مجلة كلية الشرطة للعلوم الأمنية والمجتمعية
عدد خاص - المؤتمر السنوي الثاني لسنة ١٤٤٧ هـ-٢٠٢٥ م

إستراتيجية تعزيز دور الطالب الجامعي في إدارة الأزمات السيبرانية

(دراسة تحليلية)

Strategy To Enhance The Role Of University Student In Managing Cyber Crices

(An Analytical Study)

ا.م.د. فاضلة علي جيجان
كليه الإدارة والاقتصاد
الجامعة المستنصرية

ا.م.د. سلمى غضبات حسين
كلية الإدارة والاقتصاد
الجامعة المستنصرية

الرائد الدكتور علي قاسم محمد
مديرية التدريب والتأهيل
وزارة الداخلية

Assistant Professor. Dr.
Fadhela Ali Jigan
College of Administration and Economics,
Al-Mustansiriya University

Assistant Professor. Dr.
Salma Ghadbat Hussein
College of Administration and Economics,
Al-Mustansiriya University

Major Dr.
Ali Qasim Mohammed
Directorate of Training and Development,
Ministry of Interior

١٤٤٧هـ

٢٠٢٥مـ

الملخص:

في ظل التحول التكنولوجي المتسارع والبنية التكنولوجية المتطورة في العراق، أصبحت الحاجة إلى سرعة استجابة الحكومة العراقية للأزمات أمرًا حيويًا لمواجهة التهديدات المتزايدة، لا سيما في مجال الأمن السيبراني، إذ تمكّن البنية التكنولوجية المتقدمة الحكومة من إصدار التوجيهات واتخاذ القرارات الفورية لدعم المؤسسات التعليمية. وتعتمد فعالية هذه الاستجابة بشكل كبير على جاهزية الجامعات والمعاهد، باعتبارها اللبنة الأساسية للمجتمع، إذ تُمكّن هذه الجاهزية المؤسسات التعليمية من تنفيذ الإجراءات الوقائية والتصحيحية بسرعة وفاعلية، بما يضمن تطبيق السياسات القانونية والتقنية المقررة وحماية الأنظمة الرقمية والمعلومات الحساسة.تستند فعالية هذه الاستجابة أيضًا إلى وجود إطار قانوني واضح للأمن السيبراني وبنية تكنولوجية متطورة، مما يمكّن الجامعات من تطبيق السياسات والإجراءات الوقائية والتصحيحية بسرعة ودقة. تركز الدراسة على تقييم استعداد الجامعات لمواجهة الأزمات السيبرانية وعلاقته بعدة عوامل تشمل: الوعي بالأمن السيبراني، جهود الجامعة في تعزيز الأمن، السياسات والقوانين الجامعية، استخدام الأنظمة الرقمية، الثقافة الأمنية في المجتمع الجامعي، والخبرة الشخصية مع الحوادث، بالإضافة إلى دور الطلاب في دعم الأمن السيبراني من خلال الالتزام بالممارسات الوقائية والمشاركة الفعّالة في برامج التوعية .أظهرت نتائج الدراسة، التي استندت إلى استبانة إلكترونية شارك فيها ٢٠٠ طالب وطالبة وتحليلها باستخدام برنامج SPSS ، الى أن تعزيز استعداد الجامعات يتطلب برامج توعية متكاملة، واستخدام فعال للتقنيات الرقمية بالإضافة إلى ذلك الوعي العام بالأمن السيبراني ، واستنادا على ما توصلت إليه الدراسة من نتائج فقد وضعت مجموعة من التوصيات كان من أهمها تكثيف برامج التوعية وبناء بيئة تقنية متكاملة تدعم الأمن السيبراني

مع متابعة تأثير السياسات والقوانين بشكل متزامن لتقليل أي تأثير سلبي محتمل، وتعزيز مشاركة الطلاب بشكل إيجابي ومدروس.

الكلمات المفتاحية : ازمات، الامن السيبراني، التطور التكنلوجي.

Abstract:

In light of the rapid technological transformation and advanced technological infrastructure in Iraq, the Iraqi government's prompt response to crises has become vital in addressing growing threats, particularly in the area of cybersecurity. An advanced technological infrastructure enables the government to issue directives and make immediate decisions to support educational institutions. The effectiveness of this response depends largely on the preparedness of universities and institutes, as they are the cornerstone of society. This preparedness enables academic institutions to implement preventive and corrective measures quickly and effectively, ensuring the implementation of established legal and technical policies and the protection of digital systems and sensitive information. The effectiveness of this response also depends on the presence of a clear legal framework for cybersecurity and an advanced technological infrastructure, which enables universities to implement preventive and corrective policies and procedures quickly and accurately. The study focuses on assessing universities' preparedness to confront cyber crises and its relationship to several factors, including: Cybersecurity awareness, university efforts to enhance security, university policies and laws, use of digital systems, security culture in the university community, personal experience with incidents, in addition to the role of students in supporting cybersecurity through adherence to preventive practices and active participation in awareness programs. The results of the study, which

was based on an electronic questionnaire in which 200 male and female students participated and analyzed using the SPSS program, showed that enhancing university preparedness requires integrated awareness programs, effective use of digital technologies, in addition to general awareness of cybersecurity. Based on the results of the study, A set of recommendations was developed, the most important of which was to intensify awareness programs and build an integrated technical environment that supports cybersecurity, while simultaneously monitoring the impact of policies and laws to minimize any potential negative impact and enhance student engagement positively and thoughtfully.
Keywords: crises, cybersecurity, technological development.

١-مقدمة البحث

يشهد العالم المعاصر تسارعًا ملحوظًا في التحول الرقمي وتوسعًا في استخدام التقنيات الحديثة، وهو ما أفرز تحديات أمنية جديدة تتطلب استجابة مؤسسية وحكومية متوازنة وسريعة. ولا يمكن تحقيق هذه الاستجابة بفاعلية ما لم تستند على بنية تكنولوجية رصينة وإطار قانوني متكامل يحدد المسؤوليات ويوجه السياسات المرتبطة بالأمن السيبراني.

وفي هذا الإطار، تبرز الجامعات والمعاهد بوصفها مؤسسات تعليمية وبحثية رائدة، تمثل النواة الأساسية للمجتمع، إذ تتهيأ داخلها بيئة رقمية متشابكة تُستخدم فيها الأنظمة والمنصات الإلكترونية بشكل مكثف، مما يجعلها عرضةً للعديد من التهديدات السيبرانية. ومن هنا تبرز أهمية دراسة مستوى جاهزيتها لمواجهة هذه الأزمات، ليس من زاوية توافر الموارد التكنولوجية فحسب، بل من خلال مدى انسجام سياساتها الداخلية مع التشريعات الوطنية في مجال الأمن السيبراني أيضًا.

يُشكِّل الطلاب إحدى الركائز الأساسية في منظومة الجامعات، إذ يمثلون الفئة الأكثر تفاعلًا مع البيئة الأكاديمية والتقنيات المستخدمة فيها. ومن هنا، تبرز أهمية دمج الطلاب في خطط إدارة الأزمات، ليس كمتلقين للقرارات فحسب، بل كشركاء فاعلين يساهمون في تخطيط وتنفيذ الحلول لمواجهة التحديات ايضاً. كما أن تعزيز الوعي الأمني السيبراني لدى الطلاب يعد من الأولويات في عصر يتزايد فيه الاعتماد على الأنظمة الرقمية والخدمات الإلكترونية داخل الجامعات، لما لذلك من أثر مباشر في حماية البيانات الأكاديمية والخصوصية المؤسسية.

وعلى الرغم من ذلك، تواجه الجامعات تحديات في استثمار دور الطلاب بشكل فعال بسبب محدودية البرامج التوعوية، ضعف الموارد، وقلة المعرفة التقنية في بعض الأحيان لذلك يستهدف

هذا البحث دراسة وتحليل دور الطلاب في إدارة الأزمات وضمان الأمن السيبراني في الجامعات، مع التركيز على تحديد المستويات الحالية للوعي الأمني، والعوامل التي تؤثر على مشاركة الطلاب، واقتراح استراتيجيات فعالة لتعزيز دورهم .

وبناءً على ما سبق، يسعى هذا البحث إلى دراسة استعداد الجامعة للأزمات من خلال تحليل مجموعة من العوامل المؤثرة، وعلى رأسها دور الطالب في دعم الأمن السيبراني وتعزيز ثقافة الوقاية والاستجابة .كما يتناول البحث مستوى وعي الطلبة بالأمن السيبراني، وإسهامهم في خطط الجامعة لمواجهة الأزمات، إلى جانب استعراض العوامل الأخرى ذات الصلة التي تؤثر في مستوى الاستعداد المؤسسي.

ويتركز البحث على مشكله البحث واهميته واهدافه، وكذلك يبحث إدارة الأزمات والأمن السيبراني ، الإطار القانوني والحوكمي لإدارة الأزمات ، والأمن السيبراني والى دور الجامعات في تعزيز الامن السيبراني ودور الطالب ، أدوات الحماية في الأمن السيبراني بالجامعات.

١-١ أهمية البحث

تكمن أهمية هذا البحث في:

١- تعزيز مشاركة الطلاب كشركاء فعّالين في إدارة الأزمات الجامعية، مما يسهم في تحسين سرعة الاستجابة ويقلل من تأثير الأزمات.

٢- رفع الوعي الأمني السيبراني لدى الطلاب، وهو أمر ضروري وحيوي لحماية البيانات والمعلومات من التهديدات المتزايدة في عصر التحول الرقمي.

٣- تطوير برامج توعوية فعالة تعتمد على مشاركة الطلاب بشكل مباشر، بما يخلق بيئة تعليمية أكثر أمانًا واستقرارًا.

٤- سد فجوة البحث العلمي في موضوع دمج الطلاب في إدارة الأزمات والأمن السيبراني، خصوصًا في السياقات الجامعية.

٢-١هدف البحث

يهدف هذا البحث إلى:

- تقييم مستوى استعداد الجامعة للأزمات السيبرانية.

- تحديد أثر كل من الوعي بالأمن السيبراني، جهود الجامعة، دور الطالب، السياسات والقوانين، استخدام الأنظمة الرقمية، الثقافة المجتمعية، والخبرة الشخصية مع الحوادث السيبرانية على استعداد الجامعة.

٣- 1مشكلة البحث

على الرغم من تزايد اعتماد الجامعات على الأنظمة الرقمية في إدارة شؤونها الأكاديمية والإدارية، إلا أن استعدادها لمواجهة الأزمات السيبرانية ما يزال محدوداً ، وهو ما ينعكس على ضعف ثقافة الأمن السيبراني، وتفاوت مستوى تطبيق السياسات والإجراءات الوقائية، وقصور دمج الطلاب في خطط الاستجابة وتتمثل المشكلة الرئيسة في وجود فجوة بين متطلبات الأمن السيبراني وبين جاهزية الجامعات فعليًا للتعامل مع الأزمات، بما يجعل دور الطالب في هذا السياق غير مستثمر بالشكل الأمثل .

وتتمثل مشكلة البحث في السؤال الرئيس التالي :كيف يمكن تعزيز دور الطلاب في إدارة الأزمات وضمان الأمن السيبراني في الجامعات من خلال تطوير برامج توعية واستراتيجيات تشاركية فعالة؟

٢- الجانب النظري

٢-١ إدارة الأزمات

اصبحت الأزمات، بمختلف أشكالها، واقعًا تواجهه المؤسسات في عصر العولمة، إذ تتسم البيئة الحديثة بتغيرات سريعة وتفاعلات معقدة بين العوامل الاقتصادية والسياسية والتكنولوجية. ومن ثم، لم يعد مفهوم إدارة الأزمات مقتصرًا على التعامل مع الكوارث الطبيعية أو الأزمات التنظيمية، بل تطوّر ليشمل أبعادًا جديدة تتعلق بالبنية التكنولوجية والتحول الرقمي. تهدف إدارة الأزمات إلى الاستعداد الاستباقي لمواجهة المخاطر، والاستجابة الفاعلة عند وقوعها، والحد من آثارها السلبية لضمان استمرارية العمل وتحقيق الاستقرار المؤسسي.

وقد مثّلت جائحة كورونا (COVID-19) نموذجًا بارزًا لتحديات الأزمات المعاصرة، إذ أجبرت الجامعات على تبنّي التعليم الإلكتروني والتحول الرقمي بشكلٍ مفاجئ، مما كشف عن الحاجة إلى بنى تحتية رقمية قوية وإجراءات قانونية وتنظيمية تضمن حماية البيانات واستمرار العملية التعليمية. أبرزت هذه التجربة الدور الحيوي الذي يمكن أن تؤديه الجامعات في إدارة الأزمات متعددة الأبعاد، من خلال التخطيط المسبق، وتنسيق الجهود بين الإدارات، وتفعيل القدرات التقنية والبشرية لمواجهة المتغيرات الطارئة ومن خلال هذه التجربة، ظهرت علاقة وثيقة بين إدارة الأزمات الصحية وإدارة الأزمات السيبرانية؛ فكلاهما يتطلب استجابة سريعة، وتنسيقًا مؤسسيًا، ورفعًا لمستوى الوعي والجاهزية فالتحول المفاجئ إلى التعليم الإلكتروني خلال الجائحة أدى إلى زيادة الاعتماد على الأنظمة الرقمية، مما جعل الجامعات أكثر عرضة للتهديدات السيبرانية مثل الاختراق، وتسريب البيانات

وتعطيل الخدمات وهكذا، تطورت إدارة الأزمات في الجامعات من إطارها التقليدي إلى إطار رقمي وقانوني متكامل يعالج المخاطر السيبرانية بوصفها امتدادًا طبيعيًا لتجربة الأزمات السابقة. وفي هذا الإطار، أصبح لزامًا على الجامعات أن تعتمد استراتيجيات استباقية للأمن السيبراني تشمل:

المراقبة والكشف المبكر: الإفادة من الأنظمة والتقنيات المتقدمة للكشف المبكر عن التهديدات.

تحديد الأولويات: تصنيف الحوادث بناءً على شدتها وتأثيرها على الأعمال.

الاستجابة التقنية والقانونية: معالجة الثغرات الأمنية، واحتواء الهجمات، والتعاون مع جهات إنفاذ القانون عند الحاجة.

الاسترداد وإعادة التشغيل: استعادة البيانات من النسخ الاحتياطية وإعادة تشغيل الأنظمة مع الحفاظ على سلامتها.

التعلم والتحسين: تحليل الأسباب الجذرية للاختراق واتخاذ الإجراءات اللازمة لمنع تكراره.

لقد أسهمت تجربة جائحة كورونا في ترسيخ الوعي بأهمية الجاهزية الرقمية داخل الجامعات ومهّدت الطريق أمام مفهوم إدارة الأزمات السيبرانية، الذي يربط بين البنية التكنولوجية والإطار القانوني والوعي الطلابي ومن هنا برزت أهمية الطالب الجامعي كشريك فاعل في منظومة الأمن السيبراني، قادر على دعم استدامة البيئة التعليمية الرقمية، والمساهمة في الوقاية والاستجابة السريعة لأي أزمة رقمية محتملة (الحيالي ، ٢٠٢١: ٦٦-٨٣).

٢-٢ الأمن السيبراني

الأمن السيبراني هو مجموعة من السياسات والإجراءات والتقنيات المصممة لحماية الأنظمة والشبكات والبرامج والمعلومات الرقمية من التهديدات والهجمات السيبرانية إذ ان سرية البيانات

وسلامتها من أهدافها الرئيسة ومع تسارع التحول الرقمي، لم يعد الأمن السيبراني خيارًا تقنيًا بحتًا؛ بل أصبح عنصرًا استراتيجيًا في جميع القطاعات، بما في ذلك الجامعات والمؤسسات التعليمية، التي تعتمد بشكل كبير على البنية التحتية الرقمية للتعليم والبحث والحكومة (الشمري ,٢٠٢١: ١٥٣-١٥٦).

٣-٢ الإطار القانوني والحوكمي لإدارة الأزمات والأمن السيبراني

تشكل الحوكمة أحد الركائز الأساسية لضمان سرعة وكفاءة الاستجابة للأزمات على مستوى الدولة، بما في ذلك الأزمات السيبرانية التي قد تؤثر على المؤسسات والخدمات الحكومية. وتتمثل أهمية الحوكمة في تحديد الأدوار والمسؤوليات بين الجهات الحكومية المختلفة، ووضع السياسات والإجراءات الموحدة، وضمان تدفق المعلومات بسرعة ودقة لاتخاذ القرارات الحاسمة في الوقت المناسب.

تشمل عناصر الحوكمة لإدارة الأزمات والأمن السيبراني ما يأتي (شنشول ،٢٠٢٥: ١٢-١٥):

١. تحديد القواعد والإجراءات التي يجب اتباعها من قبل جميع المؤسسات الحكومية والخاصة، بما في ذلك الجامعات، لضمان التوافق والتنسيق الفعّال.

٢. تحديد الجهات المسؤولة عن الرصد، الاستجابة، التعافي، والتنسيق مع الهيئات الأخرى لضمان سرعة التعامل مع الحوادث.

٣. إنشاء مراكز وطنية لمراقبة التهديدات السيبرانية واكتشافها بشكل مبكر، بما يتيح التدخل السريع قبل تفاقم الأزمة.

٤. ضمان التعاون بين القطاعات الحكومية، القطاع الخاص، والجامعات لتبادل المعلومات والخبرات وأفضل الممارسات في مواجهة الأزمات.

٥.توفير بيانات دقيقة وتحليلات مستمرة لدعم صانعي القرار في إدارة الأزمات، وتقليل التأثيرات السلبية على المجتمع والخدمات العامة.

يؤكد تقرير ENISA (2022) أن وجود إطار حوكمي متكامل يمثل عاملًا حاسمًا لفعالية إدارة الأزمات السيبرانية، إذ يسمح للجهات الرسمية بتنسيق الجهود بسرعة وفعالية، ويضمن إعداد المؤسسات، بما فيها الجامعات، لتطبيق السياسات الحوكمة بشكل متناسق كما يشير إطار عمل NIST CSF 2.0 (2024) إلى أن الحوكمة تعد العنصر الأول لضمان استجابة سريعة ومنسقة، من خلال وضع السياسات والمعايير وتحديد المسؤوليات بوضوح ،كما يُشكل دور الطلاب جزءًا محوريًا من هذا الإطار، إذ يمكن أن يكونوا نقطة قوة أو ضعف في مواجهة الأزمات، اعتمادًا على مدى وعيهم والتزامهم بالسياسات القانونية والتقنية إن دمج الطلاب في برامج التوعية والمبادرات الأمنية، وتوضيح حقوقهم وواجباتهم القانونية، يعزز من فعالية الاستجابة الجماعية ويخلق ثقافة أمنية شاملة داخل البيئة الجامعية.

٤-٢ الامن السيبرانية في الجامعات

في السياق الأكاديمي، أصبحت الجامعات بيئة رقمية معقدة، تعتمد على منصات التعلم الإلكتروني، وقواعد البيانات الضخمة، وأنظمة الاتصال والتعاون عن بُعد. هذا يجعلها عرضة لمجموعة واسعة من التهديدات السيبرانية تشمل هذه التهديدات محاولات اختراق قواعد البيانات الأكاديمية، وسرقة الأوراق البحثية، وهجمات حجب الخدمة الموزعة (DDoS) التي قد تُعطل منصات التعلم، وهجمات التصيد الاحتيالي التي تستهدف الطلاب وأعضاء هيئة التدريس لذلك أصبحت إدارة الأزمات السيبرانية في الجامعات ضرورة مُلحة. يجب أن تتضمن خطط الطوارئ استراتيجيات وقائية للحد من احتمالية وقوع الهجمات، وإجراءات للاستجابة السريعة للحوادث،

وآليات للتعافي لضمان استمرارية العملية التعليمية. يجب أن تشمل هذه الإدارة أيضًا الجوانب التقنية والقانونية والتعليمية، بمشاركة جميع الأطراف من إدارة الجامعة إلى أعضاء هيئة التدريس والطلاب (العمير ،٢٠١٩: ٩).

٥-٢ دور الجامعات في تعزيز الأمن السيبراني

تلعب الجامعات دوراً مهماً في بناء وتعزيز نظام الأمن السيبراني في المجتمع، وذلك عبر عدة جوانب أساسية تشمل التعليم، البحث العلمي، والتوعية وهي كما يأتي(العمير،٢٠١٩: ١٠-١٢):

١-تعديل المحتوى التعليمي بانتظام: لضمان مواكبة أحدث التقنيات والأساليب في حقل الأمن السيبراني، وبالتالي تجهيز الطلاب بمهارات حديثة تلبي متطلبات سوق العمل من خلال التعامل مع الحوادث واستخدام أدوات الكشف والرد على الهجمات

2-تشجيع البحث العلمي عبر دعم الدراسات المتقدمة في مجالات الأمن السيبراني التي تجمع الأسس النظرية والتطبيق العملي، وكذلك نشر البحوث والدراسات في المؤتمرات مما يرفع من مستوى المعرفة العلمية ويسهم في بناء مجتمع بحثي متكامل يعزز الأمن السيبراني على المستوى المحلي والدولي.

3-زيادة مستوى الوعي بين الطلاب والموظفين يعد من أهم الدعائم لتعزيز الأمن السيبراني من خلال: تنظيم ورش عمل ودورات تدريبية حول (كيفية التعامل مع البريد الإلكتروني المشبوه، طرق تحديث البرامج، التوعية بالهجمات السيبرانية الشائعة، وأساسيات حماية البيانات الشخصية) .

٤- بناء ثقافة أمنية شاملة داخل الحرم الجامعي من خلال حملات توعوية مستمرة عبر وسائل التواصل الاجتماعي، الإعلانات الجامعية، واستخدام المنصات رقمية، ملصقات، مسابقات، وأحداث تفاعلية والنشرات التثقيفية التي تهدف إلى خلق ثقافة أمنية بين أفراد المجتمع الجامعي.

٥- تعاون المؤسسات التعليمية مع القطاع الصناعي والحكومي ضرورية لتبادل المعلومات الأمنية، الخبرات، وأفضل الممارسات . لتعزيز التكامل بين التعليم والواقع العملي.

٦-٢ دور الطلاب في إدارة الأزمات

في ظل التوسع الهائل في استخدام التكنولوجيا والأنظمة الرقمية داخل الجامعات، برزت أهمية الأمن السيبراني كأحد الأزمات الاساسية التي تواجه البيئة الأكاديمية. لم يعد الأمن السيبراني مجرد جانب تقني فحسب، بل تحول إلى قضية استراتيجية تؤثر بشكل مباشر على استقرار العملية التعليمية وحماية خصوصية بيانات الطلاب وأعضاء الهيئة التدريسية ، تلعب الفئة الطلابية دورًا حيويا في مواجهة الأزمات الأمنية السيبرانية، إذ يمكن أن يكون الطلاب إما نقطة ضعف تعرض الأنظمة للتهديدات، أو قوة فاعلة تساهم في تعزيز الحماية السيبرانية من خلال: (العازمي،٢٠٢٣: ٥١) .

١- يتوجب على الطلاب أن يكونوا على دراية بأنواع التهديدات السيبرانية التي قد تصادفهم مثل البرمجيات الخبيثة، والتصيد الاحتيالي، والهجمات على الشبكات ويأتي ذلك من خلال المشاركة الفعالة في برامج التوعية وورش العمل التي تقيمها الجامعات، بهدف تعزيز معرفتهم ومهاراتهم في مجال الأمن السيبراني.

٢- الامتثال للبروتوكولات التي تفرضها إدارة الجامعة أثناء الأزمات إذ ينبغي على الطلاب الالتزام التام بالسياسات والقواعد التي تعتمدها الجامعة لحماية الأنظمة والمعلومات، كاستخدام

كلمات مرور قوية وتحديث البرامج بشكل دوري، فضلاً عن تجنب مشاركة المعلومات الحساسة أو الدخول إلى الأنظمة بطرق غير مصرح بها.

٣- المشـــاركة في فرق عمل تهدف إلى ابتكار حلول تقنية وتنظيمية وتقديم أفكار مبتكرة لمواجهة التهديدات الرقمية ما يعزز من دورهم كعناصـر فعالة في إدارة الأزمات وتطوير الحلول الأمنية وإجراءات أمان .

٤- مساندة زملائهم نفسيًا واجتماعيًا في أوقات الأزمات، مما يخفف من آثارها السلبية.

٥- الإبلاغ المبكر عن الوقائع الأمنية للجهات المعنية داخل الجامعة، مما يســـاعد في تقليل الأضرار وتأمين البيئة الرقمية بسرعة وكفاءة.

٦- يتحمل الطلاب مســـؤولية حماية بياناتهم وبيانات الآخرين، والتقيد بالتشـــريعات والانظمة الخاصة بحماية المعلومات وعدم الكشف عن أي بيانات حساسة بصورة غير مسموح بها.

٧-٢ التحديات التي تواجه دور الطلاب في إدارة الأزمات وضمان الأمن السيبراني

تواجه الجامعات والطلاب معًا عدة صعوبات، منها :(عبد الحمزة، ٢٠٢٢: ٥٣٣-٥٣٤)

١- نقص الوعي والمهارات التقنية والتدريب الكافي لدى بعض الطلاب. واللازمة لمواجهة التحديات الرقمية.

٢- محدودية الموارد المالية والبشرية لدعم البرامج التوعوية والتدريبية المخصصة للطلاب.

٣- ضعف التفاعل والمشاركة الطلابية في بعض الحالات نتيجة لغياب آليات تشجيعية أو قلة الدعم المؤسسي.

٤- تطور مستمر في التهديدات السيبرانية يتطلب تحديثًا مستمرًا للمهارات والمعرفة، وهو ما يمثل تحديًا للجامعات والطلاب على حد سواء.

٨-٢ الوســـائل والإجراءات القانونية التي تتبعها الجامعات عند التعرض لانتهاكات إلكترونية بمشاركة الطلاب

يعد الإطار القانوني للأمن السيبراني أحد الركائز الأساسية في بناء منظومة أمن معلومات فعالة داخل الجامعات. تعمل القوانين واللوائح الجامعية، بالتنســـيق مع التشـــريعات الوطنية والدولية، على وضع قواعد واضحة تحكم حماية البيانات الرقمية وخصوصية المستخدمين.

يشتمل هذا الإطار على عدة عناصر هامة، منها :(البعاج،٢٠٢٣: ٤٥٩-٤٦٠)

١- تفعيل اللوائح والسياسات الجامعية الخاصة بالأمن السيبراني والتي تنظم كيفية التعامل مع الحوادث الأمنية، وتحدد المسؤوليات والصلاحيات لكل الأطراف، بما في ذلك الطلاب.

٢- في حال وجود الانتهاكات تشـــمل جرائم إلكترونية مثل الاختراق أو ســـرقة البيانات، تقوم الجامعة بإبلاغ الجهات القضائية المختصة (كالشرطة أو وحدات مكافحة الجرائم الإلكترونية).

٣- تُنشـــئ الجامعة لجنة تحقيق تضـــم خبراء في الأمن الســـيبراني والقانون لفحص الحادثة ، تُستدعى الأطراف ذات العلاقة (بما في ذلك الطلاب، إن لزم الأمر) للتحقق من الوقائع ، تطبيق العقوبات التأديبية أو القانونية.

٤- حماية حقوق الأفراد فيما يخص الخصوصية الرقمية وحق الوصول إلى المعلومات.

٥- تقوم الجامعات بتنظيم ورش عمل وندوات لتعريف الطلاب بحقوقهم وواجباتهم القانونية المتعلقة بالأمن السيبراني.

وتبرز أهمية هذا الإطار القانوني في:

أ - تعزيز ثقة الطلاب بالدور الذي تقوم به الجامعة في حماية بياناتهم ومعلوماتهم الشـخصـية، مما يزيد من التزامهم بالقوانين والسياسات الأمنية.

ب- دعم ثقافة الالتزام والمسؤولية داخل المجتمع الجامعي، وهو ما يسهم في بناء بيئة تعليمية رقمية آمنة ومستقرة.

ج - توفير قاعدة قانونية تدعم التدابير التقنية والتنظيمية التي تتخذها الجامعة لمواجهة التهديدات السيبرانية.

٩-٢ أدوات الحماية في الأمن السيبراني بالجامعات:(شنشول،٢٠٢٥: ١٢-١٥)

١- جدران الحماية(Firewalls) : تعمل على تصفية حركة المرور الشبكي بين الشبكة الداخلية للجامعة والإنترنت، لمنع الوصول غير المصرح به والتهديدات الخارجية.

٢- أنظمة كشف ومنع التسلل (IDS/IPS) : تكشف وتحظر الهجمات الإلكترونية أو السلوكيات المشبوهة في الشبكة، مثل محاولات الاختراق أو استغلال الثغرات.

٣- برامج مكافحة الفيروسات والبرمجيات الخبيثة(Antivirus/Anti-malware) : تقوم بفحص الأجهزة والأنظمة لاكتشاف وحذف البرمجيات الضارة التي قد تهدد سلامة البيانات.

٤- التشفير(Encryption) : حماية البيانات الحساسة من خلال تحويلها إلى صيغة غير قابلة للقراءة إلا لمن يمتلك مفتاح فك التشفير، سواء كانت البيانات مخزنة أم أثناء نقلها

٥- إدارة الهوية والوصول(IAM – Identity and Access Management) : أدوات للتحكم بمن يمكنه الوصول إلى الأنظمة والبيانات، باستخدام آليات مثل كلمات المرور، التوثيق المتعدد العوامل(MFA) ، والامتيازات المحددة.

٦- النسخ الاحتياطي والاستعادة (Backup and Recovery) : نسخ احتياطية منتظمة للبيانات لضمان استعادتها في حال فقدانها بسبب هجوم أو عطل تقني.

٧- أنظمة إدارة معلومات وأحداث الأمن (SIEM) : تجمع وتحلل بيانات أمان الشبكة في الوقت الحقيقي، مما يساعد في اكتشاف الحوادث الأمنية بسرعة واتخاذ الإجراءات اللازمة.

٨- تحديثات وتصحيحات الأمان(Patching) : تحديث البرمجيات والأنظمة بشكل دوري لسد الثغرات التي يمكن للمهاجمين استغلالها.

٩- التوعية والتدريب الأمني: ليست أداة تقنية فحسب، بل برنامج مستمر لتعليم المستخدمين (الطلاب، الموظفين) أفضل الممارسات للحماية الشخصية والجامعية.

١٠- الشبكات الخاصة الافتراضية (VPNs) : توفر اتصالًا آمنًا ومشفرًا بين المستخدمين.

٣- الجانب العملي :

استخدم الباحثون المنهج الوصفي التحليلي نظرا لملائمة هذا المنهج لهذا النوع من الدراسات إذ تم جمع عينة مكونة من ٢٠٠ طالب وطالبه من مجتمع الدراسة (كلية الادارة والاقتصاد – الجامعة المستنصرية) ولتحليل البيانات واختبار فرضية البحث والمتمثلة بـ ("ما مدى تأثير العوامل الفردية والمؤسسية والتي تتمثل بـ (وعي الطلاب، جهود الجامعة، دور الطلاب، السياسات والقوانين، استخدام الأنظمة الرقمية، الثقافة الأمنية، والخبرة الشخصية مع الحوادث السيبرانية، على استعداد الجامعة لمواجهة الأزمات السيبرانية ؟"

تم استخدام العديد من الاساليب الاحصائية المناسبة باستخدام برنامج spss وكانت النتائج كالاتي

١-صدق أداة الدراسة :-

لقياس ثبات الداخلي للاداة الدراسة تم استخدام معامل ثبات (كرونباخ الفا) وكما موضح في الجدول ادناه إذ بلغت القيمة الكلية (٠.٩٨) وهذا يدل على قوة الاتساق الداخلي للأداة وان

استبانة الدراسة تتمتع بثبات مقبول احصائيا وصالحة لتحليل وتفسير نتائج الدراسة، ، كما تراوحت معاملات ثبات اداة الدراسة مابين (981. ، 992.) وجميعها قيم عالية وهذا يشير إلى أن جميع المحاور تسهم بشكل فعّال في قياس البنية الكامنة للأداة، ولا يوجد أي محور شاذ أو ضعيف وأن حذف أي محور لا يحسن الثبات بل قد يؤدي إلى انخفاضه الطفيف، الأمر الذي يعزز ضرورة الإبقاء على جميع المحاور داخل المقياس. وبناءً على ذلك يمكن القول إن الأداة تتميز بدرجة عالية من الموثوقية والاتساق الداخلي، وتصلح للاستخدام في دراسة استعداد الجامعة للأزمات السيبرانية، إذ تقيس بشكل متكامل الأبعاد المختلفة للمفهوم محل الدراسة.

جدول رقم (١): معامل ألفا كرونباخ لقياس ثبات أداة الدراسة

المحور	عدد العبارات	معامل الثبات
تقييم استعداد الجامعة للأزمات السيبرانية	٣	.981
الخبرة الشخصية مع الحوادث السيبرانية	٤	.983
ثقافة الأمن السيبراني في المجتمع الجامعي	٤	.992
استخدام الأنظمة الرقمية في الجامعة	٤	.981
السياسات والقوانين الجامعية ودعم الطالب	٥	.980
دور الطالب في دعم الأمن السيبراني وإدارة الأزمات	٥	.982
جهود الجامعة في تعزيز الأمن السيبراني	٧	.980
الوعي بالأمن السيبراني	٥	.981
الثبات الكلي	٣٧	٠.٩٨٤

٢- المعالجات الاحصائية

الجدول (٢) المتوسطات الحسابية والانحرافات المعياريه لتقديرات افراد عينة الدراسة علي فقرات مجالات الاستبانة

المحور	المتوسط	الانحراف المعياري
الوعي بالأمن السيبراني		
لدي معرفة واضحة بمفهوم الأمن السيبراني وأهميته في البيئة الجامعية .	3.70	.93
أستخدم كلمات مرور قوية ومعقّدة لحساباتي الجامعية والشخصية.	4.19	.89
أتجنب فتح الروابط أو الملفات المشبوهة وغير الموثوقة.	4.42	.81
أحرص على تحديث البرامج وأنظمة التشغيل بانتظام.	4.11	.89
أدرك أثر الهجمات السيبرانية على أمن الجامعة وسلامة بياناتها.	3.96	.95
المجال ككل	4.08	0.85
جهود الجامعة في تعزيز الأمن السيبراني		
توفر الجامعة برامج توعية وتدريب فعّالة في مجال الأمن السيبراني.	3.73	1.14
أنظمة الجامعة الرقمية محمية بمستوى أمني مرتفع.	3.87	.84
توجد وحدة متخصصة بالأمن السيبراني مزوّدة بكوادر مؤهلة للتعامل مع الحوادث.	3.74	.98
يتم تنظيم ورش عمل ودورات تدريبية دورية للطلبة والموظفين.	3.87	1.08
الموارد التقنية والمالية المخصصة للأمن السيبراني كافية.	3.48	1.10
الطلبة على دراية بدور وحدة الأمن السيبراني وإجراءاتها.	3.51	1.12
تستجيب الوحدة بسرعة وجدية للحوادث الإلكترونية.	3.76	.95
المجال ككل	3.71	0.99
دور الطالب في دعم الأمن السيبراني وإدارة الأزمات		
ألتزم بتطبيق الممارسات الآمنة مثل استخدام كلمات مرور قوية وتحديث البرامج.	4.23	.81
أبلغ فورًا عن أي نشاط إلكتروني مشبوه أو حادثة سيبرانية.	4.16	.89
أشارك في المبادرات وحملات التوعية التي تنظمها الجامعة.	3.88	.94
أعرف الإجراءات الواجب اتباعها عند وقوع حادثة سيبرانية.	3.74	.99
أؤمن بأهمية التعاون بين الطلبة ووحدة الأمن السيبراني لتحقيق بيئة آمنة.	4.25	.73
المجال ككل	4.05	0.83
السياسات والقوانين الجامعية ودعم الطالب		
أنا ملم بسياسات وإجراءات الجامعة الخاصة بالأمن السيبراني.	3.71	1.01

الجامعة توفر قنوات رسمية وسهلة للإبلاغ عن الحوادث.	3.70	1.07
أحصل على الدعم القانوني والتقني عند تعرضي لحادثة إلكترونية.	3.86	.98
تلتزم الجامعة بسرية المعلومات أثناء التحقيقات.	3.96	.89
تتعاون الجامعة مع الجهات الأمنية المختصة عند الحاجة.	4.01	.86
المجال ككل	3.84	0.93
استخدام الأنظمة الرقمية في الجامعة		
أستخدم المنصات الإلكترونية الجامعية بانتظام في دراستي.	3.93	.88
أواجه أحيانًا صعوبات تقنية أو أمنية أثناء استخدام هذه الأنظمة.	3.75	.86
الأنظمة الرقمية سهلة وآمنة من وجهة نظري.	3.68	.90
توفر الجامعة إرشادات واضحة لاستخدام المنصات بأمان.	3.76	.95
المجال ككل	3.78	0.87
ثقافة الأمن السيبراني في المجتمع الجامعي		
يهتم زملائي بقضايا الأمن الرقمي.	3.50	.98
أعضاء هيئة التدريس يقدمون توجيهًا منتظمًا حول الأمن السيبراني.	3.73	3.07
تُقام حملات توعية دورية لتعزيز ثقافة الأمن الرقمي.	3.62	1.09
إدارة الجامعة تبدي التزامًا واضحًا بالأمن السيبراني	3.61	1.09
المجال ككل	3.62	1.29
الخبرة الشخصية مع الحوادث السيبرانية		
تعرضت سابقًا لحوادث أو محاولات اختراق.	2.79	1.17
أبلغت الجهات المختصة داخل الجامعة عن الحادثة.	2.92	1.11
كانت استجابة الجامعة مناسبة وفعّالة.	3.11	1.09
تلقيت الدعم اللازم بعد الحادثة.	3.07	1.09
	3.62	1.29
تقييم استعداد الجامعة للأزمات السيبرانية		
لدى الجامعة خطة واضحة للتعامل مع الأزمات الإلكترونية.	3.58	1.01
يتم إبلاغ الطلبة بسرعة عند حدوث خرق أمني.	3.66	1.02
إجراءات احتواء الأزمات في الجامعة فعّالة وسريعة.	3.64	.99
المجال ككل	2.97	1.09

بعد ان تم جمع البيانات بواسطة ادارة الدراسة (الاستبانة) تم حساب المتوسطات والانحرافات المعيارية لتقديرات افراد عينة الدراسه وكما موضح بالجدول اعلاه وكانت النتائج كالاتي :

١- في محور الوعي بالأمن السيبراني نلاحظ ان المتوسطات الحسابية تتراوح بين ٤.٤٢- ٣.٧٠ إذ جاء أتجنب فتح الروابط أو الملفات المشبوهة في المرتبة الاولى باعلى متوسط حسابي

إذ بلغ ٤.٤٢ وبانحراف معياري 0.81 ، بينما جاء ت معرفة واضحة بمفهوم الأمن و السيبراني وأهميته في المرتبة الاخيرة وبمتوسط حسابي بلغ 3.70 وبانحراف معياري 93. ، وبلغ المتوسط الحسابي للاداه ككل 4.08 وبانحراف معياري 0.85 وهذا المؤشر واضح الى ان الطلبة يمتلكون مستوى وعي مرتفع بأهمية الأمن السيبراني، ويطبقون معظم الممارسات الأساسية للوقاية، مع وجود تفاوت بسيط بين الطلبة في الالتزام ببعض الإجراءات مثل التحديث المستمر للأنظمة وهذا يدعوا الي ضرورة تعزيز الجانب المعرفي والتوعي من خلال الدورات والمحاضرات لرفع الادراك الى مستوى الممارسة العملية.

٢- في محور جهود الجامعة في تعزيز الأمن السيبراني تبين ان المتوسطات الحسابية تتراوح بين 3.87- 3.48 إذ جاءت الفقرتان (أنظمة الجامعة الرقمية محمية وتنظيم ورش عمل ودورات تدريبية) في المرتبة الاولى باعلى متوسط حسابي إذ بلغ ٣.٨٧ وبانحراف معياري 84.و 1.08 على التوالي ، بينما جاء ت الموارد التقنية والمالية في المرتبة الاخيرة وبمتوسط حسابي بلغ ٣.٤٨ وبانحراف معياري.1.10 وبلغ المتوسط الحسابي للاداة ككل ٣.٧١ ، ويعود هذا السبب الى ان الجامعة تبذل جهودا واضحة في مجال الامن السيبراني من خلال البرامج والورش التدريبية وتامين الانظمة الا ان هناك بعص التحديات التي تواجهها وهو الحاجة الى زيادة الموارد المالية والتقينة المخصصة للامن السيبراني وتوسيع المشاركة في البرامج التدريبة لتصبح اكثر شموليه.

٣- في المحور الثالث والمتمثل دور الطالب في دعم الأمن السيبراني وإدارة الأزمات وجد ان المتوسطات الحسابية تقد تراوحت بين ٤.٢٥- ٣.٧٤ إذ جاءت الفقرة (أؤمن بأهمية التعاون بين الطلبة) في المرتبة الاولى بأعلى متوسط حسابي إذ بلغ ٤.٢٥ وبانحراف معياري ٠.٧٣

، بينما جاء ت الفقرة (أعرف الإجراءات الواجب اتباعها عند وقوع حادثة سـيبرانية) في المرتبة الاخيرة وبمتوسط حسابي بلغ٣.٧٤ وبانحراف معياري٠.٩٩ وهذا يعني أن المعرفة بالإجراءات الرسمية عند وقوع الحوادث ما تزال بحاجة إلى تعزيز في حين بلغ المتوسط الحسابي للأداة ككل 4.08 وتؤكد هذه النتيجة الى ان الطلبة يتمتعون بوعي جيد جدًا في دورهم بدعم الأمن السـيبراني وإدارة الأزمات، خصـوصًـا فيما يتعلق بالتعاون مع وحدة الأمن السـيبراني وتبني الممارسـات الوقائية. ولكن كل هذا يحتاج الي توعيه وتدريب لتعزيز هذا الدور وبشـكل اكبر لمعرفه الاجراءات المتبعة عند وقوع الحوادث السيبرانية.

٤- في المحور الرابع السـياسـات والقوانين الجامعية ودعم الطالب إذ تراوحت المتوسـطات الحسابية بين 4.01 - 3.70 إذ جاءت الفقرة (تتعاون الجامعة مع الجهات الأمنية المختصة عند الحاجة) بالمرتبة الاولى باعلى متوسـط حسـابي إذ بل 4.01 وبانحراف معياري .86 بينما جاء ت (الجامعة توفر قنوات رسـمية وسـهلة للإبلاغ عن الحوادث) في المرتبة الاخيرة وبمتوسط حسابي 3.70 وبانحراف معياري 1.07 وبلغ المتوسط الحسابي للمحور ككل 3.84 وتعود هذه النتيجة إلى أن الطلبة يثقون في التزام الجامعة بالسرية والتعاون مع الجهات الأمنية المختصة، وهو ما يُعد من أبرز جوانب القوة. في المقابل، برزت بعض جوانب الضعف المتمثلة في محدودية معرفة الطلبة بالسياسات والإجراءات الرسمية، وعدم وضوح قنوات الإبلاغ عن الحوادث، إضافة إلى تفاوت مستوى الدعم القانوني والتقني المقدم. وعليه، فإن تعزيز نشر الوعي، وتبسيط آليات الإبلاغ، وتطوير قنوات الدعم يمثل ضرورة لتحسين فعالية السياسات المؤسسية للأمن السيبراني.

٥- تراوحت المتوسطات الحسابيه الخاصة بالمحور الخامس والمتمثل "استخدام الأنظمة الرقمية في الجامعة" بين 3.93- 3.68 إذ يبن ان الطلاب يعتمدون بشكل يومي وكبير على منصات الالكترونية وباعلى متوسط بلغ 3.93 ، بالمقابل يظهر الطلاب بعض التحفظ حول الانظمة الرقمية لوجود بعض المشاكل وبمتوسط 3.68 في حين بلغ المتوسط الحسابي للاداة ككل 3.78 وهذا يشير إلى تقييم إيجابي للأنظمة الرقمية، مع تقارب كبير في آراء الطلاب بـ(انحراف معياري 0.87)، مما يعكس رضاً عامًا واستقراراً في استخدام هذه الأنظمة.

٦- اما ثقافة الأمن السيبراني في المجتمع الجامعي فتراوحت متوسطات الحسابية بين 3.73- 3.50إذ يقوم بعض أعضاء هيئة التدريس بتقديم توجيهًا منتظمًا حول الأمن السيبراني المرتبة الاولى وباعلى متوسط حسابي إذ بلغ 3.73 وبانحراف معياري 3.07 في حين بلغ متوسط اهتمام الطلبه الاخرين بقضايا الأمن الرقمي 3.50 وبانحراف معياري 98. وبلغ المتوسط العام للمحور 3.62 وهذا يدل إلى حاجة الجامعة لتعزيز الثقافة الرقمية بشكل أكبر، خاصة في إشراك الطلاب وزملائهم وأعضاء هيئة التدريس.

٧- في المحور (الخبرة الشخصية مع الحوادث السيبرانية) وجد ان الفقرة التي نصت على (كانت استجابة الجامعة مناسبة وفعّالة). قد احتلت المرتبة الاولى بمتوسط حسابي إذ بلغ 3.11 وبانحراف معياري 1.09، بينما جاء ت الفقرة التي كان نصها (تعرضت سابقًا لحوادث أو محاولات اختراق.) في المرتبة الاخيرة وبمتوسط حسابي بلغ2.79 وبانحراف معياري1.17 وهذا يعني إلى أن نسبة غير قليلة من الطلبة لم يتعرضوا بشكل مباشر لحوادث اختراق، أو أن تعرضهم كان محدودً في حين بلغ المتوسط الحسابي للاداة ككل 3.6 .4 ويعود تفسير هذه النتيجة .

٨- في محور تقييم استعداد الجامعة للأزمات السيبرانية تبين ان المتوسطات الحسابية تتراوح بين 3.66- 3.58 إذ بلغت اعلى متوسط عند الفقرة (يتم إبلاغ الطلبة بسرعة عند حدوث خرق أمني) إذ بلغ ٣.٦٦ وبانحراف معياري 1.02 ، المتوسط الحسابي للاداة ككل 2.97 ، ويعود هذا السبب الى ان الجامعة مستعدة بشكل جيد للتعامل مع الأزمات السيبرانية، مع سرعة عالية في الإبلاغ وفعالية الإجراءات، لكنها تحتاج لمراجعة مستمرة لضمان الاستجابة المثالية.

٣- اختبار فرضية الدراسة

ينص فرضية الدراسة (لا يوجد تأثير العوامل الفردية والمؤسسية، بما في ذلك وعي الطلاب، جهود الجامعة، دور الطلاب، السياسات والقوانين، استخدام الأنظمة الرقمية، الثقافة الأمنية، والخبرة الشخصية مع الحوادث السيبرانية)، على استعداد الجامعة لمواجهة الأزمات السيبرانية؟"

أ – معامل الارتباط

الجدول رقم (٣) تقييم الاداء الاحصائي للنموذج

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.984[a]	.969	.967	.18036

يشير الجدول اعلاه الى قيم معامل الارتباط R بلغ .984[a] مما يدل على وجود علاقة قوية بين المتغير التابع والمتغيرات المستقلة ، اما قيمة معامل التحديد 969. يدل على ان المتغيرات المستقلة تؤثر على المتغير التابع بنسبة ٩٧ % اما نسبة ٣٪ يرجع تفسيرها الى متغيرات اخرى غير متضمنة في النموذج ، قيمة مربع معامل الارتباط المعدل تشير الى ان ٩٦.٧ % من التباين من استعداد الجامعة للازمات يمكن تفسيره بواسطة النموذج بعد التعديل لاخذ عدد المتغيرات في الحسبان .

ب- جدول تحليل التباين ANOVA

جدول رقم (٤)

تحليل التباين

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	192.545	7	27.506	845.553	.000[b]
	Residual	6.246	192	.033		
	Total	198.791	199			

يتضـــح في الجدول اعلاه الى وجود علاقة طردية ذات دلالة احصـــائية عند مســـتوى معنوي ٠.٠٥ بين من الجدول الســـابق وجود علاقه ارتباط معنوية طردة بين المتغيرات المســـتقلة (الخبرة الشـخصـية مع الحوادث السـيبرانية، ثقافة الأمن السـيبراني في المجتمع الجامعي، الوعي بالأمن السـيبراني، اسـتخدام الأنظمة الرقمية في الجامعة، دور الطالب في دعم الأمن السـيبراني وإدارة الأزمات، الســـياســـات والقوانين الجامعية ودعم الطالب، جهود الجامعة في تعزيز الأمن الســـيبراني) والمتغير المعتمد (تقييم اســـتعداد الجامعة للأزمات الســـيبرانية)، ويظهر ذلك من خلال قيمه F والتي بلغت 845.553 .

ج – تحليل الانحدار

جدول رقم (٤)

معاملات الانحدار

Model	B	Std. Error	Beta	t	Sig.
(Constant)	-.249	.100		-2.493	.014
الوعي بالأمن السيبراني	.338	.087	.287	3.881	.000
جهود الجامعة في تعزيز الأمن السيبراني	.883	.103	.882	8.580	.000
دور الطالب في دعم الأمن السيبراني وإدارة الأزمات	-.193	.089	-.161	-2.180	.030
السياسات والقوانين الجامعية ودعم الطالب	-.763	.106	-.712	-7.224	.000
استخدام الأنظمة الرقمية في الجامعة	.748	.087	.652	8.638	.000
ثقافة الأمن السيبراني في المجتمع الجامعي	.016	.018	.021	.884	.378
الخبرة الشخصية مع الحوادث السيبرانية	.017	.035	.018	.473	.637

تشـــير النتائج في الجدول اعلاه إلى أن أكثر العوامل تأثيرًا إيجابيًا في رفع مســـتوى اســـتعداد الجامعة لمواجهة الأزمات السيبرانية هما:

١. جهود الجامعة في تعزيز الأمن الســـيبراني (مثل الخطط، البرامج، الحماية التقنية)، إذ ظهر أنه العامل الأقوى في تحسين الاستعداد.

٢. اســـتخدام الأنظمة الرقمية بكفاءة داخل الجامعة، وهو ما يعزز الجاهزية والقدرة على الاستجابة.

٣.وعي الطلبة بالأمن السيبراني، الذي كان ذو أثر إيجابي واضح أيضًا، إذ إن زيادة الوعي تقلل من المخاطر وتدعم الممارسات الآمنة.

في المقابل، ظهر أن:

- سياسات والقوانين الجامعية
  - ظهر لها معامل انحدار سلبي قوي ومعنوي.(−0.712)
  - هذا لا يعني أن السياسات بحد ذاتها تضر، بل قد يشير إلى أن السياسات الموجودة غير فعّالة أو غير مطبقة كما يجب، وربما معقدة أو شكلية، مما يجعلها لا تترجم إلى تحسين حقيقي للاستعداد.
  - أي أن المشكلة ليست في وجود السياسات، بل في جودتها وفاعليتها وآلية تطبيقها.
- دور الطالب في دعم الأمن السيبراني
  - ظهر له معامل سلبي ومعنوي.(−0.161)
  - هذا يوحي أن الأدوار الحالية الموكلة للطلبة غير مفعلة أو ضعيفة، وربما لا تتجاوز كونها توعوية سطحية، أو أن مشاركة الطلبة في القرارات وإدارة الأزمات محدودة.
  - النتيجة لا تعني أن "الطلاب لا يمكن أن يكونوا داعمين"، بل تعني أن الدور الحالي لا يحقق الأثر المتوقع، وبالتالي يمثل ثغرة أو نقطة ضعف.

أما الثقافة العامة للأمن السيبراني في المجتمع الجامعي والخبرة الشخصية مع الحوادث السيبرانية، فقد تبين أنهما غير مؤثرين بشكل معنوي في مستوى الاستعداد الكلي، أي أن تأثيرهما محدود أو غير مباشر.

٤-الاستنتاجات

١- يستخدم الطلاب المنصات الرقمية بانتظام، مع وجود بعض المخاوف التقنية أو الأمنية.

٢- الاهتمام بالأمن الرقمي متباين بين الطلاب، مما يستدعي برامج توعية مكثفة.

٣- دور هيئة التدريس غير منتظم، ويجب وضع سياسات واضحة لتوجيه الطلاب بشكل دوري.

٤- حملات التوعية الحالية غير كافية لتعزيز ثقافة مؤسسية قوية للأمن الرقمي.

٥- التزام إدارة الجامعة موجود، لكنه يحتاج إلى تعزيز عبر سياسات واضحة، ورش تدريبية، ودعم فني مستمر.

٦- الثقافة الأمنية داخل الجامعة متوسطة إلى جيدة، مع حاجة لتحسين الممارسات اليومية وتوحيد الجهود بين الإدارة والهيئة التدريسية.

٧- ضعف الإبلاغ عن الحوادث يمثل تحديًا مهمًا، ويؤثر على قدرة الجامعة في معالجة التهديدات بفعالية.

٨- استجابة الجامعة مقبولة لكنها بحاجة لتطوير لتصبح أسرع وأكثر فعالية ووضوحًا.

٩- الاستعداد الجامعي يعتمد بالدرجة الأولى على جهود الإدارة والأنظمة التقنية المطبقة، بينما تظل السياسات الرسمية ودور الطلبة بحاجة إلى مراجعة وتفعيل أوسع لتصبح عناصر داعمة بدلًا من أن تكون نقاط ضعف.

٥-التوصيات

١. إعداد برامج تدريبية وحملات توعية مستمرة حول الأمن السيبراني وتشجيع الطلبة للمشاركة فيها .

٢. تفعيل وحدات الأمن السيبراني في الجامعات مع تعزيز دورها القانوني والفني.

٣.تطوير منصات رقمية آمنة وسهلة للإبلاغ عن الحوادث الإلكترونية بسرية تامة.

٤.تطوير برامج توعية تدريبية لتعزيز مهارات الطلاب في الاستخدام الآمن للأنظمة الرقمية

٥.تعزيز التعاون بين الجامعات والجهات الأمنية الوطنية في مجال مكافحة الجرائم السيبرانية.

٦. مراقبة ملاحظات الطلاب بشكل دوري لتحديث وتطوير المنصات بما يتوافق مع احتياجاتهم.

٦-المقترحات

بناءً على التوصيات يقترح الباحثون الاستفادة من المنصة التعليمية والتوعوية للأمن السيبراني التي تم تصـــميمها كنموذج عملي (في الملحق)، بهدف تعزيز وعي الطلاب ومهاراتهم في الممارسات الرقمية الآمنة. كما يمكن للمنصة تشجيع الطلاب على التفاعل والمشاركة الفاعلة في الإبلاغ عن الملاحظات أو الحوادث الأمنية بطريقة آمنة ومنظمة، تحت إشـــراف فريق مختص من إدارة الكلية لضمان توافق المنصة مع أنظمة الجامعة وإدارتها بكفاءة وفعالية.

٧-المصادر

١ -البعاج، هـــديل ، تومان .(2023) .الوعي الاجتماعي بالأمن السيبراني لدى الطلبة: دراسة ميدانية على طلبة الجامعات — طلبة كلية الإمام الكاظم نموذجًا .مجلة لارك.

٢- الحيالي، آلاء وهب .(2021) .استخدام التعليم الإلكتروني كأداة لإدارة الأزمات التعليمية في ظل جائحة كوفيد-١٩ (رسالة ماجستير). كلية الإدارة والاقتصاد، جامعة الموصل.

٣- شنشول، نسرين رياض & .,حمد، أنور حامد (٢٠٢٥). الأمن السيبراني وحماية الاقتصاد العراقي: التهديدات السيبرانية واستراتيجيات المواجهة (ورقة سياسات). مركز البيان للدراسات والتخطيط.

٤-العازمي، عائشة عبيد الله مبارك قويضي. (٢٠٢٣). الوعي الاجتماعي بالأمن السيبراني لدى الطلبة: دراسة ميدانية على طلبة كلية الإمام الكاظم (ع)/ أقسام واسط .مجلة لارك، ٥٠.(2).

٥ -العمير، لطيفة بن عبد الرحمن. (٢٠١٩). الأمن السيبراني في التعليم: اتجاهات معاصرة في التربية .كلية التربية، جامعة الإمام محمد بن سعود الإسلامية، السعودية.

٦-الشمري، مصطفى إبراهيم. (٢٠٢١) الأمن السيبراني وأثره في الأمن الوطني العراقي .مجلة العلوم القانونية والسياسية، ١٠ .(1)جامعة ديالى، العراق.

٧-عبد الحمزة، ســامر محي. (٢٠٢٢) الســياســة التشــريعية العراقية لحماية الأمن الوطني السيبراني: دراسة في اتجاهات المنظمات الدولية .مجلة لارك، ٦ .(4)العراق.


منصة الإبلاغ عن الحوادث السيبرانية
إرسال بلاغ
لوحة التحكم
التوعية
إرسال بلاغ
نوع الحادث:
اختراق حساب
وصف الحادث:
إرفاق ملف (اختياري):
No file chosen
Choose File
إرسال البلاغ كمجهول
إرسال البلاغ
لوحة التحكم (عرض البلاغات)
التوعية الأمنية
لا تشارك كلمة المرور مع أي شخص.
تأكد من الروابط قبل النقر عليها.
استخدم التحقق بخطوتين لحساباتك.