الوعي بالأمن السيبراني وعلاقته بالمواطنة الرقمية لدى طلبة الجامعة

م. د زيدان خلف حمد علي

وزارة التربية/ المديرية العامة لتربية كركوك

zedan.k.hamad@tu.edu.iq

المستخلص

يهدف البحث الحالي، إلى دراسة العلاقة بين الوعي بالأمن السيبراني والمواطنة الرقمية، وشمل مجتمع البحث طلبة جامعة تكريت للعام الدراسي (٢٠٢٤–٢٠٢٥)، والبالغ عددهم (١٤٠٠٧) طالباً وطالبة، بواقع (٣٢٥٩) طالباً و(١٠٧٤٨) طالبة، تم اختيار عينة مكونة من (٥٠٠) طالب وطالبة باستخدام العينة الطبقية العشوائية ذات التوزيع المتناسب بحسب الجنس أعدّ الباحث مقياسين الأول لقياس الوعي بالأمن السيبراني، تكون في صورته النهائية من (٣٥) فقرة بعد التحقق من صدقه وثباته، والثاني لقياس المواطنة الرقمية وتكون من (٣٨) فقرة، وتم التحقق من خصائصه السيكومترية، سعى البحث إلى تحقيق عدة أهداف، منها التعرف على مستوى الوعي بالأمن السيبراني لدى الطلبة، والفروق ذات الدلالة الإحصائية وفق متغير الجنس، إضافة إلى التعرف على مستوى المواطنة الرقمية والفروق بين الجنسين، والكشف عن طبيعة العلاقة الارتباطية بين المتغيرين وأظهرت النتائج أن الطلبة يتمتعون بمستوى متوسط من الوعي بالأمن السيبراني والمواطنة الرقمية، مع وجود فروق دالة في الوعي السيبراني لصالح الاناث، وعدم وجود فروق بين الجنسين في المواطنة الرقمية، كما بينت النتائج وجود علاقة ارتباطية طردية دالة بين المتغيرين ومن خلال النتائج أوصى الباحث بضرورة إدراج برامج تدريبية توعوية حول الأمن السيبراني والمواطنة الرقمية في المناهج الجامعية كما اقترح الباحث تنظيم ورش عمل ودورات إلزامية للطلبة وأعضاء هيئة التدريس لرفع الوعي بالممارسات الآمنة والمسؤولة في الفضاء السيبراني وأوصى بضرورة إجراء دراسات مستقبلية تتناول العلاقة بين الوعي السيبراني ومتغيرات أخرى مثل القيم الأخلاقية، والتحصيل الأكاديمي، والاستخدام الآمن للتكنولوجيا في التعليم.

الكلمات المفتاحية: الوعي بالأمن السيبراني، المواطنة الرقمية، طلبة الجامعة.

Cybersecurity awareness and its relationship to digital citizenship among university students

Lecturer Dr. Zeidan Khalaf Hamad Ali

Republic of Iraq, Ministry of Education, Kirkuk General Directorate of Education Kirkuk

zedan.k.hamad@tu.edu.iq

Abstract:

The current research aims to study the relationship between cybersecurity awareness and digital citizenship. The research community included Tikrit University students for the academic year (٢٠٢٤-٢٠٢٥), numbering (١٤,٠٠٧) male and female students, comprising (٣,٢٥٩) male stud ents and (١٠,٧٤٨) female students. A sample of (٥٠٠) male and female students was selected us ing a stratified random sample with proportional distribution according to sex. The researcher p repared two scales: the first to measure cybersecurity awareness, consisting in its final form of (٣٥) items after verifying its validity and reliability, and the second to measure digital citizenship, consisting of (٣٨) items, and its psychometric properties were verified. The research sought to a chieve several objectives, including identifying the level of cybersecurity awareness among stud ents, and the statistically significant differences according to the sex variable, in addition to ide

ntifying the level of Digital citizenship and sex differences, and exploring the nature of the corre lation between the two variables. The results showed that students had an average level of awa reness of cybersecurity and digital citizenship, with significant differences in cybersecurity awar eness in favor of males, and no sex differences in digital citizenship. The results also revealed a significant direct correlation between the two variables. Based on the results, the researcher re commended the inclusion of awareness training programs on cybersecurity and digital citizensh ip in university curricula. The researcher also suggested organizing mandatory workshops and c ourses for students and faculty members to raise awareness of safe and responsible practices in cyberspace. He also recommended the need to conduct future studies that address the relation ship between cybersecurity awareness and other variables such as ethical values, academic achi evement, and the safe use of technology in education.

Keywords: cybersecurity awareness, digital citizenship, university students

الفصل الأول تعريف بالبحث

اولاً: مشكلة البحث:

يُعدّ الأمن السيبراني من المفاهيم الحديثة نسبياً، إذ برز بشكل واضح مع التطورات المتسارعة في تكنولوجيا المعلومات والاتصالات في ظل الثورة الرقمية المعاصرة، التي أسهمت في زيادة تدفق المعلومات وتنوع قنوات الاتصال عبر شبكات الإنترنت والأجهزة الذكية والحواسيب المحمولة. وقد ترافق ذلك مع بروز تحديات وتهديدات رقمية متنامية، من أبرزها الاختراقات، والهجمات الإلكترونية، والابتزاز، وانتهاك الخصوصية، وتسريب المعلومات، الأمر الذي جعل الأمن السيبراني محور اهتمام الحكومات والمؤسسات والباحثين باعتباره الضمانة الرئيسة لحماية الأفراد والمجتمعات من المخاطر الرقمية. [١: ٢-٣].

ويُنظر إلى المواطنة الرقمية باعتبارها إطاراً شاملاً يُعنى بتمكين الأفراد من الاستخدام الواعي والمسؤول للتكنولوجيا والفضاء السيبراني، بما يعزز القيم الأخلاقية والسلوكيات الرقمية السليمة التي تتوافق مع القوانين والأعراف المجتمعية ويُعَدّ الوعي بالأمن السيبراني أحد المقومات الرئيسة لتحقيق المواطنة الرقمية، إذ إن ضعف هذا الوعي يُفضي إلى سلوكيات رقمية غير آمنة، ويزيد من احتمالية تعرض الأفراد لمخاطر الابتزاز، أو التضليل الإعلامي، أو انتهاك الخصوصية. [٢: ٢-٣].

ومن خلال ملاحظات الباحث لواقع استخدام طلبة الجامعة لمواقع التواصل الاجتماعي والفضاء السيبراني، تبيّن أن هذه المنصات تُستثمر أحياناً بصورة إيجابية في التعلم والتواصل وتبادل المعرفة، لكنها في الوقت ذاته تُستغل أحياناً أخرى بشكل سلبي من خلال انتشار بعض الممارسات غير المسؤولة مثل نشر الشائعات، أو انتهاك الخصوصية، أو ممارسة الابتزاز الإلكتروني، وهو ما يعكس تبايناً في مستوى الوعي بالأمن السيبراني لدى فئة الشباب الجامعي.

ويرى الباحث ان هذا الاختلاف يشير الى تساؤلات مهمة حول طبيعة العلاقة بين مستوى الوعي بالأمن السيبراني ومفهوم المواطنة الرقمية لدى طلبة الجامعة، خصوصاً في ظل حاجة المجتمعات الحديثة إلى أفراد يمتلكون مهارات رقمية متقدمة وسلوكيات مسؤولة تعزز قيم المواطنة في البيئة الرقمية ومن هنا تتحدد مشكلة البحث الحالي في محاولة الكشف عن مستوى الوعي بالأمن السيبراني لدى طلبة الجامعة، ومدى انعكاس هذا الوعي على سلوكياتهم الرقمية ذات الصلة بالمواطنة الرقمية، باعتبار ذلك خطوة أساسية لفهم جوانب القصور، والعمل على تطوير برامج تربوية وتثقيفية تعزز من هذا الوعي وتدعم ممارسات المواطنة الرقمية الرشيدة وتتحدد مشكلة البحث بالتساؤل الآتي ما طبيعة العلاقة بين الوعي بالأمن السيبراني والمواطنة الرقمية لدى طلبة الجامعة؟

الوعي بالأمن السيبراني وعلاقته بالمواطنة الرقمية لدى طلبة الجامعة

م. د زيدان خلف حمد علي

ثانياً: أهمية البحث:

شهد العالم مع الثورة الرقمية والتطور التكنولوجي المعاصر بروز قضايا جديدة تتعلق بتدفق المعلومات وانتشارها بشكل غير مسبوق، وذلك بفعل تعدد وتنوع وسائل الاتصال عبر الحواسيب والأجهزة الذكية المحمولة هذا التوسع السريع في تداول البيانات أفرز تحديات أمنية جدية تمثلت في التهديدات الإلكترونية والجرائم الرقمية، مما استدعى ولادة مفهوم الأمن السيبراني بوصفه إطاراً وقائياً وتنظيمياً لحماية المعلومات وضمان سلامة البنية الرقمية، وقد أصبح هذا المفهوم محوراً مهماً لاهتمام الباحثين والمؤسسات الرسمية نظراً لارتباطه الوثيق بالسياسات الدفاعية الحديثة، إذ يُنظر إليه على أنه جزء جوهري من أي منظومة أمنية وطنية، وتشير الدراسات إلى أنّ أكثر من (١٣٠) دولة أنشأت وحدات وهيئات متخصصة بالحرب السيبرانية ضمن تشكيلات أمنها الوطني لمواجهة القرصنة، والجرائم الإلكترونية، والاحتيال، وسائر المخاطر الرقمية . [٣: ١٩٩].

ويُعَدّ الأمن السيبراني من الركائز الرئيسة لأي عملية تحول رقمي، لكونه يرتبط ارتباطاً مباشراً بحماية البيانات والبنية التحتية، وهو ما يشكّل هاجساً مستمراً للحكومات والجمهور والقطاعات المتنوعة، ومن بينها قطاع التعليم، ومع تزايد حجم الهجمات الإلكترونية وتطور أساليبها، أصبح من الضروري إيجاد آليات مبتكرة لمعالجتها والتصدي لها، ويُنظر إلى الأمن السيبراني بوصفه الحل الأكثر فاعلية لمواكبة التوسع الكبير في استخدام شبكة الإنترنت وتطبيقاتها المختلفة، فضلاً عن دوره في الحد من المخاطر المترتبة على الاستخدام غير السليم لها، إذ تنتشر عبر الفضاء الرقمي محتويات غير قانونية أو غير مرغوب فيها، قد تؤثر سلباً في قيم المجتمع وأخلاقياته، وتنعكس على شخصية الأفراد بما يعزز السلوكيات المنحرفة لديهم [٤: ٤٥].

ويهدف الأمن السيبراني إلى حماية البيانات التي تخص الأفراد والمؤسسات في العالم وحماية أجهزة الحاسوب والشبكات والبرمجيات من الوصول غير المصرح به أو الهجمات التي تهدف إلى الاستغلال، لذلك يجب أن يمتلك الأفراد ما يكفي من المعرفة والمهارات اللازمة للحفاظ على الأمن السيبراني الشخصي لتلبية جميع احتياجاتهم بأمان دون التعرض للأذى في البيئة الافتراضية، كما أصبحت الكفاءة في الحفاظ على الأمن السيبراني شرطاً لا غنى عنه لأي شخص [٥: ٤٩٩].

ومع التطور الهائل في تكنولوجيا المعلومات وظهور شبكة الإنترنت، أصبح جزء كبير من التفاعل الاجتماعي يتم عبر الشبكة العنكبوتية ومختلف منصات التواصل الاجتماعي، وقد أتاح هذا التحول في طبيعة العلاقات الاجتماعية فرصاٍ واسعة أمام بعض الأفراد ذوي النوايا السيئة لاستغلال هذه الفضاءات الرقمية من أجل الوصول بسهولة إلى ضحاياهم، خصوصاً في ظل غياب الرقابة الأسرية أو ضعف الحماية المجتمعية، ويُعد الأطفال والمراهقون والطلبة من أكثر الفئات عرضة لمثل هذه الجرائم الإلكترونية المرتبطة بالفضاء السيبراني،ومع التزايد المستمر في أعداد مستخدمي وسائل التواصل الاجتماعي من مختلف الأعمار، ظهرت إشكاليات جديدة ترتبط بظاهرة الإدمان على الاستخدام المفرط لهذه الوسائل، وهو ما يحمل انعكاسات سلبية عديدة على الصعيد النفسي والاجتماعي، وتؤثر هذه الانعكاسات بصورة ملحوظة على فئات واسعة من المجتمع، ولا سيما الطلبة الذين يُعدون من أكثر الشرائح تفاعلاً مع هذه التقنيات الحديثة. [٦: ٢٩٠].

ويواجه الطلبة العديد من المخاطر في الفضاء السيبراني، كاختراق الحسابات الشخصية، واستغلالهم بصورة قد تضرهم، وتعرضهم للمخاطر المختلفة، لا بد من تعزيز حمايتهم خلال استخدام الأنترنت ومواقع التواصل الاجتماعي، وتزويدهم بالمعارف والخبرات التي تعزز حمايتهم من الاستغلال والمخاطر المختلفة التي قد تواجههم، والحفاظ على بياناتهم من الهجمات الإلكترونية [٤: ٧٨].

يرى الباحث أنّ التكنولوجيا الرقمية ينبغي أن توظَّف لخدمة الجميع، باعتبارها أداة تسهم في تنمية الوعي بالتمييز بين الصواب والخطأ، وتمكّن الأساتذة من الانخراط مع طلبتهم في حوارات ومناقشات تتصل بمواقف واقعية من الحياة، ومن ثمّ،

تبرز الحاجة الملحّة إلى منحها مكانة متقدمة ضمن العادات التي يكتسبها الفرد منذ الصغر، وفي صلب المناهج الدراسية، إذ إنّ طلاب الحاضر هم صنّاع مستقبل الغد.

وتظهر أهمية المواطنة الرقمية من خلال ما اظهرته العديد من الدول المتقدمة من اهتمام بالغ بهذا المجال، حيث قامت كل من بريطانيا والولايات المتحدة وكندا بإدراج موضوعات المواطنة الرقمية ضمن المناهج الدراسية الخاصة بالطلبة، وذلك ضمن إطار ما يعرف بالتربية الرقمية وفي نفس السياق أطلقت أستراليا مشروعاً وطنياً تحت شعار الاتصال بثقة تطوير مستقبل أستراليا الرقمي، يهدف إلى تعليم الطلبة المواطنة الرقمية وتدريب المعلمين وأولياء الأمور على مفاهيمها من خلال خطة شاملة على مستوى الدولة، كما تتبنى فرنسا المواطنة الرقمية كقضية وطنية مركزية تتطلب الاهتمام والرعاية على أعلى المستويات الحكومية والمؤسساتية وان من الضرورة القصوى وجود المواطنة الرقمية بقواعدها وقوانينها التي تتبّع من ظهور العديد من المشكلات التي تحدث في العالم الرقمي، والتي إن لم يكن هناك قوانين تجرمها، فنكون أمام كارثة تفسد الحياة العامة بكل المقاييس [٧: ٤١].

ويلخص الباحث أهمية المواطنة الرقمية في دورها المحوري في إعداد طالب قادر على فهم القضايا الثقافية والاجتماعية والإنسانية المرتبطة بالتكنولوجيا، وفي مقدمتها الممارسة الآمنة، والاستخدام المسؤول والقانوني والأخلاقي للمعلومات والتقنيات، إلى جانب ترسيخ السلوك الإيجابي في التعامل معها، بما يعزز روح التعاون، والتعلم، والإنتاجية، وتحمل المسؤولية الشخصية عن التعلم مدى الحياة، كما تمنح التقنيات الرقمية مستخدميها فرصاً واسعة للوصول إلى كم متزايد من المعلومات، غير أن هذه الفرص قد تتقلص ما لم تتوافر آلية منهجية تضمن تنظيم استخدامها بصورة ملائمة وفعّالة.

كما تسهم المواطنة الرقمية في تمكين المتعلمين من التمييز بين الصواب والخطأ، كما تساعدهم على المشاركة في حوارات ومناقشات مرتبطة بمواقف حياتية حقيقية، وفهم القضايا والمشكلات الاجتماعية والثقافية والسياسية والاقتصادية في البيئة الرقمية وطرق التعامل معها [٨: ١٠٢].

ثالثاً: اهداف البحث: ان لأهداف البحث أهمية كبرى في تحديد

١. التعرف على مستوى الوعي بالأمن السيبراني لدى طلبة الجامعة.
٢. التعرف على الفروق ذات الدلالة الإحصائية لدى طلبة الجامعة في الوعي بالأمن السيبراني وفق متغير الجنس (ذكور – اناث).
٣. التعرف على مستوى المواطنة الرقمية لدى طلبة الجامعة.
٤. التعرف على الفروق ذات الدلالة الإحصائية في المواطنة الرقمية لدى طلبة الجامعة.
٥. التعرف على طبيعة العلاقة الارتباطية بين الوعي بالأمن السيبراني والمواطنة الرقمية لدى طلبة الجامعة.

رابعاً: حدود البحث: يقتصر البحث الحالي على طلاب وطالبات كلية التربية للعلوم الإنسانية الدراسة الصباحة في جامعة تكريت للعام الدراسي (٢٠٢٤-٢٠٢٥م).

خامساً: تحديد المصطلحات:

١. **الوعي (Awareness):** هو "حالة تفهم واعية للمعلومات والمفاهيم المحيطة بالشخص، ويشمل الوعي الفهم والإدراك للواقع والأحداث والتحديات من حوله، ومقدرة الشخص على التفكير واتخاذ القرارات استناداً إلى هذا الفهم". [٤: ٥٤].
٢. **الأمن السيبراني(Cybersecurity Awareness):** "مجموعة من الإجراءات والتدابير التقنية والسلوكيات التي تهدف إلى حماية الأنظمة الإلكترونية والبيانات من الاختراقات والهجمات الإلكترونية، يشمل الأمن السيبراني حماية البيانات الحساسة والمعلومات الشخصية من التهديدات المتعلقة بالتكنولوجياً". [٩: ٦٤٠].

تبنى الباحث تعريف الظويفري،٢٠٢١في بناء مقياس الوعي بالأمن السيبراني.

٣. **الوعي بالامن السيبراني اجرائياً:** درجة الفهم والإدراك النشط والمستمر للتحديات والمخاطر المرتبطة بالأمن السيبراني لدى طلبة الجامعة ويقاس من خلال اجابتهم على فقرات المقياس الذي أعده الباحث لهذا الغرض.

٤. **المواطنة الرقمية**(Digital Citizenship) هي "عملية من خلالها يتم تزويد الطالب بمجموعة من المهارات في مجال استخدام تويتر والتدوين الإلكتروني والفيس بوك، إضافة إلى إكسابه القدرة على استخدام بعض المواقع الإلكترونية الشهيرة لغرض التعلم والدراسة، منهج المواطنة الرقمية يعلم الطالب كذلك مهارات محورية؛ مثل: مهارات البحث، والتواصل، ومهارات حل المشكلات، إضافة إلى أثراء معرفته بثقافة بلاده وتاريخها، وتعزيز إيمانه بقيم الحرية والعدالة والديمقراطية".[١٠: ٣٩].

تبنى الباحث تعريف حماد، ٢٠٠٤ في بناء مقياس المواطنة الرقمية.

٥. **المواطنة الرقمية إجرائياً:** يقصد بها مجموعة المبادئ والسلوكيات والضوابط التي ينبغي أن تتوافر لدى طلبة المرحلة الجامعية، بما يعرّفهم بحقوقهم وواجباتهم في التفاعل مع الفضاء الافتراضي، ويوجههم نحو الاستخدام الأمثل للعالم الرقمي، ويتم قياسها بالدرجة التي يحصل عليها الطالب عند إجابته عن المقياس المصمم لهذا الغرض.

الفصل الثاني: خلفية نظرية ودراسات سابقة

القسم الأول: الخلفية النظرية

أولاً: الوعي بالأمن السيبراني

أهداف الأمن السيبراني :يسعى الأمن السيبراني إلى تحقيق مجموعة من الأهداف الأساسية التي تمثل جوهر دوره في حماية الأنظمة الرقمية وضمان سلامة المعلومات، وأبرز هذه الأهداف والتي يمكن تفصيلها كالآتي:

١. **إتاحة البيانات (التوافرية):** ويقصد بها ضمان وصول الأفراد المصرح لهم إلى المعلومات في أي وقت يحتاجون إليه، مع القدرة على استخدامها أو تعديلها بشكل آمن، هذا الهدف يضمن استمرارية تدفق البيانات بشكل موثوق دون انقطاع، ومن أبرز الوسائل المعتمدة لتحقيق ذلك: أنظمة النسخ الاحتياطي للحواسيب، والدعم الفني المستمر، إضافة إلى الإجراءات المادية لحماية الخوادم ومصادر البيانات.

٢. **سلامة المعلومات (النزاهة):** تعني الحفاظ على دقة البيانات وصحتها وحمايتها من أي تعديل غير مصرح به، ويقتضي ذلك التأكد من أن مصدر البيانات حقيقي وموثوق، وأن أي تغيير فيها يتم وفق ضوابط محددة، ومن أبرز الآليات المعتمدة لتحقيق النزاهة: استخدام النسخ الاحتياطية الدورية، اعتماد رموز التحقق، وتطبيق تقنيات الكشف عن أي تعديل غير مشروع.

٣. **السرية (الخصوصية):** وتعادل مفهوم الخصوصية في التعامل مع المعلومات؛ إذ تُعنى بمنع وصول غير المخوّلين إلى البيانات، وضمان أن الاطلاع عليها يقتصر على الأشخاص المصرح لهم فقط، ومن أكثر الوسائل استخداماً في هذا المجال: التشفير، وأنظمة التحكم في الصلاحيات، وآليات المصادقة، والتفويض، فضلاً عن إجراءات الأمن المادي لحماية مراكز البيانات. [١١: ٨٨– ٨٩].

أنواع الأمن السيبراني:

يُقسم الأمن السيبراني إلى أنواع متعددة وفقاً لطبيعة المجال الذي يُعنى بحمايته، ومن أبرز هذه الأنواع ما يلي:

١. **أمن الشبكات:** يركز على حماية أجهزة الحاسوب المرتبطة بالشبكة من أي هجمات أو اختراقات داخلية أو خارجية، ومن أبرز التقنيات المستخدمة في هذا المجال جدار الحماية الذي يعمل حاجزاً واقياً بين النظام الداخلي ومصادر الخطر الخارجية، إلى جانب تقنيات حماية البريد الإلكتروني.

٢. **أمن التطبيقات:** يهتم بحماية البرامج والتطبيقات المستخدمة في الحواسيب أو الأجهزة الذكية، وتشمل وسائله إجراءات متعددة مثل: اعتماد كلمات مرور قوية، تفعيل أنظمة المصادقة، وتضمين أسئلة تحقق للتأكد من هوية المستخدم.

٣. **الأمن السحابي:** مع توسع الاعتماد على خدمات التخزين السحابي عبر الإنترنت، برزت الحاجة إلى تأمين هذه البيئة الرقمية، ويهدف الأمن السحابي إلى حماية البيانات المخزنة على المنصات السحابية وضمان سرية استخدامها، خصوصاً مع توجه الأفراد والمؤسسات إلى استبدال التخزين المحلي بالاعتماد على هذه الخدمات.

٤. **الأمن التشغيلي:** يتعلق بإدارة المخاطر التي قد تواجه الأنظمة الداخلية للمؤسسات، ويشمل هذا النوع وضع استراتيجيات بديلة لاستعادة البيانات في حال تعرضها لهجوم إلكتروني، إلى جانب تدريب الموظفين وتوعيتهم بممارسات الاستخدام الآمن، بما يسهم في تقليل احتمالية الوقوع في مخاطر رقمية [١٢: ٥٧].

المفاهيم المرتبطة بالأمن السيبراني: يشمل الأمن السيبراني مجموعة من المفاهيم التي ترتبط بحماية الأفراد من المخاطر والانتهاكات التي قد يتعرضون لها في البيئة الرقمية، ومن أبرز هذه المفاهيم ما يلي:

١. التنمر الإلكتروني (Cyber Bullying):يقصد به استغلال تقنيات الاتصال الحديثة للإيذاء أو الإساءة، سواء عن طريق التهديد أو التحرش أو المضايقة أو الابتزاز أو الإزعاج بوسائل مختلفة، وقد أوضحت بعض الإحصاءات أن ما يقارب (٢٢٪) من التدريسيين في كل من الولايات المتحدة الأمريكية وبريطانيا تعرضوا لشكل من أشكال التنمر الإلكتروني، ومع التوسع الكبير في استخدام الهواتف الذكية والأجهزة اللوحية، أصبح هذا السلوك من أبرز التهديدات السيبرانية شيوعاً.

٢. التشهير الإلكتروني (Cyber Defamation): ويتمثل في نشر محتويات أو أخبار تهدف إلى إلحاق الضرر الأدبي أو المعنوي بشخص أو مؤسسة معينة، وقد تتنوع أشكاله؛ كاختراق الموقع الشخصي للضحية وتغيير محتواه، أو إنشاء موقع مزيف لبث شائعات وأخبار ملفقة، ولا يقتصر هذا النوع على الأفراد فقط، بل قد يطال مؤسسات تعليمية أو أنظمة سياسية ودينية عبر مواقع مخصصة للتشهير أو نشر فضائح مفبركة.

٣. الاحتيال الإلكتروني (Cyber Fraud):وهو أحد أشكال النصب الحديثة التي يمارسها الجناة عبر الشبكة، حيث يُضلَّل الضحايا من خلال مشروعات وهمية أو هويات مزيفة بغرض الاستيلاء على أموالهم أو بياناتهم، وقد يتم ذلك عبر الاتصالات المباشرة بالضحايا أو من خلال التلاعب ببيانات الحاسب [١٣: ٣٣].

٤. الهندسة الاجتماعية (Social Engineering): يشير هذا المفهوم إلى جملة من الأساليب النفسية والاجتماعية التي يستغلها المهاجمون لإقناع الأفراد بالكشف عن معلومات حساسة أو القيام بتصرفات تساعد على اختراق أنظمتهم، ويطلق عليه أحياناً فن اختراق العقول لقدرته على التلاعب بقناعات الضحايا.

٥. التصيد الإلكتروني (Phishing): يُعرف أيضاً بالخداع الإلكتروني، ويتم فيه استهداف المستخدمين للحصول على بيانات حساسة مثل الحسابات المصرفية أو كلمات المرور، وغالباً ما تُصمم رسائل إلكترونية أو إعلانات مزيفة لتبدو وكأنها صادرة عن جهات موثوقة، ما يُسهل على الجناة خداع المستخدمين. [١٤: ٣٥].

٦. الإرجاف الإلكتروني (Cyber Rumoring): ويتمثل في نشر الشائعات أو الأخبار المثبطة التي تُحدث بلبلة وخوفاً داخل المجتمع، مما يؤدي إلى إضعاف الثقة بالمصادر الرسمية، وغالباً ما تُستخدم هذه الممارسات للتشويش على الرأي العام وصرفه عن الحقائق، حيث تُبث أنباء كاذبة حول موضوعات معينة لانتزاع المعلومات الصحيحة أو التأثير في الاتجاهات العامة.

٧. التجسس الإلكتروني (Cyber Espionage): ويُمارس عبر برامج خفية يتم زرعها في أجهزة المستخدمين بغرض جمع المعلومات دون علمهم، وغالباً ما تُدمج هذه البرامج مع تطبيقات مجانية أو برمجيات مشاركة يتم تنزيلها من الإنترنت، وبمجرد تفعيلها تبدأ بمراقبة نشاط المستخدم ونقل بياناته إلى الجهة المهاجمة.

٨. التغرير والاستدراج (Online Grooming): ويستهدف هذا الشكل عادةً الفئات العمرية الصغيرة من مستخدمي الإنترنت، إذ يقوم الجناة بإيهام الضحية بالرغبة في تكوين علاقة صداقة، وقد تتطور هذه العلاقة الافتراضية إلى لقاءات واقعية، مما يشكل تهديداً خطيراً على أمنهم. [١١: ٩٩].

نظرية الحماية التحفيزية (Protection Motivation Theory – PMT)

تُعد نظرية الحماية التحفيزية من أهم النظريات النفسية التي يمكن توظيفها لتفسير سلوك الأفراد تجاه التهديدات السيبرانية، وفهم الدوافع وراء اتخاذهم للإجراءات الوقائية في بيئة الإنترنت.

طورت هذه النظرية من قِبَل روجرز (Rogers, ١٩٧٥) لتفسير كيفية استجابة الأفراد للمخاطر الصحية، ثم طُوِّرت لاحقاً عام ١٩٨٣ لتشمل مجالات أخرى مثل المخاطر البيئية والتقنية، ومن ضمنها الأمن السيبراني

ترتكز النظرية على أن الأفراد يسعون لحماية أنفسهم عندما يُدركون أن هناك تهديداً حقيقياً يهدد مصالحهم أو بياناتهم، وأن لديهم القدرة على مواجهة هذا التهديد بطريقة فعّالة.

ويُحدَّد دافع الحماية (Protection Motivation) من خلال عمليتين رئيسيتين:

١. تقييم التهديد (Threat Appraisal): ويتضمن إدراك الفرد لخطورة التهديد (Perceived Severity) ومدى احتمالية تعرضه له (Perceived Vulnerability)، فعلى سبيل المثال، عندما يُدرك المستخدم أن اختراق بريده الإلكتروني قد يؤدي إلى تسريب بياناته الشخصية، وأن هذا الاحتمال وارد فعلاً، فإن دافعه للحماية يزداد.

٢. تقييم المواجهة (Coping Appraisal):ويتضمن مدى إيمان الفرد بفعالية السلوك الوقائي (Response Efficacy) وثقته بقدرته على تطبيقه (Self–Efficacy)، إضافة إلى تكلفة هذا السلوك (Response Cost)، فكلما شعر المستخدم أن إجراءات الأمان (مثل تغيير كلمات المرور واستخدام المصادقة الثنائية) فعّالة وسهلة التطبيق، زاد التزامه بها وتُفسّر النظرية الوعي بالأمن السيبراني بوصفه نتيجةً لتفاعل الإدراك بالتهديد مع الثقة في السلوك الوقائي، فالمستخدم الذي يُقدّر خطورة التهديد السيبراني ويؤمن بقدرته على التعامل معه، يكون أكثر وعياً وميلاً إلى تبنّي سلوكيات الحماية الإلكترونية. [١٣: ٣٧]. وقد تبنى الباحث نظرية الحماية التحفيزية في بناء أداة ومقياس الوعي بالأمن السيراني.

ثانياً: المواطنة الرقمية

خصائص المواطنة الرقمية: تتميز المواطنة الرقمية بعدة سمات أساسية، من أبرزها:

١. الوعي بمكونات العالم الرقمي وإدراك طبيعته.

٢. امتلاك المهارات اللازمة لممارسة استخدام فعّال وآمن للتكنولوجيا.

٣. الالتزام بالقواعد الأخلاقية التي تجعل التفاعل الرقمي متسماً بالمقبولية الاجتماعية. [٧: ٢٧ –٢٧].

مواصفات المواطن الرقمي: يتصف المواطن الرقمي الواعي بعدد من السمات الجوهرية، منها:

١. الالتزام بالأمانة الفكرية واحترام حقوق الملكية.

٢. احترام الثقافات والقيم المتنوعة في البيئة الافتراضية.

٣. حماية بياناته ومعلوماته الشخصية.

٤. إدارة وقته بفاعلية أثناء استخدام التكنولوجيا.

٥. تحصين نفسه من الأفكار الهدامة والمصادر غير الموثوقة.

٦. الوقوف ضد مظاهر التنمر والتسلط عبر الشبكة.

٧. إثراء المحتوى الرقمي بإنتاج معرفي هادف.
٨. التفكير الواعي في آثار أنشطته الرقمية وترك بصمة إيجابية.
٩. مراعاة الجوانب الصحية مثل الجلسة السليمة أثناء استخدام الحاسوب. [١٥: ٣٨٧].

أهداف نشر ثقافة المواطنة الرقمية: أصبح مفهوم المواطنة الرقمية مرتبطاً ارتباطاً وثيقاً بمتطلبات الحياة الرقمية المعاصرة، الأمر الذي جعل من الضروري وضع مجموعة من الأهداف الواضحة لنشر هذه الثقافة، ويمكن إبرازها على النحو الآتي:

١. العمل على غرس مفهوم المواطنة الرقمية لدى مختلف الفئات العمرية بطريقة مبسطة وجاذبة، بحيث يكون قريباً من اهتماماتهم اليومية،
٢. تعزيز ورفع مستوى الوعي بالأمان الإلكتروني بما يسهم في حماية المتعلمين من المخاطر التقنية والتهديدات السيبرانية.
٣. السعي إلى تمثيل الدولة بصورة حضارية راقية من خلال الالتزام بأنماط السلوك الرقمي السليم والمسؤول.
٤. الحد من الآثار السلبية لاستخدام شبكة الإنترنت على حياة الأفراد الواقعية، والعمل على التوازن بين العالمين الواقعي والافتراضي.
٥. ترسيخ ثقافة حرية التعبير المنضبطة بالآداب العامة بما يضمن التعبير عن الرأي دون إساءة أو تجاوز.
٦. تقديم أدلة ومرجعيات متكاملة للتعامل مع القضايا الإلكترونية المختلفة، بما يسهل على الفرد مواجهة المواقف الرقمية بصورة سليمة ومنهجية.
٧. إعادة صياغة مفهوم الرقابة من كونه رقابة مشددة أو تدخلية إلى رقابة ذاتية قائمة على الضوابط الشرعية والقيم الاجتماعية التي تضبط سلوك الفرد.
٨. توفير بيئة تواصل اجتماعي إيجابية وآمنة تخلو من العنف، وتعزز من الاحترام المتبادل بين مستخدمي الفضاء الرقمي. [٧: ٤١].

معايير المواطنة الرقمية

تتكون المواطنة الرقمية من تسعة عناصر أساسية تمثل مرتكزات للسلوك الأخلاقي المسؤول، وتهدف إلى إعداد مواطن رقمي صالح قادر على التعامل الواعي مع البيئة الافتراضية، وقد بذل الباحثون والمختصون جهداً كبيراً في صياغة هذه المعايير وتفصيل موضوعاتها بما يخدم التنمية الرقمية المستدامة، ومن بين هذه المعايير:

١. **الاتصالات الرقمية:** وتشير إلى عملية تبادل المعلومات إلكترونياً، والقدرة على استثمار الوسائط الحديثة والتقنيات الرقمية في الاتصال والتفاعل مع الآخرين على اختلاف أماكنهم وأزمنتهم، بما يحقق أهدافاً محددة عبر وسائل متعددة للتواصل [١٦: ٣٨- ٤١].
٢. **التجارة الرقمية:** ويُقصد بها إجراء عمليات البيع والشراء عبر الوسائط الإلكترونية، مع ضمان تزويد المستخدم بالمعرفة الكافية لحماية حقوقه كمستهلك، وكذلك تعليمه كيفية البحث عن أفضل العروض عبر محركات البحث، والتأكد من سلامة المعاملات المالية في العالم الرقمي، بما يشمل الوعي بآليات الدفع والاستلام الإلكتروني للأموال.
٣. **الوصول الرقمي:** يعرف بأنه الإتاحة الرقمية أو النفاذ الرقمي والمشاركة الكاملة في المجتمع، ويعني إمكانية وصول جميع الأفراد والطلبة إلى التكنولوجيا الرقمية، وعلى المؤسسة الرقمية توفير جميع الموارد الرقمية بما يتناسب مع جميع الفئات على اختلاف قدرتهم العقلية والجسمية والظروف الاقتصادية، فالإتاحة الرقمية هي تكافؤ الفرص أمام جميع الأفراد بلا استثناء فيما يتعلق بالوصول إلى التقنيات الرقمية واستخدامها [٧: ٦٩].
٤. **الثقافة الرقمية:** يشار إليها بمصطلح محو الأمية الرقمية أو التربية الرقمية وتعني عملية تعليم وتعلم التكنولوجيا واستخدام أدواتها بالشكل الملائم الذي يهدف للاستفادة منها بأكثر من طريقة لتحسين جودة التعليم، لقد أصبح مقياس مفهوم الأمية حديثاً مرتبطاً بقدرة الفرد على استخدام التكنولوجيا، لذا فإن المساهمة في محو الأمية الرقمية هي مسؤولية

فردية وجماعية على الجميع تحقيقها من أجل توفير فرص التعلم والتدريب لاستخدام التكنولوجيا بكافة أدواتها بالشكل الأمثل.

٥. **اللياقة الرقمية (Digital Etiquette):** تشير اللياقة الرقمية – والتي يُطلق عليها أحياناً الإتيكيت الرقمي أو السلوك الرقمي إلى جملة من المعايير والقواعد التي تضبط تصرفات الأفراد في البيئة الإلكترونية، ويُفترض أن يتحمل الفرد مسؤولية ذاتية في هذا المجال، بحيث يضع لنفسه ضوابط واضحة تحكم سلوكه الرقمي وتنسجم مع منظومة القيم والمبادئ التي يتبناها، ليظهر سلوكا راقيا وحضاريا عند استخدام التقنيات الحديثة. [١٨: ٥٦].

٦. **القوانين الرقمية (Digital Law):** تعرف القوانين الرقمية بأنها الجانب التشريعي والأخلاقي الذي ينظم الممارسات في العالم الرقمي، فهي تمثل حقوقا وقيوداً تضعها المجتمعات لحماية أعضائها من الانتهاكات، وتُعد مخالفة هذه القوانين نوعا من الجرائم الرقمية التي تعرض مرتكبيها للمساءلة القانونية، ومن أبرز الأمثلة على ذلك: التعدي على حقوق الملكية الفكرية للكتّاب والناشرين، وانتهاك الخصوصية، وممارسات القرصنة الإلكترونية. [٧: ٨٣].

٧. **الحقوق والمسؤوليات الرقمية (Digital Rights and Responsibilities):** يقصد بها مجموعة الحقوق التي يتمتع بها الأفراد في البيئة الرقمية وما يقابلها من التزامات، فهي تمنح المستخدم حرية الاستفادة من الموارد والخدمات الإلكترونية، لكنها في الوقت نفسه تفرض عليه واجبات تضمن احترام حقوق الآخرين وحماية المصلحة العامة، وفق الأطر القانونية التي تنظم الاستخدام الآمن والمسؤول للتقنية.

٨. **الصحة والسلامة الرقمية (Digital Health and Wellness):** ترتبط هذه البُعد بصحة الفرد النفسية والجسدية أثناء تعامله مع التكنولوجيا، فالاستخدام غير السليم للأدوات الرقمية يؤدي إلى ظهور العديد من المشكلات الجسدية مثل آلام المفاصل أو ضعف البصر، إضافة إلى الضغوط النفسية، ولذا ظهر علم الإرجونوميكس أو ما يُعرف بـ هندسة العوامل البشرية، الذي يهدف إلى توفير انسجام فيزيائي ونفسي بين الإنسان والأجهزة الرقمية المستخدمة بشكل مستمر. ([٧: ٩١].

٩. **الأمن الرقمي (Digital Security):** يعبر الأمن الرقمي عن التدابير الوقائية التي يتبعها الأفراد للحفاظ على سرية معلوماتهم وحماية هوياتهم الرقمية، وهو يتضمن إجراءات متعددة، مثل استخدام برامج الحماية من الفيروسات، وتجنب المواقع المشبوهة، والوقاية من البرمجيات الخبيثة التي قد تستهدف البيانات الشخصية أو المالية للمستخدم. ([١٧: ٦٤].

مراحل تنمية المواطنة الرقمية:

تمر عملية ترسيخ المواطنة الرقمية لدى الطلبة عبر مجموعة من المراحل المترابطة، يمكن توضيحها على النحو الآتي:

١. مرحلة الوعي (Awareness Stage): في هذه المرحلة يُعمل على تزويد الطلبة بالمعرفة التكنولوجية الأساسية، وتنمية إدراكهم بالمخاطر المحتملة المرتبطة باستخدام الأدوات الرقمية، إذ إن الكثير منهم يوظفون التقنية دون إدراك كافٍ لهدف استخدامها أو لمخاطرها.

٢. مرحلة الممارسة الموجهة (Guided Practice): وهي تهدف إلى تدريب الطلبة على التمييز بين الاستخدام السليم وغير السليم للتكنولوجيا، وتحديد الأوقات والأماكن المناسبة للتوظيف الرقمي، فضلا عن تعميق معرفتهم بالأدوات المختلفة وأهداف استخدامها. [٨: ١٤٠].

٣. مرحلة النمذجة وتقديم القدوة (Modeling and Exemplification): وفيها يُترجم ما اكتسبه الطلبة من معارف ومهارات إلى سلوك عملي، فيتعلمون من خلال مشاهدة نماذج حية كالمدرسين الذين يطبقون السلوك الرقمي الإيجابي، مما يساعدهم على الاقتداء بهم في تعاملاتهم مع التكنولوجيا.

٤. مرحلة التغذية الراجعة وتحليل السلوك (Feedback and Behavior Analysis): تتمثل في إتاحة الفرصة للطلبة كي يفكروا في تجاربهم الرقمية ويحللوا أنماط استخدامهم للتقنيات بأنفسهم، بينما يتولى المعلم دور الموجه من خلال فتح باب النقاش والإجابة عن استفسارات الطلبة، بما يعزز لديهم التفكير النقدي حول ممارساتهم الرقمية. [١٩: ٣٠٠].

النظريات المفسرة للمواطنة الرقمية: تعتمد الدراسة في بنائها النظري على مقاربتين رئيسيتين تفسّران السلوك الرقمي وقيم المواطنة الرقمية لدى الشباب الجامعي، وهما نظرية المسؤولية الاجتماعية ومدخل الحتمية التكنولوجية

أولاً: نظرية المسؤولية الاجتماعية (Social Responsibility Theory)

١. **مقدمة النظرية:** تركز نظرية المسؤولية الاجتماعية على تحقيق التوازن بين حرية وسائل الإعلام وبين واجباتها الأخلاقية تجاه المجتمع. وتفترض أن الحرية الحقيقية لا يمكن ممارستها دون وعي ومسؤولية، وأن وسائل الإعلام التقليدية والرقمية يجب أن تلتزم بالمعايير المهنية من أجل خدمة الصالح العام.

٢. **المرتكزات الأساسية للنظرية:** ترى نظرية المسؤولية الاجتماعية كما يؤكد دينيس ماكويل أن وسائل الإعلام لا تكتسب ثقة الجمهور إلا عندما تلتزم بالصدق والدقة والمصداقية والموضوعية والتوازن في الطرح والالتزام بمواثيق الشرف الإعلامي والقوانين والأخلاقيات المهنية.

٣. **مسؤوليات وسائل الإعلام وفق النظرية:** تشمل المسؤوليات الأساسية وهي تسليط الضوء على القضايا العامة ذات الأهمية وتثقيف الجمهور ودعم وعيه وتعزيز التواصل بين أفراد المجتمع.

٤. **الأبعاد الثلاثة للنظرية:** تركز النظرية على ثلاثة أبعاد محورية:
- البعد الوظيفي: الأدوار السياسية والثقافية والتعليمية والاقتصادية للإعلام.
- البعد التنظيمي المهني: التنظيم الذاتي لوسائل الإعلام عبر التشريعات ومواثيق الشرف.
- البعد الأخلاقي: التزام العاملين في الإعلام بالقيم المهنية والسلوكية.

٥. **تعريف المسؤولية الاجتماعية في سياق الدراسة:** التزام الوسائل الرقمية ومستخدميها بالقيم الأخلاقية والتشريعات المهنية عند ممارسة الدور الإعلامي، وبما يحقق توازناً بين حرية الاستخدام ومتطلبات حماية المجتمع وصيانة قيمه. [٨: ١٤٥].

٦. **تطبيق النظرية على المواطنة الرقمية(من وجهة نظر الباحث):** تساعد النظرية في تفسير:
- سلوك الشباب الجامعي السعودي على المنصات الرقمية.
- مدى التزامهم بقواعد المواطنة الرقمية والمسؤولية الأخلاقية على الإنترنت.
- كيفية استخدام الحرية الرقمية دون الإضرار بالمجتمع أو حقوق الآخرين.
- توفّر النظرية إطارًا لتقييم الوعي والسلوك والممارسات والالتزام الأخلاقي في الفضاء الرقمي.

ثانياً: مدخل الحتمية التكنولوجية (Technological Determinism)

١. **مقدمة المدخل:** يرى مدخل الحتمية التكنولوجية – الذي يعد من أبرز أعمال مارشال ماكلوهان وهارولد إنيس أن التكنولوجيا ليست مجرد أدوات، بل هي قوة محركة تشكل المجتمع، وتعيد تشكيل العلاقات الإنسانية، وتوجّه تفكير الأفراد.

٢. **المبادئ الأساسية** للمدخل وتشمل ما يأتي:
- التكنولوجيا عامل خارجي لكنه مؤثر بقوة في البنية الاجتماعية.
- التطور التقني هو المحرك الرئيسي للتغيير الاجتماعي.
- وسائل الاتصال (وليس المحتوى فقط) هي التي تحدد كيفية تفكير الأفراد وتنظيم المجتمعات.

- التحولات التقنية تؤدي إلى تغير الحواس البشرية وأساليب الإدراك.

٣. رؤية ماكلوهان أكد ماكلوهان أن الوسيلة هي الرسالة أي أن خصائص التقنية نفسها تؤثر على الإنسان أكثر من المحتوى الذي تحمله. [١٩: ٢٩٩].

٤. **تطبيق المدخل على المواطنة الرقمية (من وجهة نظر الباحث):** يساعد هذا المدخل في فهم:

- كيف أن التطورات التقنية فرضت أنماطًا جديدة من السلوك والممارسات الرقمية.
- كيف تشكل التكنولوجيا الحديثة إطار المواطنة الرقمية للشباب الجامعي.
- كيفية تكيفهم مع المنصات الجديدة والقوانين والبروتوكولات الرقمية.
- أثر البيئة الرقمية في تشكيل الوعي بالقيم والمسؤوليات الاجتماعية.
- يتيح هذا المدخل تفسير لماذا تتغيّر ممارسات الشباب في البيئة الرقمية؟ وكيف أثرت التكنولوجيا في صياغة مفهوم المواطنة الرقمية نفسه؟

القسم الثاني: دراسات سابقة:

١ – **دراسة المطيري (٢٠٢٣):** اعتمدت هذه الدراسة على المنهج الوصفي المسحي، وتم تطبيقها في مصر على عينة شملت (١٥٠) من مديري ومديرات المدارس الثانوية الحكومية في محافظة حفر الباطن، وقد هدفت إلى الكشف عن دور القيادات المدرسية في تنمية الوعي بالأمن السيبراني لدى طلاب المرحلة الثانوية، ولتحقيق هذا الهدف، قام الباحث باستخدام استبانة مكوّنة من ستة أبعاد رئيسية، تضمنت بمجموعها (٥٩) فقرة، وبعد التحقق من صدق الأداة وثباتها، توصلت النتائج إلى أن مديري المدارس يؤدون دورا محوريا وبارزا في تعزيز مستوى الوعي بالأمن السيبراني لدى طلبتهم، مما يؤكد أهمية الإدارة المدرسية في تنمية الثقافة الأمنية الرقمية داخل المؤسسات التربوية.

٢ – **دراسة العمري وطوابلة (٢٠٢٠):** أجريت هذه الدراسة في الأردن، واستهدفت التعرف على مستوى الوعي بمفهوم المواطنة الرقمية لدى طلبة الجامعات الأردنية، وارتباطه بمحاورها المختلفة، كما سعت إلى تحديد الفروق في هذا الوعي وفقا لمتغيرات الجنس، والكلية، والجامعة، والمرحلة الدراسية، وقد استخدم الباحثان المنهج الوصفي التحليلي، وتم تصميم مقياس للوعي بالمواطنة الرقمية مكوّن من (٣٣) فقرة موزعة على ثلاثة محاور: محور التعليم (١١ فقرة)، محور الاحترام (٩ فقرات)، ومحور الحماية (١٣ فقرة)، وبلغ حجم عينة الدراسة (٣٨٣) طالبا وطالبة من جامعات أردنية مختلفة، أظهرت النتائج أن مستوى وعي الطلبة بمفهوم المواطنة الرقمية كان مرتفعا بشكل عام، كما تبين وجود علاقة ارتباطية قوية بين مستوى الوعي ومحاور المواطنة الرقمية الثلاثة، أما فيما يتعلق بالفروق الإحصائية، فقد كشفت النتائج عن عدم وجود فروق تعزى لمتغيري الكلية أو المرحلة الدراسية، بينما ظهرت فروق ذات دلالة لصالح الإناث فيما يتعلق بمتغير الجنس، وكذلك لصالح طلبة الجامعات الخاصة عند المقارنة بطلاب الجامعات الحكومية.

الفصل الثالث: منهجية البحث وإجراءاته

أولاً: منهجية البحث (Research Methodology): اعتمد الباحث في هذه الدراسة على المنهج الوصفي، لما يتميز به من ملاءمة عالية لطبيعة المشكلة البحثية ولأهدافها، إذ يُعد هذا المنهج من أكثر المناهج شيوعاً في الدراسات التربوية والنفسية، كونه يركز على تشخيص الظواهر كما هي قائمة في الواقع، ثم وصفها وصفاً تفصيلياً ودقيقاً، وصولاً إلى تفسيرها وفهم أبعادها المختلفة، وبهذا فهو يساعد على تقديم صورة واضحة عن الظاهرة المدروسة [٢٠: ٣٢٤].

ثانياً: مجتمع البحث (Population of the Research):تمثل مجتمع البحث من طلبة جامعة تكريت للعام الدراسي (٢٠٢٤–٢٠٢٥)، حيث بلغ العدد الكلي (١٤٠٠٧) طالباً وطالبة موزعين على التخصصات المختلفة، ويتوزع هذا المجتمع إحصائياً بواقع (٣٢٥٩) طالباً و(١٠٧٤٨) طالبة، وهو مجتمع كبير ومتنوع يوفر بيئة مناسبة لتطبيق أدوات البحث.

ثالثاً: عينة البحث الأساسية (Basic of the Research Sample):

- **عينة التحليل الإحصائي:** لأغراض التحليل الإحصائي الأولي، اختار الباحث عينة مكونة من (٤٠٠) طالب وطالبة من بين طلبة جامعة تكريت، موزعين على كليتي العلوم والزراعة، وقد مثّلت هذه العينة أداة أساسية لإجراء الاختبارات الإحصائية والتحقق من الخصائص السيكومترية للمقاييس المستخدمة.
- **عينة التطبيق النهائي:** العينة النهائية هي الجزء من مجتمع البحث الذي يتم اختياره بصورة مقصودة وفق معايير علمية محددة، وذلك لضمان تمثيل المجتمع الكلي بشكل واقعي وصحيح، إذ يقوم الباحث عادةً باختيارها استناداً إلى ضوابط مثل التوزيع الجغرافي أو التخصص الأكاديمي أو الجنس، وقد تكونت هذه العينة النهائية من عدد مناسب من الطلبة، بما يتيح إمكانية تعميم النتائج على مجتمع البحث الأصلي بدرجة عالية من الدقة والموضوعية، وتكونت عينة البحث النهائية من (٥٠٠) طالب وطالبة تم اختيارهم بأسلوب العينة الطبقية العشوائية ذات التوزيع المتناسب وقد توزعت عينة البحث حسب متغير الجنس وبذلك تكونت عينة البحث من (٥٠٠) طالب وطالبة وبواقع (٢٥٠) طالب و(٢٥٠) طالبة من كلية التربية للعلوم الإنسانية.

رابعاً: أدوات البحث Instruments of the Research: استعملت الدراسة الحالية مقياسين هما، مقياس الوعي بالامن السيبراني ومقياس المواطنة الرقمية وهي من بناء وتصميم الباحث، وفيما يلي ا

مقياس الوعي بالأمن السيبراني

١. **تحديد الهدف من المقياس:** يهدف المقياس إلى التعرف على درجة وعي طلبة الجامعة بالأمن السيبراني بمستوياته المختلفة (المعرفية، السلوكية، الوقائية).
٢. **تحديد الأبعاد (المجالات) النظرية للمقياس:** بُني المقياس على ثلاثة أبعاد رئيسية، استنادا إلى الأدبيات النظرية والدراسات السابقة:
   - ❖ البعد المعرفي: يشمل المفاهيم والمعلومات الأساسية عن الأمن السيبراني (مثل تعريفه، مخاطره، أدوات الحماية).
   - ❖ البعد السلوكي: يشمل تصرفات الأفراد في الفضاء السيبراني (مثل مشاركة المعلومات، التعامل مع البريد الإلكتروني، كلمات المرور).
   - ❖ البعد الوقائي/الإجرائي: يشمل الإجراءات والتقنيات التي يتخذها الطالب لحماية نفسه ومعداته (مثل التشفير، التحديثات، برامج الحماية).
٣. **صياغة الفقرات الأولية (بنك الفقرات):** بعد الاطلاع على الأدبيات والدراسات ذات الصلة ونظرية الحماية التحفيزية (Protection Motivation Theory – PMT)، قام الباحث ببناء (٣٧) فقرة أولية لتشكيل مقياس الوعي بالأمن السيبراني، ثم عرضت هذه الفقرات على لجنة متخصصة من المحكمين في ميدان العلوم التربوية والنفسية لغرض التدقيق اللغوي والمراجعة المعرفية، وبناءً على الملاحظات التي وردت من اللجنة، حُذفت فقرتان لعدم ملاءمتهما، فأصبح عدد الفقرات بعد التعديل (٣٥) فقرة، وقد اعتمد الباحث مقياساً خماسياً في الاستجابة يتضمن البدائل: (تنطبق عليّ بشدة، تنطبق عليّ كثيراً، تنطبق عليّ أحياناً، تنطبق عليّ قليلاً، لا تنطبق عليّ أبداً)، ويُطلب من المستجيب اختيار البديل الذي يعبر عن موقفه بشكل أدق، وتميزت هذه الصياغة بمرونتها وتدرجها، وهو ما يسهم في تيسير عملية الاستجابة ويزيد من قبولها لدى الأفراد، كما حرص الباحث على أن تكون صياغة العبارات مستمدة من مواقف نفسية واجتماعية حقيقية

يعيشها الطالب في بيئته التعليمية، وأن تكون واضحة الدلالة وخالية من التعقيد أو الغموض، مع تجنب الإطالة أو تضمين أكثر من معنى في الفقرة الواحدة.

صلاحية الفقرات (الصدق الظاهري): للتحقق من ملاءمة الفقرات وصلاحيتها لقياس أبعاد الوعي بالأمن السيبراني وتعليماته وبدائل الاستجابة الخاصة به اذ لجأ الباحث إلى الصدق الظاهري، ويشير إيبل (Ebel) إلى أن أفضل أسلوب لتحديد الصدق الظاهري يتمثل في عرض الفقرات على مجموعة من الخبراء للحكم على مدى ارتباطها بالظاهرة المقاسة[٢١: ٥٥٥]، وعلى هذا الأساس، عرض الباحث الصيغة الأولية للمقياس على مجموعة من المتخصصين في العلوم التربوية والنفسية، وطلب منهم تحديد ما إذا كانت الفقرات صالحة أو غير صالحة أو تحتاج إلى تعديل، مع تدوين ملاحظاتهم عند الضرورة، ويُعد هذا التحليل المنطقي للفقرات خطوة أساسية في بناء المقاييس؛ إذ يحدد مدى تمثيل الفقرة بشكل ظاهري للبعد الذي أُعدت لقياسه، مما يرفع من قوتها التمييزية ويسهم في تعزيز صدقها [٢٢: ١٧١]، وقد اعتمد الباحث نسبة اتفاق لا تقل عن (٨٠٪) معياراً للحكم على بقاء الفقرة أو تعديلها أو حذفها، كما استعان باختبار مربع كاي (Chi-Square) للتحقق من مدى صلاحية الفقرات، ووفقا لرأي الخبراء والتحليل الإحصائي، حُذفت أربع فقرات: فقرة واحدة من المجال الأول (التسلسل السادس)، فقرتان من المجال الثاني (التسلسلان السابع والعاشر)، وفقرة واحدة من المجال الثالث (التسلسل الثالث)، وبهذا استقر المقياس على (٣٥) فقرة نهائية، مع العلم أن القيمة الجدولية لمربع كاي بلغت (٣.٨٤) عند مستوى دلالة (٠.٠٥).

٤. **إعداد تعليمات المقياس:** استكمالا لصياغة المقياس، وضع الباحث تعليمات واضحة ومبسطة للمستجيبين، لتكون بمثابة دليل إرشادي أثناء الإجابة، تضمنت التعليمات توضيح كيفية الاستجابة على الفقرات، والتأكيد على أهمية الصدق والموضوعية عند الإجابة، مع ضمان سرية البيانات وعدم استخدامها إلا لأغراض البحث العلمي، كما طُلب من أفراد العينة عدم تدوين أسمائهم الشخصية على الاستمارات، والحرص على الإجابة عن جميع الفقرات دون ترك أي منها فارغة.

٥. **وضوح الفقرات والوقت المستغرق:** للتحقق من وضوح الفقرات وصياغتها ومدى مناسبة الوقت المطلوب للإجابة عليها، أجرى الباحث تطبيقا استطلاعيا على عينة عشوائية مكونة من (٣٠) طالباً وطالبة، وطلب منهم تحديد أي ملاحظات تخص غموضا أو صعوبة في التعليمات أو الفقرات، وأظهرت النتائج أن الفقرات والتعليمات وطريقة الإجابة كانت مفهومة وواضحة لدى أفراد العينة، وقد تراوح الوقت المستغرق للإجابة بين (٣٧ – ٤٧) دقيقة، وكان المتوسط الحسابي (٤٠) دقيقة، وتم تحديد ذلك من خلال تسجيل زمن الانتهاء لكل طالب/طالبة على ورقة الإجابة، وتتفق هذه النتائج مع ما أشارت إليه الأدبيات السابقة حول أهمية التأكد من وضوح الفقرات والتعليمات قبل اعتماد المقياس بصورة نهائية.

٦. **التحليل الإحصائي لفقرات المقياس**

- **القوة التمييزية للفقرات:** تعني القوة التمييزية قدرة الفقرة على الفصل بين الأفراد ذوي الدرجات العليا والأفراد ذوي الدرجات الدنيا في السمة المقاسة [٢٣: ٩٧]، وللتحقق من هذه الخاصية، طبّق الباحث المقياس على عينة عشوائية قوامها (٤٠٠) طالب وطالبة من كليتي العلوم والزراعة في جامعة تكريت، وبعد تصحيح الاستجابات، رتبت الاستمارات تنازليا، ثم جرى اختيار (٢٧٪) من أعلى الدرجات لتمثل المجموعة العليا (١٠٨ طالباً/طالبة)، و(٢٧٪) من أدنى الدرجات لتمثل المجموعة الدنيا (١٠٨ طالباً/طالبة)، وتشير الدراسات التربوية إلى أن اعتماد نسبة (٢٧٪) لتحديد المجموعات المتطرفة يضمن أعلى درجات التمايز بين الطرفين[٢٤: ١٤٩]، وبلغ بذلك عدد أفراد المجموعتين (٢١٦) عولجت البيانات باستخدام برنامج الحقيبة الإحصائية للعلوم الاجتماعية (SPSS)، وذلك عبر تطبيق اختبار (T-Test) لعينتين مستقلتين (المجموعة العليا والدنيا) وأظهرت النتائج أن جميع الفقرات تمتلك قوة تمييزية جيدة؛ إذ تجاوزت قيم (ت) المحسوبة القيمة

الجدولية البالغة (١.٩٦) عند مستوى دلالة (٠.٠٥) ودرجة حرية (٢١٤)، وبناءً على ذلك، استقر المقياس على (٣٥) فقرة نهائية.

- **ثبات المقياس (Reliability):** لقياس ثبات المقياس، استخدم الباحث أسلوب ألفا كرونباخ (Cronbach's Alpha) لقياس الاتساق الداخلي بين الفقرات، وقد أجري التحليل على إجابات أفراد العينة نفسها التي استخدمت في التمييز، وأظهرت النتائج أن معامل الثبات بلغ (٠.٨٥)، وهو معامل مرتفع يعكس تجانسا جيدا بين الفقرات ويؤكد اتساقها الداخلي، وبهذا الشكل أصبح المقياس بصيغته النهائية يتكون من (٣٥) فقرة، وتتوزع درجات المقياس بين حدين: أعلى درجة ممكنة هي (١٧٥) درجة، وذلك بضرب عدد الفقرات (٣٥) × أعلى قيمة للاستجابة (٥) وأدنى درجة ممكنة = (٣٥) درجة، وذلك بضرب عدد الفقرات (٣٥) × أقل قيمة للاستجابة (١) أما المتوسط الفرضي للمقياس فقد بلغ (١٠٥) درجة، وهو ما يمثل النقطة المرجعية للحكم على مستوى الوعي بالأمن السيبراني لدى المستجيبين.

مقياس المواطنة الرقمية:

١. **تحديد الهدف من المقياس:** يهدف هذا المقياس إلى التعرف على مستوى المواطنة الرقمية لدى طلبة الجامعة، بمستوياتها الثلاثة: (المعرفية، السلوكية، القيمية)، وقياس مدى امتلاك الطلبة للمفاهيم والمهارات والسلوكيات المرتبطة بالتفاعل المسؤول في الفضاء الرقمي، مع إمكانية الكشف عن الفروق بين الأفراد بحسب متغيرات الجنس، التخصص، والخبرة الرقمية.

٢. **صياغة الفقرات الأولية (بنك الفقرات):** تم بناء (٤٠) فقرة أولية تغطي أبعاد المقياس الثلاثة بعد مراجعة الأدبيات والمقاييس السابقة، خضعت الفقرات لتنقيح لغوي ومفاهيمي من قبل لجنة من الخبراء في القياس النفسي، وتم حذف فقرتين لأسباب تتعلق بالتكرار أو الغموض، ليصبح العدد النهائي (٣٨) فقرة، وقد استخدم الباحث مقياس ليكرت الخماسي لتقدير استجابات الأفراد:(تنطبق علي بشدة – تنطبق علي كثيراً – تنطبق علي أحياناً – تنطبق علي قليلاً – لا تنطبق علي أبداً) وتمت صياغة الفقرات بلغة بسيطة وواضحة وتجنبت التعقيد، وراعت تمثيل المواقف الواقعية التي يعيشها الطالب الجامعي في بيئته الرقمية والتعليمية،

٣. **التحقق من الصدق الظاهري للفقرات:** اعتمد الباحث الصدق الظاهري بوصفه خطوة أولى في التحقق من صلاحية الفقرات، حيث عُرضت النسخة الأولية من المقياس على مجموعة من المحكّمين المتخصصين في العلوم التربوية والنفسية وقياس الاتجاهات، وطلب منهم تقييم (مدى وضوح الفقرات ومدى تمثيلها للبعد الذي تنتمي إليه واقتراح الحذف أو التعديل أو الإبقاء وتم اعتماد معيار اتفاق ٨٠٪ فأكثر لإقرار صلاحية الفقرة، وبناءً على ملاحظات المحكمين: تم حذف ثلاث فقرات غير ممثلة وتم تعديل ٦ فقرات لغوياً ومعنوياً ليصبح العدد النهائي المعتمد (٣٨ فقرة).

٤. **إعداد تعليمات المقياس:** تم إعداد تعليمات واضحة للمقياس تشمل: الغرض من المقياس (لأغراض علمية فقط) وتأكيد السرية التامة لبيانات الأفراد وطريقة الإجابة واختيار بديل واحد لكل فقرة وضرورة الإجابة على جميع الفقرات وعدم ذكر الاسم الصريح على ورقة الإجابة.

٥. **العينة الاستطلاعية لتحديد وضوح الفقرات والوقت اللازم للإجابة:** تم تطبيق المقياس على عينة استطلاعية (٣٠ طالباً وطالبة من كليتين مختلفتين هما كلية الزراعة والعلوم)، للتحقق من: وضوح التعليمات والفقرات ومدى فهم الطلبة لصيغة الإجابة الوقت اللازم للإجابة وتوصل الباحث الى ان جميع الفقرات والتعليمات واضحة ومفهومة وان متوسط الزمن المستغرق للإجابة على المقياس: ٤٥ دقيقة.

٦. **التحليل الإحصائي لفقرات مقياس المواطنة الرقمية**

- القوة التمييزية للفقرات: استخدم الباحث أسلوب المجموعتين المتطرفتين (٢٧٪) من الدرجات العليا والدنيا بعد تطبيق المقياس على عينة مكونة من (٤٠٠) طالب وطالبة من جامعة تكريت، تم استخدام اختبار (T–Test) لعينتين

مستقلتين لتحليل دلالة الفروق، وقد أظهرت النتائج أن جميع الفقرات ذات دلالة إحصائية، حيث تجاوزت القيم التائية المحسوبة القيمة الجدولية (١.٩٦) عند مستوى (٠.٠٥)، مما يدل على تميز الفقرات.

- **ثبات المقياس (الاتساق الداخلي):** لحساب ثبات المقياس تم استخدام معامل ألفا كرونباخ، وجاءت النتيجة: (٠.٨٧) وهي قيمة ممتازة تشير إلى اتساق داخلي قوي بين الفقرات، وبالتالي يُعد المقياس صالحاً للتطبيق.

خامساً: الوسائل الإحصائية: لجأ الباحث في استخراج نتائج البحث الى الحقيبة الإحصائية (SPSS) لمعالجة بيانات البحث الحالي واستخدم فيها مربع كاي والاختبار التائي لعينة واحدة (T- Test) والاختبار التائي لعينتين مستقلتين (T-Test) و معامل إرتباط بيرسون ومعامل ألفا كرونباخ.

الفصل الرابع: عرض النتائج ومناقشتها

أولاً: عرض النتائج (The view of results): بعد الانتهاء من تطبيق أدوات البحث على أفراد العينة البالغ عددهم (٥٠٠) طالب وطالبة، قام الباحث بإدخال الإجابات في برنامج SPSS لإجراء التحليل الإحصائي اللازم ومن خلال هذه المعالجة، أمكن التوصل إلى نتائج تتعلق بأهداف البحث، وكما يأتي:

الهدف الأول: التعرف على مستوى الوعي بالأمن السيبراني لدى طلبة الجامعة: لتحقيق هذا الهدف، تم احتساب المتوسط الحسابي لدرجات أفراد العينة، فبلغ (١٠٦.٣٢) بانحراف معياري قدره (٢.٨٥)، وبمقارنة هذا المتوسط مع المتوسط الفرضي للمقياس البالغ (١٠٥) ظهر وجود فرق لصالح المتوسط الحسابي، ولتحديد دلالة هذا الفرق إحصائياً، استُخدم اختبار (t) لعينة واحدة، حيث كانت القيمة المحسوبة (١٠.٣٩)، وهي أكبر من القيمة الجدولية البالغة (١.٩٦) عند مستوى دلالة (٠.٠٥) ودرجة حرية (٤٩٩) وهذا يشير بوضوح إلى أن أفراد العينة يتمتعون بمستوى متوسط من الوعي بالأمن السيبراني. ويوضح الجدول (١) ذلك:

جدول (١) درجات الطلبة في مقياس الوعي بالأمن السيبراني

المتغير	عدد أفراد العينة	المتوسط الحسابي	الانحراف المعياري	المتوسط الفرضي	درجة الحرية	القيمة التائية		مستوى الدلالة ٠,٠٥
						المحسوبة	الجدولية	
الوعي بالأمن السيبراني	٥٠٠	١٠٦,٣٢	٢,٨٥	١٠٥	٤٩٩	١٠,٣٩	١,٩٦	دالة

بينت نتائج هذا الهدف أن مما يشير إلى أن طلاب العينة وطلابها يتمتعون بمستوى (متوسط) من الوعي بالأمن السيبراني ويمكن للباحث ان يفسر هذه النتيجة على وفق نظرية الحماية التحفيزية (Protection Motivation Theory – PMT) إلى أن طلبة الجامعة لديهم معرفة ومهارات متوسطة تتعلق بمفاهيم الأمن السيبراني، مثل حماية البيانات الشخصية، واستخدام كلمات مرور قوية، والتعامل مع رسائل التصيّد، وغيرها، لكن هذا المستوى لا يصل إلى مرحلة الإتقان، مما يعني وجود حاجة إلى دعم إضافي لرفع مستوى الوعي إلى المستوى العالي.

الهدف الثاني:التعرف على الفروق ذات الدلالة الإحصائية لدى طلبة الجامعة في الوعي بالأمن السيبراني وفق متغير الجنس (ذكور – اناث).: سعى الباحث في هذا الهدف إلى معرفة ما إذا كانت هناك فروق ذات دلالة إحصائية في وعي طلبة الجامعة بالأمن السيبراني بحسب متغير الجنس (ذكور – إناث)، ولتحقيق ذلك، جرى حساب المتوسطات الحسابية والانحرافات المعيارية لكل من الذكور والإناث، فقد بلغ المتوسط الحسابي لدرجات الذكور (١٠٣.٧٦) بانحراف معياري (١.٥٦)، في حين بلغ المتوسط الحسابي للإناث (١٠٧.٢٠) بانحراف معياري (٢.٦٥)، وباستخدام اختبار (ت) لعينتين مستقلتين، تبيّن أن

القيمة التائية المحسوبة بلغت (١٣.٨٣)، وهي قيمة تفوق القيمة الجدولية البالغة (١.٩٦) عند مستوى دلالة (٠.٠٥) وبدرجة حرية (٤٩٨)، وهذا يشير بوضوح إلى وجود فروق ذات دلالة إحصائية بين المجموعتين، وقد جاءت هذه الفروق لصالح الإناث، ويوضح الجدول (٢) هذه النتائج بالتفصيل.

جدول (٢) درجات الذكور والاناث في مقياس الوعي بالأمن السيبراني

متغير الدراسة	الجنس	حجم العينة	متوسطات حسابية	انحرافات معيارية	درجة حرية	قيمة تائية		مستوى الدلالة ٠,٠٥
						محسوبة	جدولية	
الوعي بالأمن السيبراني	الذكور	٢٥٠	١٠٣,٧٦	١,٥٦	٤٩٨	١٣,٨٣	١,٩٦	دالة
	الإناث	٢٥٠	١٠٧,٢٠	٢,٦٥				

اشارت هذه النتيجة الى وجود فروق دالة إحصائية في الوعي بالأمن السيبراني حسب متغير الجنس ولصالح الاناث فوق الإناث في الوعي السيبراني قد يُعزى حسب نظرية الحماية التحفيزية (Protection Motivation Theory – PMT) إلى أنهن أكثر حرصاً على حماية خصوصيتهن الرقمية، أو أكثر التزاماً بالإرشادات الأمنية، أو أن لديهن خبرة أفضل في التعامل مع مصادر التعلم الرقمية، وقد يرتبط هذا أيضاً بالاختلافات في السلوكيات الرقمية بين الجنسين.

الهدف الثالث: التعرف على مستوى المواطنة الرقمية لدى طلبة الجامعة: هدف هذا الجزء إلى تحديد مستوى المواطنة الرقمية عند طلبة الجامعة بشكل عام، ولأجل ذلك تم استخراج المتوسط الحسابي لدرجات عينة البحث، حيث بلغ (١٠٨.٦٣) بانحراف معياري (٣.١٦)، وعند مقارنته بالمتوسط الفرضي للمقياس البالغ (١٠٥)، ظهر وجود فرق لصالح المتوسط الحسابي الفعلي، وللتأكد من دلالة هذا الفرق، استخدم الباحث اختبار (ت) لعينة واحدة، حيث بلغت القيمة التائية المحسوبة (٢٥.٧٠)، وهي قيمة تفوق القيمة الجدولية (١.٩٦) عند مستوى دلالة (٠.٠٥) وبدرجة حرية (٤٩٩) وبذلك يتضح أن طلبة الجامعة يمتلكون مستوى متوسطاً من المواطنة الرقمية وتعرض تفاصيل النتائج في الجدول (٣).

جدول (٣) درجات الطلبة في مقياس المواطنة الرقمية

متغير الدراسة	حجم العينة	متوسط حسابي	انحراف معياري	متوسط فرضي	درجة حرية	قيمة تائية		مستوى الدلالة ٠,٠٥
						محسوبة	جدولية	
المواطنة الرقمية	٥٠٠	١٠٨,٦٣	٣,١٦	١٠٥	٤٩٩	٢٥,٧٠	١,٩٦	دالة

بينت نتائج هذا الهدف ان مستوى المواطنة الرقمية لدى طلاب وطالبات الجامعة هو مستوى (متوسط) ويمكن للباحث ان يفسر هذه النتيجة إلى أن الطلبة يدركون مسؤولياتهم الرقمية بدرجة متوسطة، مثل احترام حقوق الآخرين على الإنترنت، والتفاعل الأخلاقي على المنصات الرقمية، والمشاركة الفعالة في الفضاء السيبراني المستوى المتوسط يشير إلى إمكانية تطوير هذه المهارات بشكل أفضل من خلال التوعية والتدريب.

الهدف الرابع: التعرف على الفروق ذات الدلالة الإحصائية في المواطنة الرقمية لدى طلبة الجامعة: ركز الباحث في هذا الهدف على معرفة ما إذا كانت هناك فروق إحصائية بين الذكور والإناث في مستوى المواطنة الرقمية، وقد بينت النتائج أن المتوسط الحسابي لدرجات الذكور بلغ (١٠٨.٨٠) بانحراف معياري (٣.٢٤)، في حين كان المتوسط الحسابي للإناث

(١٠٨.٥٧) بانحراف معياري (٣.١٤) وبعد تطبيق اختبار (ت) لعينتين مستقلتين، تبيّن أن القيمة التائية المحسوبة (٠.٧١) وهي أقل من القيمة الجدولية (١.٩٦) عند مستوى دلالة (٠.٠٥) وبدرجة حرية (٤٩٨) وهذا يعني أن الفروق غير دالة إحصائياً بين الذكور والإناث، أي أن الجنس لم يكن متغيراً مؤثراً في مستوى المواطنة الرقمية. ويبين الجدول (٤) تفاصيل ذلك

جدول (٤) درجات الذكور والاناث والذكور في مقياس المواطنة الرقمية

المتغير	الجنس	عدد أفراد العينة	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	القيمة التائية		مستوى الدلالة ٠,٠٥
						المحسوبة	الجدولية	
المواطنة الرقمية	الذكور	٢٥٠	١٠٨,٨٠	٣,٢٤	٤٩٨	٠,٧١	١,٩٦	غير دالة
	الإناث	٢٥٠	١٠٨,٥٧	٣,١٤				

بينت نتيجة هذا الهدف عدم وجود فروق في المواطنة الرقمية حسب متغير الجنس وهذا يدل على أن كلاً من الذكور والإناث لديهم مستوى متقارب من المواطنة الرقمية، وربما تلقوا نفس القدر من التوجيه الرقمي، أو يتفاعلون في بيئات رقمية مشابهة لا تختلف فيها فرص ممارسة المواطنة الرقمية.

الهدف الخامس: التعرف على طبيعة العلاقة الارتباطية بين الوعي بالأمن السيبراني والمواطنة الرقمية لدى طلبة الجامعة، لتحقيق هذا الهدف تم حساب معامل إرتباط بيرسون للتعرف على طبيعة العلاقة الإرتباطية بين الوعي بالأمن السيبراني والمواطنة الرقمية

جدول (٥) العلاقة الارتباطية بين الوعي بالأمن السيبراني والمواطنة الرقمية

قيمة معامل الارتباط	درجة الحرية	القيمة الجدولية	مستوى الدلالة
٠.٦٤	٤٩٨	٠.٠٨٧	٠.٠٥

إذ تبين من خلال جدول (٥) ان قيمة معامل ارتباط بيرسون كانت (٠.٦٤) وهي دالة عند مستوى دلالة (٠.٠٥) وبدرجة (٤٩٩) إذ إنَّ القيمة الجدولية (٠.٠٨٨) وهي تعكس وجود علاقة طردية بين المتغيرين اي كلما زادت درجات الوعي بالأمن السيبراني زادت المواطنة الرقمية وبالعكس، وهذه النتيجة تعني أن الطلبة الذين لديهم وعي أعلى بالأمن السيبراني يميلون إلى التمتع بمستوى أعلى من المواطنة الرقمية ويرى الباحث بإن هذا منطقي؛ فالشخص الذي يفهم التهديدات الرقمية يميل إلى التصرف بمسؤولية في الفضاء السيبراني، ما يعكس سلوكيات مواطنة رقمية رشيدة، وتوصلت الدراسة الحالية بتمتع طلبة الجامعة بمستوى متوسط من الوعي بالأمن السيبراني وكذلك يوجد فرق دال احصائيا في متغير الوعي بالأمن السيبراني حسب متغير الجنس ولصالح الاناث كما يتمتع طلبة الجامعة بمستوى متوسط من المواطنة الرقمية وانه لا يوجد فرق دال احصائيا في متغير المواطنة الرقمية حسب متغير الجنس وكذلك يرتبط الوعي بالأمن السيبراني والمواطنة الرقمية لدى طلبة الجامعة بعلاقة إيجابية ودالة.

الاستنتاجات والتوصيات والمقترحات:

الاستنتاجات Conclusions :استناداً إلى النتائج التي تم التوصل إليها استنتج الباحث النقاط الاتية

١. مستوى الوعي بالأمن السيبراني والمواطنة الرقمية لا يزال في الوسط الجامعي بحاجة إلى تنمية، مما يشير إلى فجوة في البرامج التعليمية أو التثقيفية الموجهة للطلبة.
٢. تفوق الإناث في الوعي السيبراني، مما يدعو إلى دراسة الفروق السلوكية الرقمية بشكل أعمق.
٣. غياب الفروق في المواطنة الرقمية بين الجنسين قد يعكس توحّداً في مصادر التعلم والتفاعل الرقمي داخل الجامعة.
٤. العلاقة الموجبة بين الأمن السيبراني والمواطنة الرقمية تؤكد أهمية تعزيز الجانب الأمني لتحسين الأداء الرقمي السلوكي لدى الطلبة.

التوصيات (Recommendations): في ضوء النتائج التي تم التوصل إليها فقد وضع الباحث عدداً من التوصيات، وعلى النحو الاتي:

١. إدراج مقررات أو ورش تدريبية حول الأمن السيبراني ضمن المنهاج الجامعي، مع التركيز على المهارات العملية في حماية البيانات والتفاعل الآمن.
٢. تصميم برامج توعوية رقمية تعزز المواطنة الرقمية، وتشمل السلوكيات الأخلاقية والتفاعل المسؤول عبر الإنترنت.
٣. إجراء دراسات معمقة حول أسباب تفوق الإناث في الوعي السيبراني، من أجل فهم الفروق السلوكية الرقمية وتوظيفها في تطوير استراتيجيات التعليم.
٤. الاستفادة من العلاقة بين الأمن السيبراني والمواطنة الرقمية من خلال دمج محتوى الأمن السيبراني ضمن تدريبات المواطنة الرقمية والعكس.
٥. تفعيل حملات إلكترونية داخل الجامعة لنشر ثقافة الأمان الرقمي والمواطنة الرقمية، عبر منصات التواصل والبوابات الجامعية.
٦. تشجيع الطلبة على تطبيق ما تعلموه من خلال مسابقات أو مبادرات رقمية تطبق مبادئ الأمن السيبراني والمواطنة الرقمية في الحياة الجامعية

المقترحات (Suggestions):يمكن للباحث اقتراح الدراسات المستقبلية التي يمكن ان تسهم في حل بعض المشكلات البحثية والتي تستحق الدراسة وفقا للنحو الاتي:

١.الوعي بالأمن السيبراني وعلاقته الذكاء الاصطناعي لدى طلبة الكلية التربوية المفتوحة.
٢.المواطنة الرقمية وعلاقتها بالفضاء السيبراني لدى معلمي المرحلة الابتدائية.
٣.اجراء دراسات تتناول المواطنة الرقمية وعلاقتها بمتغيرات أخرى مثل (التفكير الريادي والتوجهات المعرفية).
٤.اجراء دراسات تتناول الوعي بالأمن السيبراني وعلاقته بمتغيرات أخرى مثل (التصالح مع الذات والثقة الزائدة).

المصادر

[١] عبد الرزاق، الاء سالم: تحسين الأمن السيبراني لشبكات إنترنت الأشياء، **رسالة ماجستير غير منشورة**، كلية الهندسة، جامعة الموصل، العراق، (٢٠٢٢).

[٢] العبيدي، سهر محمود رشيد، المواطنة الرقمية وعلاقتها بالكفاءة التواصلية لدى طلبة الجامعة، **رسالة ماجستير غير منشورة**، كلية التربية للعوم الإنسانية، جامعة ديالى، (٢٠٢٣)

[٣] شلوش، نورة: القرصنة الإلكترونية في الفضاء السيبراني التهديد المتصاعد الأمن الدول، **مجلة مركز بابل للدراسات الإنسانية**،٨ (٢)،١٨٥-٢٠٦، (٢٠١٨).

[٤] الصانع، نورة وسليمان، إيناس وعسارن، عواطف والسواط، حمد وأبو عميشة، زاهدة: وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم، **المجلة العلمية بكلية التربية جامعة أسيوط**،٣٦(٦)،٤١-٩٠، (٢٠٢٠)

[٥] Haseski, H. I. Cyber security skills of pre-service teachers as a factor in computerassisted education. International Journal of Research in Education and Science (IJRES), ٦(٣), ٤٨٤-٥٠٠.(٢٠٢٠)

[٦] الصبان، عبير والحربي، سماح: إدمان الطالب على استخدام مواقع التواصل الاجتماعي وعلاقته بالأمن النفسي والتورط في الجرائم السيبرانية، **المجلة الدولية للدراسات التربوية والنفسية**، ٦(٢)،٢٦٧-٢٩٣، (٢٠١٩).

[٧] الملاح، تامر المغاوي: **المواطنة الرقمية-تحديات وآمال**، ط١، دار السحاب للنشر والتوزيع، القاهرة، (٢٠١٧).

[٨]الحصري، كامل: مستوى معرفة معلمي الدراسات الاجتماعية بأبعاد المواطنة الرقمية وعلاقته ببعض المتغيرات، **المجلة العربية للدراسات التربوية والاجتماعية**. (٨)، ٨٩-١٤١، (٢٠١٦).

[٩] الظويفري، مشاعل: واقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بالمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية، **المجلة الدولية الدراسات التربوية والنفسية**،١٠(٣)،٦٣٥-٦٥٥، (٢٠٢١).

[١٠] حماد، حسين (٢٠١٦): تقويم منهج الدراسات الاجتماعية بالصف الثالث الاعدادي في ضوء مفهومي المواطنة والعولمة، **رسالة ماجستير غير منشورة**، جامعة الازهر، مصر، (٢٠١٦).

[١١] القحطاني، نورة (٢٠١٩): مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي دراسة ميدانية، **جمعية الاجتماعيين في الشارقة**،٣٦(١٤٤)، ٨٥-١٢٠. ١٤٤)، (٢٠١٩).

[١٢] الدسوقي، طارق: **الأمن المعلوماتي**، ط١، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، (٢٠١٥).

[١٣] الربيعة، صالح: الأمن القومي وحماية المستخدم من مخاطر الإنترنت، **الملتقى الأول بالإدارة العامة لتعليم**، جدة، (٢٠١٨).

[١٤] أبو منصور، حمين: توظيف تقنية التصنيف الربطي للكشف عن مواقع التصيد الإلكتروني، **المجلة العربية الدولية للمعلوماتية**، جامعة نايف العربية للعلوم الأمنية،٥(٩)،٣٢-٤٠، (٢٠١٧).

[١٥] الجزار، هالة: دور المؤسسة التربوية في غرس قيم المواطنة الرقمية، تصور مقترح، دراسات عربية في التربية وعلم النفسASEB،(٥٦)٣٨٥-٤١٨)، (٢٠١٤).

[١٦] المسلماني، لمياء: **التعليم والمواطنة الرقمية**: رؤية مقترحة، المركز القومي للبحوث التربوية والتنمية. عالم التربية. مصر، (٢٠١٤).

[١٧] الحربي، وفاء عواض: درجة اسهام بعض شبكات التواصل الاجتماعي في تعزيز مفهوم المواطنة الرقمية من وجهة نظر طالبات جامعة الامام محمد بن سعود بالرياض، **رسالة ماجستير غير منشورة**، كلية العلوم الاجتماعية، جامعة الامام محمد بن سعود الإسلامية، (٢٠١٦).

[١٨] خميس، محمد: **منتوجات تكنلوجيا التعليم**، دار الحكمة للطباعة والنسر، القاهرة، مصر، (٢٠٠٣).

[١٩] طوالبة، هادي: المواطنة الرقمية في كتب التربية الوطنية والمدنية دراسة تحليلية، **المجلة الأردنية في العلوم التربوية**، ١٣(٣)،٢٩١-٣٠٨، (٢٠١٧).

[٢٠] ملحم، سامي: **مناهج البحث في التربية وعلم النفس**، أربد كلية العلوم التربوية، (٢٠٠٠).

[٢١] Ebel, R L. (١٩٧٢): Essentials of educational measurement , New Jersey. Prentice Hall (١٩٧٢).

[٢٢] الكبيسي، كامل ثامر: العلاقة بين التحليل المنطقي والتحليل الإحصائي لفقرات المقاييس النفسية، جامعة بغداد، كلية التربية، **مجلة الأستاذ**، العدد ٢٥، (٢٠٠١).

[٢٣] Shaw, M.E, :Scales for the measurement of Attitited, New York, Mc Grw - Hall, USA (١٩٦٧).

[٢٤] فرج، صفوت: **القياس النفسي**، ط١، دار الفكر العربي، القاهرة، مصر، (١٩٨٠).