

The Interactive of E-Learning Unit to employ The Students Skills in Cyber Security According to Determinates of Digital Citizenship

فاعلية وحدة الكترونية تفاعلية في توظيف مهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية

Ghadeer Ali Almeahdi

Assistant Professor of Education Technology, Umm Al-Qura University, Makkah, Saudi Arabia

غدير بنت علي الحمادي

أستاذة تقنيات التعليم المساعد، جامعة أم القرى، المملكة العربية السعودية.

Received: 27/09/2022

Accepted: 19/10/2022

تاريخ الاستلام: 2022/09/27 تاريخ القبول: 2022/10/19

المستخلص: هدفت الدراسة إلى تصميم وحدة إلكترونية تفاعلية في توظيف مهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية، ومن ثمَّ قياس فاعليتها. اتبعت الدراسة المنهج الوصفي، والمنهج شبه التجريبي؛ ولتحقيق أهدافها تم بناء أدوات القياس والتي تمثلت في الاختبار المعرفي لقياس الجانب المعرفي وبطاقة الملاحظة لقياس الجانب الأدائي لمهارات الأمن السيبراني في ضوء المحددات التسعة للمواطنة الرقمية، والتي طبقت في الفصل الدراسي الثاني من العام الجامعي (1443هـ/2022م)؛ على عينة قوامها (33) من طلبة المرحلة الجامعية بجامعة أم القرى، وقد كشفت نتائج الدراسة وجود فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسطي درجات عينة الدراسة في التطبيق القبلي والبعدي للاختبار المعرفي لمهارات الأمن السيبراني كدرجة كلية، وكمجالات فرعية: مجال التعليم؛ مجال الاحترام؛ مجال الحماية، وكأبعاد فرعية للمواطنة الرقمية وكانت جميع الفروق لصالح التطبيق البعدي، كما بينت وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) بين متوسطي درجات عينة الدراسة في التطبيق القبلي والبعدي لبطاقة ملاحظة الجانب الأدائي لمهارات الأمن السيبراني كدرجة كلية، وكمجالات فرعية: مجال التعليم؛ مجال الاحترام؛ مجال الحماية، وكأبعاد فرعية للمواطنة الرقمية، وكانت جميع الفروق لصالح التطبيق البعدي. كما كشفت النتائج بأن الوحدة الإلكترونية التفاعلية ذات أثر على تنمية الجانبين المعرفي والأدائي. ووجود علاقة ارتباطية موجبة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين الجانب المعرفي والجانب الأدائي لمهارات الأمن السيبراني، وذلك بعد تطبيق البرنامج القائم على الوحدة الإلكترونية التفاعلية.

الكلمات المفتاحية: وحدة الكترونية تفاعلية، مهارات الأمن السيبراني، المواطنة الرقمية، الطلبة الجامعيين، التعليم الجامعي.

Abstract: The study aimed to design an interactive of e-learning unit to employ students' skills in cyber security according to determinants of digital citizenship then measuring its effectiveness. The study relies on the descriptive approach and the quasi-experimental approach. To achieve study objectives, measurement tools were developed, namely cognitive test and observation card to measure the cognitive and performance aspects of cyber security skills according of the nine determinants of digital citizenship, which were applied in the second semester of the academic year (1443 AH / 2022 AD); On a sample of (33) undergraduate students at Umm Al-Qura University. Study results showed that there are statistically significant differences at $\alpha \leq 0.05$ among average score of the study sample in the pre and post application of the cognitive test of cyber security skills as a total score, and as sub-domains: (Education Field, Respect Field, and Protection Field) and as sub-dimensions of digital citizenship. So, all differences were in favor of post-application. The study also showed that there are statistically significant differences at $\alpha \leq 0.05$ among average score of the study sample in the pre and post application of the observation card of the performance aspect of cyber security skills as a total score, and as sub-domains: (Education Field, Respect Field, & Protection Field), and as sub-dimensions of digital citizenship. So, all differences were in favor of the post- application. The results also showed that the interactive e-learning unit has an impact on the development of the cognitive and performance aspects. and it was found that there is a positive correlation with statistical significance at $\alpha \leq 0.05$ between the cognitive side and the performance side of cyber security skills, after applying the program based on the interactive e-learning unit.

Keywords: Interactive E-Learning Unit, Cyber Security Skills, Digital Citizenship, University Students, University Education, Performance.

مقدمة الدراسة:

والكمومية تطورت بشكل متسارع، والذي أسهم بشكل مباشر أو غير مباشر في تزايد التهديدات الإلكترونية في أغلب دول العالم، وهو ما يسهم أيضاً بشكل كبير في التغييرات في مشهد التهديدات السيبرانية (Zahri, et al., 2017)، كما توصلت دراسة (Al-Arishee, 2019) أن دول الخليج أقل قدرة على مواجهة مخاطر الهجمات السيبرانية بسبب انخفاض المهارات التقنية بما مقارنة بالدول المتقدمة.

وترجمةً لنهج قيادة بلادنا الحكيمة لهذه المتغيرات وتفاعلاتها مع مستجدات العصر الرقمي وتطوراتها، ومواكبة الرؤية الطموحة للمملكة العربية السعودية 2030م لذلك، صدر الأمر الملكي الكريم رقم 6801 وتاريخ 1439/2/11هـ بإنشاء الهيئة الوطنية للأمن السيبراني التي تعد أحد أهم روافد المشاريع الوطنية النوعية، وجاء هذا الأمر في الوقت المناسب لتكون هذه الهيئة مرجعاً وطنياً يهتم بحماية المصالح الحيوية للمملكة وأمنها السيبراني، وكافة خدماتها ومناشطها الإلكترونية.

ومن زاوية أخرى؛ جاءت تطلعات رؤية المملكة 2030م منسجمة ومتناغمة مع هذا التوجه؛ وتجدر الإشارة هنا بجهود المركز الوطني الإرشادي للأمن السيبراني التابع للهيئة في رفع مستوى الوعي والمعرفة بالأمن السيبراني لتجنب المخاطر السيبرانية، وتقليل آثارها والتصدي لها بإطلاق حملات وبرامج توعوية، والتعاون مع المراكز الإرشادية الأخرى، مما يسهم في تعزيز حماية أمن الوطن من مخاطر الهجمات الإلكترونية والبرمجيات الخطيرة المحتملة.

وفي المقابل بالرغم من كل الجهود المبذولة؛ أشار تقرير المركز الوطني لاستطلاعات الرأي العام التابع لمركز الملك عبدالعزيز للحوار الوطني (2022م) في دراسته التي طبقت على (1045) مشاركاً بالمجتمع السعودي، إلى أن المملكة محاربة إلكترونياً، حيث تعرضت لحسائر جراء تعدد الهجمات الإلكترونية، وقد احتلت المملكة المرتبة الثانية عالمياً من حيث تعرضها للهجمات الإلكترونية، كما أظهرت النتائج أن نحو ثلثي السعوديين تعرضوا لمحاولات الاحتيال المختلفة عبر وسائل إلكترونية عن طريق الإنترنت؛ وقد يعود السبب في ذلك إلى

في ظل التحولات البنوية التي يشهدها المجتمع الرقمي السعودي والتغيرات العميقة على المستويات التكنولوجية، والمعلوماتية، والثقافية التي أثرت على جودة الحياة من كافة النواحي، وأسهمت في إحداث نقلة نوعية في الاتصال والتحول الرقمي ومكينة الأداء؛ حيث ربطت أجزاء العالم المتناثرة وقربتها مسهمة في تعارفها وتواصلها ومشاركتها المعلومات والأفكار، وارتبطت فيه أغلب المناشط بانسيابية المعلومات وأمانها وتكامل أنظمتها، كل هذه التطورات النوعية فرضت تحديات قوية حتمت مزيداً من التعلم والوعي وتطوير المهارات لمواكبتها؛ حيث يتهيأ العالم الآن في ظل هذا التقدم التقني لاستقبال الثورة الصناعية الخامسة التي أساسها الازدهار ونمو التقنيات الرقمية، والمتسمة بالنمو المتسارع في قدرات المعالجة الحاسوبية وتخزينها وتبادلها.

ونظراً للمخاطر الإلكترونية التي يتم التعرض لها بشكل مستمر مع تطور التقنيات والتسارع التكنولوجي؛ أصبح مجال الأمن السيبراني من المجالات التي تحظى بعناية واهتمام على المستوى العالمي والإقليمي والمحلي، حيث أصبحت مسؤولية حماية المعلومات والبيانات من أولويات مؤسسات الدولة المختلفة ضد الهجمات الإلكترونية السيبرانية، فالأمن السيبراني فرض نفسه في القرن الحادي والعشرين (السمحان، 2020). كما أن الاعتماد على تكنولوجيا المعلومات والاتصالات ساعد على زيادة عدد مستخدمي الإنترنت من يوم لآخر؛ فقد احتلت المملكة العربية السعودية المرتبة الثالثة عالمياً في سرعة الإنترنت، كما أن متوسط انتشار الإنترنت يصل إلى نسبة (95%)، بالإضافة إلى أن المملكة العربية السعودية احتلت عالمياً في مؤشر (13) عربيًا، و(175) عالمياً، فهي الأكثر تقدمًا بين مجموعة الدول العشرين في مجال التنافسية الرقمية بحسب التقرير السنوي للرقمنة السعودية (2022م)؛ وتلك المؤشرات تؤكد الأهمية القصوى بوعي المجتمع بمهارات الأمن السيبراني لإسهاماته في تأمين وحماية البرمجيات والمواد الإلكترونية المعرضة للخطر من خلال تكنولوجيا المعلومات والاتصالات. كما أن التقنيات الجديدة كالحوسبة السحابية، والبيانات الضخمة، وإنترنت الأشياء (IoT)، والحوسبة المحمولة

والمعرفة الضرورية للاستخدام الفعال للتقنيات الرقمية من أجل المشاركة في المجتمع والتواصل مع الآخرين، وإنشاء واستهلاك المحتوى الرقمي بأمان وفعالية هادفة (Wallace, Walsh, 2020). ويمكن النظر إلى التكنولوجيا بوصفها منظومة تعليمية

تضم عناصر متنوعة ومتكاملة ومتفاعلة مع بعضها البعض (استيتية وسرحان، 2008) ونظرًا لما تحدته التكنولوجيا من إمكانيات تدعم تعلم الطلاب وتسهم في إكساب مهارتهم والتركيز عليها، فقد برزت بيئات التعلم التفاعلية عبر الإنترنت، التي تهدف إلى التفاعلية ضمن هذه المنظومة بين المتعلم والمعلم، أو بين المنظومة وبين المتعلمين باستخدام الأدوات والوسائط المتعددة والفائقة (عزمي، 2015).

ومما سبق يناط بأدوار المؤسسات التعليمية مسؤولية إكساب طلبتها المهارات المعرفية والأدائية للأمن السيبراني لكافة المراحل التعليمية المختلفة؛ ويظهر هذا الدور الرائد جليًا في جهود هيئة تقويم التعليم والتدريب في المملكة العربية السعودية التي وضعت الإطار التخصصي لمجال تعلم التقنية الرقمية (2019)؛ ساعية فيه إلى إعداد المتعلم للتعامل مع التحولات الرقمية المتسارعة والتطورات الهائلة بمختلف المجالات بطريقة إيجابية؛ مثل: قدرات المعالجة، البرمجة والخوارزميات، والذكاء الاصطناعي، تخزين البيانات، استيعاب التوجهات المعلوماتية، والاستفادة منها، والحماية من مخاطرها.

كما أكدت العديد من الدراسات والمؤتمرات على أهمية التوعية الرقمية، كدراسة محمد (2020) التي أوصت بأهمية توعية الطلاب والمعلمين في كليات التربية بخطورة الحروب السيبرانية، وضرورة توجيههم إلى كيفية الاستخدام الآمن للإنترنت، بما يسهم في الحفاظ على أمنهم الشخصي ومعلوماتهم وخصوصياتهم، ويعزز وعيهم بحقوقهم ومسؤولياتهم الرقمية، وقواعد وسلامة التعامل الرقمي. كما أوصى مؤتمر الأمن السيبراني تحديات وآفاق الذي عقد في الجامعة الفرنكوفونية (2017) بأهمية نشر ثقافة الأمن السيبراني بإعداد المناهج التعليمية ودعم الدورات التدريبية وعقد المؤتمرات التي تعنى بنشر مخاطر الجريمة السيبرانية، وفي نفس الوقت لا بد للجامعات من إدراج تخصصات تعنى بالأمن السيبراني ضمن برامجها، وضمن خطة عمل وطنية تهتم بالقيم

قوة اقتصاد المملكة، الأمر الذي يجعلها هدفًا مغريًا لقرصنة الإنترنت للحصول على بيانات الجهات الحكومية والأفراد والاستفادة منها، وخصوصًا البيانات ذات الصبغة المعلوماتية والمالية.

ومن هذا المنطلق تتبوأ المواطنة الرقمية مكانة رفيعة في إكساب المهارات للمواطن الرقمي؛ ليقوم بأدواره على أكمل وجه باستخدام التكنولوجيا بكفاءة، وفهم المحتوى الرقمي وتفسيره وتقييم مصداقيته، وفهم القضايا الثقافية والمجتمعية المتعلقة بالتكنولوجيا، وممارسة السلوك الرقمي الأخلاقي باستخدام الأمن والقانوني والمسؤول للمعلومات والتكنولوجيا؛ واتخاذ خيارات آمنة ومسؤولة ومحترمة عبر الإنترنت؛ ليظهر مظهر المسؤولية الشخصية للتعلم مدى الحياة. (Isman, & Canan Gungoren, 2014). وهنا أكدت دراسة الأحدي (2020) بضرورة إعداد المواطن الرقمي ضمن رؤية المملكة 2030م، بحيث يستطيع مواكبة المستجدات التقنية العالمية، ويتعامل معها بحرفية وأخلاق عالية، ومن هذه المتطلبات مجال القيم الأخلاقية الرقمية في المواطنة الرقمية، ومجال الأمن الرقمي، والتطوع الرقمي.

وعليه تظهر أهمية البدء بتعليم الطلبة وإكسابهم مهارات الأمن السيبراني، فمن الملاحظ في بدايتهم العمرية تظهر محدودية مهاراتهم العملية بالأمن السيبراني، لكن مع تخرجهم من المدرسة من المتوقع استعدادهم وجاهزيتهم للمشاركة الكاملة في المجتمع الرقمي. إذ إنهم في سنوات دراستهم يجب أن يتعلموا ويتقنوا مهارات الأمن السيبراني في ظل توفر المساعدة والتوجيه لهم، وفي ظل تناقص مستويات الحماية التي يحظون بها (NetSafe، 2018). ومن هنا تبرز الحاجة الملحة لتعزيز مفهوم المواطنة الرقمية في المجتمع، والعناية بتقديم المهارات اللازمة لاستخدام فاعل وهادف للإنترنت، والإسهام في تقديم بصمة رقمية واضحة للطلاب والمعلمين، ومن جهة أخرى ترسيخ المواطنة الرقمية في التعليم والتعلم الإلكتروني (الرشيدي والزيادات، 2018).

وفي ذات السياق؛ عززت المواطنة الرقمية الوعي النقدي للطلاب وقدرتهم على المشاركة والتفاعل من منظور الأمن السيبراني، فإن المواطن الرقمي هو شخص يتمتع بالمهارات

التكنولوجية في العصر الرقمي الحالي؛ ولذلك جاءت الحاجة الماسة إلى التوعية الشاملة وتزويدهم بالمهارات اللازمة في الشقين المعرفي والأدائي للتعامل مع الفضاء السيبراني وما يتعلق به من أمن الإنترنت والشبكات، وأمن الهواتف الذكية والحواسيب الشخصية؛ بغية وقاية الطلبة والمحافظة على قيمهم وأمنهم وسلامتهم ضد الاعتداءات، وحمايتهم من المخاطر الوطنية والشخصية والدينية والأخلاقية حين تواجههم في الفضاء السيبراني.

الإحساس بمشكلة الدراسة:

تقوم المؤسسات التعليمية الجامعية بمستوياتها ومراحلها بأدوار مختلفة تجاه طلبتها ومن ذلك مسؤولية نشر الوعي التقني، واستشعاراً بأهمية الأنظمة التقنية والتكنولوجيا وتطبيقاتها المتجددة وارتباطها بالاستخدام الشخصي للأفراد، وأهمية حمايتها من أي تهديدات أو مخاطر يشهدها الفضاء الإلكتروني، كان من المهم السعي لإثارة التساؤل حول تنمية مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية لدى طلبة المرحلة الجامعية؛ وتبني طرق تكنولوجية حديثة لإكساب الطلبة مهارات الأمن السيبراني معرفياً وأدائياً؛ ومن هنا تم تحديد مشكلة الدراسة من خلال الجوانب التالية:

- تطور الهجمات السيبرانية سريعاً نظراً لما تنتجه التكنولوجيا من تطبيقات وبرامج متطورة وعبر أساليب غير مشروعة واستحداث طرق متنوعة لمحاولات الابتزاز وسرقة الهوية وفقدان البيانات السرية؛ وذلك بالاصطاد الإلكتروني أو الهندسة الاجتماعية أو الانتحال وغيرها من الأساليب، والتي حتمت الوعي بسبل حماية وخصوصية المعلومات الشخصية واستعادة السيطرة بعد اختراق الجهاز الشخصي ومواقع التواصل الاجتماعي، وحماية الأجهزة والبرامج بالاستخدام الآمن للإنترنت.

- بالإشارة إلى توصيات المؤتمرات والدراسات السابقة ومقترحاتها كمؤتمر الأمن والدفاع السيبراني تحديات وآفاق الذي عقد في الجامعة في بيروت (2017) والذي أوصى بضرورة تعزيز قيم المواطنة الرقمية، ومهارات الأمن السيبراني عند طلاب الجامعة، ووضع السياسات التعليمية المناسبة لتنميتها لدى الطلاب، ودراسة المنتشري وفطاني

الأخلاقية الوطنية. وأكد مؤتمر الأمن السيبراني المنعقد في هاواي-أمريكا (2019) على أهمية الأمن السيبراني وضرورة تطبيقه بشكل فاعل في التعليم. ومن أهم المبادرات التي تم الإشادة بها المبادرة الوطنية لتعليم الأمن السيبراني (نيس-فرنسا)، التي أطرت العمل لتلبية احتياجات الحكومة المحلية والشؤون المرتبطة بالقوى العاملة والتعليم بالأمن السيبراني، وكذلك هناك مبادرة وزارة الأمن الوطني الداخلي الأمريكية التي شددت على أهمية تطبيق الأمن السيبراني في التعليم الجامعي (Conklin, et al, 2014). كما لوحظ وجود طلب متزايد على المؤهلين جيداً في الأمن السيبراني، حيث ينظر إليها على أنها مهنة المستقبل في المجتمعات المتحضرة (McGettrick, 2013). كما يشار إلى ورقة عمل المنتشري وفطاني (2019) في مؤتمر الثورة الصناعية في التعليم في توظيف المواطنة الرقمية وتطويرها في استرجاع وتقييم وتحليل المعلومات وتوجيه الطلبة نحو الاستخدام الآمن للتكنولوجيا وتأسيس جيل رقمي متكيف مع مجتمع المعرفة.

وفي هذا الإطار وبالجمع بين المتغيرين الأمن السيبراني والمواطنة الرقمية يلاحظ التداخل بين المفهومين، حيث إن المواطنة الرقمية والأمن السيبراني مكملان لبعضهما؛ فكلهما يعبر عن مجموعة من الضوابط والإجراءات والقيم التي يحتاجها الطلبة لتوجيه سلوكياتهم أثناء استخدامهم للتكنولوجيا؛ ليكونوا مواطنين صالحين مسهمين في الرقي والتقدم التكنولوجي (المنتشري وفطاني: 2019). ومن هنا يتبين الدور التنموي الذي تقوم به الجامعات لطلبتها بالمرحلة الجامعية، والذين يشكلون مورداً بشرياً فعالاً يسهم في تحقيق المواطنة الرقمية والوعي باستخدام التقنية بالشكل الأمثل.

وعلى ذلك تتضح الحاجة إلى أهمية اكتساب الوعي بالمهارات السيبرانية في ظل التعاملات التقنية المستمرة في شتى مجالات الحياة، والتي تعد عصب هذا العصر، حيث إن تعلم هذه المهارات وإتقانها أصبح مطلباً ملجأً في ظل الاستخدامات الرقمية المتعددة؛ كما أن مهارات الأمن السيبراني وما يتعلق به من جرائم واختراقات وهجمات بسبب البرمجيات الخطيرة أو الهندسة الاجتماعية، تعد من أشد التهديدات ضرراً على استخدامات الطلبة للتطبيقات

السيبراني في الجامعات، وهي متطلبات إدارية وبشرية ومادية وتقنية، ولا بد من توافر برامج التوعية بأهمية الحماية السيبرانية في الجامعات السعودية كون دول مجلس التعاون الخليجي تتصدر المراتب الأولى كهدف للهجمات السيبرانية المرتبطة بـ "البريد الإلكتروني والبرمجيات الخبيثة"، فالحسائر الاقتصادية تعدّ كبيرة جدًا؛ لذلك لا بد من تضافر الجهود البشرية والمادية لتعزيز الأمن السيبراني في الجامعات السعودية، كما أكدت دراسة الشهراني (2020) والجندي وطه (2019) بضرورة تنمية مهارات الأمن السيبراني وتضمينها في المناهج الدراسية الجامعية.

- تم تطبيق دراسة استطلاعية غير مقننة على الطالبات التي تم تدريسهن بعدد من المقررات المختلفة بالفصل الدراسي الأول من العام 1443هـ وعددهن (72) طالبة؛ بهدف معرفتهن بمهارات الأمن السيبراني معرفيًا وأدائيًا، وبينت النتائج بأن (89%) من العينة أكدن بأن هناك ضعفًا بمعرفتهن بمهارات الأمن السيبراني وطرق الحماية الإلكترونية، كما أهن يستخدمن كلمة مرور واحدة ومتطابقة للاستخدام الشخصي الإلكتروني سواء أكان في البريد الإلكتروني أم المصرف أم المواقع الإلكترونية؛ خوفًا من نسيانها، كما أن كلمة السر غير قوية، ولا يقمن بتغييرها بشكل دوري، وغيرها من الأمور المهمة في مجال الأمن السيبراني. كما أنه من خلال المناقشة المباشرة مع الطالبات أثناء التدريس تبين ضعفهن بمهارات الأمن السيبراني؛ حيث إن أغلبهن لا يقمن بحفظ نسخ احتياطية من ملفاتهن، ولا وضع كلمات سر لبياناتهن وملفاتهن.

وتأسيسًا على ما سبق؛ يظهر جليًا الدور الرائد للأمن السيبراني والمواطنة الرقمية التي أصبح الوعي بها وإكساب مهاراتها ضرورة عصرية فرضتها تغيرات العالم الرقمي وتطوراته السريعة، وعليه لا بد الاهتمام بتعزيز مهاراتها المعرفية والأدائية لدى طلبتنا في الجامعات، لدورهم المزدوج كطلبة في المرحلة الجامعية، ثم تهيئتهم كمهنيين في المستقبل، وبغية تحقيق ذلك؛ جاءت الحاجة إلى تصميم وحدة إلكترونية تفاعلية لتنمية

(2019) التي أظهرت نتائجها تدني مستوى قيم المواطنة الرقمية، وأوصت باستحداث دروس في الأمن السيبراني ذات العلاقة بالمواطنة الرقمية ملحقمة بمقررات الحاسب الآلي في التعليم العام والتعليم العالي، كما أكدت دراسة ملحم وجاب الله (2018) على ضرورة تضمين المواطنة الرقمية في المناهج الدراسية، فلا يمكن تأمين الاستخدام الملائم للإنترنت بدون مواطنة رقمية، كما دعت دراسة التخينة والسفاسفة (2017) إلى ضرورة الارتقاء بالمناهج التعليمية لتمكين المواطنة الرقمية من النهوض بالمجتمع في ظل الثورة التكنولوجية، والذي أبرز دور المواطنة الرقمية في توعية الطلبة بضرورة الابتعاد على الممارسات السلبية فيما يتعلق باستخدام الإنترنت والتقنية بشكل غير ملائم وغير آمن في نفس الوقت، في حين أكدت دراسة فلاته (2020) أنه انطلاقًا من الدور المتقدم الذي تقوم به الجامعات في إعداد المواطن وتكوينه من جميع جوانبه؛ والتي تعد بيئة ملائمة لتعزيز المواطنة الرقمية لدى طلابها، كما أوضحت دراسة الأحمدى (2020) أن رؤية المملكة العربية السعودية 2030 هي إعداد للمواطن الرقمي قيمًا ومهاريًا، ووضعت القوانين التي تكفل له الأمن الرقمي، وصنفت متطلبات إعداد المواطن الرقمي، وأوصت بتفعيل التعاون بين الجامعات في تداول البرامج التي تسهم في إعداد المواطن الرقمي، وتضمين متطلبات إعداده في المناهج التعليمية. في حين كشفت دراسة كاتونا وآخرون (Catota, et al., 2019) عن وجود قصور في تعلم الموضوعات المتعلقة بالأمن السيبراني وإستراتيجيات التحسين المرتبطة به، وأوصت بأهمية تعليم الأمن السيبراني؛ نظرًا لأنه لا تزال موضوع الدراسات المرتبطة بالأمن السيبراني قليلة نوعًا ما، وعلى ذلك كان لا بد من تشجيع اللقاءات والندوات العلمية والأبحاث في الأمن السيبراني، مما قد يساعد بشكل فاعل في تفعيل تطبيق الأمن السيبراني في المناهج الدراسية، ومن ثم سيتم الوصول إلى تنقيف وتعليم ناجح للطلبة بالأمن السيبراني (Schneider, 2013). كما حددت دراسة السمحان (2020) متطلبات تحقيق الأمن

يشكل الأمن السيبراني اليوم أهمية كبرى نظرًا لانتشار الجرائم الإلكترونية، والحروب غير التقليدية عبر الإرهاب الإلكتروني، والتجسس الإلكتروني، واختراق الشبكات، وغيرها مع ازدياد التقدم التكنولوجي في العالم، كما أن المواطنة الرقمية تحظى بالحاجة الملحة للعناية بها كونها تعد من الركائز الأساسية في العصر التكنولوجي الحديث؛ حيث تشكل طوق النجاة للدول والحصن للمجتمعات من مخاطر الاعتداء الرقمي الذي ينتشر في العصر الحالي، فهي تساعد على غرس قواعد التعامل السليم مع التكنولوجيا الرقمية، مع المحافظة على الجانب القيمي والسلوكي للأفراد في تعاملاتهم الرقمية؛ كما تنطلق أهمية الدراسة من جانبين، وهما:

الأهمية النظرية:

1- تكمن أهمية الدراسة الحالية في حداثة وندرة الدراسات الوطنية والعربية التي تبنت المنهج التجريبي ذا التصميم شبه التجريبي المرتبط بموضوع الدراسة الحالي، والتي تربط مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية لدى طلبة المرحلة الجامعية - حسب اطلاع الباحثة -.

2- قد يحظى موضوع الأمن السيبراني في الوقت الحالي باهتمام عالمي في ضوء التحول الرقمي، وكذلك اهتمام محلي وفي طليعة ذلك تحقيق رؤية المملكة العربية السعودية لعام 2030م.

الأهمية التطبيقية:

1- محاولة دعم المجال وإضافة قيمة علمية جديدة، وبدء ما انتهت عنده نتائج الأبحاث السابقة، ولاسيما أن مهارات الأمن السيبراني لها ارتباط وثيق بممارسات الإنسان التقنية في شتى مجالات الحياة، والتي قد تمثل في مظاهرها العديد من المخاطر على مستخدميها.

2- يؤمل أن تسهم الدراسة في إفادة القائمين على التعليم الجامعي وكافة الجهات ذات العلاقة حول تبني قرارات تخص الممارسات التعليمية، وضرورة تضمين مهاراتها في المقررات الجامعية لحماية الطلبة الجامعيين من المخاطر السيبرانية.

3- محاولة لإفادة الطلبة الجامعيين في تنمية مهاراتهم المعرفية والأدائية في مجال الأمن السيبراني؛ لحماية أنفسهم من

المهارات المعرفية والأدائية للأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية، وعلى ذلك حُددت مشكلة الدراسة الحالي من خلال الإجابة عن السؤال الرئيس التالي:

ما فاعلية وحدة إلكترونية تفاعلية في توظيف مهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية؟

أسئلة الدراسة:

تمحورت الأسئلة في الإجابة عن الأسئلة الآتية:

1. ما مهارات الأمن السيبراني اللازمة للطلبة الجامعيين في ضوء محددات المواطنة الرقمية؟
2. ما فاعلية وحدة إلكترونية تفاعلية في تنمية الجانب المعرفي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية؟
3. ما فاعلية وحدة إلكترونية تفاعلية في تنمية الجانب الأدائي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية؟
4. هل توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى الدلالة بين ($\alpha \leq 0.05$) بين مقدار النمو في الجانب المعرفي والجانب الأدائي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية؟

أهداف الدراسة:

سعت الدراسة إلى تحقيق الأهداف التالية:

1. بناء قائمة بمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية.
2. تصميم وحدة إلكترونية تفاعلية في توظيف مهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية.
3. الكشف عن فاعلية وحدة إلكترونية تفاعلية في تنمية الجانبين المعرفي والأدائي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية.

أهمية الدراسة:

المواطنة الرقمية (Digital Citizenship): يقصد بها مجموعة من الجهات التي تدفع سلوكيات الطلبة الجامعيين بجامعة أم القرى في المملكة العربية السعودية من أجل بناء مواطن رقمي يحمي نفسه والآخرين، ويحافظ على وطنه وهويته، ويتعامل بحرص عند استخدام التقنية في البيئة الرقمية، من خلال مجموعة من المحددات المقسمة على ثلاثة محاور هي: محور التعليم ويضم (الثقافة الرقمية، الاتصالات الرقمية، التجارة الرقمية)، محور الاحترام ويضم (الوصول الرقمي، قواعد السلوك الرقمي، القوانين الرقمية)، أما المحور الثالث فالحماية ويضم (الحقوق والمسؤوليات، الصحة والرفاهية الرقمية، الأمن الرقمي).

الإطار النظري والدراسات السابقة: المواطنة الرقمية:

يعرف العمري (2020) المواطنة الرقمية بأنها "مدى التفاعل عبر الوسائل الإلكترونية بين الفرد والآخرين في المجتمع، الممثلة بشبكة المعلومات وتطبيقاتها المختلفة؛ فهي إعداد الطلبة لحمايتهم من مخاطرها وسبل التعامل الآمن مع التكنولوجيا، فهي ليست تقنية، ولكنها ثقافة يجب أن تغرس في نفوس جميع المستخدمين الرقميين" (ص14). وبعد الاطلاع على الأطر النظرية والدراسات ذات العلاقة منها: (محمد 2020؛ المنتشري، 2020؛ فلاتة 2020؛ Choi 2016؛ Al-Zahrani 2015) يمكن تحديد عناصر المواطنة الرقمية بما يلي:

- **التجارة الرقمية:** وتتضمن عمليات الشراء إلكترونياً، فللمواطنة الرقمية دور مهم في تهيئة المجتمع لإدراك القوانين والشرائع المتعلقة بالعمليات التكنولوجية.
- **الوصول الرقمي العادل:** ويتجلى ذلك في إمكانية جميع الأفراد من استخدام التكنولوجيا الرقمية بشكل فاعل.
- **محو الأمية الرقمية:** قضية استخدام التكنولوجيا أصبح من مسؤوليات الفرد والجماعة في آن واحد، فلا بد للمنظومة التعليمية من أن تعنى بنشر الثقافة التكنولوجية بالشكل الملائم للجميع.

الجرائم السيبرانية، وإفادة الباحثين وتحفيزهم في مجال التخصص للقيام بدراسات مستقبلية في تنمية مهارات الأمن السيبراني المستجدة وربطها بمتغيرات تقنية حديثة ومختلفة.

محددات الدراسة: التزمت الدراسة بالحدود الآتية:

- **الحدود الموضوعية:** اقتصر على تناول: قياس فاعلية وحدة إلكترونية تفاعلية في تنمية مهارات الأمن السيبراني وفق محددات المواطنة الرقمية، وهي في ثلاثة محاور هي: (التعليم، الاحترام، الحماية)، متضمنة تسعة أبعاد فرعية.
- **الحدود المكانية:** طبقت هذه الدراسة في منطقة مكة المكرمة-مدينة الليث.
- **الحدود الزمانية:** طبقت الدراسة في الفصل الدراسي الثاني من العام الدراسي (1443هـ-2022م).
- **الحدود البشرية:** طالبات جامعة أم القرى.

التعريفات الإجرائية لمصطلحات الدراسة:

وحدة إلكترونية تفاعلية (Interactive Online Content): ويقصد بها وحدة تدريسية إلكترونية مصممة بنموذج (A.D.D.I.E) للتصميم التعليمي؛ لبناء الوحدة الإلكترونية التفاعلية المقسمة إلى ثلاث وحدات رئيسية: (التعليم- الاحترام-الحماية)، تتضمن بداخلها مفاهيم معرفية ومهارات عملية في موضوعات الأمن السيبراني في ضوء تسعة محددات في المواطنة الرقمية، وتم تصميمها بشكل إلكتروني بمكونات الوسائط المتنوعة التفاعلية مع المادة التعليمية، معتمدة أو غير معتمدة على شبكة الإنترنت، مع إمكانية التفاعل والتحكم في المحتوى التعليمي بشكل تفاعلي.

مهارات الأمن السيبراني (Cyber Security Skills): يقصد به مجموعة الخطوات والإجراءات الاحترازية الأمنية التي تتخذ لحماية الطلبة الجامعيين في جامعة أم القرى من الهجمات السيبرانية بهدف وقايتهم من الهجوم غير المشروع، ومن أجل حماية أنفسهم من مخاطر الاستخدام الإلكتروني للبرامج والتطبيقات والتقنيات الحديثة.

والمنتشري، 2019)، وحددت دراسة السمحان (2020) أن من أهداف الأمن السيبراني تهيئة الأفراد للتصدي للهجمات الإلكترونية التي تهدف إلى التعدي على البيانات الشخصية، وضمان الاستخدام الآمن للإنترنت، ومعالجة الممارسات المرتبطة بالتجسس الإلكتروني، والتصدي للبرمجيات التي تضر بالمستخدم بمعالجة الثغرات الأمنية في الأنظمة الإلكترونية.

وقد أقرت الهيئة الوطنية للأمن السيبراني (2018) مجموعة من الضوابط الأساسية للأمن السيبراني، منها: مجال تعزيز الأمن السيبراني، الذي يتلخص في: حماية الأنظمة والبيانات-إدارة النسخ الاحتياطية-معالجة التحديات السيبرانية-الاهتمام بهويات المستخدمين-ضمان البريد الإلكتروني-نظام تشفير فاعل.

وفي هذا الصدد تعزز المواطنة الرقمية الوعي النقدي للطلاب والتعامل مع المحتوى الرقمي، ومن منظور الأمن السيبراني فإن المواطن الرقمي هو شخص يتمتع بالمهارات والمعرفة الضرورية للاستخدام الفعال للتقنيات الرقمية؛ من أجل المشاركة في المجتمع والتواصل مع الآخرين (Walsh, Wallace, Ayling & Sondergeld, 2020).

ويتبين مما ذكر أهمية المواطنة الرقمية في المؤسسات التعليمية؛ كونها تدعم مختلف الجوانب التعليمية في الجامعات، وفي نفس الوقت تسهم في نحوض المعارف وقيم الديمقراطية، وعلى ذلك فالمواطنة الرقمية هي الداعم الأساس للمجتمع كونها تعزز مفهوم المواطنة في نفوس أفراد المجتمع بشكل عام، والجامعات بشكل خاص (العمري وطوالة، 2020، 13). كما أكد (Al-Zahrani, 2015) أن المواطنة الرقمية تسهم بالحفاظ على الهوية السعودية في هذا العالم الرقمي، والذي يرتبط إلى حد كبير بالنمو الاقتصادي السريع الذي يعكسه الاستهلاك الواسع للتكنولوجيا.

كما حدد الدوسري والعريشي (2018) مجموعة من المهام على الجامعات القيام بها لتوعية الطلبة ضد الجرائم السيبرانية، منها إدخال بعض المقررات الجديدة مثل الثقافة القانونية، وموضوعات تتعلق بثقافة أمن المعلومات، وأهمية اعتماد دبلوم أمن المعلومات، وتبادل الخبرات بين الجامعات، وأهمية توعية الطلاب من خلال البحوث والمؤتمرات والمناقشات والتدريب مع المتخصصين.

- استخدام العالم الرقمي بأسلوب حضاري: لا بد من تدريب وتأهيل الأفراد لاستخدام المهارات والمواطنة الرقمية بأسلوب لائق يراعي القوانين والأنظمة والسلوكيات التي يفرضها المجتمع.

- القوانين الرقمية: في المجتمع الرقمي لا بد من احترام الأخلاقيات الرقمية ومعالجة الممارسات التكنولوجية غير الأخلاقية ضمن ما يسمى الجرائم الرقمية.

- الصحة السلامة الرقمية: للمواطنة الرقمية دور بارز في حماية الأفراد من حالات الاستغلال النفسي والسيطرة على السلوكيات الفردية تحت مسمى "الهندسة الاجتماعية".

- سلامة الأمن الرقمي: وتشمل الحماية المقدمة ضد تهديدات الفيروسات، والقيام بنسخ احتياطية للبيانات المهمة، وتأمين المصادقية في العمل الرقمي، وتهيئة الطلبة لمعرفة عالم اللصوصية عبر الشبكة العنكبوتية.

وللمواطنة الرقمية تحديات أخرى، فقد ذكر العمري (2020) أنها تأتي في ثلاثة محاور هي: محور التعليم ويضم (الثقافة الرقمية، الاتصالات الرقمية، التجارة الرقمية)، محور الاحترام ويضم (الوصول الرقمي، قواعد السلوك الرقمي، القوانين الرقمية)، ومحور الحماية ويضم (الحقوق والمسؤوليات، الصحة والرفاهية الرقمية، الأمن الرقمي).

في حين يذكر الأحمد (2020) أنه "لا بد للمواطن الرقمي من أن يتمتع بمجموعة من الخصائص التي تجعل منه قادرًا رقميًا، منها التمتع بسلوكيات أخلاقية عند استخدام تكنولوجيا المعلومات في مختلف الأنشطة الحياتية، مع تطوير التفكير الناقد والإبداعي في الفضاء الإلكتروني، مع مراعاة الرأي الآخر في العالم الإلكتروني، واحترام الثقافات المتعددة، والابتعاد عن الأفكار السلبية للمجتمعات الأخرى" (ص502).

الأمن السيبراني:

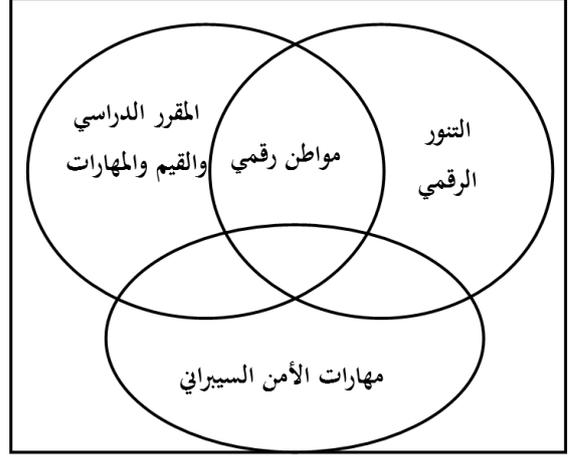
يعد مفهوم الأمن السيبراني من المفاهيم الحديثة التي تشير إلى إجراءات الحماية في وجه العمليات العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات (المنتشري

الإترنت، والسلوك الأخلاقي، والمسؤول، والسلامة أو الحماية من المخاطر، وتعزيز القيم والسلامة الرقمية والمرونة، والمشاركة الرقمية (UNESCO Bangkok، 2019).

كما هدفت دراسة "أدورجان وكيكارديللي" (Adorjan & Ricciardelli، 2019) للكشف عن تصورات الطلاب عن برامج الأمن السيبراني المدرسية في سياق المواطنة الرقمية، اعتماداً على المنهج النوعي، تم جمع البيانات من خلال مقابلات جماعية مركزة -35 مقابلة جماعية- مع عينة مؤلفة من (115) طالباً كندياً تم اختيارهم من مدارس متوسطة وثانوية في شرق وغرب كندا؛ وقد أظهرت النتائج أن الطلاب يتعرضون بشكل متكرر لرسائل ضارة؛ بما في ذلك وسائل تثير خوفهم وعادة ما تكون مجهولة المصدر. كما أشارت النتائج أيضاً إلى الحاجة لمزيد من التعلم وإتقان المعلومات العملية، مثل إدارة الخصوصية. وأظهرت أن غالبية هذه الرسائل تحدد أمنهم السيبراني وحاجتهم الماسة إلى ما يزيد من قدرتهم على الحصانة وضبط الذات كمواطنين رقميين.

الحاجة إلى برامج منظمة للأمن السيبراني في سياق محددات المواطنة الرقمية:

من واقع ما انتهى إليه "جونسون" (Johnson، 2015) في دراسته عن التنوّ الرقمي والمواطنة الرقمية في السياق التعليمي، وضح أن هناك ضعفاً في تنمية المهارات الرقمية للطلاب في المقررات، والحصول على مثل تلك المعلومات يرتبط بدرجة كبيرة بعبء المعلم الذي يدرس الطلاب، وما يحصل عليه الطلاب بالاطلاع من المصادر الخارجية. وفي دراسة "فيسك" (Fisk، 2016) التي تناول فيها البحث في استجابات الطلاب حول لأمن السيبراني في مناهج الولايات المتحدة الأمريكية، ولاحظ غياب تركيز البرامج التعليمية على الأمن السيبراني في المناهج، واقتصرها فقط على العروض التوضيحية المبسطة المقدمة من دوائر الشرطة ومحتري تقنية المعلومات. كما أكدت "كاسيدي" (Cassidy، Brown & Jackson، 2012) أنه على الرغم من انتشار أخطار الفضاء السيبراني إلا أنه ليس لديهم سياسة تثقيفية محددة للتعاطي مع التنمر السيبراني، مع التأكيد على وجود ضعف في تجهيز وإعداد



شكل (1): العلاقة بين الأمن السيبراني والمواطنة الرقمية في سياق متطلبات القرن الحادي والعشرين (NetSafe، 2018).

ويتضح من الشكل (1) أن المواطنة الرقمية تشكل مفهومًا محوريًا في سياق متطلبات القرن الحادي والعشرين؛ والمواطن الرقمي يمثل نقطة تقاطع بين العديد من المجالات الحيوية في

العصر الحالي. فالمواطن الرقمي يتحلى بالتنوّ الرقمي وهو متمكن من الكفايات الرقمية المتنوعة، ويمتلك مهارات الأمن السيبراني، كل هذا جنبًا إلى جنب مع إتقان المنهج الدراسي. وفي ذات السياق، يعد التنوّ الرقمي أو القدرة على الفهم والمشاركة الكاملة في العالم الرقمي عنصرًا أساسيًا للمواطنة الرقمية. وينطوي هذا التنوّ الرقمي على توليفة من المهارات الرقمية والاجتماعية التي تمكن الشخص من التمتع بالسلامة والأمن الرقمي في عصر المعلومات، كما أصبح إكساب المهارات المعرفية والأدائية للأمن السيبراني مهارة أساسية للمواطنة الرقمية، ولا غنى عنها للشخص حتى يكون متعلمًا واثقًا ومتصلًا، ومنخرطًا بشكل نشط، ومواطنًا رقميًا مدى الحياة (NetSafe، 2018).

وأصدرت منظمة اليونسكو تقريرين يحددان العناصر المهمة التي تلقي الضوء على العلاقة الوثيقة بين الأمن السيبراني والمواطنة الرقمية؛ التقرير الأول هو تعزيز المواطنة الرقمية من خلال الاستخدام الآمن والمسؤول لتقنيات الاتصالات والمعلومات، أما التقرير الثاني فاستبصارات حول المواطنة الرقمية والذي حدد محاور رئيسة للتعليم المرتبط بتقنيات الاتصالات والمعلومات؛ وتلك الموضوعات هي: الفوائد المترتبة على استخدام تقنيات الاتصالات والمعلومات، والمشاركة عبر

- 1- **تعلم (Learn):** يتعلم الطلاب تطوير سلوكيات إيجابية وأخلاقية في الفضاء السيبراني.
- 2- **وجه (Guide):** توفير مصادر تعلم مهني وأنشطة دروس للمعلمين لتدريس المواطنة الرقمية، ولتدشين ثقافة مدرسية إيجابية مواتية للمواطنة الرقمية.
- 3- **احم (Protect):** التقنيات، والبنية التحتية، والسياسات التي تضعها المدرسة لدعم تدشين بيئة تقنية تتمتع بالسلامة والأمن.

ب- نموذج الرفاه السيبراني المحسن (cyberwellness):
ويعد من النماذج التعليمية البارزة لترسيخ الأمن السيبراني في سياق المواطنة الرقمية، ويستند الإطار إلى مبدئين محوريين هما: احترام الذات والآخرين، والاستخدام الآمن والمسؤول، وهي عملية مؤلفة من ثلاث خطوات (اشعر، فكر، نفذ)، وتركز على تعزيز السلوكيات الإيجابية على المدى الطويل في الفضاء السيبراني، من خلال أفعال مسؤولة ومقدرة للمواطنة الرقمية (Zhou, et. al., 2016). ويُعد التعلم التطبيقي إحدى الإستراتيجيات الرئيسة المستخدمة في تعليم الطلاب كجانب من برنامج الرفاه السيبراني، ويتظافر الجهود المعنية في التعليم من المعلمين وأولياء الأمور. ويرتكز بصورة أساسية على تعزيز الهوية الرقمية للطالب، وترسيخ مبادئ المواطنة الرقمية في البيئة الإلكترونية، والقواعد السلوكية ذات الصلة باستخدام التقنية، ويتم تنفيذه من خلال خريطة تدريسية قائمة على المشروعات بمناقشة موضوعات أصيلة متعلقة بقيم الأمن السيبراني، وتتمثل أدوار المعلمين في تصميم الدروس الإرشادية التوجيهية بقيم الرفاه السيبراني، والتي يتم تعزيزها بشكل أكبر بالتعلم التطبيقي (Zhou, et. al., 2016).

ومن منطلق ما عكسته الدراسات وطرحته الأطر النظرية بالجمع بين المتغيرين الأمن السيبراني والمواطنة الرقمية والتي بينت العلاقة المتبادلة والفاعلة بين الأمن السيبراني والمواطنة الرقمية؛ حيث تمثل المواطنة الرقمية المظلة التي تنتمي لها تربية الفرد وتغذيته بالمبادئ والقيم والأخلاقيات والقوانين، ومعرفة حقوقه وواجباته عند استخدامه للتكنولوجيا وللتطبيقات الرقمية، أو خلال تعاملاته الرقمية وتواجهه في مواقع التواصل الاجتماعي، وهذه التوليفة التي من شأنها تحافظ على الطالب

الطلاب لتسليحهم بمهارات الأمن السيبراني اللازمة لمواجهة التنمر السيبراني. كما دعت (Tangen and Campbell 2010) إلى ضرورة الحد من تفاقم القضايا المتعلقة بالمخاطر السيبرانية بين الطلاب، سواء أكانت تنمرًا سيبرانيًا، أم إرسال محتوى غير لائق، أم غير ذلك من القضايا بين الطلاب، وإعداد تصور تعليمي مقترح للتوعية بالأمن السيبراني ومخاطرة. كما انتهت دراسة (Cantone et al. 2015) التجريبية التي هدفت إلى تقييم الاستجابة المجتمعية للتنمر السيبراني، وتوصلت النتيجة إلى تأثير اهتمام المؤسسة التعليمية من أكثر المداخل فعالية في الحد من سلوكيات الأمن السيبراني والوعي به.

ومما سبق ذكره؛ ينبغي أن يتم الاعتماد على برامج وخطط تربوية منظمة وهادفة لتحقيق الأمن السيبراني، وإكساب مهاراته المعرفية والأدائية للطلاب ضمن سياق المواطنة الرقمية، على أن يتم تركيز هذه البرامج على مدخل وقائي استباقي بتحقيق الأمن السيبراني استنادًا لمدخل المواطنة الرقمية.

ومن نماذج الأمن السيبراني في سياق المواطنة الرقمية، قدم "والش" وزملاءه (Walsh, Wallace & Ayling, 2020, Sondergeld) نموذجًا أو إطارًا شاملاً لأفضل ممارسات تعليم السلامة من الإنترنت وتحقيق الأمن السيبراني في ضوء المواطنة الرقمية للطلبة، وهي:

أ- نموذج "تعلم-وجه-احم" (The LEARN: GUIDE:) (PROTECT: FRAMEWORK)

في ظل الاستجابة للمتطلبات المتغيرة فيما يتعلق بالأمن السيبراني في المواطنة الرقمية، طورت مؤسسة "نيت سيف" (NetSafe Netsafe, 2018) نموذجًا جديدًا للأمن السيبراني أطلقت عليه نموذج "تعلم-وجه-احم"، ويتيح هذا النموذج للتربويين تدشين مسار تعلم مرتكز حول الطالب: يبدأ بيئة ذاتية للمتعلمين ومتعلقة بممارسات الأمن السيبراني، ويتألف هذا النموذج من ثلاثة مكونات هي: المهارات التي يتعلمها الطلاب ليحافظوا على سلامة أنفسهم؛ والتوجيه الذي يحصلون عليه ليتعلموا كيفية إدارة التحديات؛ وآليات الحماية الوقائية لتحسين السلامة من المخاطر السيبرانية، وخطوات تفسير النموذج كما يلي:

بجامعة أم القرى في الفصل الدراسي الثاني للعام الجامعي (1443هـ-2022م)، والبالغ عددهم (105) طالبة تبعًا للإحصائيات التي تم الحصول عليها من جامعة أم القرى. في حين أن عينة الدراسة التي تمثل جزءًا من مجتمع الدراسة؛ حيث تم أخذ عينة عشوائية قوامها (33) طالبة وهو عدد يمكن قبوله لعينة الدراسة، بعد أن تم استبعاد (1) طالبة بسبب انسحابها وعدم حضورها بالمقرر.

إجراءات الدراسة:

- مواد الدراسة وتصميمها: تتطلب الدراسة الحالية قياس فاعلية وحدة إلكترونية تفاعلية في تنمية مهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية. وقد قامت الباحثة ببناء مواد وأدوات الدراسة على النحو الآتي:

بناء قائمة بمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية: تهدف القائمة إلى تحديد مهارات الأمن السيبراني في ضوء المواطنة الرقمية، وتم بناء قائمة المهارات بالاطلاع والاستفادة من الأدب النظري والبحوث المتعلقة بالأمن الرقمي والمواطنة الرقمية، كدراسة (سليمان، 2021؛ والمنتشري، 1440؛ محمد، 2020؛ وفلاته، 2020؛ العمري وطالبة، 2020؛ والسبحان، 2020؛ National Cyber Security Awareness, 2020)، كما تم الاستفادة من رؤية المملكة العربية السعودية (2030)؛ الإستراتيجية الوطنية للأمن السيبراني 2021-2017م. وتم التوصل لقائمة مهارات الأمن السيبراني وفق محددات المواطنة الرقمية والمكونة من ثلاثة محاور رئيسة هي: التعليم، الحماية، الاحترام، وتضم فيها تسعة أبعاد فرعية، موزعة كما في الجدول التالي:

جدول (1): قائمة مهارات الأمن السيبراني وفق محددات المواطنة الرقمية.

عدد المهارات	المحور الفرعي	البعد الرئيس
14	الثقافة الرقمية الاتصالات الرقمية التجارة الرقمية الوصول الرقمي	التعليم
12	قواعد السلوك الرقمي القوانين الرقمية	الاحترام
15	الحقوق والمسؤوليات الصحة والرفاهية الرقمية	الحماية

وتضمن له الاستخدام الرقمي الآمن للإنترنت، ومواجهة الاعتراضات السيبرانية بأخذ التدابير والاحتياطات من مخاطرها بالتعلم والممارسة العملية.

فرضيات الدراسة:

- 1- لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسطي درجات مجموعة الدراسة في التطبيق القبلي والبعدي للاختبار المعرفي لمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية.
- 2- لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسطي درجات مجموعة الدراسة في التطبيق القبلي والبعدي لبطاقة ملاحظة الجوانب الأدائية لمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية.
- 3- لا توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين مقدار النمو في الجانب المعرفي والجانب الأدائي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية.

منهجية الدراسة:

لغرض الدراسة الحالية أُعتمد المنهج الوصفي التحليلي (Analytical Descriptive Methodology) من خلال عرض أدبيات الدراسة وإعداد قائمة مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية، وبناء الوحدة الإلكترونية التفاعلية المقترحة، كما استخدمت المنهج التجريبي ذا التصميم شبه التجريبي (Quasi- Experimental Methodology)، واستخدم في هذا المنهج التصميم تصميم المجموعة الواحدة ذي الاختبار القبلي/البعدي (One-group pre-/post-test design)، بتطبيقه على العينة التي تمثل المجموعة التجريبية؛ وتطبيق أدوات الدراسة قبليًا على العينة، ومن ثم تُعرض للمتغير التجريبي، وهو دراسة الوحدة الإلكترونية التفاعلية في توظيف مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية، ثم تطبيق أدوات الدراسة بعددًا؛ ليكون الفرق في استجابات العينة على الاختبار القبلي والبعدي ناتجًا عن تأثيرها بالمتغير التجريبي.

مجتمع الدراسة وعينتها:

شمل المجتمع جميع طلبة قسم الخدمة الاجتماعية الذين يدرسون مقرر التدريب الميداني (2) بالكلية الجامعية بالليث

البعد الرئيس	المحور الفرعي	عدد المهارات
	الأمن الرقمي	
	المجموع	41

الجندي وطه (2019)، وعند النظر إلى تنمية هذه المهارات لدى الطلبة الجامعيين، فإن ذلك ادعى للدراسة والبحث؛ لذا كان اهتمام الدراسة الحالية تقدير مدى الحاجة إليه من خلال استطلاع آراء بعض خبراء في الميدان، والتي جاءت آراؤهم موافقة ومؤيدة لأهمية إجراء هذه البحوث التي تهدف إلى التوعية بمهارات الأمن السيبراني، وإلى تصحيح الكثير من المفاهيم واتخاذ القرار حيال المواقف التي تتعرض لها والأخطاء التي يتم الوقوع فيها والتي تتعلق بمفاهيم مهارات الأمن السيبراني، وبالأخص في ظل الهجمات التقنية المستمرة وكيف التصرف في هذه المواقف التي قد يقع فيها طالبات المرحلة الجامعية.

- تحديد خصائص المتعلمين وخلفياتهم: عينة الدراسة الحالية من طالبات المرحلة الجامعية، وقد تم تحديد سلوكيات الطالبات من خلال عدة لقاءات ونقاشات عقدتها الباحثة أثناء تدريسيهن بعرض عدد من المواقف المتعلقة بمهارات الأمن السيبراني، وذلك قبل بدء التجربة التي أكدت إلى الحاجة الماسة للتوعية لمثل هذه الموضوعات.

- تحديد الموارد والقيود التعليمية: تم تحديد الموارد التعليمية التي تشتمل على البرامج والأجهزة والبرمجيات التي تستخدم في تصميم الوحدة الإلكترونية التفاعلية، وتطوير عناصرها الأساسية والفرعية. والتي تتمثل في توافر الأجهزة لدى جميع الطالبات، مع وجود الروابط التفاعلية، وتم بناء الوحدة الإلكترونية التفاعلية وإخراجها بواسطة برنامج (Storyline Articulate) لتصميم الدروس التفاعلية، كما أنه تم الاعتماد على حزمة التطبيقات المجانية، وتم تحميل ومشاركة ملفات التعلم للعينة، كما تم إدراج الوسائط الرقمية المتمثلة في الصور، والإنفوجرافيك، ومقاطع الفيديو، والمؤثرات الصوتية والحركية، كما تم الاستعانة ببعض مقاطع الفيديو المتوفرة على موقع الأكاديمية الوطنية للأمن السيبراني وهيئة الاتصالات وتقنية المعلومات بالمملكة العربية السعودية.

- المنصات ووسائل التواصل: تم الاستفادة من نظام إدارة التعلم الإلكتروني (Blackboard) وكافة أدواته لإرسال روابط محتوى الوحدة الإلكترونية التفاعلية، كما تم الاستفادة من تطبيق (Webex) كمنصة لإجراء بعض الاجتماعات

وتم التأكد من صدق قائمة المهارات وذلك من خلال عرضها على (8) من أعضاء الهيئة التدريسية ذوي الخبرة والاختصاص في المملكة العربية السعودية؛ وذلك بهدف استطلاع آرائهم حول قائمة المهارات، وتم التعديل في ضوء توجيهات السادة المحكمين، وبذلك تم الحصول على النسخة النهائية من قائمة مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية.

تصميم الوحدة الإلكترونية التفاعلية: وهي تمثل مادة المعالجة التجريبية في الدراسة الحالية في تصميم وحدة إلكترونية تفاعلية في: "مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية"، ولإعدادها تم الاطلاع على الأدبيات السابقة المتعلقة بتصميم الوحدات الإلكترونية للاستفادة منها في تصميم الوحدة الإلكترونية التفاعلية الحالية (عزمي، 2015) و(سليمان، 2021)، وتمت إجراءات المعالجة التجريبية بتبني نموذج (A.D.D.I.E) لتصميم التعليمي لبناء الوحدة الإلكترونية التفاعلية لتوظيف مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية؛ نظراً لقابلية النموذج وشموليته لمراحل إنتاج تفاعلات الوحدة الإلكترونية والأدوات التعليمية، وذلك باتباع المراحل التالية:

المرحلة الأولى:- مرحلة التحليل (Analysis Phase): في هذه المرحلة تم تحديد الهدف العام والمتمثل في الحاجة إلى تصميم وحدة إلكترونية تفاعلية تعتمد على أدوات التعلم الإلكترونية التفاعلية والمتنوعة، وقياس أثرها في تنمية مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية؛ وتتضمن هذه المرحلة عددًا من الخطوات تتمثل فيما يلي:

- تقدير الاحتياجات: في هذه الخطوة يتم معالجة أوجه النقص وتحليل خبرات المتعلمين لتحقيق المطلب الأساسي بتنمية مهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية، كما أنه التوجه نحو تنمية مهارات الأمن السيبراني كما دعت إليه الوثيقة الوطنية الأمريكية للوعي بالأمن السيبراني (National Cyber Security Awareness, 2020)، ورؤية المملكة العربية السعودية 2030، ودراسة

الخطوة الثانية: تصميم المحتوى الإلكتروني ومكوناته، وتتمثل في: إخراج المحتوى التعليمي التفاعلي وتصميم الأنشطة ومهام التعلم الإلكتروني التفاعلي، وتصميم واجهات التفاعل والوسائط الإلكترونية المتنوعة لعرض المحتوى التفاعلي، مع تحديد الإمكانيات المادية وبرامج التصميم والإنتاج، وتحديد وتصميم أدوات التقييم التكويني والنهائي. كما تم ترتيب إخراج المحتوى التفاعلي بالبداية بعرض أهمية دراسة الوحدة الإلكترونية، عرض الأهداف الإجرائية للوحدة الإلكترونية، التقييم القبلي لمحتوى الوحدة الإلكترونية، عرض المحتوى التفاعلي والأنشطة المصاحبة، التقييم التكويني لمحتوى الوحدة الإلكترونية، والتقييم البعدي لمحتوى الوحدة الإلكترونية، وأخيراً ملاحق الوحدة الإلكترونية التي تتضمن روابط إثرائية والمراجع والمصادر المستخدمة.

الخطوة الثالثة: تصميم أدوات القياس، والمتمثلة في الاختبار المعرفي وبطاقة الملاحظة لقياس مهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية.

المرحلة الثالثة:- التطوير (Development Phase): في هذه المرحلة تم الانتقال من مخرجات مرحلة التصميم التي تشمل المخططات والمسودات المبدئية إلى مواد تعليمية حقيقية، حيث تم تحديد عناصر المحتوى والخبرات الخاصة بعمليات التعلم التي ستلقاها الطالبة أثناء تعلمها لإتمام كافة المهمات التعليمية، والتي تمت من خلال توفير وإنتاج عناصر الوحدة الإلكترونية، حيث تم الاستفادة من بعض عناصر التعلم الرقمية وبعض ملفات الفيديو المرتبطة بموضوعات وأهداف التعلم، إلى جانب تصميم وإنتاج بعضها ليلائم طرح موضوعات الوحدة وتحقيق أهدافها، والتي صممت ببرنامج (Articulate Storyline) لتصميم محتوى الوحدة الإلكتروني التفاعلي، وتم تضمين عدد من الروابط والملفات الخاصة لطرح موضوعات مهارات الأمن السيبراني، والتي تتطلب إتقان جانب مهاري لموضوعات التعلم، وحث الطالبات على أهمية التمكن من مهارات الأمن السيبراني بعد دراسة الوحدة.

المرحلة الرابعة:- التنفيذ أو التطبيق (Implementation Phase): في هذه المرحلة يتم تطبيق كافة الخطوات في مرحلة التطوير على الواقع تمهيداً للتنفيذ؛ وذلك باتخاذ الموافقات

بالبطبات والنقاش التزامني والتفاعل والتواصل وارسال الروابط، والرد على الاستفسارات المتعلقة بموضوعات الوحدة الإلكترونية التفاعلية.

- تحديد المهام الخاصة بالوحدة الإلكترونية التفاعلية المقترحة: تحديد المهام الخاصة بعمليات التعلم تُعد من الخطوات المهمة في عملية التصميم، حيث تمثل تلك المهام مخرجات التعلم المتوقعة من بعد دراسة محتوى الوحدة، وقد تم إعداد قائمة المهارات الخاصة بمهارات ومهام التعلم المطلوب إنجازها بعد مراجعة الأطر النظرية والدراسات والبحوث المرتبطة بمجالات تنمية مهارات الأمن السيبراني، في ضوء محددات المواطنة الرقمية لدى الطلبة الجامعيين، وقد تم التوصل إلى المهارات الأساسية في الأمن السيبراني اللازم توظيفها في ضوء محددات المواطنة الرقمية؛ وهي وفق ثلاثة أبعاد أساسية (التعليم-الاحترام-الحماية)، كما تم تحديد المهارات الفرعية التي تنبثق من تلك المهارات الرئيسة في عدد (40) مهارة فرعية، وذلك بعد ضبط وتحكيم هذه المهارات من الخبراء، لتصبح القائمة جاهزة للاستعانة بها في تصميم وبناء الوحدة الإلكترونية المقترحة.

المرحلة الثانية:- مرحلة التصميم (Design Phase): هذه المرحلة ترجمة مخرجات مرحلة التحليل إلى خطوات قابلة للتنفيذ بصورتها الأولية، والتي تهدف إلى العديد من الإجراءات، تتمثل في صياغة الأهداف الرئيسة والواجب تحقيقها من دراسة كل موضوع من موضوعات الوحدة الإلكترونية التفاعلية، ومراجعتها من خلال تحكيم الخبراء وضبط الأهداف؛ حيث تم صياغة الأهداف الإجرائية عند مستوى (التطبيق، التحليل، التركيب، التقييم) لموضوعات مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية، إلى جانب إعداد الشروط والمواصفات الخاصة بتصميم وإنتاج الوحدة الإلكترونية التفاعلية من حيث عناصر المحتوى والوسائط المتعددة وروابط الإنجاز داخل الوحدة، وأشكال الأنشطة وأساليب التقييم. ويندرج تحت مرحلة التصميم للوحدة الإلكترونية التفاعلية الخطوات التالية:

الخطوة الأولى: تصميم بيئة النظام، وتصميم التفاعلات.

ضوء تحليل محتوى موضوعات الأمن السيبراني في ضوء محددات المواطنة الرقمية وذلك تبعاً للآتي:

أولاً: بناء الاختبار المعرفي لقياس مهارات الأمن السيبراني والتحقق من صدقها وثباتها:

1- تحديد الهدف من الاختبار المعرفي: يهدف هذا الاختبار إلى قياس مستوى التحصيل المعرفي في المستويات (التطبيق، التحليل، التركيب، التقويم) لدى طالبات قسم الخدمة الاجتماعية بجامعة أم القرى في مقر التدريب الميداني (2).

2- تحديد نوع مفردات الاختبار التحصيلي وصياغتها: بعد الاطلاع على أنواع الاختبارات في الأطر النظرية والرجوع إلى الأدب النظري اقتضى تحديد الاختبار الموضوعي ذي الاختيارات من متعدد من بين البدائل المتنوعة؛ لدقتها وفعاليتها، وتم صياغتها في نسختها الأولية والتي اشتملت على (45) سؤالاً.

3- وضع نظام تقدير الدرجات وإعداد جدول المواصفات: وُضع تقدير الدرجات في الاختبار التحصيلي حيث تُعطي درجة (1) للإجابة الصحيحة عن السؤال، ودرجة (صفر) في حالة الإجابة الخاطئة، حيث كانت الدرجة الكلية للاختبار (45). كما تم إعداد جدول المواصفات الذي يمثل بعدين: الأول محتوى الوحدة للموضوعات ذات الصلة، والآخر يمثل مخرجات التعلم المرتبطة بالموضوعات. وتم تحديد المواصفات لبناء الاختبار وصياغة الأهداف الإجرائية عند مستويات (التطبيق، التحليل، التركيب، التقويم) لمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية.

4- صدق الاختبار: تم التحقق من صدق الاختبار بالطرق التالية:

1- الصدق الظاهري للاختبار التحصيلي (Referee Validity): تم عرض الاختبار التحصيلي في صورته الأولية على (8) من الخبراء في المجال؛ وذلك بهدف تحكيم الاختبار وفقاً لمدى وضوح تعليمات الاختبار وارتباط المفردات بالأبعاد والأهداف الموضوعية ومدى دقتها العلمية وكفايتها

الرسمية وتنفيذ الإجراءات الإدارية اللازمة لتطبيق الدراسة، ومن ثم تم عقد لقاءات مباشرة مع عينة الدراسة، وتضمنت هذه اللقاءات مقدمة تمهيدية عن فكرة الدراسة وأهدافها ومهام التعلم من الوحدة الإلكترونية التفاعلية، والتي تركز على اكتساب مهارات الأمن السيبراني لفئة التعليم الجامعي.

المرحلة الخامسة:- التقويم (Evaluation Phase): في هذه المرحلة يتم التقويم البنائي للوحدة الإلكترونية، فقد اعتمد على التجريب المبدئي بعرض واختبار المحتوى الخاص بالوحدة الإلكترونية التفاعلية على مجموعة من أساتذة الجامعات الخبراء أكاديمياً وتقنياً وتربوياً؛ بهدف الفحص وإبداء الرأي وإجراء التعديلات، واختبار الروابط وكافة عناصر المحتوى الرقمي التفاعلي التي تتضمنها، وقد تم تجريب الوحدة الإلكترونية مبدئياً بهدف إجراء التعديلات النهائية بهدف تطويرها والتحقق من مناسبتها لأهداف تصميمها، ومن ثم الانتقال إلى التقويم النهائي بعرض نتائج التجربة.

الهدف العام	الهدف الخاص
1	الأهداف الإجرائية
2	تمهيد
3	الطرق والمسؤوليات الرقمية
4	الصحة والسلامة الرقمية
5	الثقة وسعر الآلية الرقمية
6	اعتمادات الرقمية والخدمة الرقمية

شكل (2): نموذج للوحدة الإلكترونية التفاعلية.

أدوات قياس الدراسة: تم بناء وإعداد أدوات جمع البيانات؛ كما هو موضح في الآتي:

أولاً: بناء الاختبار المعرفي لقياس مهارات الأمن السيبراني والتحقق من صدقها وثباتها: تم مراجعة العديد من الأدبيات والدراسات التي تناولت بناء الاختبار التحصيلي، ومنها دراسة (العلوان، 2021؛ السليماني وبلهيش، 2021؛ الشهراني، 2020؛ الأحدي، 2020؛ هاشم، 2020؛ المنتشري ووطاني، 2019؛ الجندي ووطه، 2019؛ الملحم، 2018؛ التخينة والسفاسفة، 2017؛ الهيئة الوطنية للأمن السيبراني، 2018؛ National Cyber Security Awareness, 2020)، وتم بناء الاختبار المعرفي لقياس مهارات الأمن السيبراني في

معامل الارتباط بالدرجة الكلية	معامل الارتباط بالمجال	أبعاد الاختبار	مجالات الاختبار
0.703			
**			

الدرجة الكلية للمجال الثالث: الحماية

** دال عند مستوى (0.01)، * دال عند مستوى (0.05)

يتبين من الجدول (2) أن معاملات ارتباط أبعاد الاختبار بالمجالات التي تمثلها تراوحت ما بين (-0.685-0.844)، ومعاملات ارتباطها بالدرجة الكلية للاختبار تراوحت ما بين (0.627-0.829)، وكانت هذه القيم دالة إحصائياً عند مستوى الدلالة (0.01)، مما يؤكد على أن أبعاد الاختبار المعرفي تتمتع بدرجة كبيرة من الصدق الداخلي. كما أن معاملات ارتباط مجالات الاختبار المعرفي بدرجة الكلية تراوحت ما بين (0.703-0.837)، وكانت هذه القيم دالة إحصائياً عند مستوى الدلالة (0.01)، مما يؤكد على أن مجالات الاختبار المعرفي تتمتع بدرجة كبيرة من الصدق الداخلي.

ثبات الاختبار (Test Reliability): وتم التحقق من ثبات الاختبار بطريقتين وهما: - الثبات بطريقة ألفا كرونباخ (Alpha Cronbach's): تم استخدام معامل "ألفا-كرونباخ" لحساب معاملات الثبات للمحاور وللدرجة الكلية للاختبار التحصيلي، أما الطريقة الثانية فالثبات بطريقة التجزئة النصفية: حيث تم تجزئة فقرات الاختبار إلى نصفين؛ الفقرات الفردية في مقابل الفقرات الزوجية، ثم استخدمت معامل ارتباط "بيرسون" في حساب الارتباط بين درجات النصفين، وتم تصحيح الطول باستخدام معادلة "سبيرمان براون"، وجاءت النتائج كما يوضح الجدول التالي:

جدول (3): نتائج ثبات الاختبار المعرفي لمهارات الأمن السيبراني

مجالات الاختبار	أبعاد الاختبار	الثبات بالدرجة الكلية	الثبات كرونباخ
المجال الأول: التعليم	البعد الأول: الاتصالات الرقمية	0.803	0.825
	البعد الثاني: التجارة الإلكترونية	0.827	0.806
المجال الثاني: الاحترام	البعد الثالث: الثقافة ومحو الأمية الرقمية	0.792	0.783
	البعد الرابع: الوصول الرقمي	0.819	0.832

وصحتها اللغوية، وملاءمة البدائل الأربعة المقترحة لكل سؤال وملاءمة نظام تقدير الدرجات.

وقد تم تعديل بعض الصياغة اللغوية لبعض فقرات الاختبار لتصبح أكثر وضوحاً، وتعديل البدائل لبعض الفقرات، ومراجعة تعديلات الاختبار أصبحت الصورة النهائية من الاختبار (45) مفردة، وبذلك أصبح الاختبار صالحاً للتطبيق على عينة الدراسة.

2- صدق الاتساق الداخلي (Internal Consistency Validity):

تم التحقق من الصدق الداخلي للاختبار التحصيلي بتطبيقه على عينة استطلاعية قوامها (25) طالبة وخارج العينة الأساسية للبحث. وتم حساب معامل ارتباط "بيرسون" بين درجة كل عبارة والدرجة الكلية، وأظهرت النتائج ما يلي:

جدول (2): نتائج صدق الاتساق الداخلي لأبعاد ومجالات الاختبار المعرفي لمهارات الأمن السيبراني.

معامل الارتباط بالدرجة الكلية	معامل الارتباط بالمجال	أبعاد الاختبار	مجالات الاختبار
0.741	0.763	البعد الأول: الاتصالات الرقمية	المجال الأول: التعليم
**	**	البعد الثاني: التجارة الإلكترونية	
0.708	0.729	البعد الثالث: الثقافة ومحو الأمية الرقمية	
0.627	0.685	البعد الرابع: الوصول الرقمي	
0.754			الدرجة الكلية للمجال الأول: التعليم
**			
0.829	0.844	البعد الرابع: الوصول الرقمي	المجال الثاني: الاحترام
**	**	البعد الخامس: القوانين الرقمية	
0.694	0.708	البعد السادس: اللياقة الرقمية	
0.721	0.763	البعد السابع: الحقوق والمسؤوليات الرقمية	المجال الثالث: الحماية
**	**	البعد الثامن: الصحة والسلامة الرقمية	
0.837			الدرجة الكلية للمجال الثاني: الاحترام
**			
0.772	0.754	البعد التاسع: إجراءات ضمان الوقاية والحماية الرقمية	المجال الثالث: الحماية
**	**	البعد العاشر: إجراءات ضمان الوقاية والحماية الرقمية	
0.818	0.831	البعد الحادي عشر: إجراءات ضمان الوقاية والحماية الرقمية	
**	**	البعد الثاني عشر: إجراءات ضمان الوقاية والحماية الرقمية	
0.683	0.698	البعد الثالث عشر: إجراءات ضمان الوقاية والحماية الرقمية	
**	**	البعد الرابع عشر: إجراءات ضمان الوقاية والحماية الرقمية	

والتقويم، وعلى ذلك فقد تم قبول جميع فقرات الاختبار المعرفي من حيث درجة التمييز.

حساب زمن الاختبار: وتم حساب زمن الاختبار، وذلك بحساب زمن كل طالبة من طالبات العينة الاستطلاعية للإجابة عن أسئلة الاختبار، ثم حساب متوسط زمن الإجابة، وقد بلغ متوسط زمن تطبيق الاختبار (60) دقيقة، ومن ثم أصبح الاختبار صالحًا للتحقق من فرضيات الدراسة.

الصورة النهائية للاختبار التحصيلي: اشتملت فقرات الاختبار على (45) سؤالاً بعد التأكد من صدق الاختبار وثباته، والتحقق من مناسبة مفرداته من حيث معاملي السهولة والتمييز، وأصبح الاختبار في صورته النهائية صالحًا للتطبيق ملحق (1).

ثانياً: بناء بطاقة الملاحظة لقياس مهارات الأمن السيبراني والتحقق من صدقها وثباتها: تم بناء بطاقة الملاحظة لمهارات الأمن السيبراني: وتم اشتقاقها من مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية بعد الاطلاع على الأطر النظرية والدراسات السابقة التي أسهمت في بناء قائمة مهارات الأمن السيبراني (العلوان، 2021؛ السليماني وبلهيش، 2021؛ الشهراني، 2020؛ الأحمد، 2020؛ هاشم، 2020؛ المنتشري وفطاني، 2019؛ الجندي وطه، 2019؛ الملحم، 2018؛ التخينة والسفاسفة، 2017؛ الهيئة الوطنية للأمن السيبراني، 2018) حيث تكونت بطاقة الملاحظة من (40) مفردة، ثم تم التحقق من صدقها وثباتها على النحو الآتي:

صدق بطاقة الملاحظة لمهارات الأمن السيبراني: تم عرض الصورة الأولية من قائمة المهارات على (8) من المحكمين ذوي الخبرة والاختصاص؛ وذلك للتحقق من صدق قائمة المهارات، ومدى وضوح صياغتها، ومدى صلاحيتها وانتمائها للمحور، ومناسبتها لأهداف الدراسة، وقد اتفق بعض المحكمين بحذف المفردات رقم (4) و(7) لتكرارها وتداخلها مع مفردات (2) و(13)، وعدم ارتباطها بالمحور الذي تنتمي إليه، وتم التعديل بناءً على آراء المحكمين، وقد اتفقت آراء المحكمين على دقة وشمولية مفردات قائمة مهارات الأمن السيبراني. وعلى ذلك أصبحت الصورة النهائية للبطاقة تتكون من (3) أبعاد رئيسة و(40) مهارة فرعية.

مجموعات الاختبار	أبعاد الاختبار	الثبات	الثبات
		بالفا	بالنجزئة
		كروناخ	النصفية
الاحترام	البعد الخامس: القوانين الرقمية	0.843	0.825
	البعد السادس: اللياقة الرقمية	0.851	0.841
	الدرجة الكلية للمجال الثاني: الاحترام	0.872	0.882
	البعد السابع: الحقوق والمسؤوليات الرقمية	0.794	0.790
المجال الثالث: الحماية	البعد الثامن: الصحة والسلامة الرقمية	0.862	0.853
	البعد التاسع: إجراءات ضمان الوقاية والحماية الرقمية	0.854	0.839
	الدرجة الكلية للمجال الثالث: الحماية	0.849	0.866
	الدرجة الكلية للاختبار	0.921	0.907

يتضح من الجدول (3) أن معاملات ثبات أبعاد الاختبار بطريقة "ألفا-كروناخ" تراوحت ما بين (0.792-0.862)، وبطريقة التجزئة النصفية تراوحت ما بين (0.783-0.853)، وتؤكد هذه القيم على أن أبعاد الاختبار تتمتع بدرجة مرتفعة من الثبات. كما أن معاملات ثبات مجالات الاختبار بطريقة "ألفا-كروناخ" تراوحت ما بين (0.849-0.872)، وبطريقة التجزئة النصفية تراوحت ما بين (0.847-0.882)، وتؤكد هذه القيم على أن مجالات الاختبار تتمتع بدرجة مرتفعة من الثبات. في حين معامل الثبات العام للاختبار بطريقة "ألفا كروناخ" بلغ (0.921)، وبطريقة التجزئة النصفية بلغ (0.907)، وتؤكد هذه القيم على أن الاختبار المعرفي ككل يتمتع بدرجة مرتفعة من الثبات.

تحليل فقرات الاختبار المعرفي: تم تحليل درجات العينة الاستطلاعية على الاختبار المعرفي بهدف حساب معاملات الصعوبة والتمييز لكل فقرة من فقرات الاختبار، وقد جاءت النتائج كما يلي:

1- **معاملات الصعوبة:** تراوحت ما بين (0.36-0.72)، وهي قيم تقع في المستوى المقبول في مجال القياس والتقويم، وعلى ذلك فقد تم قبول جميع فقرات الاختبار المعرفي من حيث درجة الصعوبة.

3- **معاملات التمييز:** تراوحت ما بين (0.29-0.86)، وهي قيم تقع في المستوى المقبول في مجال القياس

0.843	0.854	المجال الثاني: الاحترام
0.865	0.873	المجال الثالث: الحماية
0.892	0.908	الدرجة الكلية

يتضح من الجدول (5) السابق أن معاملات ثبات مجالات البطاقة بطريقة "ألفا-كرونباخ" تراوحت ما بين (0.854-0.892)، وبطريقة التجزئة النصفية تراوحت ما بين (0.843-0.876)، وتؤكد هذه القيم على أن مجالات بطاقة الملاحظة تتمتع بدرجة مرتفعة من الثبات. في حين أن معامل الثبات العام للبطاقة بطريقة "ألفا-كرونباخ" بلغ (0.908)، وبطريقة التجزئة النصفية بلغ (0.892)، وتؤكد هذه القيم على أن بطاقة الملاحظة ككل تتمتع بدرجة مرتفعة من الثبات. كما تم التحقق من الثبات بطريقة اتفانق الملاحظين: (Observers' agreement) بالاشتراك، فقد اشتركت الباحثة مع زميلة لها في ملاحظة مهارات الأمن السيبراني لعدد (10) طلبة من المشاركين في العينة الاستطلاعية، وسجل كل منهما ملاحظاته في ضوء مؤشرات البطاقة، وتم استخدام معادلة كوبر (Cooper) لحساب نسبة الاتفاق بين الملاحظين، وقد بلغ معامل الاتفاق العام (94.6%)، وتؤكد هذه القيمة على أن بطاقة الملاحظة تتمتع بدرجة مرتفعة من الثبات ملحق (2).

- نتائج الدراسة تحليلها وتفسيرها ومناقشتها

النتائج المتعلقة بالإجابة عن السؤال الذي ينص على: "ما فاعلية وحدة إلكترونية تفاعلية في تنمية الجانب المعرفي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية؟" وللإجابة عن السؤال، تم اختبار صحة الفرض الأول الذي ينص على: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسطي درجات مجموعة الدراسة في التطبيق القبلي والبعدي للاختبار المعرفي لمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية".

ولاختبار صحة الفرض الأول للدراسة، تم استخدام اختبار "ت" للمجموعات المرتبطة (Paired Samples T-test)؛ للتعرف على دلالة الفروق بين متوسطي درجات عينة الدراسة في التطبيق القبلي والبعدي للاختبار المعرفي لمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية، وللتأكد من فاعلية الوحدة الإلكترونية التفاعلية في تنمية

صدق بطاقة الملاحظة لمهارات الأمن السيبراني (Referee Validity)

: يتم تقدير صدق البطاقة بطريقتين: أولها الصدق الظاهري: ويقصد به المظهر العام للبطاقة من حيث نوع المفردات وكيفية صياغتها ووضوحها ووضوح تعليماتها ومدى دقتها، وتم عرضها على (8) محكمين، وقد اقتصر ملاحظات المحكمين بتعديل الصياغة اللغوية لبعض الفقرات، كما تم إعادة ترتيب بعض المهارات الفرعية وأجمع المحكمون على عدم حذف فقرات من البطاقة، وبذلك تم الحصول على الصورة النهائية من بطاقة الملاحظة. كما تم التحقق من صدق بطاقة الملاحظة بالاتساق الداخلي (Internal Consistency Validity): وتم التحقق من الصدق الداخلي لبطاقة ملاحظة مهارات الأمن السيبراني، بتطبيقها على عينة استطلاعية قوامها (25) طالبة من خارج العينة الأساسية للبحث. وتم حساب معامل ارتباط "بيرسون" بين درجة كل عبارة والدرجة الكلية للبطاقة؛ كما يتبين في الجداول (4):

جدول (4): نتائج صدق الاتساق الداخلي لمجالات بطاقة الملاحظة (ن=25)

مجالات بطاقة الملاحظة	معامل الارتباط	الدلالة الإحصائية
المجال الأول: التعليم	0.849	دال عند 0.01
المجال الثاني: الاحترام	0.769	دال عند 0.01
المجال الثالث: الحماية	0.803	دال عند 0.01

يتبين من الجدول (4) أن معاملات ارتباط مجالات البطاقة بدرجة الكلية تراوحت ما بين (0.769-0.849)، وكانت هذه القيم دالة إحصائياً عند مستوى الدلالة (0.01)، مما يؤكد على أن مجالات بطاقة الملاحظة تتمتع بدرجة كبيرة من الصدق الداخلي.

ثبات بطاقة ملاحظة لمهارات الأمن السيبراني: تم التأكد من ثبات بطاقة الملاحظة من خلال حساب معامل "ألفا كرونباخ" (Alpha Cronbach's)، واستخدمت طريقة التجزئة النصفية (Split-Half Method) لحساب الثبات، وجاءت النتائج كما يعرض الجدول التالي:

جدول (5): نتائج ثبات بطاقة الملاحظة (ن=25)

مجالات بطاقة الملاحظة	ألفا كرونباخ	التجزئة النصفية
المجال الأول: التعليم	0.892	0.876

$$MG_{Blake} = \frac{M_2 - M_1}{P - M_1} + \frac{M_2 - M_1}{P}$$

كما يظهر الجدول الآتي:

الجانب المعرفي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية، تم استخدام معادلة "بلاك" Modified Blake's () لحساب نسبة الكسب المعدلة "بلاك" (Gain Ratio)، وتم حسابها وفق المعادلة:

جدول (6): نسبة الكسب المعدلة ل Blake لفاعلية وحدة إلكترونية تفاعلية في تنمية الجانب المعرفي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية.

مجمالات الاختبار	أبعاد الاختبار	المتوسط القبلي	المتوسط البعدي	النهاية العظمى	درجة الكسب	نسبة الكسب المعدلة
المجال الأول: التعليم	البعد الأول: الاتصالات الرقمية	1.52	4.55	5	3.03	1.48
	البعد الثاني: التجارة الإلكترونية	1.36	4.58	5	3.22	1.53
	البعد الثالث: الثقافة ومحو الأمية الرقمية	1.48	4.39	5	2.91	1.41
	الدرجة الكلية للمجال الأول: التعليم	4.36	13.52	15	9.16	1.47
المجال الثاني: الاحترام	البعد الرابع: الوصول الرقمي	1.12	4.45	5	3.33	1.52
	البعد الخامس: القوانين الرقمية	0.88	4.21	5	3.33	1.47
	البعد السادس: اللياقة الرقمية	1.12	4.06	5	2.94	1.35
	الدرجة الكلية للمجال الثاني: الاحترام	3.12	12.73	15	9.61	1.45
المجال الثالث: الحماية	البعد السابع: الحقوق والمسؤوليات الرقمية	1.09	4.70	5	3.61	1.65
	البعد الثامن: الصحة والسلامة الرقمية	1.03	4.88	5	3.85	1.74
	البعد التاسع: إجراءات ضمان الوقاية والحماية الرقمية	1.06	4.82	5	3.76	1.71
	الدرجة الكلية للمجال الثالث: الحماية	3.18	14.39	15	11.21	1.70
	الدرجة الكلية للاختبار	10.67	40.64	45	29.97	1.54

* درجة الكسب = (متوسط التطبيق البعدي - متوسط التطبيق القبلي)

الحقوق والمسؤوليات الرقمية، الصحة والسلامة الرقمية، إجراءات ضمان الوقاية والحماية الرقمية) لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية. ويمكن تفسير فاعلية الوحدة الإلكترونية في تنمية الجانب المعرفي لدى الطلبة والمرتبطة بمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية للعديد من الاعتبارات منها: تفاعل الطالبات وحماهن لتعلم محتوى الأمن السيبراني نظرًا للمواقف التقنية اليومية التي يتم التعرض لها بشكل مستمر، ومن المجالات المستجدة حيث إن أي جهاز حاسب أو هاتف متصل

يتبين من الجدول (6) أن قيم نسبة الكسب لمعادلة "بلاك" بلغت على الترتيب (1.74)، (1.71)، (1.70)، (1.65)، (1.54)، (1.53)، (1.52)، (1.48)، (1.47)، (1.45)، (1.41)، (1.35)، مما يؤكد على فاعلية الوحدة الإلكترونية التفاعلية في تنمية الجانب المعرفي لمهارات الأمن السيبراني كدرجة كلية، وكمجالات فرعية: (مجال التعليم، مجال الاحترام، مجال الحماية)، وكأبعاد فرعية: (الاتصالات الرقمية، التجارة الإلكترونية، الثقافة ومحو الأمية الرقمية، الوصول الرقمي، القوانين الرقمية، اللياقة الرقمية،

(T.test)، للتعرف على دلالة الفروق بين متوسطي درجات طالبات مجموعة الدراسة في التطبيق القبلي والبعدى لبطاقة ملاحظة الجانب الأدائي لمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية، وللتأكد من فاعلية الوحدة الإلكترونية التفاعلية في تنمية الجانب الأدائي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية، تم استخدام معادلة "بلاك" لحساب نسبة الكسب المعدلة ل "بلاك" (Modified Blake's Gain Ratio)، وجاءت النتائج كما يظهر الجدول الآتي:

جدول (7): نسبة الكسب المعدلة ل Blake لفاعلية الوحدة الإلكترونية التفاعلية في تنمية الجانب الأدائي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية.

مجمالات بطاقة الملاحظة	المتوسط القبلي	المتوسط البعدى	النهاية العظمى	درجة الكسب	نسبة الكسب المعدلة
المجال الأول: التعليم	4.09	23.58	26	19.49	1.64
المجال الثاني: الاحترام	5.15	23.91	26	18.76	1.62
المجال الثالث: الحماية	3.12	23.76	26	20.64	1.69
الدرجة الكلية لطاقة الملاحظة	12.36	71.24	78	58.88	1.65

* درجة الكسب = (متوسط التطبيق البعدى - متوسط التطبيق القبلي)

يتبين من الجدول (7) أن الوحدة الإلكترونية التفاعلية ذات فاعلية في تنمية الجانب الأدائي لمهارات الأمن السيبراني كدرجة كلية، وكمجالات فرعية: (مجال التعليم، مجال الاحترام، مجال الحماية)، وكأبعاد فرعية: (الاتصالات الرقمية، التجارة الإلكترونية، الثقافة ومحو الأمية الرقمية، الوصول الرقمي، القوانين الرقمية، اللياقة الرقمية، الحقوق والمسؤوليات الرقمية، الصحة والسلامة الرقمية، إجراءات ضمان الوقاية والحماية الرقمية). حيث بلغت قيم نسبة الكسب لمعادلة "بلاك" على الترتيب: (1.69)، (1.65)، (1.64)، (1.62)، وهي قيم تتعدى الحد الذي اقترحه "بلاك" للحكم بفاعلية البرنامج، مما يؤكد على فاعلية الوحدة الإلكترونية التفاعلية في تنمية الجوانب الأدائية المرتبطة بمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية.

بالإنترنت معرض للهجمات الإلكترونية، كما أنه مجال متغير ومستجد مع تطوير التطبيقات الرقمية وإصداراتها المستمرة. كذلك تنوع الوسائط والأدوات بالتعلم من خلال وحدة إلكترونية، وإتاحة عرض المحتوى التعليمي الخاص بمهارات الأمن السيبراني بطريقة تفاعلية وجذابة للطالبات، مما كان له دور فعال وإيجابي في ترسيخ المفاهيم الخاصة بمهارات الأمن السيبراني، كما أن ربط المحتوى التعليمي الخاص بمهارات الأمن السيبراني بالعديد من الوسائط التعليمية المتنوعة من صور وفيديوهات وإتاحة الملفات المكتوبة والمسموعة، ساعد الطالبات على التعلم ورفع مستوياتها المعرفية. مما أسهم في تنمية الجانب المعرفي لديهن والذي تبين عند تطبيق الاختبار المعرفي البعدى.

وتتفق هذه النتيجة مع ما توصلت إليه العديد من توصيات الدراسات؛ كدراسة (الجندي وطه، 2019؛ محمد، 2020؛ فلاتة، 2020؛ العمري وطوالبه، 2020؛ السمحان، 2020؛ مؤتمر الأمن والدفاع السيبراني بيروت، 2017) بضرورة تعزيز المواطنة الرقمية ومهارات الأمن السيبراني عند طلاب الجامعة. كما نادت دراسة (محمد، 2020) بضرورة الوعي بخطورة الحروب السيبرانية وتعزيزها بأهمية التوجيه المستمر بالاستخدام الآمن للإنترنت، وهذا يسهم في الحفاظ على الأمن المعلوماتي والشخصي، كما اتفقت مع توصيات مؤتمر الأمن والدفاع السيبراني تحديات وآفاق الذي عقد في الجامعة الفرنكوفونية (2017) بأهمية نشر ثقافة الأمن السيبراني بإعداد المحتوى التعليمي الذي يعني بنشر المخاطر السيبرانية يرفع من زيادة الوعي المعرفي للطلاب. **النتائج المتعلقة بالإجابة عن السؤال الذي ينص على:** "ما فاعلية وحدة إلكترونية تفاعلية في تنمية الجانب الأدائي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية؟" وللإجابة عن السؤال الثاني، تم اختبار صحة **الفرض الثاني** الذي ينص على: "لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسطي درجات مجموعة الدراسة في التطبيق القبلي والبعدى للاختبار الأدائي لمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية".

ولاختبار صحة الفرض الثاني للدراسة، تم استخدام اختبار "ت" للمجموعات المرتبطة (Paired Samples)

الوحدة الإلكترونية التفاعلية، وجاءت النتائج كما يبين الجدول الآتي:

جدول (8): نتائج معامل ارتباط "بيرسون" للعلاقة الارتباطية بين الجانب المعرفي والجانب الأدائي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية.

متغيرات الدراسة	معامل الارتباط	مستوى الدلالة	الدلالة الإحصائية
الجانب المعرفي لمهارات الأمن السيبراني الجانب الأدائي لمهارات الأمن السيبراني	0.728	0.00	دال عند 0.05

يتضح من الجدول (8) أن قيمة معامل الارتباط (ر) للعلاقة بين الجانب المعرفي والجانب الأدائي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية بلغت (0.728)، مما يؤكد على وجود علاقة ارتباطية موجبة ذات دلالة إحصائية عند مستوى الدلالة (0.05) بين مقدار النمو في الجوانب المعرفية لمهارات الأمن السيبراني والجوانب الأدائية لمهارات الأمن السيبراني بعد تطبيق البرنامج القائم على الوحدة الإلكترونية التفاعلية. ويمكن أن تعزى هذه النتيجة إلى أن الوحدة الإلكترونية التفاعلية قد أسهمت في التركيز على العلاقة بين مقدار النمو في اكتساب مهارات الأمن السيبراني بشقيها المعرفي والأدائي الأمر الذي أسهم في تنميتها لوجود العلاقة والترابط بين محتوى الأمن السيبراني، كما أن المحتوى الإلكتروني التفاعلي عزز من نمو وتحسن مهارات الأمن السيبراني لدى الطالبات، كما أن التطور في إحدى المهارات يصاحبه تحسن ونمو بقدر ما في المتغير الآخر. ويستخلص من هذه النتيجة أن الوحدة الإلكترونية التفاعلية قد تسهم في تنمية مهارات الأمن السيبراني، وهذا بدوره يعزز العلاقة الارتباطية بين مقدار النمو في مهارات الأمن السيبراني بشقيها المعرفي والمهاري. وتتفق هذه النتيجة للدراسة الحالية مع نتيجة دراسة الحافظي (2019) التي كشفت عن وجود علاقة ارتباطية في نمو مفاهيم المواطنة الرقمية على التأثير في النمو مستقبلاً بشكل إيجابي على مهارات المواطنة الرقمية لدى الطلاب بجامعة الملك عبد العزيز في جدة، وأيضاً قدرة النمو في مهارات المواطنة الرقمية على التأثير مستقبلاً في النمو

ويمكن أن تعزى فاعلية وحدة إلكترونية تفاعلية في تنمية الجوانب الأدائية المرتبطة بمهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية للأسباب الآتية: شغف الطالبات وحبهن للتعلم وحماسهن لاكتساب المهارات العملية، وقد يعود السبب إلى كثرة المشكلات السيبرانية التي تواجههم ويتعرض لها الأشخاص، خصوصاً عند استخدام التطبيقات التقنية والاتصال بالإنترنت. وتنوع أدوات التعلم والوسائط التي تشرح الخطوات العملية في أجزاء وخطوات تفصيلية متسلسلة في ترتيب منطقي لموضوعات الأمن السيبراني داخل الوحدة الإلكترونية، مما يسهم في صقل المهارات الأدائية وإتقان التعلم لمهارات الأمن السيبراني، كما يمكن الرجوع إليها في أي وقت لتطبيق الممارسات العملية بالإبحار داخل الوحدة الإلكترونية التفاعلية، مما انعكس على تنمية الجوانب الأدائية.

وتتفق هذه النتيجة مع ما توصلت إليه العديد من الدراسات كدراسة (العلوان، 2021) و(الشهري، 2020) و(National Cyber Security Awareness, 2020) التي أكدت على أن استخدام التقنيات التفاعلية والبرمجيات في العملية التعليمية لها تأثير جيد على تنمية الأداء المهاري في الأمن السيبراني، كما اتفقت مع دراسة الجندي وطه (2019) بالاهتمام بتنمية مهارات الأمن السيبراني وممارستها التطبيقية وطرق توظيفها من خلال استخدام إستراتيجيات تقنية متطورة.

النتائج المتعلقة بالإجابة عن السؤال الذي ينص على: "هل توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى الدلالة بين مقدار النمو في الجانب المعرفي والجانب الأدائي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية؟". وللإجابة عن السؤال الثالث، تم اختبار صحة **الفرض الثالث** الذي نص على: "لا توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين مقدار النمو في الجانب المعرفي والجانب الأدائي لمهارات الأمن السيبراني لدى الطلبة الجامعيين في ضوء محددات المواطنة الرقمية".

ولاختبار صحة الفرض الثالث، تم استخدام معامل ارتباط "بيرسون" (Pearson's coefficient)؛ للتحقق من الدلالة الإحصائية للعلاقة الارتباطية بين درجات الطلبة في الاختبار المعرفي ودرجاتهم على بطاقة الملاحظة بعد تطبيق البرنامج القائم على

بشكل إيجابي في مفاهيم المواطنة الرقمية.

الأكاديمية الوطنية للأمن السيبراني. تاريخ الاسترجاع: 2021/9/17، من: [/https://ncac.edu.sa](https://ncac.edu.sa)

التحائية، رشاد أحمد حسن؛ والسفاسفة، محمد إبراهيم محمد. (2017).
فعالية برنامج إرشادي متعدد النماذج في تنمية المواطنة الرقمية وتحسين
مستوى إدارة الذات لدى طلبة الصف العاشر، رسالة دكتوراة غير
منشورة، عمادة الدراسات العليا، جامعة مؤتة، الأردن.
التقرير السنوي للرقمنة السعودية (2022). تاريخ الاسترجاع:
2021/4/15، من:

<https://ndu.gov.sa/sites/default/files/2021-09/ndu-annual-report.pdf>

الجندي، علياء ، ومحمد، نخير طه حسن. (2019). دور الممارسة التطبيقية
للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن
المعلوماتي لدى طالبات الجامعة. عالم التربية، ع67، ج3، 14-84.

الحافظي، فهد سليم (2019) تصميم برنامج تعليمي قائم على نظام إدارة
التعلم الإلكتروني (Blackboard) وقياس فاعليته في تنمية قيم
المواطنة الرقمية ومهارات التفكير التأملي لدى طلاب الكلية التقنية في
مدينة جدة. تكنولوجيا التربية-دراسات وبحوث: الجمعية العربية
لتكنولوجيا التربية، ع39، 119-174.

الدوسري، سلمى؛ العريشي، جبريل. (2018). دور مؤسسات التعليم العالي
في تعزيز ثقافة أمن المعلومات في المجتمع، مجلة مكتبة الملك فهد
الوطنية، 24 (2)، 302-373.

الرشيد، بسام؛ والزيادات، ماهر. (2018). مستوى وعي معلمي
الاجتماعيات في المرحلة الثانوية في دولة الكويت لمفهوم المواطنة
الرقمية من وجهة نظرهم، رسالة ماجستير غير منشورة، كلية العلوم
التربوية، جامعة آل البيت، الأردن.

سليمان، جيهان ، والعمري، عائشة. (2021). فاعلية وحدة إلكترونية
مقترحة في تنمية قيم المواطنة الرقمية لدى طالبات المرحلة المتوسطة.
المؤتمر الدولي الثاني لمستقبل التعليم الرقمي في الوطن العربي: إثراء
المعرفة للمؤتمرات والأبحاث، مج2، مكة المكرمة: إثراء المعرفة
للمؤتمرات والأبحاث والنشر العلمي، 172-199.

السمحان، منى. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة
المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية-جامعة
المنصورة، 111، 1-29.

الشهري، بيان، وفلمبان، فدوى. (2020). أثر برنامج تدريبي قائم على
تصميم ألعاب تعليمية إلكترونية باستخدام برنامج Game
Marek لإكساب مفاهيم الأمن السيبراني لدى طالبات المرحلة
المتوسطة. مجلة البحث العلمي في التربية، ع21، ج9، 614-651.

عزمي، نبيل (2015). بيئات التعلم التفاعلية، ط2. القاهرة: مكتبة الفلاح
للنشر والتوزيع.

العلوان، جعفر. (2021). الألعاب الرقمية الجادة وتنمية مهارات الأمن
السيبراني: دراسة استكشافية. مجلة المنقال للعلوم الاقتصادية والإدارية،
مج7، ع3، 83-114.

– التوصيات والمقترحات

- توظيف مفاهيم ومهارات الأمن السيبراني والمواطنة الرقمية في مختلف المقررات الدراسية في التعليم الجامعي بتصميم أنشطة لا منهجية بهدف الوعي لمجتمع آمن رقمياً.
- إثراء مجال الأمن السيبراني بمزيد من تنفيذ الورش التي تدعم التطبيق المهاري والأدائي لتعزيز مهارات الأمن السيبراني والتصدي لمخاطرها والوعي بالاستخدام الآمن للتكنولوجيا والتطبيقات الرقمية والإنترنت.
- عمل شراكة بالتعاون مع الإدارة العامة للأمن السيبراني بالجامعات السعودية والمركز الوطني الإرشادي للأمن السيبراني في تطبيق التوعية المعرفية والمهارية في الأمن السيبراني للتصدي لتحديثات الهجمات السيبرانية وطرق التغلب عليها.
- نشر أهم مستجدات المجال في مهارات الأمن السيبراني وسبل الحماية من مخاطرها عبر وسائل التواصل الاجتماعي التابعة للمؤسسات التعليمية بهدف بناء مواطن رقمي صالح يحمي نفسه والآخرين.
- إعادة تطبيق الدراسة على مستوى الجامعات السعودية وبيان أثر تعلم الأقران المدعم بالإنفوجرافيك التفاعلي على تنمية مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية.
- إعادة تطبيق الدراسة على مستوى الجامعات السعودية وبيان أثر بيئات التعلم (الشخصية-التعاونية-التشاركية) المدعمة بالأنشطة التفاعلية على تنمية مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية.

قائمة المراجع

أولاً: المراجع العربية:

- الأحمدي، إيمان. (2020). متطلبات إعداد المواطن الرقمي في ضوء المملكة العربية السعودية (2030م). مجلة الأكاديمية والنشر العلمي، 17، 490-513.
- استيتية، دلال. سرحان، موسى (2008). تكنولوجيا التعليم والتعليم الإلكتروني. ط1، عمان: دار وائل للنشر والتوزيع.

- education students. *International Education Studies*, 8(12), 203-217.
- Arafa, Rasha Mahmoud, and Al-Iraqi, Rania Mahfouz Habib. (2021). The effectiveness of the Webquest strategy in improving the level of nutritional and health awareness and acquiring some cybersecurity skills for home economics students during the Corona pandemic. *Journal of Special Education Cases*, p. 37, 965 - 1000.
- Cantone, E, Piras, A., Vellante, M., Preti, A., Daniélsdóttir, S., D'Aloja, E., Lesinskiene, S., Angermeyer, M., Carta, M. & Bhugra, D. (2015). Interventions on Bullying and Cyberbullying in Schools: A Systematic Review. *Clinical Practice and Epidemiology in Mental Health: CP and EMH 11 (Suppl 1: M4): 58-76.*
- Cassidy, W., Brown, K. & Jackson, M. (2012) 'Under the Radar': Educators and Cyberbullying in Schools. *School Psychology International*, 33 (5): 520-532.
- Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. *Journal of Cybersecurity*, 5(1), tyz001.
- Choi, M. (2016). A concept analysis of digital citizenship for democratic citizenship education in the internet age. *Theory & research in social education*, 44(4), 565-607.
- Conklin, W. A., Cline, R. E., & Roosa, T. (2014, January). Re-engineering cybersecurity education in the US: an analysis of the critical factors. In 2014 47th Hawaii international conference on system sciences (pp. 2006-2014). IEEE.
- Fisk, N. (2016). *Framing Internet Safety: The Governance of Youth Online*. Cambridge: The MIT Press.
- Isman, A., & Canan Gungoren, O. (2014). Digital citizenship. *Turkish Online Journal of Educational Technology-TOJET*, 13(1), 73-77.
- Johnson, M. (2015). Digital literacy and digital citizenship: Approaches to girls' online experiences. In J. Bailey & V. Steeves (Eds.), *eGirls, eCitizens* (pp. 339-360). Ottawa, Ontario, Canada: University of Ottawa Press.
- Mark, L. K. (2014). *Reducing cyber victimization through home and school partnerships: The effects of a cyber safety workshop on parent and educator perceptions of self-efficacy and attitudes toward family-school collaboration* (Doctoral dissertation, [Honolulu]: [University of Hawaii at Manoa], [May 2014].
- McGettrick, A. (2013). Toward effective cybersecurity education. *IEEE Security & Privacy*, 11(6), 66-68.
- National Cyber Security Awareness month (2020). *Online cypersecuirty advice for all digital citizens*.
- NetSafe. (2018). *Digital citizenship in NewZealand schools: overview*. Retrieved from https://www.researchgate.net/profile/Mark-Brown-34/publication/272942538_Learning_in_the_digital_age_How_are_the_ways_in_which_we_learn_changing_with_the_use_of_technologies/links/576bbc3808aef2a864d4c48d/Learning-in-the-digital-age-How-are-the-ways-in-which-we-learn-changing-with-the-use-of-technologies.pdf
- Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy*, 11(4), 3-4.
- Tangen, D., & Campbell, M. (2010). Cyberbullying Prevention: One Primary School's Approach. العمري، ربي ؛ وطولية، منال. (2020). درجة وعي طلبة الجامعات الأردنية لمفهوم المواطنة الرقمية. رسالة ماجستير غير منشورة، كلية العلوم التربوية، جامعة الشرق الأوسط، عمان.
- فلانه، فوزية. (2020). نحو إستراتيجية مقترحة لتفعيل دور الجامعات السعودية في تعزيز المواطنة الرقمية. مجلة كلية التربية-جامعة المنصورة، 110، 197-243.
- محمد، هبه. (2020). برنامج مقترح قائم على جغرافية الحروب السيبرانية لتنمية الوعي بمخاطرها وتعزيز قيم المواطنة الرقمية لطلاب المعلمين بكلية التربية. مجلة كلية التربية-جامعة عين شمس، 3، (44)، 81-150.
- المركز الوطني لاستطلاعات الرأي العام التابع لمركز الملك عبد العزيز للحوار الوطني. (2022). تاريخ الاسترجاع 2021/11/10، من: <https://ncpop.org.sa/Questionnaire/Archive>
- المعلم، بندر ؛ وجاب الله، عبد الحميد. (2018). تقييم مقرر المهارات الحياتية والتربية الأسرية في ضوء تضمينه لمهارات المواطنة الرقمية لدى طلاب المرحلة الثانوية، رسالة ماجستير غير منشورة، كلية التربية، جامعة القصيم، السعودية.
- المنتشري، حليلة، فطاني، هانية. (2019). الأمن السيبراني والمواطنة الرقمية المفهوم والعلاقة. ورقة عمل مقدمة للمؤتمر الدولي الثورة الصناعية الرابعة وأثرها على التعليم، ع157، صحار-عمان.
- المنتشري، حليلة ؛ وفطاني، هانية. (2019). الأمن السيبراني والمواطنة الرقمية المفهوم والعلاقة. سلطنة عمان: وزارة التربية والتعليم.
- المنتشري، حليلة؛ والمنتشري، محمد (2019). الأمن السيبراني والمواطنة الرقمية. ط1.
- مؤتمر الأمن والدفاع السيبراني تحديات وآفاق (2017). الجامعة للفنونكوفونية (بيروت-لبنان). تاريخ الاسترجاع: 2021/11/5، من: <https://www.ul.edu.lb/common/news.aspx?newsId=1191&lang=3>
- هيئة التعليم والتدريب. (2019). الإطار التخصصي لمجال تعلم التقنية الرقمية. هيئة التعليم والتدريب.
- الهيئة الوطنية للأمن السيبراني. تاريخ الاسترجاع 2021/12/7 من: <https://nca.gov.sa/pages/about.html>
- الهيئة الوطنية للأمن السيبراني. (2018). الضوابط الأساسية للأمن السيبراني.

References

- Adorjan, M. & Ricciardelli, R. (2019). Student perspectives towards cyber-risk and safety: the presumption of the prudent digital citizen. *Learning, Media and Technology*, 44 (4), 1-13.
- Al-Arishee, J. (2019). Information Security in the Arab World: Risks and Challenges. *International Journal of Informatics, Media and Communication Technology*, Vol. 1, p. 1, 57 - 157. M
- Al-Zahrani, A. (2015). Toward digital citizenship: examining factors affecting participation and involvement in the Internet society among higher

- Information Security in Society, *Journal of King Fahd National Library*, 24(2), 302-373.
- Al-Rashidi, Bassam Ajab Saad; And increases, Maher Mufleh Ahmed. (2018). The level of awareness of secondary school social teachers in the State of Kuwait of the concept of digital citizenship from their point of view, *an unpublished master's thesis*, College of Educational Sciences, Al al-Bayt University, Jordan.
- Soleimani, Jihan Belkacem Al-Tayeb, and Al-Omari, Aisha Balihesh. (2021). The effectiveness of a proposed electronic unit in developing the values of digital citizenship among middle school students. *The Second International Conference on the Future of Digital Education in the Arab World: Enriching Knowledge for Conferences and Research*, Volume 2, Makkah Al-Mukarramah: Enriching Knowledge for Conferences, Research and Scientific Publishing, 172 - 199.
- Al-Samhan, Mona Abdullah. (2020). Requirements to achieve cyber security for management information systems at King Saud University, *Journal of the College of Education - Mansoura University*, 111, 1-29.
- Al-Shahrani, Nasir Muhammad's statement, and Felimban, Fadwa Yassin. (2020). The effect of a training program based on designing electronic educational games using the Game Marek program on acquiring the concepts of cyber security among middle school students. *Journal of Scientific Research in Education*, p. 21, vol. 9, 614 - 651.
- Obeidat, Thoukan; and Abu Al-Sameed, Suhaila (2002). *Scientific research (qualitative research and quantitative research)*. , 2nd Edition, Amman: Dar Al-Fikr.
- Azmy, Nabil (2015). *Interactive Learning Environments*, 2nd Edition. Cairo: Al Falah Library for Publishing and Distribution.
- Alwan, Jaafar Ahmed Abdel Karim. (2021). Serious digital gaming and cybersecurity skills development: An exploratory study. *Mithqal Journal of Economic and Administrative Sciences*, Volume 7, Volume 3, 83-114.
- Al-Omari, Ruba Ahmed; and Tawalbeh, Manal Atta. (2020). The degree of awareness of Jordanian university students of the concept of digital citizenship. *Unpublished Master's Thesis*, College of Educational Sciences, Middle East University, Amman.
- Fallatah, Fawzia bint Ahmed bin Mohammed. (2020). Towards a proposed strategy to activate the role of Saudi universities in promoting digital citizenship. *Journal of the College of Education - Mansoura University*, 110, 197-243.
- Muhammad, Heba Hashem. (2020). A proposed program based on the geography of cyber wars to develop awareness of its dangers and enhance the values of digital citizenship for teacher students at the College of Education. *Journal of the College of Education - Ain Shams University*, 3, (44), 81-150.
- The National Center for Public Opinion Polls affiliated with the King Abdulaziz Center for National Dialogue* (2022), retrieved date 10/11/2021, from: <https://ncpop.org.sa/Questionnaire/Archive>
- Al-Mulhim, Bandar bin Mohammed Rashid; And Jaballah, Abdel Hamid Sabri Abdel Hamid. (2018). Evaluation of the life skills and family education course in light of its inclusion of digital *Journal of Psychologists and Counsellors in Schools*, 20 (2): 225–234.
- UNESCO Bangkok (2015). Fostering Digital Citizenship through Safe and Responsible Use of ICT: A review of current status in Asia and the Pacific as of December. Bangkok: UNESCO Bangkok. Retrieved from http://teams.unesco.org/ORG/fu/bangkok/public_events/Shared%20Documents/EISD/2017/Oct2017%20-%20KFIT%203%20Launch%20-%20Dig%20Citizenship/ SRU-ICT_mapping_report_2014.pdf
- UNESCO Bangkok (2019). *Digital Kids Asia-Pacific: Insights into Children's Digital Citizenship*. Retrieved from bangkok.unesco.org/content/digital-kids-asia-pacific-insights-childrens-digital-citizenship
- Walsh, K., Wallace, L., Ayling, N., & Sondergeld, A. (2020). *Best practice framework for online safety education* (Stage 1). Retrieved from: <https://eprints.qut.edu.au/202958/>
- Walsh, K., Wallace, L., Ayling, N., & Sondergeld, A. (2020). *Best practice framework for online safety education* (Stage 1). Retrieved from: <https://eprints.qut.edu.au/202958/>
- Zahri, Y., Ab Hamid, R. S., & Mustaffa, A. (2017). Cyber security situational awareness among students: A case study in Malaysia. *International Journal of Educational and Pedagogical Sciences*, 11(7), 1704-1710.
- Al-Ahmadi, Iman Abdel Aziz. (2020). Requirements for preparing the digital citizen in the light of the Kingdom of Saudi Arabia (2030). *Academic Journal and Scientific Publishing*, 17, 490-513.
- Estetia, Dalal. Sarhan, Musa (2008) *Education Technology and E-Learning. 1st floor*, Amman: Dar Wael for Publishing and Distribution.
- National Academy of Cyber Security*. Retrieval date: 9/17/2021, from: <https://ncac.edu.sa/>
- Takhaina, Rashad Ahmed Hassan; And the philosophers, Muhammad Ibrahim Muhammad. (2017). The effectiveness of a multi-model indicative program in developing digital citizenship and improving the level of self-management among tenth grade students, *unpublished Ph.D. thesis*, Deanship of Graduate Studies, Mutah University, Jordan.
- Saudi Digitization Annual Report* (2022). Retrieval date: 4/15/2021, from: <https://ndu.gov.sa/sites/default/files/2021-09/ndu-annual-report.pdf>
- Al-Jundi, Alia bint Abdullah Ibrahim, and Muhammad, Nahir Taha Hassan. (2019). The role of the applied practice of cybersecurity in developing skills and the accuracy of the practical application of information security among university students. *The World of Education*, p. 67, c.3, 14-84.
- Al-Hafezi, Fahad Saleem (2019) Designing an educational program based on the electronic learning management system (Blackboard) and measuring its effectiveness in developing digital citizenship values and reflective thinking skills among students of the Technical College in Jeddah. *Educational Technology - Studies and Research: The Arab Society for Educational Technology*, p. 39, 119-174.
- Al-Dosari, Salma Abdel-Rahman; Al-Arishi, Jibril Hassan Muhammad. (2018). The Role of Higher Education Institutions in Promoting a Culture of

- Montashari, Halima; and Al Montashari, Mohammed (2019). *Cyber security and digital citizenship*. i 1 *Cyber Security and Defense Conference: Challenges and Prospects* (2017). University of the Francophonie (Beirut - Lebanon). Retrieval date: 5/11/2021 from: <https://www.ul.edu.lb/common/news.aspx?newsId=1191&lang=3>
- Education and Training Authority. (2019). The specialized framework for the field of learning digital technology. Education and Training Authority.
- National Cybersecurity Authority Retrieved on 12/7/2021 from: <https://nca.gov.sa/pages/about.html>
- National Cybersecurity Authority. (2018). Basic controls for cyber security.
- citizenship skills among secondary school students, *unpublished master's thesis*, College of Education, Qassim University, Saudi Arabia.
- Montashari, Halima. Fatani, Hania (2019). *Cyber Security and Digital Citizenship Concept and Relationship*. Working paper presented to the *International Conference of the Fourth Industrial Revolution and its impact on education*, p. 157, Sohar - Oman.
- Montashari, Halima Youssef; And Fatani, Hania Abdel-Razzaq. (2019). *Cyber Security and Digital Citizenship Concept and Relationship*. Sultanate of Oman: Ministry of Education.