Journal of the University of Babylon for Humanities مَجلّةُ جَامعةِ بَابِل للعُلومِ الإنسَانيّة
Vol.32 / No.11/ 2024 المجلد 32 / العدد 11/ 2024

بناء مقياس الوعي بالحرب السيبرانية لدى طلاب الجامعة في الجمهورية العربية السورية

هبة عبد اللطيف ضعضع
كلية التربية/ جامعة حلب
Hdodouh1987@gmail.com

تاريخ استلام البحث: 2024/10/24 تاريخ قبول النشر: 3/ 11/2024 تاريخ نشر البحث: 27/ 11/ 2024

المستخلص

هدف البحث إلى بناء مقياس لقياس مستوى الوعي بالحرب السيبرانية لدى طلاب الجامعة في الجمهورية العربية السورية، وتحديد الفروق وفقًا لمتغيرات الجنس والمؤهل العلمي، مع تقييم مؤشرات الصدق والثبات لهذا المقياس ذي الأبعاد: المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، والاستجابة للطوارئ السيبرانية. شملت عينة الدراسة 176 طالبًا من جامعة حلب موزعة وفقاً الجنس والتخصص.

أظهرت النتائج أن الوعي بالحرب السيبرانية وأبعادها كان مرتفعاً، وكانت الفقرات "لدي معرفة بأنواع الهجمات الرقمية مثل التصيد وDDoS" و"أستطيع تمييز علامات الاختراق الرقمي على حساباتي الشخصية" "أستخدم المصادقة الثنائية عندما يكون ذلك ممكناً" و"أعمل على تحديث برامج الحماية والأمان بشكل دوري" و"علم حقوقي وواجباتي كأحد مستخدمي الإنترنت" و"أرى أهمية وجود سياسة واضحة للأمان الرقمي" "أتابع التطورات في تقنيات الأمان الرقمي السيبراني" و"أستخدم أدوات الأمان بشكل منتظم لحماية بياناتي" و"أشعر بأنني قادر على التعامل مع الحوادث السيبرانية" و"أعرف كيفية التصرف إذا تعرضت لهجوم رقمي على حساباتي الشخصية" ″أعرف كيفية التعامل مع التوتر الناتج عن التهديدات الرقمية" و"أشعر بالقلق من التهديدات الرقمية في حياتي اليومية" أدنى وزن نسبي. يوجد فروق ذات دلالة إحصائية في الوعي بالحرب السيبرانية وأبعادها تبعاً لمتغير الجنس لصالح الذكور ماعدا بعد التأثيرات الاجتماعية لم تكن دالة، لا يوجد فروق ذات دلالة إحصائية في أبعاد الوعي بالحرب السيبرانية، ماعدا في بعد المعرفة بالمخاطر السيبرانية والدرجة الكلية للوعي بالحرب السيبرانية ولصالح الكليات التطبيقية.

توصي الباحثة بتعزيز التوعية المعرفية وتطوير السلوكيات الوقائية لنقاط الضعف الواردة سابقاً في الوعي بالحرب السيبرانية ببرامج تعليمية وتدريبية لدى فئة طلاب الجامعة.

الكلمات الدالة: الوعي، السيبرانية، الحرب السيبرانية

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

Journal of the University of Babylon for Humanities مَجلّةُ جَامعةِ بَابِلَ للعُلومِ الإنسَانيّةِ
Vol.32 / No.11/ 2024 المجلد 32 / العدد 11/2024

Constructing a Scale for Measuring Cyber-War Awareness among University Students in the Syrian Arab Republic

Hiba Abdullateef Dodouh
College of Education/ University of Aleppo

Abstract

This research aimed to construct a scale to measure the level of cyber-war awareness among youth in the Syrian Arab Republic and identify differences based on gender and educational qualifications. It also evaluated the validity and reliability of the scale. The researcher used a questionnaire that included several dimensions, such as knowledge of cyber risks, personal protection strategies, understanding security responsibilities, awareness of security tools and technologies, and response to cyber emergencies. The study sample consisted of 176 students from Aleppo University, categorized by demographic variables such as gender and specialization.

The results indicated a high overall awareness of cyber war and its dimensions, with a relative weight of 80.04%. The highest-scoring items included statements such as: "I am aware of the types of digital attacks, such as phishing and DDoS," "I can recognize signs of digital breaches on my personal accounts," "I use two-factor authentication when possible,""I regularly update security and protection programs," "I am aware of my rights and responsibilities as an internet user," "I see the importance of a clear digital security policy," "I follow developments in cybersecurity technologies," "I regularly use security tools to protect my data," "I feel capable of handling cyber incidents," "I know how to act if my personal accounts are attacked," "I know how to manage stress caused by digital threats," and "I am concerned about digital threats in my daily life."

Statistically significant differences in cyber war awareness and its dimensions were found based on gender, with males scoring higher in all but the social impacts dimension, which showed no significant difference. Additionally, no statistically significant differences were found across most dimensions of cyber war awareness, except for knowledge of cyber risks and the overall awareness score, which favored students in applied sciences.

The researcher recommends enhancing cognitive awareness and developing preventive behaviors to address the previously mentioned weaknesses in cyber war awareness through educational and training programs for university students.

Keywords: Awareness, Cybersecurity, Cyber War.

1- مشكلة البحث:

شهد العالم الرقمي تصاعداً في التهديدات السيبرانية، مما يجعل من الضروري فهم الحرب السيبرانية وأثرها على الأفراد، خاصة طلاب الجامعة الذين يشكلون الشريحة الأكبر من مستخدمي الإنترنت. تُعرف السيبرانية بارتباطها بالفضاء الرقمي والأنظمة الحاسوبية، بينما شمل الأمن السيبراني جميع الإجراءات التنظيمية والتقنية لحماية المعلومات والبنية الرقمية من الهجمات الخبيثة[1]. تتنوع الهجمات السيبرانية بين التصيد الاحتيالي (Phishing Attacks) والبرمجيات الخبيثة (Malware) وهجمات الحرمان من الخدمة (DDoS) والهندسة الاجتماعية (Social Engineering) على سبيل المثال، تعرضت شركة SolarWinds لهجوم في عام 2020،

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

مما أثر على الوكالات الحكومية والشركات الكبرى [2،ص50-61]، ما حدث هجوم WannaCry في عام 2017، الذي استهدف الأنظمة التشغيلية واستغل ثغراتها، مما أثر على مئات الدول.

مع تسارع التحول الرقمي ازدادت التهديدات السيبرانية التي تستهدف الأفراد والمؤسسات على حد سواء، مما يبرز الحاجة لفهم مفهوم الحرب السيبرانية وتأثيراتها المحتملة على الأمان الرقمي، ومن هنا كان الوعي بالحرب السيبرانية أمرا بالغ الأهمية، فله أثر بارز في حماية الأفراد والمؤسسات من الهجمات السيبرانية التي تستهدف البيانات الحساسة والبنية التحتية الرقمية، وكان الجهل بهذا النوع من الحروب يشكل خطراً كبيراً ويمكن أن يؤدي إلى اختراق الأنظمة أو تسريب البيانات أو تعطيل الخدمات الحيوية على المستوى الوطني والشخصي. الأمر الذي توجب إعداد أدوات دقيقة لقياس مستوى الوعي بالحرب السيبرانية لدى الأفراد والمجتمعات، هذه الأدوات تسهم في تحديد الفجوات المعرفية واستكشاف احتياجات التوعية والتعليم. بفضل هذه الأدوات، يمكن تطوير برامج تدريبية مخصصة وتطبيق سياسات توعية لتعزيز الفهم بأهمية الأمن السيبراني وتعليم الأفراد كيفية التصرف في حالة تعرضهم للهجمات، مما يعزز الأمان الرقمي الشامل ويقلل من المخاطر المرتبطة بالجهل في هذا المجال.

تتلخص مشكلة البحث في محاولة بناء اداة لقياس مقدار الوعي السيبراني ومتطلبات تحقيقه لدى شباب في الجمهورية العربية السورية، ويمكن تلخيصيها بالتساؤل الرئيسي التالي:

ما مقدار وعي الوعي بالحرب السيبرانية وما هي متطلبات تحقيقه لدى طلاب الجامعة في الجمهورية العربية السورية؟

ويتفرع عنه التساؤلات الفرعية التالية:

1. ما هي مؤشرات الصدق والثبات لمقياس الوعي بالحرب السيبرانية ومتطلبات تحقيقه لدى طلاب الجامعة في الجمهورية العربية السورية؟
2. ما مستوى الوعي بالحرب السيبرانية (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) لدى طلاب الجامعة في الجمهورية العربية السورية؟
3. ما هي جوانب الوعي بالحرب السيبرانية في (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) التي يمتلكها طلاب الجامعة في الجمهورية العربية السورية؟
4. هل يوجد فروق ذات دلالة إحصائية في الوعي بالحرب السيبرانية (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) لدى طلاب الجامعة في الجمهورية العربية السورية تبعاً لمتغير الجنس والمؤهل العلمي؟

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

1- أهمية البحث:

1. توفير مقياس موثوق للوعي بالحرب السيبرانية أداة قياسية لتقييم مستوى المعرفة والفهم لدى طلاب الجامعة عن المخاطر والتحديات المرتبطة بالحرب السيبرانية. هذا المقياس يساعد في تحديد الثغرات في المعرفة، وباستخدام هذا المقياس يمكن للجهات المعنية وضع استراتيجيات فعالة لتعزيز الوعي وتوجيه الموارد بشكل أفضل لمواجهة التحديات المتزايدة في مجال الأمن السيبراني.
2. يعد طلاب الجامعة الفئة الأكثر استخداماً للتكنولوجيا والإنترنت، ومن ثم فمعرفة مستوى وعيهم بالحرب السيبرانية يمكن أن تساعد في تقييم مدى استعدادهم للتعامل مع التهديدات الرقمية، ويعكس فهم مستوى الوعي لدى طلاب الجامعة أيضاً قدرتهم على اتخاذ القرارات الصحيحة بشأن حماية أنفسهم من المخاطر السيبرانية، مما يسهم في بناء مجتمع أكثر أمانًا وتحصينًا ضد الهجمات السيبرانية.
3. يساهم تحديد المتطلبات اللازمة لتحقيق الوعي بالأمن السيبراني في وضع استراتيجيات ملائمة لتعزيز الوعي وتوفير الدعم الضروري من حيث الموارد والأدوات اللازمة لتحقيق الأمن السيبراني.

2- أهداف البحث:

1. التعرف على مؤشرات الصدق والثبات لمقياس الوعي بالحرب السيبرانية ومتطلبات تحقيقه لدى طلاب الجامعة في الجمهورية العربية السورية.
2. الكشف عن مستوى الوعي بالحرب السيبرانية (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) لدى طلاب الجامعة في الجمهورية العربية السورية.
3. معرفة جوانب الوعي بالحرب السيبرانية (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) التي يمتلكها طلاب الجامعة في الجمهورية العربية السورية.
4. الكشف عن الفروق في الوعي بالحرب السيبرانية (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) لدى طلاب الجامعة في الجمهورية العربية السورية تبعاً لمتغير الجنس والمؤهل العلمي.

3- مصطلحات البحث:

الوعي Awareness يُعرّف في علم النفس بأنه حالة من الإدراك الداخلي والخارجي التي تُمكن الشخص من التعامل مع المعلومات المحيطة واتخاذ القرارات استناداً إلى تلك المعلومات. الوعي يشمل الإدراك الحسي والمعرفي والوجداني[3،ص45].

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

وتعرفه الباحثة بأنه: حالة الإدراك التي تتيح للفرد فهم واستيعاب العالم من حوله والتفاعل معه بفعالية. يشمل الوعي الإدراك الحسي للأشياء والمحيط الخارجي، والإدراك الداخلي المتعلق بالأفكار والمشاعر، ويُمكّن الشخص من معالجة المعلومات واتخاذ القرارات بشكل منطقي وواعٍ.

الحرب السيبرانية (Cyber War): قدرة الدولة على استغلال شبكات الاتصالات وأنظمة الكمبيوتر والبنية التحتية الحيوية الأخرى لدولة أخرى بهدف التسبب في تأخير أو تعطيل أو إلحاق الضرر، أي هي شكل من أشكال الصراع الإلكتروني الذي يستخدم لتحقيق أهداف تخريبية عبر الفضاء السيبراني، مثل تعطيل البنى التحتية أو التجسس أو الهجمات التي تستهدف الأنظمة الحيوية [4،ص45].

وتعرفها الباحثة بأنها: شكل من أشكال الصراع الذي يقع عبر الفضاء السيبراني، حيث تستخدم الدول أو الجهات الفاعلة تقنيات الهجوم الإلكتروني لاستهداف شبكات الاتصالات وأنظمة الكمبيوتر والبنية التحتية الحيوية لدولة أو جهة أخرى بهدف إحداث أضرار أو تعطيل أو تحقيق أهداف تخريبية. تشمل الحرب السيبرانية أنشطة مثل التجسس الإلكتروني، تعطيل الخدمات، سرقة البيانات، والهجمات على الأنظمة الحيوية والمؤسسات.

4- حدود البحث: تشمل حدود البحث:

- **الحدود الموضوعية:** يشمل البحث الوعي بالحرب السيبرانية وأبعادها (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) في مدينة حلب.
- **الحدود الزمانية:** طبقت أداة البحث في النصف الثاني من عام 2024.
- **الحدود المكانية:** مدينة حلب.
- **الحدود البشرية:** طلاب الجامعة في مدينة حلب.

5-الإطار النظري والدراسات السابقة:

5-1-الإطار النظري:

أولاً: الوعي: يُعتبر من المفاهيم المعقدة التي تختلف تفسيراتها باختلاف النظريات النفسية، فوفقًا لنظرية التحليل النفسي لفرويد، يُعد الوعي الطبقة الخارجية التي تتضمن الأفكار والمشاعر التي يكون الفرد مدركًا لها، في حين توجد طبقات أعمق من اللاوعي التي تؤثر على السلوك بشكل غير مباشر [5،ص159-212] إما وفقًا لنظرية الإدراك المعرفي يُنظر إلى الوعي على أنه نتيجة للعمليات العقلية التي تسمح بدمج المعلومات الحسية والمعرفية لتشكيل تجربة ذاتية واعية[6] في المقابل، تركز نظرية الوعي الاجتماعي على أن الوعي يتشكل بالتفاعلات مع البيئة الاجتماعية، إذ إن الإدراك الذاتي يتأثر بشكل كبير بالتفاعل مع الآخرين[7]. وركزت نظرية الوعي الهرمي التي اقترحها إيدلمان وتونوني [8] على فكرة أن الوعي ينبع من النشاط الديناميكي في الدماغ الذي يدمج المعلومات من مناطق مختلفة بشكل متزامن لإنتاج تجربة موحدة وشاملة. هذه النظرية تدعم أن الوعي ليس فقط

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

نتيجة للمحفزات الخارجية، ولكن هو أيضاً نتاج تفاعلات معقدة بين الشبكات العصبية التي تتكامل لتحقيق الإدراك الواعي.

مفهوم السيبرانية والأمن السيبراني Cyber And Cybersecurity:

تطلق كلمة cyber على أي شي مرتبط بثقافة الحواسيب وتقنية المعلومات والواقع الافتراضي فالسيبرانية تعني (فضاء الإنترنت)، وقد قدمت وزارة الدفاع الأميركية تعريفاً دقيقاً لهذا المصطلح الأمن السيبراني بأنه: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها الإلكترونية والمادة ومختلف الجرائم والهجمات والمحاولات التخريبية والتجسس والحوادث الخاصة بالمعلومات"، وعرفه بوسي وساديرا [9،ص82] بأنه الإجراءات التقنية الهادفة إلى حماية البيانات والمعلومات والمعدات التقنية من أي شكل من أشكال الوصول غير السموح به.

وعرفه كرومبتون وآخرون [1،ص3] بأنه: حماية المعلومات وانظمة المعلومات من أي شكل من أشكال الاتلاف أو التلاعب أو إساءة الاستخدام أو الوصول غير المسموح به، وعرفها خليفة [10،ص137] بأنه: جميع الأدوات والسياسات ومفاهيم الأمن والضمانات الأمنية والمبادئ التوجيهية ومداخل إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والتقنيات التي يمكن استخدامها بهدف حماية الفضاء السيبراني. وعرفت الهيئة الوطنية السعودية[11،ص26] بأنه: "حماية الشبكات وأنظمة تقنيات المعلومات وانظمة التقنيات التشغيلية ومكونات من أجهزة وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع"

وتعرفه الباحثة بأنه: مجموعة من الإجراءات والتقنيات والسياسات التي تهدف إلى حماية المعلومات والأنظمة التقنية من أي تهديدات إلكترونية أو هجمات، ويشمل حماية البيانات والشبكات والأجهزة من الاختراق، التعطيل التعديل أو الوصول غير المصرح به. يتضمن الأمن السيبراني أيضاً أدوات وممارسات إدارة المخاطر والإجراءات الأمنية التي تهدف إلى ضمان سلامة وأمان الفضاء السيبراني والمعلومات التي يحتويها.

لا بد من الإشارة للفرق بين الأمن السيبراني وأمن المعلومات بكون الأمن السيبراني أوسع من أمن المعلومات حيث يشمل الأمن السيبراني حماية وتأمين البيانات والمعلومات التي تتداول بمختلف الشبكات التي تخزن في خوادم لحمايتها من الاختراقات والوصول غير المشروع، بمجموعة من الوسائل التقنية التي تستخدم لحظر الاستخدام غير المصرح، أما بالنسبة لأمن المعلومات فهو يخص بتأمين المعلومات المتداولة عبر شبكة الإنترنت عن طريق وسائل اكتشاف ورصد التهديدات وحماية المعلومات [12].

هناك عدة أنواع من **الهجمات السيبرانية** التي تستهدف الأنظمة والشبكات الرقمية، وهي تشمل:

1. **هجمات التصيد الاحتيالي(Phishing Attacks)** تُستخدم رسائل البريد الإلكتروني أو مواقع الويب المزيفة لخداع المستخدمين للكشف عن معلومات حساسة مثل كلمات المرور أو البيانات المالية، تعرضت شركتا جوجل وفيسبوك **(2013–2015)** لعملية احتيال كبيرة، حيث خُدع موظفوهما برسائل بريد إلكتروني مزيفة، مما أدى إلى سرقة حوالي 100 مليون دولار.

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

2. **هجمات البرمجيات الخبيثة (Malware)** تشمل الفيروسات وبرامج الفدية (Ransomware) وأحصنة طروادة (Trojans) والديدان(Worms) التي تتسبب في تلف أو سرقة البيانات أو التحكم في الأنظمة، ومن أمثلتها **هجوم واناكراي wannacryعام 2017** استغل ثغرة في نظام التشغيل ويندوز، مما أدى إلى إصابة أكثر من 230,000 جهاز في أكثر من 150 دولة، وطالب المهاجمون بفدية مالية لفك تشفير الملفات.
3. **هجمات الحرمان من الخدمة (Denial of Service – DoS / Distributed Denial of Service – DDoS):** تهدف إلى إغراق الخوادم أو الشبكات بحجم ضخم من الطلبات مما يؤدي إلى تعطيل الخدمات أو جعلها غير متاحة للمستخدمين، مثل **هجوم دين دانس Dyn DNS (2016)** حيث كات احد أكبر الهجمات DDoS التي أدت إلى تعطيل العديد من المواقع الشهيرة مثل تويتر، نيتفليكس، وباي بال، بمهاجمة مزود DNS باستخدام شبكة من الأجهزة المصابة بالبرمجيات الخبيثة.
4. **هجمات حقن(SQL Injection) SQL** تستغل ثغرات في قواعد البيانات بإدخال تعليمات برمجية ضارة عبر إدخال بيانات غير آمنة إلى قاعدة بيانات، مما يمكن المهاجم من سرقة أو تعديل البيانات، مثل اختراق موقع لينكد **LinkedIn** عام **(2012) فقد** سرقة بيانات ملايين الحسابات بسبب ثغرة فيSQL ، مما أدى إلى تسريب معلومات حساسة عن المستخدمين.
5. **الهجمات بالبرامج غير المصححة (Unpatched Software):** تعتمد هذه الهجمات على استغلال الثغرات الأمنية في البرامج أو الأنظمة التي لم يتم تحديثها بعد، مما يسمح للمهاجمين بالوصول غير المصرح به.
6. **هجمات الرجل في المنتصف(Man-in-the-Middle-MITM)** يحدث هذا النوع من الهجمات عندما يعترض المهاجم الاتصالات بين طرفين، مما يمكنه من الوصول إلى المعلومات السرية أو التلاعب بها دون علم الأطراف المتواصلة، مثل **هجمات Wi-Fi العامة عام (2015)** استخدمت شبكات Wi-Fi العامة غير الأمنة في العديد من الأماكن حول العالم لشن هجمات MITM على المستخدمين وسرقة معلوماتهم الشخصية مثل بيانات الحسابات البنكية.
7. **الهجمات على سلسلة التوريد(Supply Chain Attacks)** تستهدف هذه الهجمات الجهات الضعيفة في سلسلة التوريد الخاصة بالشركات للوصول إلى الأنظمة الرئيسية بمكونات خارجية أو شركاء موثوقين، مثل هجوم سولرويند **SolarWinds عام (2020) ب**اختراق أنظمة **SolarWinds**، وهي شركة تقدم برامج مراقبة للشبكات، مما أدى إلى تمكين المهاجمين من الوصول إلى بيانات حساسة لعدة وكالات حكومية وشركات في الولايات المتحدة.
8. **الهندسة الاجتماعية(Social Engineering)** تعتمد على التلاعب بالبشر لخداعهم في كشف معلومات حساسة، وغالبًا ما يحصل عبر الهاتف أو البريد الإلكتروني أو وسائل التواصل الاجتماعي، مثل ال**هجوم على شركة توتر twitter عام (2020) إذ** استغل المهاجمون مهاراتهم في الهندسة الاجتماعية للحصول على صلاحيات موظفي تويتر، مما مكنهم من الوصول إلى حسابات مؤثرة والاحتيال على المستخدمين بطلب تبرعات بالعملات المشفرة.

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

9. **هجمات برامج الفدية (Ransomware)** يحصل فيها تشفير البيانات أو الأنظمة ويطالب المهاجم بفدية مالية مقابل فك التشفير واستعادة البيانات، مثل **هجوم على مدينة أتلانتا عام (2018)** كان هذا الهجوم ببرنامج فدية أدى إلى شلل أنظمة الحكومة المحلية في مدينة أتلانتا، إذ طالب المهاجمون بفدية قيمتها 51,000 دولار مقابل فك التشفير.
10. **الهجمات الصفرية(Zero-Day Attacks)** تُستغل الثغرات الأمنية التي لم يتم اكتشافها بعد من المطورين أو المستخدمين، وتعد من أخطر الأنواع بسبب عدم وجود حماية فورية لها، **هجوم ستكنس stuxnetعام (2010)** استهدف البرنامج الخبيث المنشآت النووية الإيرانية عبر ثغرات صفرية في أنظمة التحكم الصناعية، مما أدى إلى إبطاء برنامجهم النووي بشكل كبير.

هذه الأنواع من الهجمات السيبرانية تتطلب استراتيجيات متعددة ومتطورة للدفاع والتصدي لها، بما في ذلك تحديث البرامج بانتظام، وتطبيق ممارسات أمان قوية مثل تشفير البيانات وتوعية المستخدمين.

أهمية الوعي بالحرب السيبرانية:

يشكل الوعي بالحرب السيبرانية ضرورة ملحة خاصة للشباب الذين يمثلون شريحة كبيرة من مستخدمي الإنترنت، وبالاطلاع على الدراسات التي يتناولت الأمن السيبراني كدراسة العيتبي (2022)[13،ص575-613] والشريف وآخرون(2023)[14]،ص97-140] والرحمنة(2023)[15،ص77-92] وشمس الدين وآخرون (2023)[16]،ص592-619] والمطيري(2023)[17،ص2456-2406] وفاضل وآخرون(Fazil, Et Al, 2023)[2] ودراسة الطاهر وأحمد(2023)[18،ص171-183] لخصت الباحثة أبرز النقاط التي توضح أهمية الوعي بالحرب السيبرانية:

1. **حماية المعلومات الشخصية والمجتمعية:** تعد المعلومات الشخصية والبيانات المجتمعية هدفًا رئيسيًا للهجمات السيبرانية. الوعي بالحرب السيبرانية يساعد الأفراد على التعرف على الأساليب التي تُستخدم لسرقة المعلومات أو التلاعب بها، مثل الهجمات الخبيثة والاحتيال الإلكتروني، مما يعزز من قدرتهم على حماية بياناتهم.
2. **مواجهة التهديدات السيبرانية المتزايدة:** أصبحت الهجمات على البنية التحتية الوطنية والمؤسسات الحكومية تهديداً حقيقياً للأمن القومي، الوعي بهذه التهديدات يساعد في تعزيز قدرة الأفراد والمؤسسات على التصدي لهذه الهجمات والتخفيف من تأثيرها.
3. **تعزيز السلامة الرقمية:** بتعليمهم كيفية استخدام الإنترنت بشكل آمن، وتحذيرهم من مخاطر الاختراقات، الفيروسات، وهجمات التصيد الاحتيالي، هذا الوعي يخلق بيئة إلكترونية أكثر أمانًا على المستوى الفردي والمجتمعي.

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

4. **الاستجابة الفعالة للهجمات:** الوعي المتزايد بالحرب السيبرانية يساهم في تحسين استجابة الأفراد والمؤسسات للهجمات السيبرانية. عندما يكون الناس على دراية بالتهديدات السيبرانية وكيفية التعامل معها، يكونون أكثر استعداداً لاتخاذ التدابير المناسبة لحماية أنفسهم وأجهزتهم.
5. **تعزيز الوعي الوطني والسيادة الرقمية:** يعزز فهم طلاب الجامعة لأهمية الحرب السيبرانية وأبعادها السياسية والاقتصادية الشعور بالمسؤولية الوطنية والسيادة الرقمية، ويساهم في الحفاظ على الأمن القومي ويعزز دور المواطن في حماية دولته من الهجمات السيبرانية المحتملة
6. **تعليم وتدريب الجيل القادم:** مع تزايد الاعتماد على التكنولوجيا في الحياة اليومية والتعليم والعمل، يجب على طلاب الجامعة أن يكونوا مدركين لأهمية الأمن السيبراني. الوعي بالحرب السيبرانية يشكل جزءاً من إعداد الجيل القادم ليكون قادراً على التكيف مع التطورات التكنولوجية والتصدي للتحديات الأمنية المصاحبة لها.
7. **منع انتشار المعلومات المضللة:** يمكن أن تستغل الهجمات الإلكترونية لنشر معلومات مضللة أو الدعاية الخبيثة. الوعي بهذه الأساليب يعزز قدرة الأفراد على التمييز بين الأخبار الصحيحة والمضللة، مما يسهم في الحفاظ على الاستقرار المجتمعي.

الوعي بالحرب السيبرانية لم يعد خياراً، بل ضرورة ملحة لضمان الأمن الفردي والجماعي في العصر الرقمي، يساعد هذا الوعي على تعزيز الحماية من التهديدات السيبرانية وتطوير استراتيجيات وطنية ودولية لمواجهة هذه التهديدات المتزايدة، مما يساهم في بناء مجتمع رقمي أكثر أماناً واستقراراً.

5-2- الدراسات السابقة:

دراسة العتيبي (2022) [13] بعنوان مدى توافر الوعي بالأمن السيبراني لدى أفراد الأسر في المجتمع السعودي (دراسة استطلاعية على عينة من الأسر بمحافظة جدة).

هدفت الدراسة إلى التعرف على درجة الوعي بماهية الأمن السيبراني لدى عينة من الأسر بمحافظة جدة، وتحديد اهم اشكال الجرائم ومخاطر الجرائم التي يتعامل معها الأمن السيبراني ولها علاقة بالمجتمع السعودي، بالأضافة لتحديد المعوقات الاجتماعية لتحقيق الوقاية من جرائم الفضاء السيبراني، اعتمد الباحث على المنهج المسحي حيث تكونت عينة الدراسة من (681) أسرة سعودية في جدة، واعتمدت الاستبانة أداة رئيسة لجمع البيانات. أظهرت النتائج أن الوعي بماهية الأمن السيبراني لدى عينة من الأسر بمحافظة جدة كان بدرجة مرتفعة وتمثلت أبراز جوانب الوعي في تجنب الكشف عن البيانات الشخصية والعائبية أثناء تصفح الانترنت، كما انهم على دراية كبيرة بمخاطر الفيروسات على الاجهزة الذكية والجرائم التي تقع ضمن مجال الأمن السيبراني، كما تمثلت ابرز الجرائم في الابتزاز المالي والجنسي عبر الانترنت والاحتيال والنصب الإلكتروني، أهم مخاطر الجرائم السيبرانية.

دراسة الشريف وآخرون (2023) [14] بعنوان فعالية برنامج تدريبي مقترح لتنمية الوعي السيبراني لدى طالبات كلية الآداب والعلوم الانسانية: دراسة تجريبية.

هدفت الدراسة إلى التعرف على فعالية برنامج تدريبي مقترح لتنمية الوعي بالأمن السيبراني لدى طلبات كلية الآداب والعلوم الانسانية في جامعة طيبة، وعلى معرفة درجة وعيهم بالأمن السيبراني وتحليل وقياس فعالية

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

البرنامج التدريبي المقترح، ولتحقيق أهداف الدراسة أُعدَ برنامج تدريبي لتنمية وعيهم وإعداد استبانة مكونة من (34) سؤالا وتضم محورين هما: (الوعي بمفهوم الأمن السيبراني، والوقاية من مخاطر الاختراق السيبراني)، وتطبيقها على عينة عشوائية بلغت (192) استمارة قبلية و(189) استمارة بعدية على طالبات كلية الآداب والعلوم الانسانية بجامعة طيبة، وأظهرت النتائج أن الغالبية العظمى للطالبات لم يكنّ على دراية ومعرفة سابقة في الأمن السيبراني إذ بلغت نسبة الطالبات ذوي المعرفة (38%) قبل تطبيق البرنامج و(84.8%) بعد تقديم البرنامج، وتوصلت الدراسة إلى الاحتياج للدورات التدريبية في مجال الأمن السيبراني.

دراسة الرحمنة (2023) [15] بعنوان: متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية.

هدفت الدراسة إلى التعرف على متطلبات تحقيق الأمن السيبراني في البنوك الأسلامية الأردنية، ولتحقيق أهداف الدراسة تم تطبيق استبانة لمعرفة المتطلبات مكونة من (24) فقرة) تشمل أربع أبعاد (المتطلبات الإدارية، المتطلبات المالية، المتطلبات البشرية، المتطلبات التقنية) وتطبيقها على عينة من(35) موظفا في البنوك الأسلامية الأردنية، أظهرت النتائج أن متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية كانت بدرجة كبيرة، ولا توجد فروق ذات دلالة إحصائية في المتطلبات بجميع أبعادها تبعاً لمتغير الجنس أو المسمى الوظيفي.

دراسة شمس الدين وآخرون(2023)[16] بعنوان: برنامج إرشادي قائم على توظيف التعلم الذكي وأثره على تنمية بالوعي بالأمن السيبراني وخفض مستوى النوموفوبيا لدى طلاب كلية الإقتصاد المنزلي جامعة المنوفية.

هدفت الدراسة إلى الكشف عن أثر برنامج أرشادي مقترح قائم على توظيف التعلم الذكي في تنمية الوعي بالأمن السيبراني وخفض مستوى النوموفوبيا لدى طلاب كلية الأقتصاد المنزلي في جامعة المنوفية، باختيار عينة قصدية ممن أظهروا مستويات مرتفعة في النوموفوبيا بلغ عددها(90) طالباً وطالبة وتقسيمهم إلى مجموعتين متساويتين: إحداهما مجموعة تجريبية وأخرى ضابطة، وأظهرت النتائج وجود فروق ذات دلالة إحصائية بين القياسين القبلي والبعدي للمجموعة التجريبية في مستوى الوعي بالأمن السيبراني والنوموفوبيا، ووجود فروق ذات دلالة إحصائية بين المجموعة التجريبية والضابطة في القياس البعدي في الأمن السيبراني والنوموفوبيا، ووجود علاقة عكسية بين مستوى الوعي بالأمن السيبراني ومستوى النوموفوبيا، ووجود فروق ذات دلالة إحصائية مستوى النوموفوبيا تبعاً لمتغير طبيعة السكن والتقدير الدراسي وموديل الهاتف، بينما لا توجد فروق ذات دلالة إحصائية في الوعي السيبراني تبعاً لمتغير النوع ومحل الإقامة.

دراسة المطيري(2023)[17] بعنوان: دور مدير المدرسة في تعزيز الزعي بالأمن السيبراني لدى طلاب المدارس الثانوية الحكومية بمحافظة حفر الباطن.

هدفت الدراسة لمعرفة الأسس المفاهيمية للإدارة المدرسية في ضوء أدبيات الفكر الإداري المعاصر، والتعرف على الفلسفة التربوية لتعزيز الوعي السيبراني، وتشخيص واقع أثر المدير في تعزيز الأمن السيبراني والوصول لمقترحات لتفعيل أثر مدير المدرسة، ولتحقيق أهداف الدراسة استخدم المنهج المسحي بتطبيق استبانة مكونة من (80) فقرة موزعة على ست أبعاد وهي (البعد التقني، البعد التنظيمي، البعد التعليمي، البعد الاجتماعي، البعد الديني، البعد النفسي) وتطبيقها على عينة من مدراء المداري البالغ عددهم (150) مديرا من مدراء المدارس الثانوية الحكومية بمحافظة حفر الباطن، أظهرت النتائج أن أثر مدير المدرسة في تعزيز الزعي بالأمن السيبراني

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

بالمدارس الثانوية كان مرتفعاً وتدرج كما يلي: (البعد الديني تلاه البعد التعليمي ومن ثم البعد النفسي والبعد التقني في المرتبة السادسة)، وأظهرت أيضا عدم وجود فروق ذات دلالة إحصائية في أثر مدير المدرسة في تعزيز الوعي بالأمن السيبراني وتعزى أبعاده بالمدارس الثانوية إلى نوعية المدرسة (بنين، أو بنات).

دراسة فاضل وآخرين(Fazil, et al, 2023)[2] بعنوان: تعزيز سلامة الإنترنت والوعي بالأمن السيبراني بين طلاب المرحلة الثانوية في أفغانستان: دراسة حالة من محافظة بدخشان.

Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province

هدفت هذه الدراسة إلى تحليل تأثير تعليم الأمن السيبراني على المعرفة الرقمية وسلامة الإنترنت لدى الطلاب، مع التركيز على الشباب في محافظة بدخشان، أفغانستان. سعت إلى تعزيز مبادئ المعرفة الرقمية وسلامة الإنترنت عبر مختلف الفئات العمرية والمجالات الدراسية، مع تسليط الضوء على أهمية التوعية بالممارسات الرقمية المسؤولة، مثل الخصوصية والأمان وحقوق الملكية الفكرية، ودعت أيضاً إلى تفعيل أثر الأهل في دعم هذه الجهود. ولتحقيق أهداف الدراسة سحبت عينة عشوائية طبقية مكونة من 170 طالباً وطالبة من مراحل دراسية مختلفة في المدارس الحكومية والخاصة في محافظة بدخشان، أفغانستان. تم جمع البيانات باستخدام استبيان شامل مكون من (16) فقرة. أظهرت النتائج رؤى قيمة حول سلوكيات الشباب في بدخشان على الإنترنت ومستوى وعيهم بالأمن السيبراني. كشفت النتائج عن أهمية إدماج تعليم الأمن السيبراني في المناهج الدراسية لتمكين الطلاب من التنقل بأمان في العالم الرقمي. وأكدت على ضرورة تعزيز الوعي بأهمية الخصوصية والأمان والإفادة الكاملة من الإنترنت بطريقة مسؤولة. تسهم هذه النتائج في بناء مجتمع أكثر أماناً ومسؤولية وقائم على المعرفة.

دراسة الطاهر وأحمد (2023) [18] بعنوان: الوعي بالأمن السيبراني في مؤسسات التعليم العالي الإفريقية: دراسة حالة من السودان

Cybersecurity awareness in African higher education institutions: A case study of Sudan

هدفت هذه الدراسة إلى استكشاف مستويات الوعي بالأمن السيبراني بين طلاب البكالوريوس في مؤسسات التعليم العالي الأفريقية، مع التركيز على حالة السودان، وذلك في سياق التحول السريع إلى التعليم عبر الإنترنت بسبب أزمة فيروس كورونا (COVID-19). اعتمدت الدراسة على إجراء استبيان طبّق على عينة قصدية تضم 1200طالب بكالوريوس من ست جامعات حكومية في السودان. استخدمت الدراسة أدوات استبانة أداة لجمع البيانات عن مستوى وعي الطلاب بالأمن السيبراني. أظهرت النتائج أن معظم طلاب البكالوريوس في مؤسسات التعليم العالي بالسودان يمتلكون مستويات وعي منخفضة بالأمن السيبراني. وكشفت التحقيقات الإضافية باستخدام الإحصاءات الاستنتاجية أن الطلاب الذكور لديهم مستويات وعي بالأمن السيبراني أعلى قليلاً من الطالبات. وأبدى معظم المشاركين اعتقادهم بضرورة تعليم الأمن السيبراني في المدارس ورغبتهم في تعلم المزيد عنه. ووجدت النتائج أيضًا أن الطلاب الذين يمتلكون مهارات حاسوبية متقدمة يختلفون بشكل ملحوظ عن الطلاب ذوي المهارات المتوسطة أو الأساسية في ممارسة الأمن السيبراني.

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

التعقيب عن الدراسات السابقة:

تتفق الدراسات جميعها على أهمية تعزيز الوعي بالأمن السيبراني وسيلة لحماية الأفراد والمجتمعات من المخاطر المرتبطة بالجرائم الإلكترونية. على سبيل المثال، أكدت دراسة العتيبي (2022) أن الأسر في جدة لديها وعي مرتفع بما يتعلق بالأمن السيبراني، في حين أظهرت دراسة الطاهر وأحمد (2023) أن الوعي بالأمن السيبراني منخفض بين طلاب البكالوريوس في السودان، مما يشير إلى الحاجة المستمرة للتوعية. تبرز العديد من الدراسات أهمية البرامج التعليمية والتدريبية في رفع مستوى الوعي. دراسة الشريف وآخرون (2023) تدعو إلى فعالية البرامج التدريبية لتنمية الوعي، بينما تشير دراسة فاضل وآخرين (2023) إلى ضرورة إدماج تعليم الأمن السيبراني في المناهج الدراسية، ولاحظت عدة دراسات، مثل دراسة الطاهر وأحمد (2023) ودراسة الشريف وآخرين (2023)، وجود اختلافات بين الذكور والإناث في مستوى الوعي بالأمن السيبراني، مما يستدعي تخصيص جهود تعليمية مختلفة لكل جنس.

تقوم الدراسة الحالية بأكمال وتعزيز الفهم الموجود في الأبحاث الحالية عن الأمن السيبراني بالتركيز على جوانب محددة مثل الحرب السيبرانية ومتطلبات تحقيق الوعي، مما يجعلها ذات قيمة مضافة في هذا المجال.

6-الدراسة الميدانية:

6-1- **منهج البحث:** اعتمدت الباحثة المنهج الوصفي التحليلي لملاءمته لأهداف البحث وقدرته على الاجابة على تساؤلات البحث من الخصائص السيكومترية للمقياس بالتأكد من صدق وثبات المقياس، ومعرفة مستوى الوعي بالحرب السيبرانية ودلالة الفروق وفقاً للمتغيرات الديموغرافية.

6-2- مجتمع البحث: تضمن مجتمع البحث جميع طلاب الجامعة المقيمين في مدينة حلب.

6-3- عينة البحث: تكونت الدراسة من(176) طالبا من طلاب جامعة حلب، وموزعه وفقاً المتغيرات الديموغرافية الجنس والمؤهل العلمي والتخصص:

الجدول(1). توزع أفراد العينة وفق المتغيرات الديموغرافية

الجنس	العدد	النسبة	التخصص	العدد	النسبة
ذكر	96	%54.55	نظرية	112	%63.64
أنثى	80	%45.45	تطبيقية	64	36.36
الكلي	176	%100	الكلي	176	%100

6-4- أدوات البحث: بعد الأطلاع الباحثة على الدراسات السابقة والدراسات المتعلقة بالوعي بالسيبرانية والوعي بالأمن السيبرانية والحرب السيبرانية، قامت الباحثة بتحديد محاور الأمن بالحرب السيبرانية، فكانت الفقرات من نوع التقرير الذاتي وليكرت خماسي: (أوافق بشدة، أوافق، محايد، غير موافق، غير موافق بشدة) ومصاغة بشكل أيجابي وفقاً للأبعاد التالية

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

1. المعرفة بالمخاطر السيبرانية: يركز على الوعي العملي (مثل القدرة على التعرف على التهديدات) والمعرفة النظرية أو الشعور الشخصي بالكفاءة، وكانت عدد فقراته (10 فقرات).
2. استراتيجيات الحماية الشخصية: تشمل الإجراءات الأساسية والممارسات العملية التي يتبعها الأفراد لحماية بياناتهم وأجهزتهم، تركز على الوعي الشخصي والإجراءات الفعالة مثل استخدام كلمات المرور القوية والمصادقة الثنائية، بالأضافة لتطرق للإجراءات الوقائية مثل النسخ الاحتياطية وتحديث البرامج. وكانت عدد فقراته (7 فقرات).
3. **فهم مسؤوليات الأمان:** تتناول الجوانب الأخلاقية القانونية والشخصية المتعلقة بالأمان السيبراني، بالأضافة إلى الشعور بالمسؤولية الشخصية وحماية المعلومات، والإدراك بأهمية السياسات العامة للأمان السيبراني، مما يعكس نظرة شاملة لفهم مسؤوليات الأمان وكانت عدد فقراته (6 فقرات).
4. **المعرفة بالأدوات والتقنيات الأمنية:** وتشمل جوانب الوعي بالأدوات الأمنية وتطبيقها العملي والاحتياج للتدريب والمتابعة المستمرة للتطورات. تعكس فهماً شاملاً للتقنيات والأدوات الأمنية وأثرها في تعزيز الحماية السيبرانية وكانت عدد فقراته (7 فقرات).
5. **الاستجابة للطوارئ السيبرانية:** تتناول الوعي الشخصي والاستعدادات العملية والتدريب وتبادل المعلومات، وهي نقاط أساسية لتقييم مدى كفاءة الفرد في التعامل مع الطوارئ السيبرانية وكانت عدد فقراته (7 فقرات).
6. **التأثيرات النفسية والاجتماعية للحرب السيبرانية:** تركز على مشاعر القلق والتوتر والتأثير على الثقة بالمؤسسات والعلاقات الاجتماعية، وتعكس أهمية المناقشات المجتمعية في الأمن السيبراني وكانت عدد فقراته (6 فقرات).

6-5- إجراءات البحث:

1. الاطلاع على الأدبيات والدراسات السابقة التي تشمل السيبرانية والأمن السيبراني والوعي بالأمن السيبراني والأمن الرقمي.
2. إعداد أداة البحث والتأكد من الخصائص السيكومترية (الصدق والثبات) للمقياس.
3. تطبيق المقياس على عينة البحث والاجابة عن أسئلة البحث.
4. تقديم التوصيات والمقترحات الملائمة لنتائج البحث.

6-7- الأساليب الإحصائية: قامت الباحثة باستخدام الأساليب الإحصائية التالية:

1. المتوسط الحسابي والانحراف المعياري والنسبة المئوية (لحساب الوزن النسبي والوزن النسبي المئوي).
2. معامل الارتباط بيرسون (للتأكد من الاتساق الداخلي للفقرات).
3. معامل ثبات ألفا كرونباخ، معامل ثبات التجزئة النصفية (للتأكد من ثبات المقياس).
4. اختبار ت للعينة الواحدة (لاختبار دلالة الفروق بين متوسط العينة والمتوسط الفرضي) واختبار ت للعينة المستقلة (لاختبار دلالة الفروق في الوعي بالحرب السيبرانية وفقاً للمتغيرات الديموغرافية).

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

5- الإجابة عن تساؤلات البحث:

التساؤل الأول: ما هي مؤشرات الصدق والثبات لمقياس الوعي بالحرب السيبرانية ومتطلبات تحقيقه لدى طلاب الجامعة في الجمهورية العربية السورية؟

تطبيق مقياس الوعي بالحرب السيبرانية على عينة استطلاعية مكونة من (50) راشد بغية التحقق من الخصائص السيكومترية (الصدق والثبات)، وأظهرت النتائج:

أولاً: صدق مقياس الوعي بالحرب السيبرانية:

أ. **صدق المحكمين:** قامت الباحثة بعرض مقياس الوعي بالحرب السيبرانية على عشر محكمين مختصين في المجال النفسي والتربوي في جامعة حلب ودمشق، للتأكد من سلامة صياغتها اللغوية ووضح عبارتها ومناسبتها للعينة المدروسة وتعديل بعض فقرات المقياس، وكانت نسبة أتفاق المحكمين على فقرات المقياس أعلى من (80%) على ملاءمة فقرات الاستبانة لما وضع لأجلها الذي يعد مؤشرا لتحقق صدق المحكمين.

ب. **صدق الاتساق الداخلي:** للتأكد من صدق الاتساق الداخلي قامت الباحثة بحساب معامل الارتباط بيرسون person correlated لكل فقرة من فقرات مقياس الوعي بالحرب السيبرانية وأبعادها: (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) ببعدها وبالدرجة الكلية لمقياس الوعي بالأمن السيبرانية، وباستخدام برنامج SPSS، كما موضح بالجدول التالي:

الجدول(2). صدق الاتساق الداخلي لمقياس الوعي بالحرب السيبرانية

الفقرة	ببعده	الدرجة الكلية	الفقرة	ببعده	الدرجة الكلية	الفقرة	ببعده	الدرجة الكلية
1	**0.500	**0.548	16	**0.502	**0.598	31	**0.501	**0.540
2	**0.518	**0.587	17	**0.554	**0.548	32	**0.555	**0.529
3	**0.535	**0.544	18	**0.519	**0.510	33	**0.552	**0.582
4	**0.525	**0.508	19	**0.521	**0.540	34	**0.529	**0.584
5	**0.529	**0.504	20	**0.583	**0.595	35	**0.549	**0.506
6	**0.594	**0.560	21	**0.563	**0.578	36	**0.514	**0.524
7	0.600	**0.560	22	**0.596	**0.546	37	**0.512	**0.584
8	**0.502	**0.536	23	**0.564	**0.519	38	**0.558	**0.537
9	**0.506	**0.544	24	**0.551	**0.592	39	0.600	**0.592
10	**0.521	**0.532	25	**0.564	**0.581	40	**0.530	**0.517
11	**0.593	**0.522	26	**0.504	**0.501	41	**0.587	**0.516
12	**0.598	**0.561	27	**0.573	**0.550	42	**0.511	**0.528
13	**0.581	**0.506	28	**0.520	**0.525	43	**0.526	**0.574
14	**0.557	**0.545	29	**0.527	**0.515	----	----	----
15	**0.506	**0.551	30	**0.590	**0.579	----	----	----

**دال عند مستوى دلالة (0.01) القيمة الحرجة لمعامل الارتباط بيرسون (0.354) عند مستوى دلالة (0.01) ودرجة حرية (50)

نلاحظ من الجدول السابق أن قيم معاملات الارتباط بين الفقرة والبعد وقيم معاملات الارتباط بين الفقرة والدرجة الكلية للمقياس موجبة وذات دلالة إحصائية، وهو مؤشر على الاتساق الداخلي.

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

ثبات المقياس: التأكد من ثبات الاستبانة عبر معامل ألفا كرونباخ والتجزئة النصفية لمقياس الوعي بالحرب السيبرانية وأبعاده (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية)، باستخدام برنامج SPSS كما موضح في الجدول التالي:

الجدول (3). معامل ثبات مقياس الوعي بالحرب السيبرانية وأبعادها

البعد	معامل الثبات	الفا كرونباخ	الإعادة
1	المعرفة بالمخاطر السيبرانية	0.835	0.832
2	استراتيجيات الحماية الشخصية	0.825	0.827
3	فهم مسؤوليات الأمان	0.811	0.875
4	المعرفة بالأدوات والتقنيات الأمنية	0.801	0.834
5	الاستجابة للطوارئ السيبرانية	0.897	0.876
6	التأثيرات النفسية والاجتماعية	0.893	0.818
	الدرجة الكلية	0.851	0.821

نلاحظ من الجدول السابق أن قيم معاملات الثبات ألفا كرونباخ والإعادة جيدة جداً وهي مؤشرات على امتلاك المقياس للثبات.

التساؤل الثاني: ما مستوى الوعي بالحرب السيبرانية (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) لدى طلاب الجامعة في الجمهورية العربية السورية؟

قامت الباحثة للإجابة عن هذا التساؤل بحساب المتوسط الحسابي لمقياس الوعي بالحرب السيبرانية والانحرافات المعيارية ومقارنته مع المتوسط الفرضي البالغ، ومن كون مؤشرات الاعتدالية محققة في الدرجة الكلية للوعي بالأمن السيراني وأبعاده باستخدام اختبار ت للعينة الواحدة one sample t test، لاختبار هذه الفرضية لملاءمته، باستخدام برنامج SPSS، كما موضح في الجدول التالي:

الجدول(4). دلالة الفروق في الوعي بالحرب السيبرانية وأبعادها والمتوسط الفرضي

البعد	العدد	المتوسط الحسابي	الانحراف المعياري	المتوسط النظري	قيمة ت	درجة الحرية	قيمة الدلالة	القرار	النسبة المئوية
1	176	36.681	7.482	30	11.866	175	0.000	دال	%73.36
2	176	28.136	4.488	21	21.095	175	0.000	دال	%80.39
3	176	26.909	2.835	18	41.690	175	0.000	دال	%89.70
4	176	27.591	4.175	21	20.943	175	0.000	دال	%78.83
5	176	26.864	4.478	21	17.373	175	0.000	دال	%76.75
6	176	24.364	3.106	18	27.177	175	0.000	دال	%81.21
الكلي	176	170.546	21.342	129	25.826	175	0.000	دال	%79.32

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

نلاحظ من الجدول السابق أن قيمة ت المحسوبة أكبر من قيمة ت الجدولية (1.96) عند مستوى دلالة (0.05) ودرجة حرية (175) ومن ثم يوجد فروق ذات دلالة إحصائية في متوسط الوعي بالحرب السيبرانية وأبعاده المعرفة بالمخاطر السيبرانية واستراتيجيات الحماية الشخصية وفهم مسؤوليات الأمان والمعرفة بالأدوات والتقنيات الأمنية والاستجابة للطوارئ السيبرانية والتأثيرات النفسية والاجتماعية ولصالح متوسط العينة، أي إن مستوى الوعي بالحرب السيبرانية وأبعاده كان أعلى من المتوسط بنسبة أكبر من (70%) فقد احتلت فهم مسؤوليات الأمن بنسبة (89.39%) أعلى نسبة وعي تلتها التأثيرات النفسية والاجتماعية بنسبة (81.21%) وكان بُعد المعرفة بالمخاطر السيبرانية أقل بُعد بنسبة تحقق (73.36%).

إن التزايد الكبير في استخدام التكنولوجيا والإنترنت في الحياة اليومية، جعل الأفراد أكثر تعرضاً لمخاطر التهديدات السيبرانية. وساهمت الحملات التوعوية والتعليمية التي تركز على الأمن السيبراني وزيادة الاهتمام العالمي بمخاطر الهجمات الرقمية في تعزيز المعرفة بمفاهيم الحرب السيبرانية واستراتيجيات الحماية الشخصية وفهم مسؤوليات الأمان، مما أدى إلى رفع مستوى الوعي بين الأفراد.

التساؤل الثالث: ما هي جوانب الوعي بالحرب السيبرانية في (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) التي يمتلكها طلاب الجامعة في الجمهورية العربية السورية؟

للاجابة عن هذا التساؤل قامت الباحثة بحساب الأوزان النسبية والانحراف المعيارية والأوزان النسبية المئوية لكل فقرة من فقرات مقياس الوعي بالحرب السيبرانية وأبعادها، باستخدام برنامج SPSS وبرنامج EXCEL، وأظهرت النتائج ما يلي:

الجدول(5). الوزن النسبي والوزن النسبي المئوي والانحراف المعياري لفقرات المقياس

البعد	ت	الفقرات	الوزن النسبي	الانحراف المعياري	الوزن النسبي المئوي	الترتيب
المعرفة بمخاطر الحرب السيبرانية	1	تعد الهجمات التقنية الالكترونية خطراً حقيقيًا على الأفراد	4.86	0.34	%97.27	1
	2	لدي فهم جيد لأنواع التهديدات الرقمية (مثل الفيروسات، البرمجيات الخبيثة).	3.68	0.93	%73.64	5
	3	أنا على علم بالمخاطر المحتملة على بياناتي الشخصية على الإنترنت.	3.95	1.07	%79.09	3
	4	يمكنني معرفة الرسائل البريد الإلكتروني المشبوهة	3.32	0.97	%66.36	8
	5	أشعر بأنني أمتلك المعرفة اللازمة لحماية نفسي من مخاطر الأمن الرقمي.	3.36	0.88	%67.27	7
	6	لدي وعي بالحرب الرقمية وتأثيراتها	3.91	1.09	%78.18	4
	7	استطيع تمييز علامات الأختراق الرقمي على حساباتي الشخصية	3.18	1.27	%63.64	9
	8	لدي معرفة بأنواع الهجمات الرقمية (مثل التصيد و DDoS)	2.77	1.35	%55.45	10
	9	أدرك تأثير الهجمات الرقمية على المؤسسات الحكومية.	4.14	1.02	%82.73	2
	10	أستطيع تحديد بعض الأمثلة على الهجمات الرقمية معروفة	3.50	1.20	%70.00	6
		الدرجة الكلية للبعد	**3.67**	**1.01**	**%73.36**	-----
استراتيجيات الحماية	1	أستخدم كلمات مرور قوية وغير متوقعة لحساباتي على الإنترنت.	4.09	0.85	%81.82	4
	2	أتجنب مشاركة معلوماتي الشخصية على الشبكات الاجتماعية.	4.27	0.75	%85.45	1
	3	أستخدم المصادقة الثنائية عندما يكون ذلك ممكنًا.	3.73	1.14	%74.55	7
	4	أعمل على تحديث برامج الحماية والأمان بشكل دوري	3.86	1.14	%77.27	6

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

	5	أحتفظ بنسخ احتياطية من بياناتي المهمة بشكل منتظم	4.18	1.16	%83.64	2
	6	أستخدم شبكات الإنترنت العامة بحذر.	4.09	0.67	%81.82	3
	7	أنا على دراية كافية بإجراءات حماية البيانات الشخصية	3.91	0.90	%78.18	5
	الدرجة الكلية للبعد		**4.02**	**0.94**	**%80.39**	-----
فهم مسؤوليات الأمان	1	أعتقد أن كل فرد يجب أن يتحمل مسؤولية الأمان الرقمي	4.45	0.58	%89.09	4
	2	يتطلب استخدام الإنترنت سلوكًا أخلاقيًا.	4.64	0.57	%92.73	2
	3	قد يؤدي الجهل بالأمن الرقمي إلى مشاكل قانونية.	4.59	0.65	%91.82	3
	4	أعلم حقوقي وواجباتي بوصفي أحد مستخدمي الإنترنت	4.23	1.00	%84.55	6
	5	أشعر بأنني مسؤول عن حماية معلوماتي.	4.68	0.47	%93.64	1
	6	أرى أهمية وجود سياسة واضحة للأمان الرقمي	4.32	0.82	%86.36	5
	الدرجة الكلية للبعد		**4.48**	**0.68**	**%89.70**	-----
المعرفة بالأدوات والتقنيات الأمنية	1	لدي معرفة بأدوات الأمان المتاحة (مثل برامج مكافحة الفيروسات).	3.77	0.95	%75.45	4
	2	أستخدم أدوات الأمان بشكل منتظم لحماية بياناتي	3.68	1.06	%73.64	6
	3	أعد المعرفة بأدوات الحماية جزءا أساسيا من التعليم الرقمي	4.32	0.76	%86.36	3
	4	أشعر بأنني بحاجة إلى مزيد من التدريب على استخدام أدوات الأمان	4.36	1.03	%87.27	1
	5	أتابع التطورات في تقنيات الأمان الرقمي السيبراني.	3.36	1.11	%67.27	7
	6	أستطيع تحديد الأدوات المناسبة لحماية المعلومات الشخصية	3.77	0.90	%75.45	5
	7	أعد الفهم الجيد للتقنيات الأمنية معززا للأمان الرقمي	4.32	0.88	%86.36	2
	الدرجة الكلية للبعد		**3.94**	**0.96**	**%78.83**	-----
الاستجابة للطوارئ السيبرانية	1	أعرف كيفية التصرف إذا تعرضت لهجوم رقمي على حساباتي الشخصية	3.14	1.22	%62.73	6
	2	أعد وجود خطة للاستجابة للطوارئ أمرا ضروريا.	4.41	0.65	%88.18	2
	3	أفهم كيفية الإبلاغ عن حوادث الأمان في الجامعة.	3.50	1.12	%70.00	5
	4	أشعر بأنني قادر على التعامل مع الحوادث السيبرانية.	3.05	1.11	%60.91	7
	5	معرفة الإجراءات الوقائية للهجمات الرقمية يقلل من الأضرار	4.45	0.66	%89.09	1
	6	أفيد من تجارب الآخرين في التعامل مع الهجمات الرقمية	3.95	0.98	%79.09	4
	7	أرى أهمية تبادل معلومات الحوادث السيبرانية بين الطلاب	4.36	0.71	%87.27	3
	الدرجة الكلية للبعد		**3.84**	**0.92**	**%76.75**	-----
التأثيرات النفسية والاجتماعية	1	أشعر بالقلق من التهديدات الرقمية في حياتي اليومية	3.91	0.85	%78.18	5
	2	أرى أن الحروب الرقمية تؤثر على المجتمع بشكل عام.	4.45	0.58	%89.09	1
	3	أعتقد أن الهجمات الرقمية يمكن أن تؤدي إلى فقدان الثقة في المؤسسات	3.95	0.71	%79.09	4
	4	أعد المناقشات في الأمن الرقمي مهمة للوعي الاجتماعي.	4.32	0.63	%86.36	2
	5	أعرف كيفية التعامل مع التوتر الناتج عن التهديدات الرقمية	3.68	0.82	%73.64	6
	6	أشعر بأثر الحرب الرقمية على العلاقات بين أفراد المجتمع.	4.05	0.64	%80.91	3
	الدرجة الكلية للبعد		**4.06**	**0.71**	**%81.21**	-----
	الدرجة الكلية للمقياس		**4.00**	**0.87**	**%80.04**	

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

من الجدول السابق نلاحظ أن الوزن النسبي المئوي للوعي بالحرب السيبرانية (80.04%) للشباب في الجمهورية العربية السورية، وأظهرت النتائج:

1. **المعرفة بمخاطر الحرب السيبرانية:** إن الفقرات ("تعد الهجمات التقنية الإلكترونية خطراً حقيقياً على الأفراد" و"أدرك تأثير الهجمات الرقمية على المؤسسات الحكومية") أعلى وزن نسبي في حين أن الفقرات ("لدي معرفة بأنواع الهجمات الرقمية) مثل التصيد وDDoS" و"أستطيع تمييز علامات الاختراق الرقمي على حساباتي الشخصية") أدنى وزن نسبي.
2. **استراتيجيات الحماية الشخصية:**إن الفقرات("أتجنب مشاركة معلوماتي الشخصية على الشبكات الاجتماعية" و" أحتفظ بنسخ احتياطية من بياناتي المهمة بشكل منتظم") أعلى وزن نسبي، في حين أن الفقرات ("أستخدم المصادقة الثنائية عندما يكون ذلك ممكنً" و"أعمل على تحديث برامج الحماية والأمان بشكل دوري") أدنى وزن نسبي.
3. **فهم مسؤوليات الأمان:** إن الفقرات("أشعر بأنني مسؤول عن حماية معلوماتي" و"يتطلب استخدام الإنترنت سلوكًا أخلاقيًا") أعلى وزن نسبي، وأن الفقرات("أعلم حقوقي وواجباتي بوصفي أحد مستخدمي الإنترنت" و"أرى أهمية وجود سياسة واضحة للأمان الرقمي") أدنى وزن نسبي.
4. **المعرفة بالأدوات والتقنيات الأمنية** إن الفقرات ("أشعر بأنني بحاجة إلى مزيد من التدريب على استخدام أدوات الأمان" و"أعد الفهم الجيد للتقنيات الأمنية معززا للأمان الرقمي") أعلى وزن نسبي، والفقرات ("أتابع التطورات في تقنيات الأمان الرقمي السيبراني" و"أستخدم أدوات الأمان بشكل منتظم لحماية بياناتي") أدنى وزن نسبي.
5. **الاستجابة للطوارئ السيبرانية: إن الفقرات**("معرفة الإجراءات الوقائية للهجمات الرقمية يقلل من الأضرار" و" أعد وجود خطة للاستجابة للطوارئ أمرا ضروريا") أعلى الوزن النسبي، في حين الفقرات ("أشعر بأنني قادر على التعامل مع الحوادث السيبرانية "و" أعرف كيفية التصرف إذا تعرضت لهجوم رقمي على حساباتي الشخصية ") أدنى وزن نسبي.
6. **التأثيرات النفسية والاجتماعية:** إن الفقرات ("أرى أن الحروب الرقمية تؤثر على المجتمع بشكل عام" و"أعد المناقشات في الأمن الرقمي مهمة للوعي الاجتماعي") أعلى وزن نسبي، في حين كانت الفقرات (أعرف كيفية التعامل مع التوتر الناتج عن التهديدات الرقمية" و"أشعر بالقلق من التهديدات الرقمية في حياتي اليومية") أدنى وزن نسبي.

أظهرت النتائج توافقًا كبيراً مع الإطار النظري والدراسات السابقة عن أهمية الوعي بالحرب السيبرانية، فأشارت إلى أن التعليم والتدريب السيبراني فعّالان في تعزيز الوعي بين طلاب الجامعة، وهو ما أكدته دراسات مثل **الشريف وآخرين (2023) وفاضل وآخرون (2023)** وأوضحت النتائج وجود فجوات في مستوى الوعي بين طلاب الجامعة، مما يتفق مع نتائج **الطاهر وأحمد (2023)** التي أكدت على ضرورة إدماج تعليم الأمن السيبراني في المناهج الدراسية. علاوة على ذلك، أكدت النتائج أهمية الأدوات المستخدمة لقياس الوعي بدقة، بما

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

يتماشى مع دراسة **الرحمنة .(2023)** في النهاية، تشير هذه النتائج إلى ضرورة تطوير استراتيجيات تعليمية شاملة تستهدف الفئات المختلفة لضمان تعزيز الأمان الرقمي في المجتمع.

التساؤل الرابع: هل يوجد فروق ذات دلالة إحصائية في الوعي بالحرب السيبرانية (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) لدى طلاب الجامعة في الجمهورية العربية السورية تبعاً لمتغير الجنس؟

للاجابة عن هذا التساؤل قامت الباحثة باختبار دلالة الفروق في الوعي بالحرب السيبرانية وأبعادها: (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) لدى طلاب الجامعة في الجمهورية العربية السورية تبعاً لمتغير الجنس باستخدام اختبار ت للعينات المستقلة Independent Sample T Test، وباستخدام برنامج spss، أظهرت النتائج:

الجدول(6). دلالة الفروق في الوعي بالحرب السيبرانية وأبعادها تبعاً لمتغير الجنس

البعد	الجنس	العدد	المتوسط الحسابي	الانحراف المعياري	القيمة التائية	درجة الحرية	قيمة الدلالة	القرار
1	ذكور	96	39.417	7.137	5.794	174	0.000	دال
	إناث	80	33.400	6.509				
2	ذكور	96	28.917	4.687	2.567	174	0.011	دال
	إناث	80	27.200	4.070				
3	ذكور	96	27.833	1.733	5.060	174	0.000	دال
	إناث	80	25.800	3.451				
4	ذكور	96	29.333	3.392	6.805	174	0.000	دال
	إناث	80	25.500	4.081				
5	ذكور	96	27.917	4.541	3.528	174	0.001	دال
	إناث	80	25.600	4.080				
6	ذكور	96	24.417	2.736	0.247	174	0.805	غير دال
	إناث	80	24.300	3.516				
الكلي	ذكور	96	177.833	19.379	5.338	174	0.000	دال
	إناث	80	161.800	20.380				

من الجدول السابق نلاحظ أن قيمة ت المحسوبة أكبر من قيمة ت الجدولية (1.974) في الدرجة الكلية للوعي بالحرب السيبرانية وأبعادها (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية)، ومن ثم، توجد فروق ذات دلالة إحصائية في الوعي بالحرب السيبرانية وأبعادها: (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية) تبعاً لمتغير الجنس ولصالح الذكور، في حين لم تكن الفروق في بعد التأثيرات الاجتماعية دالة.

تظهر الفروق بين الجنسين في الوعي بالحرب السيبرانية لصالح الذكور في الأبعاد التقنية مثل المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، وفهم الأدوات والتقنيات الأمنية، مما يشير إلى أن الذكور قد

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

يكونون أكثر انخراطًا أو تعرضًا للتدريب التقني والممارسات الأمنية. في المقابل، لم تظهر فروق في التأثيرات النفسية والاجتماعية للحرب السيبرانية بين الجنسين، مما يدل على أن كلا الجنسين يعانيان من تأثيرات نفسية واجتماعية متشابهة نتيجة للتهديدات السيبرانية، مثل القلق والخوف من الأمان الرقمي، بغض النظر عن الفروق في المعرفة التقنية.

التساؤل الرابع: هل يوجد فروق ذات دلالة إحصائية في الوعي بالحرب السيبرانية (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) لدى طلاب الجامعة في الجمهورية العربية السورية تبعاً لمتغير التخصص؟

للاجابة عن هذا التساؤل قامت الباحثة باختبار دلالة الفروق في الوعي بالحرب السيبرانية وأبعادها (المعرفة بالمخاطر السيبرانية، استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) لدى طلاب الجامعة في الجمهورية العربية السورية تبعاً لمتغير التخصص باستخدام اختبار ت للعينات المستقلة Independent Sample T Test، وباستخدام برنامج spss، أظهرت النتائج:

الجدول(7). دلالة الفروق في الوعي بالحرب السيبرانية وأبعادها تبعاً لمتغير الأختصاص

البعد	الجنس	العدد	المتوسط الحسابي	الانحراف المعياري	القيمة التائية	درجة الحرية	قيمة الدلالة	القرار
1	نظرية تطبيقية	112 64	33.786 41.750	7.115 4.983	7.911	174	0.000	دال
2	نظرية تطبيقية	112 64	27.929 28.500	3.690 5.634	0.812	174	0.418	غير دال
3	نظرية تطبيقية	112 64	26.857 27.000	2.040 3.871	0.321	174	0.749	غير دال
4	نظرية تطبيقية	112 64	27.929 27.000	3.824 4.701	1.424	174	0.156	غير دال
5	نظرية تطبيقية	112 64	26.929 26.750	4.320 4.774	0.254	174	0.800	غير دال
6	نظرية تطبيقية	112 64	24.500 24.125	3.304 2.734	0.769	174	0.443	غير دال
الكلي	نظرية تطبيقية	112 64	167.929 175.125	19.357 23.907	2.175	174	0.031	دال

من الجدول السابق نلاحظ أن قيمة الدلالة أكبر من (0.05) في الأبعاد الأربعة (استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية) ومن ثم لا توجد فروق ذات دلالة إحصائية في أبعاد الوعي بالحرب السيبرانية (استراتيجيات الحماية الشخصية، فهم مسؤوليات الأمان، المعرفة بالأدوات والتقنيات الأمنية، الاستجابة للطوارئ السيبرانية، التأثيرات النفسية والاجتماعية)، إلا أن قيمة الدلالة أصغر من (0.05) في بعد المعرفة بالمخاطر السيبرانية والدرجة الكلية للوعي بالحرب السيبرانية ولصالح الكليات التطبيقية.

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

وتفسر الباحثة أن التخصصات التطبيقية غالباً ما تتضمن مناهج تحتوي على معلومات تقنية وعملية تتعلق بأمن المعلومات والسيبرانية، مما يمنح الطلاب فهماً أعمق للمخاطر السيبرانية وكيفية التعامل معها. هذا التأثير يأثر في الدرجة الكلية للوعي، وأن التركيز المعرفي في هذه الكليات يؤدي إلى زيادة المعرفة والتوعية بالحرب السيبرانية بشكل شامل.

التوصيات:

1. يُنصح بتنظيم ورش تدريبية متخصصة لتعريف طلاب الجامعة بمخاطر الهجمات الرقمية، مثل التصيد وهجماتDDoS ، وكيفية التعرف على علامات الاختراق.
2. توصي بإعداد حملات توعية مجتمعية لتوضيح التأثير السلبي للهجمات الإلكترونية على الأفراد والمؤسسات، مع تقديم أمثلة واقعية لتعزيز الوعي.
3. ينصح بإرشاد المستخدمين حول أهمية استخدام المصادقة الثنائية وتحديث برامج الأمان بشكل دوري.
4. يُنصح بإنشاء برامج تعليمية تثقيفية تركز على حقوق وواجبات المستخدمين في الفضاء الرقمي وأهمية اتباع السياسات الأمنية.
5. يُوصى بتقديم خطط واضحة للتعامل مع الحوادث السيبرانية، مع تدريب المستخدمين على تطبيق هذه الخطط بفعالية.
6. ينصح بتوفير جلسات توعوية حول كيفية التعامل مع التوتر الناتج عن التهديدات الرقمية والتخفيف من آثارها النفسية.

المقترحات:

1. تقييم مستوى الوعي بالحرب السيبرانية بين طلاب الجامعة: دراسة ميدانية في الجامعات السورية.
2. العوامل المؤثرة في الوعي بالمخاطر السيبرانية لدى طلاب الجامعة في المجتمعات العربية.
3. فعالية البرامج التعليمية في تعزيز الوعي بالحرب السيبرانية: دراسة تحليلية لتأثير التعليم الإلكتروني.
4. الوعي بالحرب السيبرانية دراسة مقارنة للاتجاهات والمعرفة بالحرب السيبرانية.
5. استراتيجيات الحماية الشخصية ودورها في تعزيز الأمان السيبراني لدى طلاب الجامعة.
6. تأثير التهديدات الرقمية على الصحة النفسية والاجتماعية للشباب: دراسة تحليلية للوعي السيبراني.
7. تطوير نماذج تدريبية لزيادة الوعي بالحرب السيبرانية لدى طلاب التعليم العالي.
8. أثر الثقافة الرقمية في تعزيز الوعي بالحرب السيبرانية بين الفئات العمرية الشابة.
9. مستوى المعرفة بالأدوات والتقنيات الأمنية لدى مستخدمي الإنترنت: دراسة استقصائية.

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

CONFLICT OF IN TERESTS

There are no conflicts of interest

المراجع:

[1] Crompton، B.،Thompson، D.،Reyes، M.،Zhou،X.، and Zou.، X. (2016). Cybersecurity awareness Shrewsbury public schools. School of professional studies. Paper 3.

[2] Fazil, A. W., Hakimi, M., Sajid, S., Quchi, M. M., & Khaliqyar, K. Q. (2023). Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province. American Journal of Education and Technology, 2(4).

[3] Smith, J., & Doe, A. (2019*). Understanding Consciousness: Psychological Perspectives*. Academic Press.

[4] Thaba, J. M., & Mtsweni, J. S. (2023, June). Developing robust cyber war capabilities for the African battlespace. In Proceedings of the European Conference on Cyber War and Security (ECCWS) 2023, Athens, Greece, June 2023.

[5] Freud, S. (1915). *The Unconscious*. In *The Standard Edition of the Complete Psychological Works of Sigmund Freud* (Vol. 14). Hogarth Press.

[6] Baars, B.J. (1988).*A Cognitive Theory of Consciousness*. Cambridge University Press.

[7] Vygotsky, L. S. (1978). *Mind in Society: The Development of Higher Psychological Processes*. Harvard University Press.

[8] Edelman, G. M., & Tononi, G. (2000). *A Universe of Consciousness: How Matter Becomes Imagination*. Basic Books.

[9] Pusey، P. & Sadera، W. (2011). Cyberethics، Cybersaftey، and Cybersecutity: Preservice teacher knowledge، preparedness، and the need for teacher education to make a difference. Journal of digital learning in teacher education. 28(2).

[10] خليفة، إيهاب. (2017). الأمن السيبراني: الأدوات والسياسات والمبادئ التوجيهية. دمشق: دار النشر.

[11] لهيئة الوطنية السعودية للأمن السيبراني .(2018) .*حماية الشبكات وأنظمة تقنيات المعلومات وأنظمة التقنيات التشغيلية ومكونات من أجهزة*) .صفحة 26). الرياض، السعودية: الهيئة الوطنية السعودية للأمن السيبراني.

[12] صائغ، محمد .(2018) .*الأمن السيبراني وأمن المعلومات: الفروقات الأساسية وطرق الحماية* .دار النشر العربية.

[13] العتيبي، سعود شباب سدر. مدى توافر الوعي بالأمن السيبراني لدى أفراد الأسر في المجتمع السعودي (دراسة استطلاعية على عينة من الأسر بمحافظة جدة). المجلة الدولية لنشر البحوث والدراسات. المجلد 3. العدد 27.

[14] الشريف، مرام خالد يحيى. الحربي، ليان سعد عوض الله. الحربي، العنود عبد العزيز مصلح. السليماني، أمل عبيد الله عبد العزيز. فعالية برنامج تدريبي مقترح لتنمية الوعي السيبراني لدى طالبات كلية الآداب والعلوم الانسانية: دراسة تجريبية. المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات. المجلد3.العدد 4.

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq

[15] الرحمنة، عبد المجيد أحمد. متطلبات تحقيق الأمن السيبراني في البنوك الأسلامية. مجلة العلوم الإسلامية والدنية. المجلد 8. العدد1.

[16] شمس الدين، منى كامل البسيوني. أبو الخير، اماني كمال. سلام، نجلاء محمد عبد الفتاح. (2023). برنامج إرشادي قائم على توظيف التعلم الذكي وأثره على تنمية بالوعي بالأمن السيبراني وخفض مستوى النوموفوبيا لدى طلاب كلية الإقتصاد المنزلي جامعة المنوفية. مجلة التربية النوعية و التكنولوجيا بحوث علمية وتطبيقية. المجلد2. العدد29.

[17] المـــطيري، بدر عبد الله. (2023). دور مدير المدرسة في تعزيز الوعي بالأمن السيبراني لدى طلاب المدارس الثانوية الحكومية بمحافظة حفر الباطن .مجلة كلية التربية بالمنصورة المجلد4.العدد 124، 2403.

[18] Eltahir, M. E., & Ahmed, O. S. (2023). Cybersecurity awareness in African higher education institutions: A case study of Sudan. Inf. Sci. Lett, 12(1).

Online ISSN: 2312-8135 Print ISSN: 1992-0652
www.journalofbabylon.com/index.php/JUBH Email: humjournal@uobabylon.edu.iq