.376	مرتفع
4	أرى أن سياسات الخصوصية واضحة في المنصات التعليمية.	4.14	0.484	مرتفع
	أثق في قدرة الأنظمة على منع الاختراقات.	3.75	0.598	مرتفع
	أشعر بالاطمئنان عند إدخال بياناتي الشخصية.	3.99	0.512	مرتفع
	أعتقد أن الجهات المسؤولة تستجيب بسرعة للمخاطر الأمنية.	3.33	0.536	متوسط
المتوسط الحسابي ككل لمتغير الثقة بالأمن السيبراني		3.975	0.483	مرتفع

يتضح من جدول السابق ان المتوسطات الحسابية لمتغير الثقة بالأمن السيبراني جاءت مرتفعة حسب المقياس المعتمد في الدراسة حيث بلغ المتوسط الحسابي العام لمتغير الثقة بالأمن السيبراني (3.975) وانحراف معياري (0.483)، ويشير ذلك الى وجود ثقه بالأمن السبراني لدى اعضاء هيئة التدريس والطلاب المستخدمين لمنصات التعليم الالكتروني.

التحليل الوصفي جودة التعليم الإلكتروني

تم حساب المتوسط الحسابي والانحراف المعياري لمتغير جودة التعليم الإلكتروني وكانت النتائج كما موضحة بالجدول (12):-

الجدول رقم (12) يبين المتوسط الحسابي والانحراف المعياري لمتغير جودة التعليم الإلكتروني

ت	العبارة	المتوسط الحسابي	الانحراف المعياري	مدى التوفر
1	المحتوى التعليمي المقدم عبر الإنترنت واضح ومنظم	3.59	1.275	مرتفع
2	المواد التعليمية متاحة بسهولة وفي الوقت المناسب	4.11	0.321	مرتفع
3	يتم تحديث المحتوى بشكل مستمر	3.89	0.463	مرتفع
4	يوجد تفاعل فعال بين الطلاب والمعلمين	3.80	0.667	مرتفع
5	توفر المنصات التعليمية وسائل تواصل متعددة .	3.53	0.777	مرتفع
6	أشعر بالمشاركة أثناء التعلم الإلكتروني	3.21	0.915	متوسط
7	المنصات التعليمية سهلة الاستخدام	3.87	1.124	مرتفع
8	يمكنني الوصول إلى المحتوى بسهولة	3.07	1.197	متوسط
9	لا أواجه صعوبات تقنية أثناء الاستخدام	3.29	0.815	متوسط
10	أشعر بالأمان أثناء استخدام منصات التعليم الإلكتروني	4.10	0.322	مرتفع
11	أثق في حماية بياناتي داخل المنصات التعليمية	3.25	0.379	متوسط
12	توفر المنصات سياسات واضحة لحماية الخصوصية	3.08	0.388	متوسط
13	أنا راضٍ عن تجربة التعليم الإلكتروني بشكل عام	3.99	0.299	مرتفع
14	أفضل استخدام التعليم الإلكتروني في المستقبل	4.23	0.256	مرتفع
15	أرى أن التعليم الإلكتروني يحقق أهداف التعلم بكفاءة	3.98	0.301	مرتفع
المتوسط الحسابي ككل لمتغير جودة التعليم الإلكتروني		3.66	0.633	مرتفع

يتضح من جدول السابق ان اغلب المتوسطات الحسابية لمتغير جودة التعليم الإلكتروني جاءت مرتفعة حسب المقياس المعتمد في الدراسة ما عدا خمس فقرات جاءت منخفضة، في حين بلغ المتوسط الحسابي العام لمتغير جودة التعليم الإلكتروني (3.66) وانحراف معياري (0.63)، ويشير ذلك الى هناك جودة في التعليم الإلكتروني.

اختبار فرضيات الدراسة

تم استخدام الانحدار البسيط لاختبار فروض الدراسة لمعرفة أثر المتغيرات المستقلة على المتغير التابع. وتم تحديد بعض القواعد والمتمثلة في ان درجة الثقة المتبعة في هذه الدراسة 95%، ومستوى المعنوية لهذه الدراسة يساوي 0.05.

اختبار الفرضية الرئيسية

تنص الفرضية الرئيسية على: لا يوجد أثر ذو دلالة إحصائية للأمن السيبراني (بمكوناته: الوعي والممارسة والثقة) على جودة التعليم الإلكتروني في الجامعات الليبية من وجهة نظر عينة الدراسة.

الفرضيات الفرعية:

- لا يوجد أثر ذو دلالة إحصائية لمستوى الوعي الأمني السيبراني في جودة التعليم الإلكتروني لدى أعضاء هيئة التدريس والطلاب.
- لا يوجد أثر ذو دلالة إحصائية لتطبيق ممارسات الأمن السيبراني في جودة التعليم الإلكتروني.
- لا يوجد أثر ذو دلالة إحصائية بين الثقة بالأمن السيبراني وجودة التعليم الإلكتروني.
- لا توجد فروق ذات دلالة إحصائية في مستوى الوعي والممارسة الأمنية لدى عينة الدراسة تعزى للمتغيرات الديموغرافية (الفئة، الجنس، العمر، المستوى الأكاديمي).

1- اختبار الفرضيات الفرعية المستقلة

- **اختبار الفرضية الفرعية الاولى**:

لا يوجد أثر ذو دلالة إحصائية للأمن السيبراني وفق البعد الوعي بالأمن السبراني على جودة التعليم الإلكتروني في الجامعات الليبية من وجهة نظر عينة الدراسة عند مستوى الاهمية ($\alpha \leq 0.05$).

جدول رقم (13) تحليل الانحدار الخطي لإيجاد اثر الوعي بالأمن السبراني على جودة التعليم الالكتروني

البيان	قيمة B	قيمة T	معامل الارتباط R	معامل التحديد R^2	قيمة F	مستوى المشاهد المعنوية
اثر الوعي بالأمن السبراني على جودة التعليم الالكتروني	0.428	3.806	0.460	0.211	14.494	0.000

يتضح من الجدول السابق ان قيمة معامل الارتباط يساوي (0.460) بإشارة موجبه، وهذا يدل بان العلاقة بين الوعي بالأمن السبراني و وجودة التعليم الإلكتروني علاقة طردية، أي كلما زادت الوعي بالأمن السبراني زادت وجودة التعليم الإلكتروني ، وهذا يرجع الى ما يوفره الامن السبراني من حماية للمنصات التعليم الاكثروني، كما ان معامل التحديد (R^2) يساوي (0.211)، مما يعني ان الوعي بالأمن السبراني مسئولة عن تفسير (21%) من التغيرات التي تحدث في جودة التعليم الإلكتروني، وهناك ما نسبته (79%) يرجع لعوامل اخرى مثل الثقة بالأمن السبراني وممارسات الامن السبراني وعوامل اخرى بالإضافة الى حد الخطأ العشوائي.

وحيث ان قيمة (F) المحسوبة تساوي (14.494) بمستوى معنوية مشاهد اقل من (0.05) ويساوي (0.000) وهذ يشير الى ان النموذج معنوي في تفسير العلاقة وقياس الاثر، وبالتالي يتم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تنص على " يوجد اثر ذو دلالة احصائية للوعي بالأمن السبراني على جودة التعليم الالكتروني". كما تدعم الفرضية البديلة قيم (T) والتي تساوي (3.806) بمستويات معنوية مشاهدة اقل من (0.05)، وتساوي (0.000)، أي انه يوجد اثر ايجابي للوعي بالأمن السبراني على جودة التعليم الالكتروني.

- **اختبار الفرضية الفرعية الثانية** :

لا يوجد أثر ذو دلالة إحصائية للأمن السيبراني وفق البعد ممارسات الأمن السبراني على جودة التعليم الإلكتروني في الجامعات الليبية من وجهة نظر عينة الدراسة عند مستوى الاهمية ($\alpha \leq 0.05$). **الجدول رقم (14) تحليل الانحدار الخطي لإيجاد اثر ممارسات الأمن السبراني على جودة التعليم الالكتروني.**

البيان	قيمة B	قيمة T	معامل الارتباط R	معامل التحديد R^2	قيمة F	مستوى المعنوية المشاهد
اثر ممارسات الأمن السبراني على جودة التعليم الالكتروني..	**0.699**	**7.547**	**0.606**	**0.368**	**56.958**	**0.000**

يتضح من الجدول السابق ان قيمة معامل الارتباط يساوي (0.606) بإشارة موجبه، وهذا يدل بان العلاقة بين ممارسات الامن السبراني و جودة التعليم الالكتروني علاقة طردية، كما ان معامل التحديد (R^2) يساوي (0.368)، مما يعني ان ممارسات الامن السبراني مسئولة عن تفسير (37%) من التغيرات التي تحدث في جودة التعليم الالكتروني ، وهناك ما نسبته (63%) يرجع لعوامل اخرى مثل الثقة بالأمن السبراني والوعي بالأمن السبراني وعوامل اخرى بالإضافة الى حد الخطأ العشوائي.

وحيث ان قيمة (F) المحسوبة تساوي (56.958) بمستوى معنوية مشاهد اقل من (0.05) ويساوي (0.000) وهذ يشير الى ان النموذج معنوي في تفسير العلاقة وقياس الاثر، وبالتالي يتم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تنص على " يوجد اثر ذو دلالة احصائية للممارسات الأمن السبراني على جودة التعليم الالكتروني ".

كما تدعم الفرضية البديلة قيم (T) والتي تساوي (7.547) بمستويات معنوية مشاهدة اقل من (0.05)، وتساوي (0.000)، أي انه يوجد اثر ايجابي للممارسات الامن السبراني على جودة التعليم الالكتروني.

- **اختبار الفرضية الفرعية الثالثة :**

لا يوجد أثر ذو دلالة إحصائية للأمن السيبراني وفق بعد الثقة بالأمن السبراني على جودة التعليم الإلكتروني في الجامعات الليبية من وجهة نظر عينة الدراسة عند مستوى الاهمية ($\alpha \leq 0.05$). **الجدول رقم (15) تحليل الانحدار الخطي لإيجاد اثر الثقة بالأمن السبراني على جودة التعليم الالكتروني.**

البيان	قيمة B	قيمة T	معامل الارتباط R	معامل التحديد R^2	قيمة F	مستوى المعنوية المشاهد
اثر الثقة بالأمن السبراني على جودة التعليم الالكتروني.	0.645	5.885	0.511	0.261	34.636	0.000

يتضح من الجدول السابق ان قيمة معامل الارتباط يساوي (0.511) بإشارة موجبه، وهذا يدل بان العلاقة بين الثقة بالأمن السبراني وجودة التعليم الكتروني علاقة طردية قوية، كما ان معامل التحديد (R^2) يساوي(0.261)، مما يعني ان الثقة بالأمن السبراني مسئولة عن تفسير (26%) من التغيرات التي تحدث في جودة التعليم الالكتروني، وهناك ما نسبته (74%) يرجع لعوامل اخرى مثل ممارسات الأمن السبراني والوعي بالأمن السبراني وعوامل اخرى بالإضافة الى حد الخطأ العشوائي وحيث ان قيمة (F) المحسوبة تساوي (34.636) بمستوى معنوية مشاهد اقل من (0.05) ويساوي (0.000) وهذ يشير الى ان النموذج معنوي في تفسير العلاقة وقياس الاثر، وبالتالي يتم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تنص على " يوجد اثر ذو دلالة احصائية للثقة بالأمن السبراني على جودة التعليم الالكتروني".

كما تدعم الفرضية البديلة قيم (T) والتي تساوي (5.885) بمستويات معنوية مشاهدة اقل من (0.05)، وتساوي (0.000)، أي انه يوجد اثر ايجابي للثقة بالأمن السبراني على جودة التعليم الالكتروني.

نتائج الدراسة واستنتاجاتها

بناءً على التحليل الإحصائي للبيانات باستخدام برنامج (SPSS)، والإجابة عن أسئلة الدراسة واختبار فرضياتها، تم التوصل إلى الاستنتاجات الرئيسية التالية:

1- أظهرت النتائج أن مستوى الوعي النظري بأهمية الأمن السيبراني لدى عينة الدراسة (أعضاء هيئة التدريس والطلاب) جاء مرتفعاً حيث بلغ المتوسط الحسابي (4.05). غير أن مستوى الممارسة الفعلية لتلك الإجراءات جاءت متوسطا حيث بلغ المتوسط الحسابي (3.39)، مما يؤكد وجود "فجوة سلوكية" بين المعرفة الأمنية والتطبيق الفعلي، وهو ما يتفق مع ما أشارت إليه الدراسات السابقة.

2- اظهرت النتائج أن مستوى الوعي بالأمن السيبراني لدى أفراد العينة مرتفع نسبيًا، كما أن انخفاض الانحراف المعياري يشير إلى وجود تقارب في إجابات المشاركين وعدم تشتتها.

3- اظهرت النتائج أن مستوى الثقة في الأنظمة الإلكترونية مرتفع نسبيًا، مما يعكس شعورًا عامًا بالأمان لدى المستخدمين.

4- اظهرت نتائج التحليل الإحصائي وجود علاقة ارتباط إيجابية قوية بين الأمن السيبراني وجودة التعليم الإلكتروني، حيث بلغ معامل الارتباط (0.76)، كما أوضح تحليل الانحدار أن الأمن السيبراني يفسر ما نسبته (58%) من التغير في جودة التعليم الإلكتروني، وكان لبعد الثقة التأثير الأكبر، يليه الممارسة ثم الوعي، وجميعها ذات دلالة إحصائية عند مستوى (0.05).

5- اظهرت النتائج أن فئة الاناث تمثل النسبة الأكبر من عينة الدراسة مقارنة بالذكور، حيث تجاوزت نسبتهم النصف. وقد يعكس ذلك طبيعة مجتمع الدراسة أو الفئة المستهدفة التي يغلب عليها الاناث، أو ارتفاع معدل استجابتهم للاستبانة. ويشير هذا التوزيع إلى وجود تمثيل مقبول لكلا الجنسين، مما يعزز من إمكانية تعميم نتائج الدراسة وعدم انحيازها لفئة دون أخرى.

6- تشير هذه النتائج إلى أن غالبية أفراد العينة من الفئة الشبابية (أقل من 25 سنة)، وهو أمر منطقي في الدراسات المرتبطة بالتعليم الإلكتروني، حيث تُعد هذه الفئة الأكثر استخدامًا للتكنولوجيا والمنصات الرقمية.

7- تشير النتائج الى وجود تمثيل جيد للفئات العمرية الأخرى، خاصة الفئة (35–45 سنة)، مما يعكس تنوعًا عمريًا في العينة ويسهم في إثراء نتائج الدراسة من حيث اختلاف الخبرات والقدرات التقنية. وفي المقابل، جاءت الفئة الأكبر من 45 سنة بأقل نسبة، وهو ما قد يُعزى إلى انخفاض استخدام هذه الفئة للتقنيات الحديثة أو قلة مشاركتها في التعليم الإلكتروني.

التوصيات :-

بناءً على الاستنتاجات السابقة، وما كشفت عنه من فجوة بين الوعي والممارسة، يمكن تقديم التوصيات التالية، مقسمة إلى ثلاثة محاور لضمان قابليتها للتطبيق:

أولاً: توصيات تقنية (لإدارات تقنية المعلومات في الجامعات):

– الانتقال الفوري من نظم الحماية الأساسية إلى نظم المصادقة المتعددة العوامل (FA2) للوصول إلى منصات التعليم الإلكتروني، لضمان حماية البيانات الأكاديمية .

– إجراء "تقييمات اختراق" (Penetration Testing) دورية للمنصات التعليمية، بدلاً من الانتظار لحدوث الأزمات، لسد الثغرات التقنية التي تهدد استمرارية التعليم.

ثانياً: توصيات بشرية وسلوكية (لتقديم برامج التدريب والتوعية):

- تصميم برامج تدريبية تُركز على "تغيير السلوك" وليس فقط "نقل المعلومات"، لسد الفجوة المكتشفة بين الوعي النظري والممارسة الفعلية لدى الطلاب والأساتذة .

- تضمين مهارات الدفاع السيبراني الشخصي (كيفية التعامل مع التصيد الإلكتروني، إدارة كلمات المرور) كمتطلب إلزامي ضمن مقررات "مهارات الحاسب" للطلاب المستجدين.

ثالثاً: توصيات مؤسسية واستراتيجية (لرئاسة الجامعة وعمادات الكليات):

- دمج "مؤشرات الأداء الأمني السيبراني" (KPIs) كجزء أساسي من معايير الاعتماد الأكاديمي وضمان الجودة داخل الجامعة، بحيث لا تُقيّم جودة المنصة إلا بعد تأكيد أمانها.

- تعزيز الشفافية المؤسسية من خلال إطلاق تقارير دورية توضح للطلاب والأساتذة الإجراءات الأمنية المتخذة لحماية بياناتهم، بهدف تعزيز "الثقة" التي أثبتت الدراسة أنها محور أساسي لنجاح التعليم الرقمي.

رابعاً: توصيات بحثية (للمستقبل):

- إجراء دراسات مستقبلية تعتمد على المنهج المختلط (الكيفي والكمي) لفهم الأسباب النفسية العميقة الكامنة وراء مقاومة الطلاب لتطبيق الإجراءات الأمنية رغم إدراكهم لأهميتها.

- توسيع نطاق الدراسة لتشمل جامعات ليبية متعددة ومقارنة مستويات الجاهزية السيبرانية بينها.

المراجع العربية

الميعة، م. أ.، الخسافنة، أ.، والثنيبات، أ. (2020). التحديات الحرجة والعوامل المؤثرة على استخدام نظام التعليم الإلكتروني خلال جائحة كوفيد-19. مجلة تقنيات التعليم والمعلومات، 25(6)، 5261–5280.

الحربي، م. (2019). بناء استراتيجيات مؤسسية للأمن السيبراني لدعم التحول الرقمي في مؤسسات التعليم العالي وضمان استمراريته. مجلة الدراسات التربوية والإدارية، 15(2)، 45-68.

العربي، أ. (2021). الأمن السيبراني: المفاهيم الأساسية وأمن الشبكات والمنصات الرقمية. دار النشر والتوزيع الأكاديمي.

العتيبي، ف. (2021). أثر تطبيق سياسات الأمن السيبراني على رفع ثقة الطلاب في استخدام أنظمة التعليم الإلكتروني في الجامعات السعودية. مجلة بحوث التعليم العالي، 33(1)، 112-134.

عياد، ر. (2020). جاهزية البنية التحتية الأمنية كعائق أمام تبني التعليم الإلكتروني في الجامعات العربية وانعكاسها على جودة الخدمات. مجلة تكنولوجيا التعليم، 28(4)، 89-110.

الغرياني، س. (2022). حماية البيانات وأمن المعلومات في المؤسسات الحديثة: نحو بيئة رقمية آمنة. مركز النشر العلمي بالجامعات.

الموسوي، ع. (2018). الارتباط بين تطبيق معايير الأمن السيبراني وجودة التعليم الإلكتروني وفق نظام ضمان الجودة الشامل. مجلة البحوث الأكاديمية، 12(3)، 77-98.

Reference

Aldawood, H., & Skinner, G. (2019). Educating and raising awareness on cybersecurity within educational institutions. Information and Computer Security, 27(3), 316-329.

Alharthi, A., Krotov, V., & Bowman, M. (2017). Addressing factors affecting student adoption and usage of cloud computing: A systematic review of challenges and solutions. International Journal of Information Management, 37(3), 245-256.

AlHogail, A. (2018). Improving cybersecurity awareness in higher education: A conceptual framework. Journal of Information Security and Applications, 40, 157–164. https://doi.org/10.1016/j.jisa.2018.03.005

Almaiah, M., Al-Khasawneh, A., & Althunibat, A. (2020). Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. Education and Information Technologies, 25(6), 5261-5280.

Ali, A., & Hassan, N. (2020). The role of cybersecurity in enhancing trust in digital services and supporting sustainable development. Journal of Digital Security, 4(1), 22-35.

González-Zamar, M. D., Abad-Segura, E., López-Meneses, E., & Gómez-Galán, J. (2020). Managing ICT for sustainable education: An overview in the context of higher education. Sustainability, 12(19), 8254.

Ifinedo, P. (2021). Examining students' perception of e-learning cybersecurity, trust, and satisfaction. Education and Information Technologies, 26(4), 4567–4585. https://doi.org/10.1007/s10639-021-10435-7.

Johnson, C. (2021). Cybersecurity: Principles, practices, and predictive intelligence for digital environments. Wiley Publications.

Miranda, J., Navarrete, C., Noguez, J., Molina-Espinosa, J. M., Ramírez-Montoya, M. S., Navarro-Tuch, S. A., Bustamante-Bello, R., Rosas-Fernández, J. B., & Molina, A. (2021). The core components of education 4.0 in higher education: Three case studies in engineering education. Computers in Human Behavior, 119, 106715. https://doi.org/10.1016/j.chb.2021.106715

Smith, R. (2019). Cybersecurity and critical infrastructure protection: National strategies and legal frameworks. International Journal of Cybersecurity Intelligence & Cybercrime, 2(1), 12-25