Afro-Asian Journal of Scientific Research (AAJSR)
المجلة الأفروآسيوية للبحث العلمي (AAJSR)
E-ISSN: 2959-6505
Volume 2, Issue 3, July - September 2024, Page No: 217-230
Website: https://aajsr.com/index.php/aajsr/index
SJIFactor 2023: 3.908 **معامل التأثير العربي (AIF) 2023: 0.51** **ISI 2023: 0.337**

دور الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية في مؤسسات التعليم العالي
دراسة تطبيقية علي طلبة كلية الاقتصاد بجامعة بني وليد

أ. خالد ميلاد محمد [1*]، د. ميلاد سالم المختار مغرا ف [2]
[2،1] قسم التجارة الالكترونية، كلية الاقتصاد والعلوم السياسية، جامعة بني وليد، بني وليد، ليبيا

The role of cybersecurity in protecting Internet users and reducing the risk of negative digital phenomena in higher education institutions
A field study on students of the Faculty of Economics at Bani Waleed University

Khalid Milad Mohamed [1*], Dr. Milad Salem Mokhraf [2]
[1,2] E-commerce Department, Faculty of Economics and Political Sciences, Bani Waleed University, Bani Walid, Libya

*المؤلف المراسل	khalidsalem@bwu.edu.ly	*Corresponding author
تاريخ الاستلام: 2024-06-20	**تاريخ القبول:** 2024-08-08	**تاريخ النشر:** 2024-08-16

الملخص

يهدف البحث لمعرفة الدور الفعال للأمن السيبراني في حماية البيانات والمعلومات ومستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية المتمثلة في الابتزاز الإلكتروني والتنمر الإلكتروني والقرصنة والجريمة الإلكترونية، ولتحقيق ذلك تم استخدام المنهج الوصفي التحليلي بدراسة ميدانية على طلبة كلية الاقتصاد جامعة - بنى وليد وبتوزيع صحيفة استبيان على عينة عشوائية بسيطة بلغت (50) مفردة، وخلص إلى إن الأمن السيبراني له دور فعال ورئيس وهام، وأوصى البحث بالاستفادة القصوى من مخرجاته.

الكلمات المفتاحية: الأمن الرقمي، الأمن السيبراني، الظواهر الرقمية السلبية.

Abstract:

The research aims to find out the effective role of cybersecurity in protecting data, information and users of the international network and reducing the risk of negative digital phenomena represented in electronic extortion, cyberbullying, piracy and cybercrime, and to achieve this, the descriptive analytical approach was used in a field study on students of the Faculty of Economics, University - Bani Walid, and by distributing a questionnaire sheet to a simple random sample of (50) single, and concluded that cybersecurity has an effective, major and important role, and the research recommended making the most of its outputs.

Keywords: Digital security, Cyber security, Negative digital phenomena.

1- المقدمة:

يعتبر الأمن الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور أي نشاط بعيدا عن تحققه، سواء أكان ذلك على المستوى التقني أو القانوني وقد تحول الأمن مع بروز مجتمع المعلومات والفضاء السيبراني الي واحد من قطاعات الخدمات التي تشكل قيمة مضافة ودعامة أساسية لأنشطة الحكومات والأفراد على السواء كما هو الحال، مع التطبيقات الخاصة بالحكومة الإلكترونية والصحة الإلكترونية والتعليم عن بعد والتجارة الإلكترونية. ومع دخول العصر الرقمي وانفجار الثورة المعلوماتية وما نتج من تداعيات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكل تحديا كبيرًا للأمن القومي وكذلك الدولي، لدرجة ان العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية تبلورت بشكل أساسي في ظهور الأمن الرقمي والأمن السيبراني كبعدين جديدين ضمن أجندة حقل الدراسات الأمنية، وقد اكتسب اهتمامات العديد من الباحثين في هذا المجال.

ومن هنا تبرز الحاجة الى ضرورة فهم ماهية الأمن الرقمي والأمن السيبراني ودراسته دراسة علمية مستفيضة من مختلف جوانبه بعمق كمتغير جديد في العلاقات الدولية.

وقد تم تقسيم البحث على النحو الآتي:

المبحث الأول: الإطار العام للبحث (خطة البحث).

المبحث الثاني: الإطار النظري للبحث ويشمل مفاهيم الأمن الرقمي والأمن السيبراني والظواهر السلبية الرقمية.

المبحث الثالث: الإطار العملي للبحث ويشمل التحليل الإحصائي للبيانات المفرغة من الاستبيان الموزع على عينة البحث واثبات أو نفي فرضيات البحث.

المبحث الرابع: النتائج والتوصيات والمصادر والمراجع.

المشكلة البحثية:

من خلال ولوجنا لعديد المواقع الإلكترونية ووسائل التواصل الاجتماعي والمنصات الرقمية وما نسمع ونشاهد عن وجود اختراقات أمنية وظهور الظواهر السلبية الرقمية مثل القرصنة الإلكترونية "التهكير" والتنمر الإلكتروني والابتزاز الإلكتروني والجريمة الإلكترونية، لاحظنا بأن لابد من وجود وسيلة أمنية يكون لها دور فعال في حماية مستخدمي الشبكة الدولية وكشف الظواهر السلبية الرقمية وهو ما يعرف بالأمن الرقمي والأمن السيبراني، ونحن كباحثين ومن قسم التجارة الإلكترونية سنحاول توضيح وجود هذه الوسيلة الأمنية الرقمية، لذا تتمحور مشكلة بحثنا هذا عن دور الأمن الرقمي والأمن السيبراني في حماية وكشف ما سبق ووجدنا أنفسنا أمام سؤال يطرح نفسه الا وهو:

"هل للأمن السيبراني دور في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية في مؤسسات التعليم العالي؟"

أهداف البحث:

الهدف محاولة معرفة الاتي:

- مفهوم الأمن الرقمي والأمن السيبراني.
- المفاهيم الأساسية للظواهر السلبية الرقمية.
- الدور الذي يلعبه الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية.
- مدى أسهام الأمن الرقمي والأمن السيبراني في التحول الرقمي والاقتصاد المبني على المعرفة.

أهمية البحث:

تكمن أهمية البحث في الدور الفعال للأمن الرقمي في حماية البيانات والمعلومات ومستخدمي الشبكة الدولية والدور الفعال والرئيسي للأمن السيبراني في كشف الظواهر السلبية الرقمية.

أهمية علمية:

- تعود على الجامعة خاصة باتخاذه مرجعاً يستفيد منه الطلاب وبالتالي إمكانية تطويره.
- استخدام هذا البحث كمرجع يستفيد من الباحثين والاطلاع على معلومات كثيرة بداخله.

أهمية عملية:

- العمل على تعزيز الأمن الرقمي والأمن السيبراني وحماية للأمن القومي.
- كشف الظواهر السلبية الرقمية.
- العمل على تدليل أحد عوائق التجارة الإلكترونية.

فرضيات البحث:
يوجد دور ذو دلالة إحصائية للأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من الظواهر السلبية الرقمية.

منهجية البحث:
استخدم المنهج الوصفي التحليلي في البحث لتحقيق الأهداف واثبات أو نفي الفرضيات عن طريق المصادر والمراجع والمواقع الالكترونية لوصف الموضوع وتحليل البيانات التي تم الحصول عليها من استمارة الاستبيان والوصول إلى أهم النتائج.

مصادر جمع البيانات:
1 – مصادر أولية والمتمثلة في البيانات المتحصل عليها من استمارة الاستبيان.
2 – مصادر ثانوية والمتمثلة في عدد من المواقع الإلكترونية والكتب والمراجع.

مجتمع وعينة البحث:
1 – مجتمع البحث: كلية الاقتصاد جامعة - بنى وليد.
2 – عينة البحث: بعض طلبة كلية الاقتصاد جامعة - بنى وليد بلغت (50) (مفردة.
3 – وحدة العينة: عينة عشوائية بسيطة.
9-1حدود البحث: كلية الاقتصاد جامعة - بنى وليد.

الحدود الموضوعية: دور الأمن الرقمي والأمن السيبراني في حماية مستخدمي الشبكة الدولية وكشف الظواهر السلبية الرقمية.
الحدود المكانية: كلية الاقتصاد جامعة - بنى وليد.
الحدود الزمنية: عام 2024 م.

المفاهيم الأساسية للبحث:

الأمن الرقمي:
هو العلم الذي يعمل على توفير الحماية للبيانات والمعلومات من المخاطر التي تهددها أو الحاجز الدي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازمة لحماية البيانات المعلومات من المخاطر الداخلية أو الخارجية لمنع وصولها إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

الأمن السيبراني:
هو عبارة عن مجموعة من الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافق واستمرارية عمل نظم المعلومات وتعزيز وحماية وخصوصية البيانات الشخصية واتخاد جميع التدابير اللازمة.

الظواهر السلبية الرقمية:
كل ما يؤثر على مستخدمي الشبكة والشبكة الدولية في حد ذاتها والمتمثلة في (الابتزاز والتنمر الإلكتروني والقرصنة الالكترونية والجريمة الالكترونية والاختراقات).

الأمن الرقمي:
تمهيد
أمن البيانات والمعلومات هو أحد فروع العلم الباحث في مجال توفير الحماية اللازمة للمعلومات ومنع الوصول إليها وهدرها من غير ذوي الصلاحية ، وحمايتها من أي تهديد خارجي ، ويشمل هذا المصطلح الأدوات و الطرق و الإجراءات اللازمة الواجب توفرها لتحقيق الحماية من المخاطر التي قد تواجهها من الداخل و الخارج ، ويعتبر هذا العلم نوعا من تمكين المستخدم فرض سيطرته على المعلومات بشكل كامل ، ومنع الآخرين من الاطلاع عليها أو إجراء أي تغيير عليها دون إذن مسبق ، فأمن البيانات و المعلومات هو عبارة عن حزمة من العمليات و الطرق و الإجراءات التي يتم انتهاجها لبسط أقوى طرق الحماية على المعلومات الخاصة بها وعلى أنظمتها ووسائطها لمنع الوصول إليها لغير المصرح لهم بذلك كما تمتاز حماية البيانات والمعلومات بالاستمرارية في مواكبة كل ما هو مستحدث ومتطور من درجات الأمان وأساليبها في حماية هذه المعلومات، كما تتطلب الاستمرارية بفرض الرقابة على المخاطر وافتراضها، والسعي الدائم لوجود حلول وابتكارات دائمة، ولذا لا يطلق اسم النظام المعلوماتي الحقيقي على نظام أي منظمة إلا في حال كان فعالا ومحققا للاستمرارية في مواكبة العمليات الأمنية و النقدية سعيا للوصول إلى الأمن الرقمي.
تعريف بالأمن الرقمي: هو العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم لحماية المعلومات من المخاطر الداخلية أو الخارجية لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

العناصر أو المبادئ الأساسية لأمن المعلومات: (CIA)

1 - السرية أو الموثوقية (CONFIDENTIALITY).
وتعني التأكد من إن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
2 - التكاملية وسلامة المحتوى (INTEGRITY).
التأكد من إن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.
3 - توافر المعلومات أو الخدمة (AVAILABILITY).
التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها. (الحناوي ،2010، ص 21).

مخاطر الانترنت على أمن المعلومات:
من التهديدات الأمنية الخطيرة التي تتعرض لها المواقع من قبل المخترقين والمجرمين والعابثين:
1 – التقمص (spoofing)
التكلفة المنخفضة لبناء موقع على الإنترنت وسهولة نسخ صفحات من مواقع شبكية حالية، يجعل الأمر سهل جدا لبناء مواقع غير شرعية تتقمص واجهة مواقع حقيقية لخداع الزوار لإعطاء معلوماتهم الشخصية وبطاقات الائتمان الخاصة بهم ظنا منهم إن المواقع المتقمصة هي مواقع لشركات محترمة.
2 – التنصت (Eavesdropping)
عند تصفح المواقع الشبكية على الانترنت والقيام بعمليات شراء، تنتقل المعلومات (أرقام بطاقات الائتمان، المعلومات الشخصية) عبر الإنترنت وان كانت غير مشفرة تكون عرضة للمخترقين لسرقتها عن طريق التنصت.
3 – التخريب المتعمد (Deliberate sabotage).
قد يلجأ منافس أو عميل ما إلى اختراق موقع المنشأة وتغيير بعض الصفحات للإساءة للمنشأة أو تعطيل الموقع بحيث يرفض خدمة العملاء المحتملين.
4 – تغيير البيانات (Data alteration).
لا يمكن فقط التنصت على بيانات الانترنت بل يمكن تغيير البيانات كقيمة المنتج، الخدمة، المعلومات الشخصية. (نصير ،2005, ص 47).

أمن التجارة الإلكترونية:
يتصدر موضوع الأمن على شبكة الإنترنت قائمة الاهتمامات لدى معظم المستخدمين خاصة ممن يرغبون في الشراء عبر الإنترنت ولذلك تجد الأغلبية الساحقة من المستخدمين خاصة الجدد منهم يمتنعون عن الشراء عبر الإنترنت ويؤجلون الخوض في مثل هذه التجربة حتى تكتمل الصورة لديهم ويتعرفون على المزيد من درجة الأمان في استخدام بطاقات الائتمان وهن ا لابد أن نتطرق إلى بروتوكولات الأمن للسداد الإلكتروني.

البروتوكولات الأمنة للسداد الإلكتروني:
1 - SET بروتوكول التعاملات الإلكترونية الأمنة " Secure Electronic Transactions ":
هو البروتوكول الأمن الأول المعتمد بواسطة شركة الائتمان لاستخدام بطاقات الائتمان لتنفيذ العمليات التجارية فهو يوفر " الخصوصية، التأكد من الهوية، التكامل وعدم الإنكار " ونظرا لصعوبة استخدامه وتعقيده لجأ الكثيرين إلى استخدام بروتوكول طبقة المخرج الأمنةSSL. 2 - SSL بروتوكول طبقة المخرج الأمنة " Secure Socket Layers "
"فارس التجارة الإلكترونية":
هو بروتوكول تشفير متخصص لنقل البيانات والمعلومات المشفرة بين جهازين عبر شبكة الانترنت بطريقة آمنة بحيث لا يمكن لأحد من الناس قراءتها غير المرسل والمستقبل وفي نفس الوقت تكون قوة التشفير فيها قوية ويصعب فكها، وهي تختلف عن بقية طرق التشفير في شيء واحد ألا وهو عدم الطلب من مرسل البيانات اتخاذ أي خطوات لتشفير المعلومات المراد حمايتها وكل الذي يفعلها المستخدم هو التأكد من استخدام هذا البروتوكول بالقوة المطلوبة. (المختار، سالم: 2018 ,ص ص414 415).

الأمن السيبراني:
تمهيد:
إن التطور الهائل في استخدام شبكة الانترنت في كافة المجالات تولد منه ظهور تهديدات ومعوقات تعمل على تدمير المنظمات المستخدمة للفضاء الالكتروني مما استدعى ظهور الأمن السيبراني وتطوير برامجه لحماية كل المكونات

المستخدمة لشبكة الانترنت. لقد أصبحت دراسة الأمن السيبراني واحد من مستحدثات التطور التكنولوجي الرقمي حيث يشهد العالم بكافة ارجائه تطور كبير لا يمكننا باي حال ان نغفله ولعل من اهم أسباب دراسة الأمن السيبراني هو حماية مستخدمي الشبكة وحماية الشبكة الدولية من الظواهر السلبية الرقمية المتمثلة في الابتزاز والتنمر والاختراق الالكتروني والجريمة والقرصنة الالكترونية.

مفهوم الأمن السيبراني:

مصطلح الأمن السيبراني: فهو مكون من كلمتي (الأمن) و (السيبراني)، وهذا المصطلح المركب نظرا الحداثة مصطلح الأمن السيبراني، فقد اختلفت عبارات الباحثين ووجهات نظرهم في تحديده، وضبط مفهومه، وسنورد شيئًا من تلك التعريفات، وماذا تعني السيبرانية.

تعريف الأمن: لقد تعددت معاني الأمن في اللغة منها الثقة، الحفظ، الأمان السلم التصديق، الدين القوة الإجارة وطلب الحماية، والمراد به هنا الأمن ضد الخوف، وإطلاق لفظ الأمن مجردا يؤدى إلى نوع من الالتباس خلط بين المعاني، إنما بحسب طبيعة الموقف المراد التعبير عنه بأحد هذه المعاني.

تعريف الأمن اصطلاحاً: الأمن عدم توقع المكروه في زمن آت.

تعريف السيبرانية: مأخوذة من كلمة(سيبر) Cyber، وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي فالسيبرانية، تعني: (فضاء الانترنت).

الأمن السيبراني: عرف بأنه أمن الشبكات والأنظمة والمعلوماتية، والبيانات والمعلومات والأجهزة المتصلة بالأنترنت وعليه فهو مجال يتعلق بإجراءات ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات ومنع التعديات والحد من آثارها في أقسي واسوأ الأحوال. (البشير: 2021، ص458).

وأيضا عُرف بأنه عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة الحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

ويرى الباحثان أنه من التعريفات السابقة الذكر يمكن تلخيص تعريف الأمن السيبراني: بأنه "مجموعة الأنشطة أو العمليات التي يتم عن طريقها حماية نظم المعلومات والاتصالات وجميع المعلومات المنتقلة فيها والتصدي لأي خطر أو ضرر يلحق بها.

نشأة الأمن السيبراني:

إن نشأة الأمن السيبراني تعود إلى تطور استخدام التقنية الرقمية حيث أن ظهور الانترنت أدى إلى استخدام الشبكات الإلكترونية بشكل أساسي ومحدود في القطاع العسكري والحكومي، ومع زيادة استخدام الإنترنت وانتشاره في العالم بدأت تظهر تهديدات جديدة تتعلق بأمن المعلومات والبيانات، ومع الانفجار الهائل في استخدام الانترنت أصبح هناك اعتماد كبير على البنية التحتية الرقمية ونقل المعلومات الحساسة عبر الشبكات، وهذا أدى إلى زيادة التهديدات السيبرانية مثل الاختراقات الإلكترونية وسرقة المعلومات والبرمجيات الخبيثة والاحتيال الإلكتروني والابتزاز والتنمر الإلكتروني مع تزايد التهديدات السيبرانية وتطور أساليبها أصبح واجبا تطوير استراتيجيات الحماية وبرامجها ومجلاتها.

أهمية الأمن السيبراني:

تتجلى في أهمية الأمن السيبراني في الاتي:(www.elnoronline.net)

1. حماية البيانات الحساسة
2. الحفاظ على استقرار الأنظمة
3. الحفاظ على سمعة الشركة
4. حماية البنية التحتية
5. المساهمة في تحقيق التنمية الاقتصادية

وبذلك نخلص إلى أن الأمن السيبراني له أهمية كبيرة في تحقيق البيئة الرقمية آمنة ومحمية، يمكن للشركات والأفراد أن يستخدموا التكنولوجيا في الفضاء الالكتروني بثقة ويركزوا على توسيع أعمالهم وابتكار منتجات وخدمات جديدة.

أهداف الأمن السيبراني:

من أهم أهداف الأمن السيبراني: (السمحان:2020، ص،12)

1- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.

2- التصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.

3- توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.

4- صمود البني التحتية الحساسة للهجمات الإلكترونية.

5- توفير المتطلبات الأزمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.

6- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
7- سد الثغرات في أنظمة الأمن المختلفة.
8- مقاومة البرمجيات الخبيثة.
9- حد من التجسس والتخريب الإلكتروني على كافة المستويات.
10-ا اتخاذ جميع الاجراءات اللازمة لحماية مستخدمي الشبكة من المخاطر المحتملة.

أبعاد الأمن السيبراني: (السمحان:2020، ص15**)**
1- الأبعاد العسكرية.
2- الأبعاد السياسية.
3- الأبعاد الاقتصادية.
4- الأبعاد القانونية.

متطلبات تحقيق الأمن السيبراني: (السمحان: 2020، ص16)
1.الموثوقية: وتعني استخدام المواقع الموثوق بها عند تقديم معلومات شخصية، والقاعدة الأساسية هي التحقق من عنوان URL، وإذا كان الموقع يتضمن https في بدايته، فهذا يعني أنه موقع آمن، أما إذا كان عنوان URL يحتوي على http بدون**s**؛ فيجنب الحذر من إدخال أي معلومات حساسة مثل بيانات بطاقة الائتمان، أو رقم التأمين الاجتماعي.
2.البريد الاحتيالي: ويعني عدم مرفقات البريد الإلكتروني أو النقر فوق روابط الرسائل من المصادر غير المعروفة، إذ إن إحدى الطرق الأكثر شيوعا التي يتعرض فيها الأشخاص للسرقة أو الاختراق هي عبر رسائل البريد الإلكتروني المتخفية على أنها مرسلة من شخص موثوق به.
3.التحديثات (Always up-to-date) وتعنى الحرص دائما على تحديث الأجهزة، فغالبا ما تحتوي تحديثات البرامج على تصحيحات مهمة لإصلاح مشكلات الأمان، وإن هجمات المخترقين الناجحة تتركز على الأجهزة القديمة بنسبة كبرى، والتي لا تملك أحدث برامج الأمان.
4.النسخ الاحتياطي ويتطلب هذا عمل نسخ احتياطية من الملفات بانتظام لمنع هجمات الأمان على الإنترنت.

مميزات الأمن السيبراني:

هناك عدة مزايا للأمن السيبراني اهمها:(www.sotor.com**)**
1.توفير الحماية للبيانات.
2.اكتشاف التهديدات السيبرانية.
3.حماية السمعة التجارية.
4.تعزيز الإنتاجية.
5.تعزيز الأمن الوظيفي.
6.دعم بيئات العمل عن بعد.
7.تقليل أعطال الكمبيوتر**.**

تحديات الأمن السيبراني:(بوقرص:2022، ص17)
1.الإنسان: أن أكبر وأخطر تحديات الأمن السيبراني هو العنصر البشري والمتمثل فيما يلي:
ا. التمكن من التحكم في ردود الفعل العاطفية.
ب. السياسة الأمنية معقدة وتستند إلى أحكام بشرية.
ج. أنظمة الأمن هي من تصميم الإنسان والإنسان هو الذي يسيرها ويثبت معايرها ويستعملها.
د. إساءة استخدام الحقوق: حتى نظام أو تطبيق جيد وموثوق به يمكن أن يتعرض للهجوم من قبل الأشخاص الذين ينتهكون حقوقهم.
هـ. الموارد البشرية: يعد نقص المتخصصين في مجال أمن منظومات الأمن تحديا حقيقيا للشركات.
2.المنظمات تخاطر عند استعمالها للفضاء السيبراني.
3. التشفير له نقاط ضعف وكلمات المرور يمكن كسرها.
4. الابتكار في خدمة الهجمات السيبرانية ولهذا فإن المراقبات التقليدية للمخاطر يجب أن تتكيف مع التهديدات الحالية والمستقبلية.
5. ظهور تقنيات جديدة وبالتالي نقاط ضعف جديدة وباستمرار وحتى للشركات التي لديها موارد لا بأس بها.

6. توسع وتطور رقعة الهجومات السيبرانية وذلك راجع الى الارتفاع المذهل لعدد الأشياء المتصلة بالإنترنت (IOT) وكذا عدد مستعملي الإنترنت من جهة وتهديدات الدول فيما بينها والذي أدى الى تصاعد عدد الحروب السيبرانية والتجسس السيبراني من جهة أخرى.
7. المرونة السيبرانية باعتبارها ميزة الشركات التي تتمتع بالقدرة على الاستعداد والتكيف مع التهديدات المتطورة وكذلك استرداد قدراتها بسرعة من الهجمات السيبرانية. في هذا الإطار يلاحظ عدم إقامة تدريبات حل الأزمات لعدد كبير من الشركات.
8. القوانين التشريعية في ميدان الأمن السيبراني والتي من المفروض أن تكون متطورة وسريعة تساير وتتكيف مع تطور الجرائم السيبرانية من أجل مكافحتها في الوقت المناسب.

مقارنة بين الأمن الرقمي والأمن السيبراني:

يرتبط الأمن الرقمي والأمن السيبراني ارتباطا وثيقا لدرجة انه غالبا ما يعتقد انهما مرادفين لنفس المعني، ولكن هناك بعض الفروقات الهامة بين الاثنين، يهتم الأمن الرقمي (أمن البيانات والمعلومات) بالتأكد من أمان البيانات والمعلومات بأي شكل من الأشكال سواء كانت الكترونية أو مستندات ورقية أو غيرها وهو أوسع قليلا من الأمن السيبراني لذا من المحتمل أن يكون شخص خبيرا في أمن البيانات والمعلومات دون أن يكون خبيرا في الأمن السيبراني.
أما الأمن السيبراني يدور حول البياتة والمعلومات الموجودة في شكل الكتروني مثل :(أجهزة الكمبيوتر والخوادم والشبكات والأجهزة المحمولة وغيرها) من التعرض للخطر أو الهجوم القادم من الفضاء الإلكتروني، جزء من ذلك هو تحديد البيانات المهمة وأين توجد والمخاطر المحتملة والتكنولوجيا التي يجب عليك تنفيذها من أجل حمايتها.
هذا يجعل الأمن السيبراني (Cyber security) مجموعة فرعية من الأمن الرقمي ولكن جرائم الأنترنت التي تنطوي على تهديد للمعلومات ليست جزء من الأمن الرقمي ولكنها في الواقع مصدر قلق للأمن السيبراني وعلى نفس المنوال فأن تهديدات البيانات والمعلومات الغير الكترونية تخضع للأمن الرقمي وليست تحت الأمن السيبراني.

جدول رقم (أ) يوضح الفرق بين الأمن الرقمي والأمن السيبراني.

الأمن الرقمي	الأمن السيبراني
الأمر كله يتعلق بحماية البيانات والمعلومات من الاستخدام والوصول والتعديل غير المصرح به.	انها ممارسة لحماية البيانات والمعلومات من المصادر الخارجية على الأنترنت.
يتعامل مع حماية البيانات والمعلومات من أي شكل من اشكال التهديد.	يتعلق بالقدرة على حماية استخدام الفضاء الالكتروني من الهجمات الإلكترونية.
حماية البيانات والمعلومات بغض النظر عن مكان وجودها أو شكلها.	حماية أي شيء في عالم الأنترنت.
يسعي لمنع الوصول غير المصرح به وتعديل واتلاف البيانات.	يهاجم جرائم الأنترنت والاحتيال عبر الأنترنت وانفاد القانون من خلال الوصول للمهاجمين ومعاقبتهم.

موقع أبحاث :www.ab7as.com 2024-1-9

الإطار العملي للبحث

نبذة عن جامعة بني وليد (محل البحث):

أنشأت جامعة بني وليد بقرار من اللجنة الشعبية العامة للتعليم (سابقا) باسم جامعة الأقسام سنة2000م وضمت أقسام الاقتصاد والزراعة والقانون وقسمي العلوم والآداب الذين كانا كليتين تابعتين لجامعة المرقب منذ سنة 2002 م.
تم ضم هذه الأقسام لجامعة مصراته ثم جامعة الزيتونة بترهونة ثم أخيرا تم اصدار قرار من وزارة التعليم باستقلالية جامعة بني وليد فهي الأن تضم 10 كليات وأكثر من 9000 طالب وطالبة. (**المصدر:** مقابلات شخصية مع المسؤولين في جامعة بني وليد).
تم تحديد حجم العينة والتي اقتصرت على طلبة كلية الاقتصاد والعلوم السياسية وكان عددها (50) استمارة استبيان وزعت على مختلف مستويات طلبة كلية الاقتصاد وذلك لتعاملهم مع عدد كبير من المواقع وخاصة ذات الطبيعة التجارية ولذلك كانت العينة عشوائية بسيطة توجه للطلبة المحتمل كثرة دخولهم للمواقع التجارية مع العلم أن عدد طلبة كلية الاقتصاد حوالي 1300 طالب مسجلين في 8 أقسام وقد تحصلنا على (47) استمارة استبيان واستبعد (3)، وتم تفريغ وتحليل البيانات للتوصل إلى نتائج تمكننا من الاستفادة منها في استخلاص أهم الجوانب التي يجب التركيز عليها والتحذير منها للمحافظة على الأجيال القادمة من خطر المواقع الهدامة وتعزيز الأمن السيبراني.

أولاً: صدق أداة الدراسة الاستبانة

يقصد بصدق الاستبانة أن تقيس أسئلة الاستبانة ما وضعت لقياسه وثم بالتأكد من صدق الاستبانة بطريقتين:
لغرض قياس ثبات أداة الدراسة فقد تم توزيع عدد 20 نسخة منها، وباستخدام الحزمة الإحصائية للعلوم الاجتماعية Statistical Package For Social Sciences(SPSS) وذلك عن طريق المقارنة الطرفية للصدق واستخراج اختبار ألفا كرونباخ (α) الثبات:

أولاً: صدق أداة الدراسة:

1. **المقارنة الطرفية:** وهو حساب قيمة اختبار (ت) لدلالة الفروق بين متوسط قيم الربيع الأدنى (27% من القيم الدنيا) ومتوسط قيم الربيع الأعلى (27 % من القيم العليا) لجميع مقاييس الدراسة، وجاءت النتائج لكل مقياس من مقياس الدراسة كما يلي:

الجدول رقم (1) نتائج اختبار ت للمقارنة الطرفية.

27% من القيم الدنيا ن= 6		27% من القيم العليا ن= 6		قيمة اختيار (ت) المحسوبة	قيمة مستوى المعنوية المشاهدة
المتوسط الحسابي	الانحراف المعياري	المتوسط الحسابي	الانحراف المعياري		
2.64	0.352	4.06	0.068	11.292	0.000 دال إحصائيا

يتضح من الجدول رقم (1) إن قيمة (ت) المحسوبة للمقارنة بين الربيع الأدنى والربيع الأعلى لعبارات الاستبيان (11.292) كانت أكبر من قيمة ت الجدولية التي تساوي (2.145)، وإن قيمة مستوى المعنوية المقابلة لها أقل من (0.05) مستوى المعنوية المعتمد في الدراسة وعليه يمكن القول انه توجد دالة إحصائيا بين الربيع الأدنى والربيع الأعلى الاستبيان.

ثانياً: ثبات أداة الدراسة:

يقصد بثبات أداة جمع البيانات دقتها واتساقها بمعنى إن تعطي أداة جمع البيانات النتائج نفسها إذا تم استخدامها أو إعادتها مرة أخرى تحت ظروف مماثلة.

ألفا كرونباخ: يعد ألفا كرونباخ من الاختبارات الإحصائية المهمة لتحليل بيانات الاستبانة، وهو اختبار يبين مدى الاتساق الداخلي لعبارات الاستبانة (محمود المهدي البياتي: تحليل البيانات الإحصائية باستخدام البرنامج الإحصائي SPSS، 2005 صفحة 49، دار الحامد، عمان). وتكون قيمة معامل ألفا كرونباخ ما بين (0 , 1) ويبين مدى الارتباط بين إجابات مفردات العينة فعندما تكون قيمة معامل ألفا صفر فيدل ذلك على عدم وجود ارتباط مطلق ما بين إجابات مفردات العينة، أما إذا كانت قيمة معامل ألفا كرونباخ واحد صحيح فهذا يدل على أن هناك ارتباط تام بين إجابات مفردات العينة، ومن المعروف أن أصغر قيمة مقبولة لمعامل كرونباخ ألفا (α) هي 0.6 وأفضل قيمة تتراوح بين (0.7 إلى 0.8) وكلما زادت قيمته عن 0.8 كان ذلك أفضل، فإن هذه الأسئلة تكون مرتبطة ببعضها كما بالجدول رقم (2) .

جدول رقم (2) نتائج اختبار كرونباخ ألفا.

الاستبيان	عدد العبارات	معامل ألفا كرونباخ (الثبات)
دور الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية الخدمة التعليمية	12	0.814

يتضح من الجدول السابق رقم (2) إن معامل الثبات الاستبيان 0.814 وهي أكبر من 0.8 وهي قيمة تعتبر ممتازة وهذا يدل ان هناك ترابط بين عبارات الاستبيان.
وبذلك يكون قد تم التأكد من صدق وثبات مقياس الدراسة مما يجعلها على ثقة بصحة المقياس 1صلاحيته لتحليل النتائج والإجابة على فرضيات أو تساؤلات الدراسة.

أولاً: تحليل المعلومات الأولية

1) **الجنس: في** الجدول رقم (3) والشكل رقم (1) تبين لتوزيع مفردات مجتمع الدراسة حسب الجنس.

الجدول رقم (3) يبين التوزيع التكرار الجنس.

الجنس	العدد	النسبة
ذكر	28	%59.6
انثى	19	%40.4
المجموع	47	%100

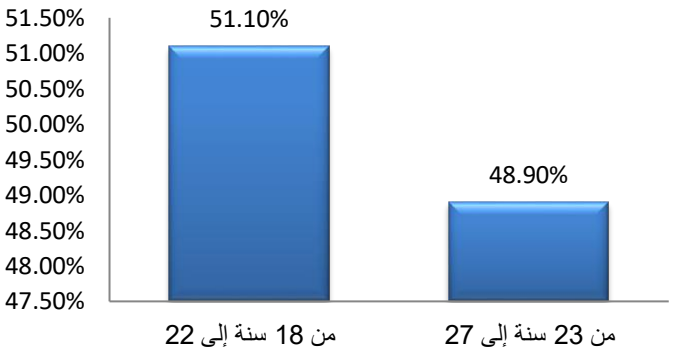
الشكل رقم (1) يوضح نسب لمفردات مجتمع الدراسة حسب الجنس.

يتبين من الجدول رقم (3) والشكل رقم (1) أن أعلى نسبه من مفردات عينة الدراسة الذكور بلغت نسبتهم59.6%، ونسبة الانات فبلغت 40.4%.

2) العمر: في الجدول رقم (4) والشكل رقم (2) تبين لتوزيع المجيبين حسب العمر.

الجدول رقم (4) يبين التوزيع التكراري والنسب لعمر المجيبين.

فئات السنوات	العدد	النسبة
من 18 سنة إلى 22	24	%51.1
من 23 سنة إلى 27	23	%48.9
المجموع	**47**	**%100**



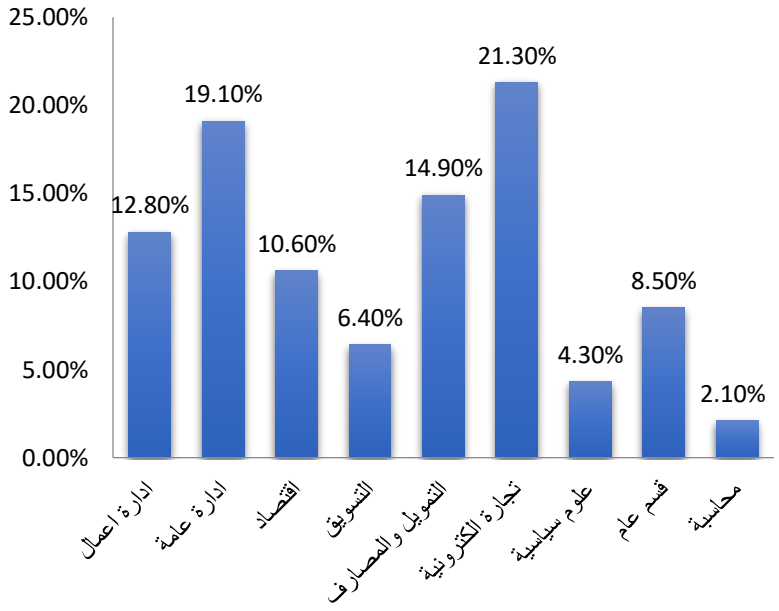
الشكل رقم (2) يوضح نسب لمفردات عينة الدراسة لعمر المجيبين.

يتضح من الجدول السابق رقم (4) والشكل رقم (2) أن أعلى نسبه من المجيبين الذين عمرهم من 18 سنة إلى 22 سنة فقد بلغت نسبتهم 51.1% ن وكانت اقل نسبة الذين عمرهم من 23 إلى أقل من 27 سنة فقد بلغت 48.9%.

3) **التخصص العلمي: في** الجدول رقم (5) والشكل رقم (3) تبين لتوزيع مفردات مجتمع الدراسة حسب التخصص العلمي.

الجدول رقم (5) يبين التوزيع التكرار التخصص العلمي.

التخصص العلمي	العدد	النسبة
ادارة اعمال	6	%12.8
ادارة عامة	9	%19.1
اقتصاد	5	%10.6
التسويق	3	%6.4
التمويل والمصارف	7	%14.9
تجارة الكترونية	10	%21.3
علوم سياسية	2	%4.3
قسم عام	4	%8.5
محاسبة	1	%2.1
المجموع	**47**	**%100**



الشكل رقم (3) يوضح نسب لمفردات مجتمع الدراسة حسب التخصص العلمي.

يتبين من الجدول رقم (5) والشكل رقم (3) أن أعلى نسبة من المجيبين تخصصهم تجارة الكترونية وبلغت نسبتهم 21.30% ويليهم اللذين تخصصهم إدارة عامة بلغت نسبتهم 19.10% ويليها اللذين تخصصهم التمويل والمصارف نسبتهم 14.90 %، وأقل نسبة اللذين تخصصهم محاسبة.

ثانياً: تحليل عبارات الدراسة

لتحقيق أهداف الدراسة وتحليل البيانات التي تم تجميعها، فقد تم استخدم الباحث الطريقة الرقمية في ترميز الإجابات المتعلقة بمقياس ليكيرث الخماسي كما بالجدول (6):

الجدول رقم (6) توزيع الدرجات على الإجابات المتعلقة بعبارات المقياس.

الإجابة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1

يتم بعد ذلك حساب المتوسط الحسابي (المتوسط المرجح) لتحديد أوزان العبارات حسب قيم المتوسط المرجح المتحصل عليها نتيجة لتحليل الإجابات كما في الجدول رقم (6) وذلك بعد أن تم ترميز وإدخال البيانات إلى الحاسب الآلي، ولتحديد طول خلايا المقياس الخماسي (الحدود الدنيا والعليا) المستخدم في محاور الدراسة، تم تقسيمه على عدد خلايا المقياس للحصول على طول حساب المدى (5-1= 4) وبعد ذلك تم تقسيم المدى على خمس مستويات 4÷ 5= 0.80 (وهذا الرقم يعتبر طول الفئة الواحدة أو المستوى الواحد، وهكذا الاوزان كما هو موضح في جدول المتوسط المرجح التالي:

الجدول رقم (7) المتوسط المرجح المتحصل عليه من تحليل الإجابات.

	منخفض جدا	منخفض	متوسط	مرتفع	مرتفع جدا
المتوسط المرجح	من 1 إلى أقل من 1.80	من 1.80 إلى أقل من 2.60	من 2.60 إلى أقل من 3.40	من 3.40 إلى أقل 4.20	من 4.20 إلى 5

لتحليل عبارات دور الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية من حيث درجة الموافقة سنوضح المتوسط الحسابي والانحراف المعياري لكل عبارة وأهميتها نحو كل فقرة وللفقرات وترتيبها تنازلياً حسب متوسطات الموافقة في الجدول التالي:

رقم العبارة	العبارة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الدرجة	الرتبة
1	لديك وعي إلكتروني كافي لمخاطر الهجمات السيبرانية على مستخدمي شبكة الانترنت عامة وعلى المنظومة الالكترونية لجامعة بني وليد خاصة	3.40	0.825	%68.1	مرتفع	5
2	تستخدم التوقيع الالكتروني المتمثل في كلمات مرور قوية ومتغيرة لحساباتك عند الدخول لأي شبكة متصلة بالأنترنت. للحماية من الاختراق ومحاربة الظواهر السلبية	4.04	0.721	%80.9	مرتفع	1
3	تقوم بإجراء نسخ احتياطية لبياناتك الشخصية والعلمية بشكل دوري للحماية من الحذف والفيروسات	4.00	1.063	%80.0	مرتفع	2
4	تم اختراق حساباتك على شبكة الانترنت أو شعرت بأي أداء غير طبيعي أو مشبوه في نظام حساباتك الشخصية.	2.40	1.035	%48.1	منخفض	11
5	تقوم بتحديث برامج الحماية على أجهزتك الشخصية للحفاظ على سلامة بياناتك الشخصية والعلمية.	3.74	1.242	%74.9	مرتفع	4
6	تقوم بفحص رسائل البريد الالكتروني المشبوهة قبل فتحها أو تنزيل المرفقات للحماية من الفيروسات	4.00	0.834	%80.0	مرتفع	2
7	تخاف من الإفصاح عن المعلومات الشخصية أو المالية عند القيام بعمليات تجارية الكترونية لمقاومة ظواهر الاختراق والفيروسات	3.81	1.154	%76.2	مرتفع	3
8	يتم استخدام خدمة VPNلحفظ سرية المعلومات على شبكة Wi-Fiللحصول على أكثر حماية للمنظومة	3.36	0.919	%67.2	متوسط	6
9	توجد مواقع تزورها دائما ولا تحصل منها على فوائد وأصبحت مدمنا عليها.	2.87	1.191	%57.4	متوسط	9
10	تشعر بأن تدفق المعلومات لحساباتك الشخصية محمية بشكل جيد من التهديدات السيبرانية.	3.09	0.905	%61.7	متوسط	7

11	تقوم الدولة ممثلة في وزاراتها الحكومية بتحذير مستخدمي شبكة الانترنت من بعض المواقع التي تستخدم من خلالها التهديدات السيبرانية.	2.98	1.151	%59.6	متوسط	8
	الإجمالي	3.35	0.427	%67	متوسط	

من خلال النتائج الموضحة أعلاه يتضح ان درجة الموافقة على العبارات ككل مرتفع حيث كانت درجة المتوسط الحسابي الكلية للمحور (3.35) وبوزن نسبي 67%وهي في خانة المرتفع في جدول المتوسط المرجح، وتم ترتيب الفقرات ترتيباً تنازلياً حسب موافقة أفراد عينة الدراسة عليها كالتالي:

1. **جاءت العبارة رقم (2)** والتي تشير إلى " تستخدم التوقيع الالكتروني المتمثل في كلمات مرور قوية ومتغيرة لحساباتك عند الدخول لأي شبكة متصلة بالأنترنت للحماية من الاختراق ومحاربة الظواهر السلبية " **بالمرتبة الأولى** من حيث موافقة أفراد عينة الدراسة بدرجة مرتفعة بمتوسط (4.04) وبوزن نسبي 80.9%.
2. **جاءت العبارات رقم (6/3).** والتي تشير " تقوم بإجراء نسخ احتياطية لبياناتك الشخصية والعلمية بشكل دوري للحماية من الحذف والفيروسات /تقوم بفحص رسائل البريد الالكتروني المشبوهة قبل فتحها أو تنزيل المرفقات للحماية من الفيروسات " **بالمرتبة الثانية** من حيث موافقة أفراد عينة الدراسة بدرجة مرتفعة بمتوسط (4) وبوزن نسبي 80%.
3. **جاءت العبارة رقم (7)** والتي تشير إلى " تخاف من الإفصاح عن المعلومات الشخصية أو المالية عند القيام بعمليات تجارية الكترونية لمقاومة ظواهر الاختراق والفيروسات **بالمرتبة الثالثة** من حيث موافقة أفراد عينة الدراسة بدرجة مرتفعة بمتوسط (3.81) وبوزن نسبي 76.2%.
4. **جاءت العبارة رقم (5)** والتي تشير إلى تقوم بتحديث برامج الحماية على أجهزتك الشخصية للحفاظ على سلامة بياناتك الشخصية والعلمية. " **بالمرتبة الرابعة** من حيث موافقة أفراد عينة الدراسة بدرجة مرتفعة بمتوسط (3.74) وبوزن نسبي 74.9%.
5. **جاءت العبارة رقم (1)** والتي تشير إلى " لديك وعي إلكتروني كافي لمخاطر الهجمات السيبرانية على مستخدمي شبكة الانترنت عامة وعلى المنظومة الالكترونية لجامعة بني وليد خاصة " **بالمرتبة الخامسة** من حيث موافقة أفراد عينة الدراسة بدرجة مرتفعة بمتوسط (3.40) وبوزن نسبي 68.1%.
6. **جاءت العبارة رقم (8)** والتي تشير إلى " يتم استخدام خدمة VPNلحفظ سرية المعلومات على شبكة Wi-Fi للحصول على أكثر حماية للمنظومة **بالمرتبة السادسة** من حيث موافقة أفراد عينة الدراسة بدرجة متوسطة بمتوسط (3.36) وبوزن نسبي 67.2%.
7. **جاءت العبارة رقم (10)** والتي تشير إلى "" تشعر بأن تدفق المعلومات لحساباتك الشخصية محمية بشكل جيد من التهديدات السيبرانية " **بالمرتبة السابعة** من حيث موافقة أفراد عينة الدراسة بدرجة متوسطة بمتوسط (3.09) وبوزن نسبي 61.7%.
8. **جاءت العبارة رقم (11)** والتي تشير إلى " تقوم الدولة ممثلة في وزاراتها الحكومية بتحذير مستخدمي شبكة الانترنت من بعض المواقع التي تستخدم من خلالها التهديدات السيبرانية.." **بالمرتبة الثامنة** من حيث موافقة أفراد عينة الدراسة بدرجة متوسطة بمتوسط (2.98) وبوزن نسبي 76%.
9. **جاءت العبارة رقم (9)** والتي تشير إلى "" توجد مواقع تزورها دائما ولا تحصل منها على فوائد وأصبحت مدمنا عليها." **بالمرتبة التاسعة** من حيث موافقة أفراد عينة الدراسة بدرجة متوسطة بمتوسط (2.87) وبوزن نسبي 57.4%.
10. **جاءت العبارة رقم (12)** والتي تشير إلى " تعرضت للظواهر السلبية من قبل وكان لأنظمة وبرامج وتطبيقات الأمن السيبراني دور فعال في كشف هذه الظواهر والحد من خطورتها.." **بالمرتبة العاشرة** من حيث موافقة أفراد عينة الدراسة بدرجة منخفض بمتوسط (2.53) وبوزن نسبي 50.6%.
11. **جاءت العبارة رقم (4)** والتي تشير إلى "" تم اختراق حساباتك على شبكة الانترنت أو شعرت بأي أداء غير طبيعي أو مشبوه في نظام حساباتك الشخصية " **بالمرتبة الحادية عشر** من حيث موافقة أفراد عينة الدراسة بدرجة متوسطة بمتوسط (2.40) وبوزن نسبي 48.1%.

التحقق من فرضيات الدراسة

الفرضية الأولى:

الفرضية الصفرية: لا يوجد دور الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية.

الفرضية البديلة: يوجد دور الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية.

للتحقق من الفرضية تم استخدام المتوسط الحسابي والانحراف المعياري وقيم اختبار t ((One Sample T-test ومستوى الدلالة للتأكيد ان كان المستوى عالي ودو دلالة احصائية، وجاء النتائج كما في الجدول التالي:

جدول رقم (9) المتوسطات الحسابية وقيم اختبار ت ومستوى الدلالة.

العينة	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	قيمة t	مستوى الدلالة
47	3.35	0.427	46	5.663	0.000

يتضح من الجدول رقم (9) السابق إن المتوسط الحسابي يساوي (3.35) وقيمة اختبار ت المحسوبة تساوي (5.663) عند درجة حرية 46 وهي أكبر من قيمة ت الجدولية (2) ومستوى دلالة أقل من مستوى الدلالة 0.05 المعتمد في الدراسة، ومن خلال ذلك نرفض الفرضية الصفرية ونقبل **الفرضية البديلة القائلة يوجد دور الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية.**

الفرضية الثانية

الفرضية الصفرية: لا توجد فروق ذات دلالة إحصائية عند مستوى دلالة (0.05 ≥) في مستوى إجابات العينة دور الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية وتبعا لمتغير الجنس.

الفرضية البديلة: توجد فروق ذات دلالة إحصائية عند مستوى دلالة (0.05 ≥) في مستوى إجابات العينة دور الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية وتبعا لمتغير الجنس.

للتعرف على ما إذا كانت هنالك فروق ذات دلالة إحصائية في متوسطات إجابات أفراد عينة الدراسة طبقًا الجنس تم استخدام اختبار ت Independent Sample T-test " لتوضيح دلالة الفروق لأفراد عينة الدراسة وجاءت النتائج كما يوضحها الجدول التالي:

جدول رقم للفروق في متوسطات :Independent Sample T-test " نتائج اختبار " ت

جدول رقم (9) إجابات أفراد عينة الدراسة طبقًا إلى اختلاف متغير الجنس.

الجنس	العدد	المتوسط	الانحراف	درجة الحرية	قيمة ت	مستوى الدلالة	الدلالة
ذكر	28	3.31	0.435	45	0.783	0.438	غير دال عند 0.05
انثى	19	3.41	0.419				

يتضح من خلال النتائج الموضحة في الجدول رقم (9) أعلاه إن قيمة ت ل (0.783) وهي أقل من قيمة ت الجدولية البالغة (2) عند درجة الحرية 45، ومعدل الدلالة أكبر من 0.05، وهذا **يشير إلى إنه لا توجد فروق ذات دلالة إحصائية عند مستوى دلالة (0.05 ≥) في مستوى إجابات العينة دور الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية وتبعا لمتغير الجنس.**

النتائج:

1. يوجد دور للأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية.
2. لا توجد فروق ذات دلالة إحصائية عند مستوى دلالة (0.05 ≥) في مستوى إجابات العينة دور الأمن السيبراني في حماية مستخدمي الشبكة الدولية والحد من خطر الظواهر السلبية الرقمية وتبعا لمتغير الجنس.
3. أغلب المستخدمين يقضي ساعات طويلة على الشبكة الدولية ويعزلهم عن قضاء احتياجاتهم.
4. اكثر المستخدمين لا يمتلك نظام حماية قوي لحماية معلوماته من الاختراق أو التخريب أو السرقة.
5. أن أغلب الطلبة لا يستفيد من الشبكة الدولية في تطوير مستوى تعليمه وزيادة معرفته ويقتصر استخدامهم في الدخول إلى غرف الدردشة وغيرها.
6. هناك نوع من الإدمان على بعض المواقع التي تنشر الأفكار الهدامة من قبل بعض الطلبة.
7. يوجد بعض الطلبة تعرضوا لخطر الظواهر السلبية الرقمية ولم يفصحوا عن ذلك إلى أهلهم أو أقاربهم.

8. هناك عدد من الطلبة يفصحون دائما عن معلوماتهم الشخصية والمالية عند دخولهم للمواقع على الشبكة الدولية مما يعرضهم لخطر التنمر والابتزاز والقرصنة الالكترونية.

التوصـــيات:

1. عند الدخول إلى منصات التواصل الاجتماعي يجب تجنب قبول طلبات الصداقة أو الرد والتجاوب مع محادثات ترد من مصدر أو أشخاص مجهولين وتحصين الجهاز بنظام حماية قوي ولا يعطى المعلومات الخاصة قبل التأكد من الموقع مزيف أم لا.
2. لابد على مستخدمي الانترنت الابتعاد عن المواقع المشبوهة وتحصين أنفسهم من مخاطر الاختراق عند ممارسة أعمالهم وتسوقهم على الشبكة لحماية أنفسهم من خطر الظواهر السلبية الرقمية.
3. يمكن ان يعزز المستخدم العاد حمايته اثناء استخدام الأجهزة الإلكترونية عن طريق تحديث البرامج وأنظمة التشغيل واستخدام الشبكات الافتراضية الخاصة VPN وتجنب المواقع التي لا تعتمد بروتوكول: http ونسخ البيانات احتياطيا على وحدة تخزين خارجية.
4. على الجهات المختصة ضرورة إصدار التشريعات والقوانين اللازمة أو تطويرها إن وجدت لتطبيق الأمن السيبراني تعزيز الأمن الرقمي والأمن السيبراني والحماية الذاتية الالكترونية وادراجهم ضمن المناهج في المؤسسات التعليمية.
5. أن هذا الموضوع شديد الأهمية وينبغي أن نبذل فيه كل الجهـود الممكنة والمتوفرة وأن يحظى بكل العنايـة اللازمـة وكل الاهتمام المستطاع تقديمه.

كما يوصي الباحث ذوي الاختصاص والباحثين والأكاديميين بمواصلة مشوار البحث العلمي في موضوع البحث ونقترح عليهم العناوين التالية والمتعلقة بالأمن السيبراني وهي:

1 – الحماية الذاتية الالكترونية.

2- تأثير الانترنت العميق والإنترنت المظلم على الاقتصاد والأمن الرقمي.

المراجع:

أولاً: الكتب:

1.أمنة علي البشير، جامعة الازهر-مصر-2021 الأمن السيبراني في ضوء مقاصد الشريعة.

2.الحناوي، محمد صالح ،2010 مقدمة في الأعمال في عصر التكنولوجيا، الدار الجامعية طبع نشر توزيع، الإسكندرية مصر.

3.ساعد بوقرص، 2022جامعة العلوم والتكنلوجيا هواري بومدين-الأمن السيبراني: مخاطر وتحديات وتهديدات.

4.منى عبد الله السمحان، 2020جامعة المنصور كلية التربية -متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات.

5.نصير محمد طاهر، التسويق الالكتروني، دار الحامد للنشر والتوزيع، عمان، 2005.

ثانياً المواقع الالكترونية:

1. موقع أبحاث: www.ab7as.com. تاريخ الزيارة 31/ 1 / 2024.
2. موقع www.elnoronline.net تاريخ الزيارة 05/ 03 / 2024.
3. موقع أبحاث: www.sotor.com. تاريخ الزيارة 06/ 04 / 2024.

ثالثاً: البحوث العلمية:

1. المختار ميلاد سالم، سالم خالد ميلاد، المخدرات الرقمية كأحد أنواع الابتزاز الإلكتروني وتأثيرها على مستخدمي الانترنت، بحث منشور، المؤتمر الدولي الثاني لكلية الاقتصاد والتجارة حول الثورة التكنولوجية واقتصاديات القرن الواحد والعشرين، 2018.