E-ISSN: 2706-9931
P-ISSN: 1994-473X

Al-Adab Journal Vol. 68, No. 3, Supplement (September) 2026

The Role of Security Awareness in Enhancing Electronic Confidence Among University Students (A field study on the art of students at the University of Sharjah)

Ali Sultan Al-Ketbi[1] Dr. Alaa Al-Taii [2] (Corresponding Author) Dr. Nora Guenifa [3]

[1] University of Sharjah, College of Arts, Humanities, and Social Sciences, Department of Sociology U23101508@sharjah.ac.ae

[2] University of Sharjah, College of Arts, Humanities and Social Sciences, Department of Sociology aaltaii@sharjah.ac.ae

[3] University of Sharjah, College of Arts, Humanities and Social Sciences, Department of Sociology NGuenifa@sharjah.ac.ae

Copyright (c) 2026 **Ali Sultan Al-Ketbi. Dr. Alaa Al-Taii .Dr. Nora Guenifa**

DOI: https://doi.org/10.31973/rp7krr08

This work is licensed under a Creative Commons Attribution 4.0 International License.

Publication Dates

(Received 2025-10-19) (Revised 2025-10-20) (Accepted 2025-10-20) (Published 2026-09-15)

Abstract:

This study aims to explore the role of security awareness in enhancing e-trust among students at the University of Sharjah within the context of rapid digital transformation. The research employed a descriptive-analytical approach using a survey distributed to a sample of 300 students from various faculties and disciplines. The findings revealed that students demonstrated relatively high awareness of the importance of digital privacy protection (M=4.05), while actual participation in cybersecurity awareness workshops remained low (M=2.91), highlighting a gap between theoretical knowledge and practical application. Results also indicated that more than half of the respondents had experienced phishing attempts (51.3%), and 57% had not received any formal cybersecurity training. ANOVA tests showed no statistically significant differences across gender or field of study, while the type of electronic device used significantly influenced perceptions of trust and cultural barriers. It is concluded that enhancing e-trust requires more comprehensive institutional strategies, including integrating cybersecurity awareness into academic curricula, strengthening digital protection systems, and intensifying media campaigns, thereby fostering a secure and sustainable digital environment that supports the UAE's digital transformation journey.

***The authors has signed the consent form and ethical approval**

Keywords: Cybersecurity, E-trust, Security awareness, University of Sharjah students, UAE society.

Al-Adab Journal Vol. 68, No. 3, Supplement (September 2026)
E-ISSN: 2706-9931 P-ISSN: 1994-473X

دور التوعية الامنية في تعزيز الثقة الالكترونية لدى الشباب الجامعي (دراسة ميدانية على عينة من طلبة جامعة الشارقة)

الباحث علي سلطان الكتبي
جامعة الشارقة، كلية الآداب والعلوم الإنسانية والاجتماعية، قسم علم الاجتماع

د. آلاء الطائي (المؤلف المراسل)
جامعة الشارقة، كلية الآداب والعلوم الإنسانية والاجتماعية، قسم علم الاجتماع

د. نورة قنيفة
جامعة الشارقة/ كلية الآداب والعلوم الإنسانية والاجتماعية/ قسم علم الاجتماع

تواريخ المنشور

الإستلام	النسخة النهائية	الموافقة	النشر الالكتروني
(٢٠٢٥/١٠/١٩)	(٢٠٢٥/١٠/٢٠)	(٢٠٢٥/١٠/٢٠)	(٢٠٢٦/٩/١٥)

(مُلَخَّصُ البَحث)

تهدف هذه الدراسة إلى استكشاف دور التوعية الأمنية في تعزيز الثقة الإلكترونية لدى طلاب جامعة الشارقة في ظل التحولات الرقمية المتسارعة. اعتمدت الدراسة على المنهج الوصفي التحليلي باستعمال أداة الاستبانة، إذ شملت العينة (٣٠٠) طالبًا وطالبة من مختلف الكليات والتخصصات. وقد بينت النتائج أن الطلبة يمتلكون وعيًا مرتفعًا نسبيًا بأهمية حماية الخصوصية الرقمية (م=٤.٠٥)، إلا أن المشاركة الفعلية في الورش التوعوية كانت منخفضة (م=٢.٩١)، مما يعكس فجوة بين المعرفة النظرية والتطبيق العملي. كما أظهرت النتائج أن أكثر من نصف العينة تعرضوا لمحاولات احتيال إلكتروني (٥١.٣%)، وأن ٥٧% لم يحصلوا على أي تدريب رسمي في الأمن السيبراني. وأشارت اختبارات ANOVA إلى عدم وجود فروق دالة إحصائيًا باختلاف الجنس أو التخصص، بينما ظهر تأثير نوع الجهاز المستعمل على إدراك الطلبة لمستوى الثقة والمعوقات الثقافية. وتخلص الدراسة إلى أن تعزيز الثقة الإلكترونية يتطلب استراتيجيات مؤسسية أكثر تكاملاً تشمل إدماج التوعية السيبرانية في المناهج الجامعية، وتطوير أنظمة الحماية الرقمية، وتكثيف الحملات الإعلامية، بما يضمن بناء بيئة إلكترونية آمنة ومستدامة تدعم مسيرة التحول الرقمي في دولة الإمارات.

الكلمات المفتاحية: التوعية الأمنية، الثقة الإلكترونية، الأمن السيبراني، طلاب جامعة الشارقة، المجتمع الإماراتي.

*** وقع المؤلفون على نموذج الموافقة والموافقة الأخلاقية الخاصة بالمساهمة البشرية في البحث**

مقدمة:

يشهد العالم اليوم تحولات رقمية غير مسبوقة بفضل التقدم الهائل في تكنولوجيا المعلومات والاتصالات، إذ أصبحت هذه التقنيات جزءًا أساسيًا من الحياة اليومية للأفراد والمؤسسات على حد سواء (Boumediene, Abdelkader, & Waddou، ٢٠٢١). ولم يقتصر أثر هذا التحول على الجوانب التقنية فحسب، بل امتد ليؤثر في أنماط التفاعل الاجتماعي والاقتصادي والثقافي، مما مهد لظهور ما يُعرف بالمجتمع الرقمي الذي يتسم بالاتصال المستمر والتفاعل الذكي. وقد برز ضمن هذا السياق مفهوم الفضاء السيبراني، وهو البيئة الافتراضية التي يتم فيها تبادل المعلومات والتواصل عبر الإنترنت، متضمنًا البنى التحتية والأجهزة والتطبيقات والبيانات المتدفقة (Belfred & Barquq, 2024; Al Neyadi، ٢٠٢٤)

هذا الفضاء السيبراني لم يعد مجرد قناة تقنية، بل أصبح ساحة تُعاد فيها صياغة مفاهيم الثقة والأمان، حيث أضحى التعامل الرقمي تجربة اجتماعية ونفسية معقدة تتداخل فيها الخصوصية والانكشاف والاعتماد المتبادل (Ibrahim، ٢٠٢٤). ورغم ما يتيحه من فرص للتواصل والمعرفة والإنتاج، فإنه يواجه تحديات متزايدة مثل الهجمات السيبرانية وتسريب البيانات، ما يجعل الحاجة ملحّة إلى بناء بيئة آمنة وموثوقة تعزز من الثقة الإلكترونية (Khoisan، ٢٠٢٠).

وفي ظل هذا التحول الرقمي، تشكّل فئة الشباب في الإمارات النسبة الأكبر من مستعملي المنصات الرقمية، ما يجعلهم أكثر عرضة للمخاطر كالتمر والتضليل وتسريب المعلومات (Jarboua & Boutmine، ٢٠٢٣) . هنا تبرز التوعية الأمنية كعامل أساسي في تمكين هذه الفئة من مواجهة التهديدات، من خلال رفع الوعي بممارسات الحماية الرقمية وتعزيز ثقافة الاستخدام الآمن. فالثقة الإلكترونية ليست مجرد شعور فردي، بل هي علاقة متشابكة بين عناصر تقنية واجتماعية وثقافية، حيث يؤدي ارتفاع مستوى الأمان الرقمي إلى زيادة التعاون والتفاعل الإيجابي بين الأفراد، والحد من السلوكيات السلبية كالابتزاز والتشهير (Ahleihal، ٢٠٢٤)، وعليه، تزداد الحاجة إلى دراسات علمية تفسر كيف تسهم التوعية الأمنية في بناء الثقة الإلكترونية داخل المجتمع الإماراتي، من خلال استكشاف العوامل المؤثرة على سلوك الأفراد الرقمي، وفهم انعكاساتها على تحقيق الأمن السيبراني (UNICEF، ٢٠٢١).

مشكلة البحث

المجتمع الإماراتي خلال السنوات الأخيرة تطوراً كبيراً في مجال التحول الرقمي، حيث بات الاعتماد على الخدمات الإلكترونية جزءاً أساسياً من الحياة اليومية للأفراد والمؤسسات. غير أن هذا التحول، على الرغم من ما يحمله من فرص لتيسير الخدمات وتحقيق الكفاءة، أفرز تحديات معقدة تتعلق بمدى ثقة الأفراد في البيئة الرقمية، إذ أدت الهجمات السيبرانية وتسريب البيانات الشخصية إلى خلق حالة من القلق والشك لدى المستخدمين تجاه التعاملات الإلكترونية (Khoisan, 2020; Telecommunications and Digital Government Regulatory Authority TDRA، ٢٠٢٣) ويكشف ذلك عن فجوة بين سرعة التطور التقني ومستوى استعداد الأفراد للتفاعل معه بثقة واطمئنان (Ibrahim، ٢٠٢٤).

وفي ظل هذا الواقع، تبرز التوعية الأمنية كأداة محورية لسد هذه الفجوة، إذ تسهم في رفع مستوى إدراك الأفراد بالمخاطر الرقمية، وتعزيز قدرتهم على تبني ممارسات وقائية مثل استخدام كلمات مرور قوية وتجنب الروابط المشبوهة (Ahleihal، ٢٠٢٤). غير أن فعالية هذه التوعية ما زالت بحاجة إلى دراسة معمقة لقياس دورها في بناء الثقة الإلكترونية داخل المجتمع الإماراتي، لا سيما بين فئة الشباب التي تُعد الأكثر استخداماً للتكنولوجيا والأكثر عرضة للتهديدات الرقمية (Jarboua & Boutmine، ٢٠٢٣) . وبناءً على ما سبق، تتحدد مشكلة الدراسة في محاولة الإجابة عن السؤال الرئيس:

ما دور التوعية الأمنية في تعزيز الثقة الإلكترونية داخل المجتمع الإماراتي؟

أهداف الدراسة

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف الرئيسة والفرعية، ويمكن تلخيصها فيما يلي:

١. التعرف على مستوى الثقة الإلكترونية في المجتمع الإماراتي ومدى تأثرها بالتحديات الأمنية المرتبطة بالفضاء السيبراني.
٢. تحليل دور التوعية الأمنية في تعزيز الوعي بالمخاطر الرقمية وتشجيع الأفراد على تبني ممارسات وقائية تحمي بياناتهم الشخصية.
٣. استكشاف العلاقة بين التوعية الأمنية والثقة الإلكترونية من منظور اجتماعي وثقافي، لفهم كيف تؤثر البرامج التوعوية في السلوكيات الرقمية للأفراد.
٤. تحديد أبرز المعوقات الثقافية والمجتمعية التي قد تحد من فعالية

برامج التوعية الأمنية في بناء الثقة الإلكترونية.

٥. اقتراح استراتيجيات عملية لتعزيز دور المؤسسات التعليمية والإعلامية والحكومية في نشر التوعية الأمنية بما يسهم في ترسيخ بيئة رقمية آمنة ومستدامة في المجتمع الإماراتي.

أهمية الدراسة

تتجلى أهمية هذه الدراسة في جانبين رئيسيين:

١. **الأهمية العلمية:**

- إثراء الأدبيات العربية حول التوعية الأمنية والثقة الإلكترونية بربط الأبعاد التقنية والاجتماعية والثقافية.
- فتح المجال لدراسات مقارنة تعزز تراكم المعرفة.
- تقديم تصور جديد يوضح علاقة التوعية الأمنية بالسلوكيات الرقمية في البيئات الجامعية والمجتمعية.

٢. **الأهمية العملية:**

- تمكين صناع القرار من تصميم برامج توعوية أكثر فاعلية.
- تقديم توصيات قابلة للتطبيق في الحملات الإعلامية والمؤسسات التعليمية.
- دعم الاستراتيجيات الوطنية للتحول الرقمي ببناء بيئة إلكترونية آمنة.
- مساعدة المؤسسات على معالجة المعوقات الثقافية والمجتمعية المؤثرة في الثقة الإلكترونية.

أسئلة الدراسة

تسعى هذه الدراسة للإجابة عن التساؤل الرئيس الآتي:

ما دور التوعية الأمنية في تعزيز الثقة الإلكترونية في المجتمع الإماراتي؟

ويتفرع عن هذا السؤال الرئيس عدد من الأسئلة الفرعية:

١. ما مستوى الثقة الإلكترونية لدى أفراد المجتمع الإماراتي؟
٢. ما مدى وعي الأفراد بالمخاطر الرقمية وأهمية التوعية الأمنية في التعامل معها؟
٣. كيف تسهم برامج التوعية الأمنية في تعزيز السلوكيات الرقمية الآمنة لدى الأفراد؟
٤. ما العوامل الاجتماعية والثقافية التي تؤثر في فعالية التوعية الأمنية في بناء الثقة الإلكترونية؟
٥. ما أبرز المعوقات التي تحد من دور التوعية الأمنية في تعزيز الثقة الإلكترونية؟
٦. ما الاستراتيجيات المقترحة لتعزيز فعالية التوعية الأمنية في المجتمع الإماراتي؟

مفاهيم الدراسة

مصطلحات الدراسة

١. الأثر – The Impact

– اصطلاحياً: الأثر هو ما ينتج عن التفاعل بين الغياب والحضور في آن واحد، كعلامة على التغير أو الاستمرار (Makkawi،2009).

– إجرائياً: يُقصد به التغير الناتج عن العلاقة بين المتغير المستقل (الثقة الإلكترونية) والمتغير التابع (الأمن السيبراني)، ويُقاس بدرجة تأثير الثقة الإلكترونية على مستوى الأمان والحماية الرقمية لدى الشباب.

٢. الثقة الالكترونية – E-Trust

– اصطلاحياً: هي الاطمئنان الناتج عن التعامل مع الأنظمة الإلكترونية المختلفة ضمن الأطر الأخلاقية والقانونية، بما يضمن هوية الأفراد وحماية بياناتهم وسرية المعلومات (Dakrour et al، 2018؛ El Metwally et al ، ٢٠٢٠).

– إجرائياً: مستوى اليقين الذي يضعه الشباب الجامعي في أمان وموثوقية الأنظمة الرقمية، اعتماد على حماية بياناتهم الشخصية ومصداقية الخدمات المقدمة عبر الإنترنت.

٣. الأمن السيبراني – Cybersecurity

– اصطلاحياً: منظومة من السياسات والتقنيات والممارسات التي تهدف إلى حماية البيانات والأنظمة الرقمية من الهجمات، وضمان سريتها وسلامتها واستمراريتها (Al Muhairi, 2023; Al Mutairi, 2025; Al Neyadi,2024)

إجرائياً: مجموعة من التدابير التقنية والإدارية التي تهدف إلى حماية الأنظمة الإلكترونية وبيانات المستخدمين من التهديدات، ويتجسد من خلال سلوكيات الثقة الإلكترونية لدى الشباب الجامعي.

الإطار النظري والدراسات السابقة

أولاً: الإطار النظري:

نظرية السلوك الاجتماعي

تُعد نظرية السلوك الاجتماعي من أبرز النظريات التفسيرية في علم الاجتماع، إذ ترى أن السلوك الإنساني لا ينشأ بمعزل عن الآخرين فحسب، بل يتشكل من خلال التفاعلات المستمرة مع البيئة الاجتماعية والمؤسسات المحيطة. فالفرد يتأثر بالقيم والمعايير والتوقعات المجتمعية التي تحدد أنماط سلوكه وتوجهاته (Al-Ayyashi & Al-Farfar، ٢٠٢١)

نشأة النظرية

ظهرت هذه النظرية في أواخر القرن التاسع عشر، متأثرة بالاتجاهات الوظيفية والتفاعلية الرمزية، وساهم في تطويرها علماء مثل جورج هربرت ميد و تشارلز كولي وإرفنغ غوفمان، الذين ركزوا على دور التفاعل الرمزي في تشكيل الهوية

والسلوك الاجتماعي (Al-Ayyashi & Al-Farfar، ٢٠٢١).

أهم الافتراضات :

- السلوك نتاج للتفاعل الاجتماعي: أي أن تصرفات الأفراد تتحدد من خلال تفاعلهم مع الآخرين، وليس بمعزل عن المجتمع (Touati & Maataoui، ٢٠٢٤).
- تأثير القيم والمعايير الاجتماعية: اذ تمارس الثقافة والتوقعات الجماعية ضغطاً يوجّه السلوك الفردي ((Ben Halima، ٢٠٢١.
- بناء الذات عبر التفاعل: يرى ميد وكولي أن مفهوم "الذات" يتشكل عبر انعكاس نظرة الآخرين وتصوراتهم للفرد Al-Ayyashi & Al-Farfar، ٢٠٢١)).

دور النظرية في تفسير الثقة الإلكترونية

في سياق البيئة الرقمية، تفسر هذه النظرية كيفية تشكّل الثقة الإلكترونية لدى الشباب الجامعي كنتيجة للتفاعلات الاجتماعية والثقافة السائدة في المجتمع الأكاديمي. فكلما عززت المؤسسات التعليمية قيم الأمن الرقمي وقدمت برامج توعية، زاد استعداد الأفراد لتبني ممارسات آمنة في الفضاء السيبراني (Qandil، ٢٠٢). وبذلك، تسهم هذه النظرية في فهم أثر التوقعات والتفاعلات الاجتماعية على مستوى الثقة الإلكترونية، وانعكاسها على تعزيز الأمن السيبراني لدى طلاب الجامعات (López Mendoza، ٢٠٢٥).

ثانياً: الدراسات السابقة

أولاً: دراسات تتناول الأمن السيبراني

دراسة Al Mutairi, B. A. (٢٠٢٥). بعنوان متطلبات تنمية الوعي بالأمن السيبراني لدى طلاب المدارس الثانوية الحكومية: تصور مقترح: هدفت الدراسة إلى التعرف على متطلبات تنمية الوعي بالأمن السيبراني لدى طلاب المدارس الثانوية الحكومية في المملكة العربية السعودية، وتحديد الفروق الإحصائية بين متوسطات درجات أفراد عينة الدراسة فيما يتعلق بهذه المتطلبات بناءً على متغيرات الدراسة. كما سعت الدراسة إلى الوصول إلى تصور مقترح لتنمية الوعي بالأمن السيبراني لدى طلاب المدارس الثانوية الحكومية، استخدمت الدراسة المنهج الوصفي بأسلوبه المسحي، حيث تم تطبيق استبانة على عينة بلغت ١٢٤٤ فرداً من المديرين والوكلاء والمعلمين في المدارس الثانوية الحكومية بالمناطق الإدارية الخمس في المملكة: الرياض، وجازان، ومكة المكرمة، والشرقية، والحدود الشمالية، أظهرت الدراسة نتائج عدة من أبرزها أن هناك حاجة ملحة لتنمية الوعي بالأمن السيبراني لدى طلاب المدارس الثانوية في المملكة، وأن هذه التنمية تتطلب جهوداً تقنية وتنظيمية وتعليمية واجتماعية ودينية

ونفسية. كما كشفت الدراسة عن وجود فروق إحصائية في متوسطات درجات عينة الدراسة بناءً على متغيرات الدراسة، وأوصت الدراسة بضرورة التركيز على تطوير متطلبات تنمية الوعي بالأمن السيبراني عبر مختلف الأبعاد، بما في ذلك تعزيز الجوانب التقنية، وتحسين البنية التنظيمية، وتطوير المناهج التعليمية التي تشمل مفاهيم الأمن السيبراني، فضلاً عن التوعية الاجتماعية والدينية والنفسية.

دراسة López Mendoza et al.،.)٢٠٢٥) بعنوان الأمن السيبراني بين طلاب الجامعات من الجيل Z: دراسة مقارنة لبرامج البكالوريوس في الإدارة والمحاسبة العامة في جامعتين مكسيكيتين (تاماولي باس وخاليسكو) ، هدفت الدراسة إلى مقارنة عادات الأمن السيبراني بين طلاب الجيل زد في برامج البكالوريوس في المحاسبة العامة والإدارة في جامعتين مكسيكيتين، وتحليل العلاقة بين مستوى المعرفة الذاتية للمشاركين حول الكمبيوتر وعاداتهم في مجال الأمن السيبراني. واستخدمت الدراسة المنهج الوصفي التحليلي، واعتمدت على استبيان تم توزيعه على ٥٦٣ طالباً في جامعتين مكسيكيتين (تاماولي باس و خاليسكو)، أظهرت الدراسة نتائج عدة من أبرزها: أن طلاب خاليسكو سجلوا درجات أعلى في معرفة الأمن السيبراني والممارسات الخطرة، كما تم العثور على علاقة ضعيفة بين مستوى معرفة الطلاب الذاتية حول الأمن السيبراني وعاداتهم في هذا المجال. وأوصت الدراسة بتوفير تدريب أكاديمي وغير أكاديمي في مجال الأمن السيبراني لزيادة الوعي وتحسين الممارسات السيبرانية بين الطلاب.

دراسة AlNeyadi, M. S. S. (٢٠٢٤) ، بعنوان "الأمن السيبراني بدولة الإمارات العربية المتحدة: دراسة تحليلية"، هدفت الدراسة إلى تحليل استراتيجيات الأمن السيبراني في دولة الإمارات العربية المتحدة وكيفية تطويرها لمواجهة التهديدات السيبرانية المتزايدة. واستعملت الدراسة المنهج التحليلي، واعتمدت على تحليل السياسات الوطنية والأبحاث المتعلقة بالأمن السيبراني. أظهرت الدراسة نتائج عدة من أبرزها: دولة الإمارات تتمتع برؤية متقدمة في إدارة الأنظمة السيبرانية وتعمل على تعزيز التعاون الدولي لمكافحة التهديدات الإلكترونية. الحكومة الإماراتية تدعم الأبحاث والابتكار في مجال الأمن السيبراني، مما يعزز من قدرتها على التصدي للتحديات المتطورة. وأوصت الدراسة بتعزيز البنية التحتية الحساسة ضد الهجمات الإلكترونية، كما أوصت بتعزيز الوعي بأهمية الأمن السيبراني على جميع المستويات.

دراسة Al Mazrouei (٢٠٢٤) بعنوان "أهمية دور الأمن السيبراني في تحقيق الأمن الإلكتروني بدولة الإمارات العربية المتحدة" هدفت الدراسة إلى تسليط الضوء على أهمية الأمن السيبراني في تحقيق الأمن الإلكتروني في دولة الإمارات العربية المتحدة، ودوره في حماية المعلومات والشبكات من الهجمات السيبرانية في ظل التقدم التكنولوجي والتحول الرقمي السريع في البلاد. واستخدمت الدراسة المنهج الوصفي الاستقرائي، إذ تم دراسة السياسات والاستراتيجيات المتبعة في الإمارات لتعزيز الأمن السيبراني فضلا عن القوانين التي تنظم البيانات وتحد من الجرائم الإلكترونية. أظهرت الدراسة أن الإمارات تتبنى سياسات متقدمة لحماية البنية التحتية الرقمية وضمان استمرارية الخدمات الحيوية، كما أشارت إلى أهمية التعاون الدولي لمكافحة التهديدات العابرة للحدود. وأوصت الدراسة بتطوير المزيد من السياسات القانونية التي تحمي البيانات، وتعزيز التعاون الدولي في مجال الأمن السيبراني لضمان بيئة إلكترونية آمنة ومستقرة تدعم النمو الاقتصادي والاجتماعي في الإمارات.

دراسة Al Ketbi (٢٠٢٤)بعنوان "الأمن الرقمي في دولة الإمارات العربية المتحدة: دراسة تحليلية في أبعاد الأمن السيبراني"، هدفت الدراسة إلى تحليل أهمية الأمن الرقمي في دولة الإمارات العربية المتحدة وتحديد الأبعاد المتعلقة بالأمن السيبراني. واستخدمت الدراسة المنهج التحليلي، و اعتمدت على تحليل البيانات القانونية والتقنية المتعلقة بالأمن السيبراني في الإمارات. أظهرت الدراسة عدة نتائج من أبرزها: تزايد الاعتماد على التكنولوجيا الحديثة في الإمارات يزيد من تعرضها لتهديدات سيبرانية متنوعة. دولة الإمارات تعمل على تطوير إطار قانوني شامل لمكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني. وأوصت الدراسة بضرورة تعزيز القدرات التقنية في مجال الأمن السيبراني، كما أوصت بتعزيز الثقافة الأمنية وتطوير قوانين فعالة لحماية البيانات الشخصية والخصوصية.

دراسة Aldmour (٢٠٢٤) بعنوان "الجرائم السيبرانية وأثرها على الأمن المجتمعي بدولة الإمارات العربية المتحدة" هدفت الدراسة إلى التعرف على تأثير الجرائم السيبرانية على الأمن المجتمعي في دولة الإمارات العربية المتحدة، واستعملت الدراسة

المنهج التحليلي الوصفي، واعتمدت على الاستبيان عبر الإنترنت لجمع البيانات. تم أخذ عينة من حوالي ٦٥ موظفاً في وحدة الجرائم السيبرانية ومركز الدعم الاجتماعي بشرطة الشارقة، أن تم اختيار ٥٥ شخصاً بنسبة ٧١.٦%. أظهرت الدراسة نتائج عدة من أبرزها: أن الجرائم السيبرانية تتميز عن الجرائم التقليدية من حيث السرعة في التنفيذ والمهارات التقنية العالية المطلوبة، كما تبين أن تأثير الجرائم السيبرانية يمتد إلى ثقافة المجتمع وعاداته وتقاليده، إذ تسهم في إدخال ثقافات جديدة وغريبة على المجتمع، وتؤثر في الروابط الأسرية وتقليل العلاقات الاجتماعية، مما يؤدي إلى الفوضى الاجتماعية. كما تبين أن الجرائم السيبرانية تساهم في زيادة انعدام الأمان داخل المجتمع، أن تساعد في نشر الخوف. وأوصت الدراسة بضرورة تعاون جميع الجهات المعنية لمكافحة الجرائم السيبرانية، والإبلاغ عن أي حالات أو تهديدات تستهدف الأفراد أو المؤسسات، وتكثيف الرقابة الأمنية على المواقع الإلكترونية لمنع انتشار الجرائم السيبرانية والفوضى داخل المجتمع الإماراتي.

دراسة Goliath, S., Tsibolane, P., & Snyman, D (٢٠٢٤) ، بعنوان "الفجوة بين الوعي السيبراني والمرونة: تحليل سلوكيات الطلاب في التعليم العالي، سعى الباحثون إلى تحليل مواقف وسلوكيات الطلاب في مؤسسات التعليم العالي تجاه الأمن السيبراني، في ظل التزايد الملحوظ للهجمات الرقمية التي تستهدف هذا القطاع، وهدفت الدراسة إلى الكشف عن مدى وعي الطلاب بممارسات الحماية الرقمية وتحديد الفجوة بين هذا الوعي والقدرة على التعامل الفعلي مع التهديدات الإلكترونية. اعتمدت الدراسة على المنهج الكمي التحليلي، واستندت إلى نظرية السلوك المخطط كإطار نظري، واستخدم الباحثون استبياناً معدلاً يُعرف بـ الاستبيان البشري لأمن المعلومات، طُبّق على عينة من ٢٦٦ طالباً وطالبة من مرحلتي البكالوريوس والدراسات العليا في إحدى الجامعات الجنوب إفريقية. وقد أظهرت النتائج وجود فجوة واضحة بين الوعي والسلوك الأمني، حيث تفوّق طلاب الدراسات العليا على زملائهم في البكالوريوس في إدارة كلمات المرور، وتأمين البريد الإلكتروني، واستخدام وسائل التواصل الاجتماعي، وحماية الأجهزة

المحمولة. وقد صاغت الدراسة مفهوماً جديداً بعنوان "فجوة الصمود السيبراني"، للدلالة على التحول الملحوظ في الوعي والسلوك الأمني بين مرحلتي الدراسة. وأوصت الدراسة بضرورة تطوير برامج توعوية موجهة لطلاب البكالوريوس في مرحلة مبكرة، لتعزيز مرونتهم الرقمية وتقليص الفجوة الأمنية، وبناء بيئة أكاديمية أكثر أماناً واستقراراً.

دراسة Abdelmaksoud (٢٠٢٤) بعنوان"استكشاف دور الأمن السيبراني في تعزيز الثقة الرقمية لوكالات السفر والسياحة المصرية"، هدفت الدراسة إلى تعزيز الوعي بتطبيق الأمن السيبراني والنظافة السيبرانية في قطاع السياحة، وتوضيح دور الأمن السيبراني في تعزيز الثقة الرقمية لوكالات السفر. استخدمت الدراسة المنهج الوصفي التحليلي، واعتمدت أداة الاستبيان التي طبقت على عينة مكونة من ٤٠٣ من المديرين والموظفين المعنيين في وكالات السفر المصرية. أظهرت الدراسة عدة نتائج، منها: أن وكالات السفر المهتمة بالأمن السيبراني يمكنها تعزيز الثقة الرقمية لعملائها، وأن استخدام الأمن السيبراني بشكل فعال يمكن أن يساعد في حماية الشبكات السياحية من المخاطر الأمنية. أوصت الدراسة بضرورة إكساب الموظفين المهارات اللازمة لتحقيق الأمن السيبراني، وضرورة وجود قسم مختص بالأمن السيبراني في وكالات السفر لضمان الوقاية والحماية الفعالة.

دراسة Al Muhairi (٢٠٢٣) بعنوان "دور دولة الإمارات العربية المتحدة في تحقيق الأمن الإلكتروني"، هدفت الدراسة إلى استعراض دور دولة الإمارات في تحقيق الأمن الإلكتروني من خلال سياساتها التشريعية وجهودها التقنية لتعزيز الأمن الرقمي. واستعملت الدراسة المنهج التحليلي، و اعتمدت على تحليل السياسات والتشريعات المتعلقة بالأمن الإلكتروني في الإمارات. أظهرت الدراسة عدة نتائج، منها: إنشاء العديد من مواقع الإنترنت لمكافحة الإرهاب الإلكتروني والأمن الرقمي، بما في ذلك المبادرات الحكومية والقطاع الخاص. وأن الإمارات تسعى لتحقيق التطور الشامل في البنية التحتية الرقمية بما يتماشى مع التقدم العالمي. وأوصت الدراسة بضرورة التعاون وتضافر الجهود في جمع المعلومات الاستخبارية وتبادلها، كما أوصت بالتعاون الدولي في التحقيقات والملاحقات القضائية.

دراسة Qandil (٢٠٢٣) بعنوان "آليات تحقيق الأمن المعلوماتي في دولة الإمارات العربية المتحدة". هدفت الدراسة إلى التعرف على آليات تحقيق الأمن المعلوماتي في دولة الإمارات العربية المتحدة، واستعملت الدراسة المنهج الوصفي التحليلي، واعتمدت على جمع البيانات وتحليلها وعرض النتائج وكتابة التقرير النهائي. أظهرت الدراسة عدة نتائج من أبرزها: أن أمن المعلومات يمثل حجر الزاوية في نهضة تكنولوجيا المعلومات والاتصالات وتطورها، وأن هناك قصوراً تشريعياً في بعض الأحيان في بعض التصرفات التي قد تُنتهك بها أُطر الأمن المعلوماتي، فضلاً عن وجود مجموعة من الإجراءات والتدابير لتوفير الحماية للمعلومات الرقمية مثل حملات التوعية والتثقيف المرتبطة بالأمن المعلوماتي. وأوصت الدراسة بضرورة معالجة القصور التشريعي وتطوير برامج وحملات توعية أكثر فعالية لتعزيز الأمان المعلوماتي في الإمارات.

دراسة Alhamiri (٢٠٢٣) بعنوان "دور السلامة السيبرانية والأمن الرقمي في دولة الإمارات العربية المتحدة". هدفت الدراسة إلى الكشف عن دور السلامة السيبرانية والأمن الرقمي في دولة الإمارات العربية المتحدة، واستعملت الدراسة المنهج الوصفي التحليلي، واعتمدت على تحليل البيانات المتاحة حول الأمن السيبراني في الدولة. أظهرت الدراسة عدة نتائج من أبرزها: أن الإمارات قد طورت استراتيجية وطنية للأمن السيبراني تهدف إلى تحسين مستوى الأمان الإلكتروني وحماية المعلومات والبنية التحتية الرقمية، كما تناولت الدراسة مفهوم الأمن السيبراني وتحدياته، بالإضافة إلى أبعاده وأنواعه المختلفة. وأوصت الدراسة بضرورة تعزيز التعاون الدولي في التحقيقات والملاحقات القضائية، وتطبيق التدابير اللازمة لحماية الأنظمة الحاسوبية والشبكات الإلكترونية من الاختراق.

ثانياً: دراسات تتناول الثقة الإلكترونية

دراسة Qandil (٢٠٢٥) بعنوان أثر مشاريع التحول الرقمي في تحسين بطاقة أداء الثقة الرقمية بالتطبيق على وزارة التربية والتعليم الفني المصرية، هدفت الدراسة إلى الكشف عن أثر تطبيق مشاريع التحول الرقمي على أبعاد الثقة الرقمية في وزارة التربية والتعليم المصرية. استعملت الدراسة المنهج الوصفي التحليلي، إذ اعتمدت على استبيان لجمع البيانات الإحصائية من أفراد عينة الدراسة. اشتمل الاستبيان على ٤١ فقرة موزعة على خمسة أبعاد: البعد الأول لقياس مشاريع التحول الرقمي، وأربعة أبعاد للثقة الرقمية وهي: البيئة الرقمية، تجارب المستعملين ، اتجاهات ومشاعر

المستخدمين، ومشاركة المستخدمين، أظهرت نتائج الدراسة أن جميع الأبعاد الواردة في هذا المقياس جاءت بدرجة عالية. حيث بلغ الوزن النسبي لبعد استعمال التكنولوجيا ووسائل التواصل الاجتماعي ٧٦%، وجاء في المرتبة الأولى، بينما حصل بعد اتجاهات ومشاعر المستعملين على وزن نسبي ٧٣.٨% في المرتبة الثانية، وحصل بعد خبرة المستخدمين على وزن نسبي ٧١.٣% في المرتبة الثالثة، بينما جاء بعد البيئة الرقمية في المرتبة الرابعة بنسبة ٦٩.٦%. كما أظهرت الدراسة وجود علاقة ارتباط وأثر معنوي بين التحول الرقمي والثقة الرقمية بأبعادها الأربعة، مما يشير إلى أن لمشاريع التحول الرقمي دوراً مهماً وفعالاً في تحسين أبعاد الثقة الرقمية، وأوصت الدراسة بضرورة تعزيز وتوسيع تطبيق مشاريع التحول الرقمي في وزارة التربية والتعليم المصرية، والعمل على تحسين بيئة التكنولوجيا ووسائل التواصل الاجتماعي لضمان تعزيز الثقة الرقمية بين المستخدمين، خاصة في مجال التعليم.

دراسة Babbah (٢٠٢٤) بعنوان "دور الثقة الرقمية في نجاح الإدارة الإلكترونية" هدفت الدراسة إلى استكشاف تأثير الثقة الرقمية على نجاح تطبيقات الإدارة الإلكترونية في المؤسسات الحكومية. استعملت الدراسة المنهج الوصفي التحليلي،إذ اعتمدت على استبيان لجمع البيانات من الأفراد والمؤسسات المشاركة في العمليات الرقمية. أظهرت الدراسة عدة نتائج من أبرزها أن الثقة الرقمية تُعد أحد العوامل الأساسية في نجاح التحول الرقمي، إذ تؤثر بشكل مباشر على مدى استعمال الأفراد للمنصات الإلكترونية وجودة تفاعلهم مع الخدمات الرقمية. كما تبين أن الأمان الرقمي والأمن القانوني هما من العوامل الحيوية التي تعزز من الثقة الرقمية وتزيد من قبول المستعملين للخدمات الإلكترونية. وأوصت الدراسة بضرورة تعزيز الجهود لتحسين الأمان الرقمي وتعزيز الشفافية القانونية بما يتوافق مع التحولات الرقمية الحديثة، مع التركيز على بناء الثقة بين جميع أطراف الإدارة الإلكترونية لضمان نجاحها واستدامتها.

دراسة Sabaa (٢٠٢٣) بعنوان "توسيط الثقة الإلكترونية في العلاقة بين تسويق المحتوى والاحتفاظ بالعميل: دراسة تطبيقية على مستخدمي مواقع التسوق الإلكتروني"، هدفت الدراسة إلى بيان التأثير المباشر وغير المباشر لأبعاد تسويق المحتوى على الاحتفاظ بالعميل من خلال توسيط الثقة الإلكترونية. واعتمدت الدراسة على المنهج الوصفي التحليلي، وعلى استبيان تم تطبيقه على عينة من ٤٣٣ فرداً من مستعملي مواقع

التسوق الإلكتروني في جمهورية مصر العربية. أظهرت الدراسة عدة نتائج من أبرزها: وجود تأثير معنوي إيجابي لأبعاد تسويق المحتوى على الاحتفاظ بالعميل، باستثناء المصداقية والقيمة. وجود تأثير معنوي إيجابي للثقة الإلكترونية على الاحتفاظ بالعميل. وأوصت الدراسة بضرورة تحسين أبعاد تسويق المحتوى مثل المصداقية والجاذبية لتعزيز الاحتفاظ بالعميل، كما أوصت بزيادة الاهتمام بتطوير الثقة الإلكترونية على مواقع التسوق الإلكتروني من خلال التركيز على الجدارة والنزاهة.

Al Dakroury (٢٠٢٣) بعنوان "الدور الوسيط لحب العلامة والثقة الإلكترونية في العلاقة بين تجربة العلامة عبر الإنترنت والكلمة المنطوقة الإلكترونية: دراسة تطبيقية على عملاء مواقع التسوق الإلكتروني". هدفت الدراسة إلى التعرف على التأثيرات المباشرة وغير المباشرة لتجربة العلامة التجارية عبر الإنترنت على الكلمة المنطوقة الإلكترونية، مع توسيط حب العلامة والثقة الإلكترونية، واستخدمت الدراسة المنهج الاستنباطي، واعتمدت على جمع البيانات من خلال موقع Google Drive باستخدام عينة شبكية حجمها ٦٨١ مفردة، أو ما يعرف بعينة كرة الثلج (Snowball Sample). أظهرت الدراسة عدة نتائج من أبرزها: وجود تأثير معنوي إيجابي لتجربة العلامة عبر الإنترنت على حب العلامة والثقة الإلكترونية، بالإضافة إلى تأثير معنوي إيجابي لتجربة العلامة على أبعاد الكلمة المنطوقة الإلكترونية مثل قادة الرأي والباحثين عن الرأي وتمرير الرأي. كما توصلت الدراسة إلى وجود تأثير غير مباشر لتجربة العلامة عبر الإنترنت على الكلمة المنطوقة الإلكترونية بتوسيط كل من حب العلامة والثقة الإلكترونية. وأوصت الدراسة بضرورة التواصل المستمر مع العملاء وتوفير أدوات تكنولوجية مثل Chatbot وتحسين الموقع لتلبية احتياجات العملاء وتعزيز تجربتهم.

دراسة Andi Arini Syahidah, Muhammad Fikry Aransyah (٢٠٢٣)، بعنوان "تأثير جودة الخدمة الإلكترونية والثقة الإلكترونية على ولاء العملاء الإلكترونيين لدى مستخدمي المحفظة الرقمية DANA من خلال الرضا الإلكتروني كمتغير وسيط"، أجريت الدراسة في إندونيسيا في جامعة مولواَرمان (Universitas Mulawarman) هدفت الدراسة إلى تحليل العلاقة بين جودة الخدمة الإلكترونية والثقة الإلكترونية ومدى تأثيرهما على ولاء العملاء الإلكترونيين، مع دراسة دور الرضا الإلكتروني كمتغير وسيط. اعتمدت الدراسة على المنهج الكمي التفسيري (Explanatory Research)، استعملت

استبياناً إلكترونياً كأداة لجمع البيانات، وتم تطبيقه على عينة من ١٠٠ مستعمل لمحفظة DANA الإلكترونية ممن قاموا بإجراء معاملتين غير نقديتين على الأقل خلال الأشهر الستة الأخيرة. وتم استعمال تحليل النمذجة بالمعادلات الهيكلية (Structural Equation Modelling) باستعمال برنامج SmartPLS ٤.٠. وتوصلت الدراسة إلى عدة نتائج، من أهمها: أن جودة الخدمة الإلكترونية والثقة الإلكترونية تؤثران بشكل إيجابي على الرضا الإلكتروني، وأن الرضا الإلكتروني بدوره يؤثر بشكل إيجابي ومباشر على ولاء العملاء، في حين أن التأثير المباشر لكل من جودة الخدمة والثقة الإلكترونية على ولاء العملاء لم يكن معنوياً. وأوصت الدراسة بأهمية تحسين جودة الدعم الفني وخدمة العملاء، لضمان تعزيز رضا وولاء مستعملي المحفظة الرقمية.

دراسة Al-Sarayrah and Al-Kasasbeh (٢٠٢٢) ، بعنوان "أثر الثقة الإلكترونية في نجاح المنظمات الافتراضية في الأردن"، هدفت الدراسة إلى التعرف على الثقة الإلكترونية بأبعادها (مصداقية المصدر، جودة المعلومات، جودة الموقع الإلكتروني، العلاقة مع العملاء) وأثرها في نجاح المنظمات الافتراضية بأبعادها (القيادة الافتراضية، فرق العمل الافتراضية، الكفاءة، الفاعلية).اعتمدت الدراسة على المنهج الوصفي التحليلي، وعلى الاستبانة كأداة رئيسة لجمع البيانات. تم تطبيق الدراسة على عينة من العاملين في المنظمات الافتراضية في الأردن، والتي بلغت (٦٨٧) عاملاً في (١٥) منظمة افتراضية، تم توزيع (٢٤٦) استبانة واسترداد (٢٣٥) استبانة صالحة للتحليل بنسبة (٩٥.٥%). أظهرت الدراسة عدة نتائج، منها: ١) وجود أثر ذو دلالة إحصائية للثقة الإلكترونية بأبعادها في نجاح المنظمات الافتراضية في الأردن. ٢) تأثير الثقة الإلكترونية في القيادة الافتراضية وكفاءة الفرق الافتراضية. وأوصت الدراسة بضرورة اهتمام إدارة المنظمات الافتراضية في الأردن بإدامة المعلومات على المواقع الإلكترونية بكل وضوح وموضوعية للعملاء، وزيادة الاهتمام بالعلاقة مع العملاء لتعزيز القيادة الافتراضية ونجاح المنظمات.

دراسة Abdel-Ati (٢٠٢٢) بعنوان "مستويات الثقة في المواقع الإلكترونية الصحية التي يتعرض لها الشباب وعلاقتها بالمراق الإلكتروني لديهم: دراسة ميدانية"، هدفت الدراسة إلى تحليل تأثير الثقة في المعلومات الصحية المتاحة على الإنترنت على سلوكيات المراهق الإلكتروني (الوسواس الإلكتروني) لدى الشباب، فضلا عن دراسة العوامل الاجتماعية والديموغرافية المرتبطة بالاستعمال المستمر لهذه المعلومات.

اعتمدت الدراسة على المنهج الوصفي واستعملت مقياس ليكرت ذو السبع نقاط لقياس سلوكيات المراهق الإلكتروني والوسواس المرضي، إلى جانب مقياس "ويتلى" الذي طوره "بلوسكاي" لتقييم كفاءة المحتوى والفائدة المتوقعة من المعلومات الصحية وسهولة استعمال المواقع الإلكترونية الصحية. طبقت الدراسة على عينة من الشباب الذين تتراوح أعمارهم بين ١٨-٣٥ عاماً، نظراً لأنهم الفئة الأكثر استعمالا للإنترنت في البحث عن المعلومات الصحية. وأظهرت النتائج أن الثقة في المعلومات الصحية على الإنترنت مع استمرارية استعمال المواقع الإلكترونية الصحية يؤدي إلى ظهور سبعة أنواع من سلوكيات المراهق الإلكتروني، كما أوضح تحليل التباين الأحادي أن الاستعمال المستمر لهذه المعلومات يرتبط بزيادة القلق الصحي الإلكتروني لدى الأفراد. وأوصت الدراسة بضرورة تعزيز وعي الشباب حول كيفية تقييم مصداقية المعلومات الصحية التي يحصلون عليها عبر الإنترنت.

دراسة Albishi (٢٠٢١) بعنوان "الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة"، هدفت الدراسة إلى التعرف على واقع الأمن السيبراني في جامعة بيشة وأثره في تعزيز الثقة الرقمية وفقاً لوجهة نظر أعضاء هيئة التدريس. اعتمدت الدراسة على المنهج الوصفي التحليلي، و أداة الاستبيان التي شملت مواضيع الأمن السيبراني والثقة الرقمية، وتم تطبيق الاستبيان على عينة من ٢١٠ أعضاء هيئة تدريس، منهم ١٨٢ موظفاً. أظهرت الدراسة نتائج عدة ، منها: (١) أن واقع الأمن السيبراني في الجامعات السعودية يعتبر عالياً من وجهة نظر أعضاء هيئة التدريس بنسبة ٧٣.١٨%، و(٢) أن مستوى الثقة الرقمية في الجامعات السعودية من وجهة نظر أعضاء هيئة التدريس مرتفع أيضاً بنسبة ٧٤.٥٨%. وأوصت الدراسة بتوصيات عدة ، أبرزها: تخصيص ميزانية لتوفير متطلبات الأمن السيبراني وتطبيقاتها، والاهتمام بشكل أكبر بحماية المعلومات وبرامج الأمان نظراً لتأثيرها على الثقة الرقمية للمستفيدين.

دراسة Khadem and Moqaddem (٢٠٢١) بعنوان "دور بناء الثقة في تطوير المعاملات الرقمية: فرنسا أنموذجا". هدفت الدراسة إلى استكشاف دور بناء الثقة في تطوير المعاملات الرقمية في فرنسا، واعتمدت الدراسة على المنهج التحليلي، و على دراسة النموذج الفرنسي من خلال ثلاثة مرتكزات رئيسة هي: الأمن القانوني، والتعاقدي، والرقمي. أظهرت الدراسة نتائج عدة من أبرزها: أن بناء الثقة في المعاملات

الرقمية يعتمد بشكل كبير على تعزيز الأطر القانونية والتعاقدية، فضلاً عن توفير بيئة رقمية آمنة لضمان حماية حقوق الأفراد والمستهلكين. وأوصت الدراسة بضرورة تعزيز الشفافية والأمن القانوني في المعاملات الرقمية من خلال تطوير التشريعات وتنظيماتها، مع التأكيد على أهمية بناء ثقة المستخدمين في الأنظمة الرقمية عبر ضمان أمان البيانات والمعلومات.

دراسة Kokash and Al Badri (٢٠١٩)، بعنوان "الأثر المعدل للمخاطر المدركة على العلاقة بين الثقة عبر الإنترنت والنية في الشراء لدى مواقع التسوق الإلكترونية في الأردن"، هدفت الدراسة إلى الكشف عن أثر الثقة عبر الإنترنت على نية العميل للشراء بوجود متغير معدل المخاطر المدركة. استعملت الدراسة المنهج الكمي، وأداة الاستبانة لجمع البيانات، إذ طبقت على عينة من ٧٦٠ طالباً من سبع جامعات خاصة في مدينة عمان. أظهرت الدراسة نتائج عدة أبرزها: أن مستوى الثقة عبر الإنترنت في مواقع التجارة الإلكترونية كان مرتفعاً، كما توصلت إلى وجود أثر ذو دلالة إحصائية لجميع اتجاهات الثقة عبر الإنترنت على نية العميل للشراء. وأوصت الدراسة بضرورة تعزيز الثقة عبر الإنترنت في مواقع التجارة الإلكترونية من خلال تأكيد الشفافية والأمن، بالإضافة إلى الاهتمام بتقليل المخاطر المدركة التي قد تؤثر سلباً على نية الشراء.

ودراسة Boumediene (٢٠١٩) بعنوان "آليات بناء الثقة الرقمية في المغرب". هدفت الدراسة إلى استعراض آليات بناء الثقة الرقمية في المغرب، واستعملت الدراسة المنهج التحليلي، واعتمدت على تقسيم البحث إلى عنصرين رئيسيين أن إشكاليات البيئة الرقمية تشمل قلة ثقة المستعملين في الخدمات الإلكترونية والبنية التحتية للنظم المعلوماتية، فضلا عن ضعف الإطار القانوني والتنظيمي. كما أظهرت الدراسة أن المغرب قد بذل جهوداً كبيرة لتعزيز الثقة الرقمية من خلال تأهيل الإطار القانوني وتطوير الهيكل التنظيمي، مع التركيز على دور الهيئات مثل المجلس الوطني لتكنولوجيات المعلومات والاقتصاد الرقمي، واللجنة الوطنية لحماية المعطيات الشخصية، وهيئات المصادقة الإلكترونية. وأوصت الدراسة بضرورة تعزيز التعاون بين جميع أصحاب المصلحة في مجتمع المعلومات لبناء الثقة في تكنولوجيا المعلومات والاتصالات وضمان أمنها.

دراسة Dakrory et al. (٢٠١٨) بعنوان "أثر أخلاقيات البيع الإلكتروني على الثقة الإلكترونية: دراسة تطبيقية على عملاء مواقع التسوق الإلكتروني"، هدفت الدراسة إلى اختبار تأثير أخلاقيات البيع الإلكتروني بأبعادها المختلفة المتمثلة في الخصوصية، الأمن، عدم الخداع التسويقي، والمصداقية على الثقة الإلكترونية لعملاء مواقع التسويق الإلكتروني. واستخدمت الدراسة المنهج الكمي، واعتمدت أداة الاستقصاء لجمع البيانات، ومن تم تطبيقها على عينة من ٤٢٨ مستجيباً. أظهرت الدراسة نتائج عدة أبرزها: وجود تأثير معنوي لأبعاد أخلاقيات البيع الإلكتروني على الثقة الإلكترونية، كما أظهرت أن الخصوصية والأمن كان لهما تأثير كبير على تعزيز الثقة الإلكترونية لدى العملاء. وأوصت الدراسة بضرورة تعزيز أخلاقيات البيع الإلكتروني ولاسيما في مجالات الخصوصية والأمن ،فضلا عن ضرورة وضع استراتيجيات لضمان المصداقية وتجنب الخداع التسويقي في المواقع الإلكترونية.

دراسة Adheem and Al-Ma'aytah (٢٠١٨) بعنوان "أثر خصائص مواقع التواصل الاجتماعي على عملية شراء الزبون: الثقة الإلكترونية كمتغير وسيط: دراسة ميدانية: طلاب الجامعات الأردنية في مدينة عمان"، هدفت الدراسة إلى شرح كيفية تأثير مواقع التواصل الاجتماعي على عملية اتخاذ قرارات الشراء لدى المستهلكين، وإذا كان هذا التأثير يختلف في مراحل مختلفة من هذه العملية. استخدمت الدراسة المنهج الكمي، واعتمدت أداة الاستبيان التي تم توزيعها على عينة من ٣١٠ فرداً في منطقة عسير بالمملكة العربية السعودية. أظهرت الدراسة عدة نتائج، منها: أن تأثير مواقع التواصل الاجتماعي يختلف حسب مراحل اتخاذ القرار الشرائي، حيث كان التأثير أكبر في مرحلة المعلومات بعد الشراء، يليه تأثير مرحلة اتخاذ قرار الشراء، وأن الثقة الإلكترونية تؤدي دوراً وسيطاً في التأثير على قرارات الشراء. وأوصت الدراسة بتوصيات عدة ، أبرزها: ضرورة أن يستغل المسوقون قوة تأثير مواقع التواصل الاجتماعي في مراحل مختلفة من عملية الشراء، وأهمية تعزيز الثقة الإلكترونية لدى المستهلكين لضمان فعالية أكبر في التأثير على قرارات الشراء.

منهجية الدراسة

٣-١ منهجية البحث

اعتمدت الدراسة على منهج المسح الاجتماعي بالعينة ، نظراً لملاءمته في دراسة الظواهر الاجتماعية المرتبطة بسلوكيات الأفراد داخل البيئة الرقمية، اذ يتيح هذا المنهج وصف الظاهرة كما هي، وتحليل أبعادها وعلاقتها بالمتغيرات الأخرى. وباعتباره المنهج الأكثر شيوعاً لقياس اتجاهات وسلوكيات الأفراد، إلى جانب الاعتماد على مراجعة الأدبيات والدراسات السابقة لتوفير الأساس النظري للدراسة واغنائها بالمفاهيم العلمية ذات الصلة.

٣-٢ مجتمع وعينة الدراسة

يتمثل مجتمع الدراسة في طلاب جامعة الشارقة من مختلف الكليات والتخصصات. وقد تم اختيار عينة طبقية عشوائية، شملت طلبة من مساقات مختلفة لضمان التنوع والتوازن بين الذكور والإناث، وبين التخصصات الإنسانية والعلمية. بلغ حجم العينة (٣٠٠) استبانة مكتملة، وهو حجم مناسب لإجراء التحليل الإحصائي واستخلاص النتائج بدرجة عالية من الموثوقية.

حدود الدراسة :

الحدود الزمانية: تقتصر هذه الدراسة على مدة زمنية محددة، حيث تم جمع البيانات خلال العام الدراسي – فصل الصيف ٢٠٢٤-٢٠٢٥. وستكون هذه الفترة هي الإطار الزمني الرئيسي الذي سيتم فيه إجراء الدراسة وتحليل النتائج.

الحدود المكانية: ركزت الدراسة على جامعة الشارقة في دولة الإمارات العربية المتحدة، هذا يحدد المجال الجغرافي الذي ستتم فيه الدراسة، إذ تم جمع البيانات من الطلاب داخل حرم الجامعة، ومن ثم، تقتصر نتائج هذه الدراسة على البيئة الجامعية في الشارقة.

الحدود البشرية: تقتصر الدراسة على عينة عشوائية من طلبة جامعة الشارقة (الذكور والإناث) من مختلف الكليات والمستويات الدراسية.

الحدود الموضوعية: اقتصرت الدراسة على تحليل تأثير الثقة الإلكترونية في تعزيز الأمن السيبراني لدى طلاب جامعة الشارقة، من خلال فحص العلاقة بين درجة الثقة في الأنظمة الرقمية والممارسات الأمنية المتبعة من قبل الطلاب، وتقييم أثر ذلك على مستوى الأمن السيبراني لدى الشباب.

٣-٣ أداة الدراسة

تتمثل أداة الدراسة في استبانة مصممة من ١٠ عبارات بالاعتماد على الأدبيات النظرية والدراسات السابقة ذات الصلة بموضوع الثقة الإلكترونية والأمن السيبراني لقياس دور التوعية والتثقيف السيبراني في تعزيز الثقة في الأمن الإلكتروني لدى طلاب جامعة الشارقة في البيئة الرقمية.

٣-٤ صدق وثبات الأداة

أولاً: إجراءات التحكيم

قبل تطبيق الاستبانة على العينة، تم عرضها على لجنة تحكيم مكونة من خمسة أساتذة متخصصين في علم الاجتماع بقسم علم الاجتماع في كلية الآداب والعلوم الإنسانية والاجتماعية، وذلك للتأكد من صلاحية الفقرات، ووضوحها، ودقتها في قياس الأبعاد المحددة. وبعد الأخذ بملاحظات المحكّمين وإجراء التعديلات اللازمة، تم اعتماد النسخة النهائية من الاستبانة من قِبل المشرفين على الرسالة.

ثانياً: الثبات (معامل كرونباخ ألفا)

لقياس ثبات أداة الدراسة، تم حساب معامل كرونباخ ألفا لكل محور من محاور الاستبانة وللاستبانة ككل. وأظهرت النتائج أن قيمة معامل كرونباخ ألفا الكلية بلغت (٠.٨٨) وهي قيمة مرتفعة جداً تعكس اتساقاً داخلياً جيداً جداً.

٣-٥ طريقة التوزيع وجمع البيانات

بعد اعتماد الاستبانة، تم توزيعها ورقياً على طلبة مساق مجتمع الإمارات (مساق للطلاب وآخر للطالبات)، وذلك لتغطية شريحة مباشرة من المجتمع الطلابي داخل قاعات الدرس. كما تم توزيع نسخة إلكترونية عبر رابط مخصص على باقي طلبة الجامعة من مختلف الكليات، ما ساهم في توسيع نطاق المشاركة وضمان تمثيل متوازن للعينة. وقد استُخدمت كل من الاستبانات الورقية والإلكترونية لتحقيق أعلى مستوى من الشمولية في جمع البيانات.

٣-٦ أسلوب تحليل البيانات

بعد جمع الاستجابات، تم إدخال البيانات في برنامج SPSS لإجراء التحليلات الإحصائية المناسبة. شملت الإجراءات الإحصائية: التكرارات والنسب المئوية لتوزيع المتغيرات، والمتوسطات الحسابية والانحرافات المعيارية لقياس اتجاهات العينة، بالإضافة إلى اختبارات الفروق (مثل اختبار (T) وتحليل التباين (ANOVA) لقياس الفروق الدالة إحصائياً بين أفراد العينة وفق المتغيرات الديموغرافية.

عرض وتحليل النتائج

أولاً: البيانات الديموغرافية

١. الجنس

تشير النتائج جدول (٢) إلى أن نسبة الإناث بلغت أكثر من نصف العينة (٦٢%)، مقابل ٣٨% للذكور. وهذا يعكس مشاركة واسعة للطالبات، مما قد يعكس اهتماماً أكبر أو وعياً متزايداً بين الإناث تجاه قضايا الأمن السيبراني.

٢. التخصص الدراسي

يتضح من الجدول (٣) أن طلبة التخصصات الإنسانية والاجتماعية شكّلوا النسبة الأكبر من العينة، اذ بلغ عددهم

(١٠٣ طالباً) بنسبة ٣٤.٣%. يشير ذلك إلى تمثيل مرتفع لهذه الفئة، وهو ما يعكس اهتماماً متزايداً من طلبة هذه التخصصات بموضوعات الثقة الإلكترونية والأمن السيبراني، رغم أن طبيعة تخصصاتهم ليست تقنية بالدرجة الأولى.

أما طلبة التخصصات العلمية مثل الهندسة وعلوم الحوسبة فقد بلغ عددهم (٨٠ طالباً) بنسبة ٢٦.٧%، مما يُبرز حضوراً قوياً لفئة يُتوقع أن تمتلك وعياً تقنياً أكبر نظراً لطبيعة تخصصاتهم المرتبطة بالأنظمة الرقمية والأمن المعلوماتي.

وجاءت التخصصات القانونية والادارية في المرتبة الثالثة بعدد (٧٤ طالباً) بنسبة ٢٤.٧%. ويعكس ذلك اهتماماً متنامياً من طلبة القانون وإدارة الأعمال بالجوانب المرتبطة بالثقة الرقمية، خاصة في ظل ارتباط هذه المجالات بالتعاملات الإلكترونية وحماية البيانات.

في حين شكّل طلبة التخصصات الصحية النسبة الأقل (٤٣ طالباً) بنسبة ١٤.٣%. قد يُفسَّر ذلك بطبيعة هذه التخصصات التي تركز على الجوانب الطبية والعلمية التطبيقية، ما يجعل اهتمام طلبتها بالموضوعات الرقمية أقل مقارنة بغيرهم، أو بسبب ضغوط ومتطلبات الدراسة في هذه التخصصات.

٣. السنة الدراسية

يوضح الجدول (٤) أن طلبة السنة الخامسة فما فوق يشكّلون النسبة الأعلى في العينة، إذ بلغ عددهم (٦٨ طالباً) بنسبة ٢٢.٧%. يشير ذلك إلى أن شريحة كبيرة من العينة تتكون من طلبة في مراحل دراسية متقدمة، ما قد يعني امتلاكهم خبرة تراكمية أوسع في التعامل مع المنصات الرقمية.

تليهم مباشرة فئة طلبة السنة الأولى بعدد (٦٥ طالباً) بنسبة ٢١.٧%، ما يعكس تمثيلاً كبيراً للطلبة الجدد الذين ما زالوا في بداية تجربتهم الجامعية، وهو ما يتيح مقارنة مهمة بين وعي الطلبة الجدد ووعي الطلبة المتقدمين.

في المرتبة الثالثة، جاءت فئة طلبة السنة الرابعة بعدد (٦٠ طالباً) بنسبة ٢٠.٠%، وهي نسبة قريبة من طلبة السنة الثالثة الذين بلغ عددهم (٥٩ طالباً) بنسبة ١٩.٦%، ما يظهر توازناً في تمثيل السنوات المتوسطة والمتقدمة.

أما طلبة السنة الثانية فقد شكّلوا النسبة الأقل في العينة (٤٨ طالباً) بنسبة ١٦.٠%، وهو ما قد يعكس عوامل مثل انخفاض المشاركة أو ضغط المواد الدراسية خلال هذه المرحلة.

٤. الأجهزة الإلكترونية المستخدمة

أظهرت النتائج جدول (٥) أن الهاتف الذكي جاء في المرتبة الأولى كأكثر الأجهزة استعمالا لتصفح الإنترنت بنسبة ٢٦% من أفراد العينة، وهو ما يعكس المكانة المركزية للهواتف المحمولة في حياة الطلبة اليومية واعتمادهم عليها بشكل أساسي في الأنشطة الرقمية. ويليه استعمال الهاتف مع الحاسوب المحمول (١٥.٣%)، مما يشير إلى أن شريحة معتبرة من الطلبة تدمج بين المرونة التي يتيحها الهاتف وبين القدرات الأكاديمية والتنظيمية التي يوفرها اللابتوب.

أما فئة الطلبة الذين يستخدمون الهاتف + اللابتوب + التابلت فقد شكّلوا نسبة ١٣.٧%، وهو ما يعكس تنوعاً في تفضيلات الطلبة ورغبتهم في الاستفادة من خصائص متعددة للأجهزة المختلفة. كما بلغت نسبة الاعتماد على الحاسوب المكتبي فقط ١٠.٣%، وهي نسبة أقل مقارنة بالأجهزة المحمولة، ما يؤكد تراجع دور الأجهزة المكتبية لصالح البدائل الأكثر تنقلاً. من ناحية أخرى، بلغت نسبة مستخدمي الأجهزة اللوحية (التابلت) بشكل منفرد ٧.٧%، في حين أظهرت النتائج أن فئة "الهاتف + اللابتوب + المكتبي + التابلت" تمثل ٦% من العينة، وهو مؤشر على وجود مجموعة صغيرة من الطلبة الذين يعتمدون على تعددية الأجهزة بشكل كبير. كما توزعت باقي النسب على تراكيب مختلفة مثل: الهاتف + التابلت (٥.٧%)، الهاتف + اللابتوب + المكتبي (٥.٣%)، والهاتف + المكتبي (٥%).

بشكل عام، توضح هذه النتائج أن معظم الطلبة يعتمدون على الأجهزة المحمولة (الهاتف الذكي واللابتوب) سواء بشكل منفرد أو ضمن تركيبات مع أجهزة أخرى، في حين يبقى الاعتماد على الحاسوب المكتبي محدوداً نسبياً. وهذا يعكس التحول نحو الأجهزة الأكثر مرونة وتنقلاً، مما يستدعي تركيز استراتيجيات التوعية والتثقيف في مجال الأمن السيبراني على هذه الأجهزة بالتحديد.

٥. محاولات الاختراق

أفاد نحو ثلث العينة (٢٩.٧%) بتعرضهم لمحاولة اختراق إلكتروني، وهو مؤشر يستحق الاهتمام نظراً لتأثيره المباشر على الثقة والأمان الرقمي. جدول (٦).

٦. التعرض لمحاولات الاحتيال

أكثر من نصف الطلبة (٥١.٣%) مروا بمحاولة احتيال إلكتروني، ما يعكس انتشار هذه الظاهرة بصورة تفوق الاختراقات التقنية المباشرة، و يرتبط غالباً بالهندسة الاجتماعية.

٧. الحصول على تدريب في الأمن السيبراني

٥٧% من الطلبة لم يحصلوا على أي نوع من التدريب في الأمن السيبراني، مما

يبرز فجوة واضحة في التثقيف المؤسسي ويشير إلى الحاجة لتكثيف البرامج التوعوية.

٨. نوع التدريب أو المعرفة المكتسبة

يتضح من الجدول (٩) أن الفئة الأكبر من الطلبة صنّفوا خبرتهم التدريبية ضمن خيار "أخرى"، بعدد (١٢٣ طالباً) بنسبة ٤١.٠%، وهو ما يعكس غياب إطار تدريبي موحّد، أو اعتماد الطلبة على مصادر متفرقة وغير رسمية، وقد يشير أيضاً إلى ضعف تكامل البرامج التدريبية الجامعية مع احتياجات الطلبة.

أما فئة المعرفة الذاتية (من الإنترنت أو الكتب) فقد جاءت في المرتبة الثانية بعدد (٩٠ طالباً) بنسبة ٣٠.٠%، ما يدل على اعتماد ملحوظ للطلبة على التعلم الذاتي في مجال الأمن السيبراني، خاصة من خلال الموارد الرقمية المفتوحة.

السؤال الأول: إلى أي مدى تثق في المواقع الإلكترونية التي تطلب معلومات شخصية (مثل الاسم أو البريد الإلكتروني)؟

يتضح من النتائج أن الغالبية العظمى من الطلبة (٦٢.٧%) يبدون قدراً محدوداً من الثقة في المواقع الإلكترونية، بينما ٢٤.٣% لا يثقون بها إطلاقاً، و١٣% فقط عبروا عن ثقة مرتفعة. وهذا يعكس وجود نزعة حذرة لدى الطلبة في التعامل مع المواقع التي تطلب بيانات شخصية.

السؤال الثاني: هل تتحقق من وجود علامات الأمان مثل رمز القفل أو بروتوكول (https) عند الدخول إلى المواقع الإلكترونية؟

تشير النتائج إلى أن ٤١.٧% من الطلبة دائماً ما يتحققون من مؤشرات الأمان قبل الدخول إلى المواقع، بينما ٣٨.٣% يفعلون ذلك أحياناً. في المقابل، هناك نسبة لا بأس بها (٢٠%) تتوزع بين من نادراً ما يهتمون أو لا يهتمون إطلاقاً. هذه الأرقام تدل على وجود وعي نسبي بأهمية عناصر الأمان الإلكتروني، إلا أن الثغرات ما زالت موجودة عند شريحة من المستخدمين.

السؤال الثالث: هل تستخدم وسائل الدفع الإلكتروني مثل البطاقات المصرفية أو المحافظ الرقمية؟

تشير النتائج إلى أن غالبية الطلبة (٨٥.٧%) يستخدمون وسائل الدفع الإلكتروني، مقابل ١٤.٣% لا يستخدمونها. هذا يدل على انتشار الاعتماد على المعاملات الرقمية بشكل واسع بين الطلبة.

السؤال الرابع: عند تلقي رسالة من جهة غير معروفة تطلب الضغط على رابط، ماذا تفعل عادةً؟

توضح النتائج أن نصف العينة تقريباً (٥٠.٣%) يتجاهلون الرسائل المشبوهة، بينما ٣٥% يتحققون من المصدر قبل اتخاذ أي إجراء، في حين أن ٨.٧%

يقومون بالتبليغ عنها، و٦% يفتحون الروابط مباشرة. هذا يعكس أن معظم الطلبة يتعاملون مع هذه الرسائل بحذر نسبي، مع وجود فئة صغيرة أكثر عرضة للمخاطر.

ثانياً: نتائج الاستبيان: دور التوعية والتثقيف السيبراني في تعزيز الثقة في الأمن الإلكتروني لدى طلاب جامعة الشارقة في البيئة الرقمية

يُعَدّ التثقيف السيبراني أحد الركائز الأساسية في بناء بيئة رقمية آمنة وتعزيز ثقة الأفراد في استخدام التقنيات الحديثة. فكلما ازدادت معرفة الطلبة بالمخاطر الإلكترونية وآليات الحماية، ارتفعت قدرتهم على التعامل مع التهديدات بوعي ومسؤولية. ويسهم التثقيف السيبراني في نشر ثقافة الحذر والوقاية الرقمية، ويُعد أداة وقائية فعالة تقلل من فرص الوقوع ضحية للهجمات أو محاولات الاحتيال الإلكتروني. ومن هذا المنطلق، يتناول هذا المحور اتجاهات طلبة جامعة الشارقة نحو أهمية برامج التوعية والمحاضرات التدريبية والإرشادات التي تهدف إلى رفع مستوى الوعي الأمني لديهم، ومدى انعكاس ذلك على ثقتهم في البيئة الرقمية.

أظهرت نتائج الجدول (١٤) أن المتوسطات تراوحت بين (٢.٩١–٤.٠٥)، بما يعكس وعياً مرتفعاً نسبياً بأهمية التوعية السيبرانية مع ضعف في الممارسة العملية. فقد تصدرت أهمية حماية الخصوصية (م=٤.٠٥)، تلتها تنبيه الآخرين والبحث عن أفضل الممارسات (م=٣.٩٦). كما برز دعم الجهود المجتمعية (م=٣.٨٦) وطرح الأسئلة (م=٣.٧٢) بمستوى معتدل، في حين تراجع الاهتمام بالمحتوى التدريبي (م=٣.٤١) والمشاركة في الورش (م=٢.٩١). وبلغ المتوسط الكلي (٣.٦٥)، مؤكداً إدراكاً جيداً يقابله قصور في التطبيق، مما يتطلب تفعيل الجهود المؤسسية. جميع قيم (Sig) أكبر من (٠.٠٥)، مما يشير إلى أن الفروق بين متوسطات الطلبة في المحور باختلاف الجنس غير دالة إحصائياً. أي أن الجنس لم يكن له تأثير جوهري على مستوى الثقة الإلكترونية أو العوامل المرتبطة بها لدى طلبة جامعة الشارقة.

تشير نتائج تحليل التباين الأحادي (ANOVA) إلى عدم وجود فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq$ ٠.٠٥) بين الطلبة في المحور الأول (مظاهر الثقة الإلكترونية)، والمحور الثاني (العوامل المساهمة في بناء الثقة الإلكترونية)، والمحور الرابع (دور التوعية والتثقيف السيبراني) باختلاف التخصص الدراسي، مما يعكس تقارباً في استجابات الطلبة من مختلف التخصصات لهذه الأبعاد. في المقابل، أظهر المحور الثالث (المعوقات الثقافية والمجتمعية) قيمة دلالة (Sig = ٠.٠٦٥) وهي قريبة من مستوى

الدلالة الإحصائية، ما قد يشير إلى وجود فروق شبه معنوية تستحق المزيد من التحليل باستخدام اختبارات مثل Scheffé لتحديد التخصصات التي تميزت في إدراكها للمعوقات.

أظهر اختبار Scheffé أن الفروق بين التخصصات في محور المعوقات الثقافية والمجتمعية لم تكن دالة إحصائياً (≤ α ٠.٠٥)، باستثناء اتجاه غير دال بين التخصصات الإنسانية والاجتماعية والصحية (p = ٠.٠٥٣٧)، حيث سجّل طلبة التخصصات الصحية متوسطات أعلى نسبياً. وهذا يشير إلى تقارب عام في إدراك الطلبة للمعوقات بغض النظر عن تخصصاتهم.

أظهرت نتائج تحليل التباين الأحادي (ANOVA) وجود فروق ذات دلالة إحصائية في المحور باختلاف نوع الجهاز المستخدم: العوامل المساهمة في بناء الثقة الإلكترونية (Sig = ٠.٠٠١)، المعوقات الثقافية والمجتمعية (Sig = ٠.٠٠١)، والتوعية والتثقيف السيبراني (Sig = ٠.٠١٩). بينما جاء محور مظاهر الثقة الإلكترونية عند الحد الفاصل (Sig = ٠.٠٥٠) دون دلالة إحصائية قوية. وتشير هذه النتائج إلى أن نوع الجهاز الإلكتروني يعد عاملاً مؤثراً في تشكيل إدراك الطلبة للثقة الإلكترونية ومعوقاتها ومستوى استفادتهم من التوعية، ما يبرز أهمية مراعاة هذا المتغير عند تصميم البرامج والاستراتيجيات الجامعية لتعزيز الثقة الرقمية.

أظهرت نتائج ANOVA وجود تأثير لنوع الجهاز المستخدم على بعض محاور الدراسة، لكن اختبار Scheffé أكد عدم وجود فروق جوهرية بين الأجهزة (p < ٠.٠٥). كما لم تظهر فروق دالة باختلاف الجنس أو التخصص. ويعكس ذلك أن التباينات في الثقة الإلكترونية تعود لعوامل تقنية وثقافية وتوعوية متداخلة، مما يؤكد الحاجة إلى برامج شاملة لتعزيز الوعي السيبراني والأمن الرقمي في البيئة الجامعية.

مناقشة نتائج الدراسة

أظهرت نتائج هذه الدراسة أن مستوى الثقة الإلكترونية لدى طلبة جامعة الشارقة يتأثر بمجموعة من العوامل المرتبطة بالتوعية الأمنية، نوع الأجهزة المستخدمة، والبرامج التثقيفية المقدمة. وقد بينت النتائج أن إدراك أهمية حماية الخصوصية الرقمية ورفع الوعي بالممارسات الوقائية يمثلان أبرز محددات الثقة، بينما تظل المشاركة العملية في الورش والبرامج التدريبية محدودة. تتفق هذه النتائج مع ما توصلت إليه Al Ketbi (٢٠٢٤) التي أكدت أن ارتفاع الوعي الأمني مرتبط بزيادة إدراك الأفراد لأهمية حماية بياناتهم الشخصية، غير أن الممارسات الفعلية تبقى متفاوتة بحسب مستوى الدعم المؤسسي. كما انسجمت مع ما أشار إليه

Al Dmour (٢٠٢٤) من أن الجرائم السيبرانية تؤثر بشكل مباشر على الثقافة المجتمعية وتخلق حالة من الحذر واليقظة الرقمية بين الشباب، وهو ما انعكس في النتائج الحالية حيث أبدى أكثر من نصف أفراد العينة تعرضهم لمحاولات احتيال إلكتروني. وفي السياق ذاته، تدعم هذه الدراسة ما أشار إليه Al Mazrouei (٢٠٢٤) و Al Neyadi (٢٠٢٤) من أن الإمارات تبذل جهوداً واضحة في تعزيز الأمن السيبراني عبر تطوير التشريعات والاستراتيجيات، غير أن فعالية هذه الجهود تعتمد إلى حد كبير على مدى مشاركة الطلبة في البرامج التوعوية. وهو ما ينسجم مع نتائج هذه الدراسة التي كشفت أن نسبة كبيرة من الطلبة (٥٧%) لم يحصلوا على تدريب رسمي في الأمن السيبراني، ما يعكس فجوة واضحة بين السياسات الوطنية ومستوى تطبيقها في البيئة الجامعية. أما فيما يتعلق بدور التخصص الأكاديمي، فقد بينت نتائج الدراسة الحالية تقارباً عاماً في إدراك الطلبة لمظاهر الثقة الإلكترونية عبر مختلف التخصصات، مع فروق شبه معنوية لدى طلبة التخصصات الصحية. وهذا يتوافق مع ما توصلت إليه Al Ketbi (٢٠٢٤) بأن الخلفية الأكاديمية والمعرفية تؤثر في تشكيل الثقافة الرقمية، كما تدعم نتائج Goliath et al. (٢٠٢٤) التي كشفت وجود فجوة بين المعرفة النظرية بالممارسات الأمنية والسلوك العملي للطلبة في التعليم العالي. إلا أن نتائجنا تشير إلى أن التخصص وحده لا يمثل عاملاً حاسماً في بناء الثقة، بل يتداخل مع عوامل أخرى كنوع الجهاز المستخدم ومستوى التوعية المؤسسية. وأخيراً، تتلاقى نتائج هذه الدراسة مع ما أوضحته Sabaa (٢٠٢٣) و Al Dakroury (2023) بأن الثقة الإلكترونية ترتبط بعوامل اجتماعية وثقافية إلى جانب العوامل التقنية، حيث إن تعزيز الثقة لا يتحقق فقط عبر البنية التحتية الرقمية، بل يتطلب دعماً مؤسسياً مستداماً، وتطوير سياسات واضحة لحماية الحقوق الرقمية وضمان بيئة آمنة للطلبة.

ثالثاً: التوصيات

استناد إلى ما توصلت إليه الدراسة من نتائج، يمكن تقديم مجموعة من المقترحات التي قد تسهم في تعزيز الثقة الإلكترونية لدى طلاب جامعة الشارقة، ومن ثم تطوير مستوى الأمن السيبراني في البيئة الجامعية:

١. تعزيز برامج التوعية السيبرانية عبر دمج موضوعات الأمن الإلكتروني في المقررات الجامعية، وتنظيم ورش عمل ودورات تدريبية إلزامية للطلبة في مختلف التخصصات.
٢. إطلاق حملات إعلامية لرفع مستوى الوعي حول أخطار التعامل مع الروابط

المشبوهة أو مشاركة المعلومات الشخصية في منصات غير رسمية.

٣. تشجيع التعلم الذاتي للطلبة من خلال توفير موارد معرفية إلكترونية موثوقة (كأدلة إرشادية، مقاطع توعوية، ومنصات تعليمية رقمية) لتعزيز المعرفة المستمرة.

٤. تعزيز دور الشراكات المؤسسية بين الجامعة والهيئات الحكومية المتخصصة في الأمن السيبراني من أجل الاستفادة من الخبرات الوطنية وتطبيق أفضل الممارسات.

٥. إجراء دراسات مستقبلية تتناول عينات أوسع من أفراد المجتمع أخرى في الدولة لمقارنة النتائج، وكذلك دراسة تأثير العوامل الثقافية والاجتماعية على الثقة الإلكترونية بعمق أكبر.

الخاتمة

خلصت الدراسة إلى أن الثقة الإلكترونية لدى طلاب جامعة الشارقة تمثل نتاجاً لمجموعة من العوامل المتشابكة، تتداخل فيها الأبعاد التقنية والسلوكية والمؤسسية والثقافية. فقد أظهرت النتائج أن الطلبة يمتلكون قدراً لا بأس به من الوعي الرقمي، ويتبنون بعض الممارسات الوقائية مثل استخدام كلمات مرور قوية وتحديث البرامج الأمنية، إلا أن هذا الوعي لا يزال متفاوتاً ويحتاج إلى تعزيز من خلال التدريب والتثقيف السيبراني المنظم. كما بينت الدراسة أن الثقة في الخدمات الرقمية الرسمية تمثل ركناً أساسياً في بناء الاعتمادية على البيئة الرقمية، في حين تظل بعض المعوقات الثقافية والمجتمعية عاملاً مؤثراً قد يحد من فعالية هذه الثقة.

إن أهمية هذه الدراسة تنبع من مساهمتها في تسليط الضوء على واقع الثقة الإلكترونية في بيئة جامعية إماراتية، وهو ما يضيف بعداً معرفياً جديداً للأدبيات في هذا المجال، ويمثل مرجعاً يمكن البناء عليه في السياسات والممارسات المؤسسية الهادفة إلى تعزيز الأمن السيبراني. وتبرز النتائج الحاجة إلى تبني مقاربة شمولية تعالج الجوانب التقنية والمعرفية والثقافية معاً، بما يضمن تمكين الطلبة من التعامل بكفاءة وثقة مع التحديات الرقمية المتنامية.

وبذلك، فإن الدراسة تؤكد أن بناء الثقة الإلكترونية ليس خياراً ثانوياً، بل هو ضرورة استراتيجية لضمان سلامة التعاملات الرقمية، ودعم مسيرة التحول الرقمي في المجتمع الإماراتي بما يتماشى مع الرؤى الوطنية للتنمية المستدامة والأمن السيبراني.

قائمة المصادر والمراجع:

المراجع

أولاً: المصادر العربية

إبراهيم، نور الدين حامد علي. (٢٠٢٤). الفضاء السيبراني: المفاهيم والأبعاد. المجلة العلمية للبحوث والدراسات التجارية، مج ٣٨، ع٢ ، ٧١١ – ٧٤٦. مسترجع من http://search.mandumah.com/Record/1505737

ابن حليمة، محمد. (٢٠٢١). تأثير القيم على السلوك الاجتماعي في الوسط الجامعي. مجلة دراسات إنسانية وإجتماعية، مج. ١٠، ع. ٢ (s)، ص. ٣١٧-٣٣٠، https://search.emarefa.net/detail/BIM-1199914

الاتحاد الدولي للاتصالات. (٢٠٠٢). دليل الأمن السيبراني للبلدان النامية. جنيف: ITU.

احليحل، كريم. (٢٠٢٤). الأمن السيبراني. *المجلة الإلكترونية الدولية لنشر الأبحاث القانونية*، مج٤، ع١٨ ، ٤٨ – ٧٤. مسترجع من ١٤٦٤٩١٢/http://search.mandumah.com/Record

ادهيم، علي حسين علي، والمعايطة، محمد. (٢٠١٨). أثر خصائص مواقع التواصل الاجتماعي على عملية شراء الزبون: الثقة الإلكترونية كمتغير وسيط: دراسة ميدانية: طلاب الجامعات الأردنية في مدينة عمان، (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من http://search.mandumah.com/Record/1296730

بلفرد، لطفي لمين، و برقوق، أمحند. (٢٠٢٤). الفضاء السيبراني: فواعل وتهديدات. *مجلة آفاق للعلوم*، مج٩، ع٣ ، ٦٢١ – ٦٣١. مسترجع من http://search.mandumah.com/Record/1480129

البوابة الرسمية – استراتيجيات الخدمات الحكومية والتحول الرقمي (٢٠٢٤): https://u.ae/ar-AE/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation

بومديان، محمد. (٢٠١٩). آليات بناء الثقة الرقمية في المغرب. مجلة المنارة للدراسات القانونية والإدارية، عدد خاص ، ٨٧ – ١٠٦. http://search.mandumah.com/Record/1058632

بومدين، بوداود، عبد القادر، صواق، و دحو، سليمان. (٢٠٢١). النمذجة البنائية لمساهمة أبعاد الأمن السيبراني للبيانات في تحقيق رضا المستهلك الإلكتروني من خلال تعزيز الثقة كمتغير وسيط: دراسة ميدانية لعينة من مستعملي بطاقات الدفع الإلكتروني لبنك التنمية المحلية BDL بولاية غرداية. *مجلة إدارة الأعمال والدراسات الاقتصادية*، مج٧، ع١ ، ٨٢٩ – ٨٥٢. مسترجع من ١٢٠٢٢٩٨/http://search.mandumah.com/Record

البيشي، منير عبد الله مفلح. (٢٠٢١). الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة. مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، مج ٢٩، ع ٦ ، ٣٥٣ – ٣٧٢. مسترجع من http://search.mandumah.com/Record/1196627

تواتي، نعيمة معطاوي، موسى. ٢٠٢٤. السلوك الاجتماعي للشباب بين معايير التنشئة الاجتماعية وفضاء المنصات الإلكترونية. معارف، مج. ١٩، ع. ١، ص. ٨٢٣-٨٤١، https://search.emarefa.net/detail/BIM-1565651

جربوعة، عادل، و بوطمين، عبدالجبار. (٢٠٢٣). الفضاء الرقمي والأمن السيبراني. *مجلة العلوم الإنسانية*، مج ٣٤، ع ٣ ، ٤٥٣ – ٤٦٤. مسترجع من http://search.mandumah.com/Record/١٤١٨٦١٦

الحميري، سهيل علي ناصر. (٢٠٢٣). دور السلامة السيبرانية والأمن الرقمي في دولة الإمارات العربية المتحدة. مجلة الباحث للدراسات القانونية والقضائية، ع٥٨ ، ٥١٧ – ٥٣٨. مسترجع من http://search.mandumah.com/Record/1414178

خادم، نبيل، ومقدم، أحلام سارة. (٢٠٢١). دور بناء الثقة في تطوير المعاملات الرقمية: فرنسا أنموذجا. مجلة الفكر القانوني والسياسي، مج٥، ع١ ، ١٤١ – ١٥٤. مسترجع من http://search.mandumah.com/Record/1200915

خريسان، باسم علي. (٢٠٢٠). الفضاء السيبراني: حتمية الاتصال وتحدي التواصل مع الآخر. *مجلة تكريت للعلوم السياسية*، ع٢٢ ، ٣ – ٢٤. مسترجع من http://search.mandumah.com/Record/١٢٠٥٥٨٤

دكروري ، منى إبراهيم محمد، عبد الغفار، محمد السعيد، والسطوحي، أحمد محمد السيد أحمد. (٢٠١٨). أثر أخلاقيات البيع الإلكتروني على الثقة الالكترونية: دراسة تطبيقية على عملاء مواقع التسوق الإلكتروني. المجلة المصرية للدراسات التجارية، مج ٤٢، ع١، ٢١٤ – ٢٣٩. مسترجع من http://search.mandumah.com/Record/958530

الدكروري، محمد السعيد عبد الغفار. (٢٠٢٣). الدور الوسيط لحب العلامة والثقة الإلكترونية في العلاقة بين تجربة العلامة عبر الإنترنت والكلمة المنطوقة الإلكترونية: دراسة تطبيقية على عملاء مواقع التسوق الإلكتروني. المجلة العلمية للبحوث والدراسات التجارية، مج ٣٧، ع٢ ، ٧١٥ – ٨٠٣. مسترجع من http://search.mandumah.com/Record/1505946

دليل الأمن السيبراني للبلدان النامية، الاتحاد الدولي للاتصالات، سويسرا، ٢٠٠٢

سبع، سنية محمد أحمد. (٢٠٢٣). توسيط الثقة الإلكترونية في العلاقة بين تسويق المحتوى والاحتفاظ بالعميل "دراسة تطبيقية على مستخدمي مواقع التسوق الإلكتروني". المجلة العلمية للدراسات والبحوث المالية والتجارية، ٤(١)، ١٢٨١-١٣١٣. doi: ٢٠٢٣.٢٥٩٩٩٧.10.21608/cfdj

الضمور، عدنان محمد. (٢٠٢٤). الجرائم السيبرانية وأثرها على الأمن المجتمعي بدولة الإمارات العربية المتحدة. الفكر الشرطي، مج ٣٣، ع١٣١ ، ١٩ - ٦٤. مسترجع من http://search.mandumah.com/Record/1521685

عبد العاطي، علاء محمد (٢٠٢٢). مستويات الثقة في المواقع الإلكترونية الصحية التي يتعرض لها الشباب وعلاقتها بالمراق الإلكتروني لديهم: دراسة ميدانية. المجلة المصرية لبحوث الرأي العام، مج. ٢١، ع. ٢، ج. ١، ص. ٥١-٨٧. https://search.emarefa.net/detail/BIM-1399375

عبد المقصود، ريهام. (٢٠٢٤). استكشاف دور الأمن السيبراني في تعزيز الثقة الرقمية لوكالات السفر والسياحة المصرية، مجلة اتحاد الجامعات العربية للسياحة والضيافة، ٢٦(١)، ١٨٥-٢٠٤. doi: 10.21608/jaauth .٢٠٢٤.٢٦٩٢٩٩.١٥٥٣

قائمة الثقة الإماراتية، (٢٠٢٣) - هيئة تنظيم الاتصالات والحكومة الرقمية: https://tdra.gov.ae

قنديل، أشرف عبد القادر. (٢٠٢٣). آليات تحقيق الأمن المعلوماتي في دولة الإمارات العربية المتحدة. الفكر الشرطي، مج ٣٢، ع١٢٦ ، ١٨٥ - ٢٢٩. مسترجع من http://search.mandumah.com/Record/1393339

قنديل، رضا حسين محمد. (٢٠٢٥). أثر مشاريع التحول الرقمي في تحسين بطاقة أداء الثقة الرقمية بالتطبيق على وزارة التربية والتعليم الفني المصرية. المجلة العربية للإدارة، ٤٥(١)، ٤٣-٦٦. doi: 10.21608/aja .٢٠٢٢.١٠٩٨٨١.١١٨٦

كوكش، ثائر جعفر، والبدري، فايز أحمد. (٢٠١٩). الأثر المعدل للمخاطر المدركة على العلاقة بين الثقة عبر الأنترنت والنية في الشراء لدى مواقع التسوق الإلكترونية في الأردن (رسالة ماجستير غير منشورة). جامعة الشرق الأوسط، عمان. مسترجع من http://search.mandumah.com/Record/1013815

المزروعي، ناصر عبدالله سعيد. (٢٠٢٤). أهمية دور الأمن السيبراني في تحقيق الأمن الإلكتروني بدولة الإمارات العربية المتحدة. مجلة الباحث للدراسات والأبحاث القانونية والاقتصادية والعلوم الإنسانية والشرعية، ع٧١، ١٢٨ - ١٤٢. http://search.mandumah.com/Record/1502303

المطيري، بدر عبد الله. (٢٠٢٥). متطلبات تنمية الوعي بالأمن السيبراني لدى طلاب المدارس الثانوية الحكومية: تصور مقترح. مجلة كلية التربية، مج١٣، ع٤٢ ، ٢٣٤ - ٢٨٢. مسترجع من http://search.mandumah.com/Record/1560444

مكاوي، خيرة (٢٠٠٩). مفهوم الأثر في فلسفة جاك دريدا. مجلة الآداب والعلوم الاجتماعية، ٦(٣)، ٩٦-١٠٩. https://asjp.cerist.dz/en/article/39866

المهيري، عبد الرحمن أحمد. (٢٠٢٣). دور دولة الإمارات العربية المتحدة في تحقيق الأمن الإلكتروني. مجلة قراءات علمية في الأبحاث والدراسات القانونية والإدارية، ع ٢٠، ٤٤١ - ٤٧١. مسترجع من http://search.mandumah.com/Record/1434464

النيـادي، محمد سـعيد سـالم. (٢٠٢٤). الأمـن السـيبراني بدولـة الإمـارات العربيـة المتحـدة: دراسـة تحليليـة. مجلـة الباحـث للدراسـات القانونيـة والقضـائية، ع٦٩، ٣٦٨ – ٣٨٠. مسـترجع مـن http://search.mandumah.com/Record/1481293

المصادر العربية المترجمة إلى اللغة الاجنبية بحسب شروط المجلة :

Ibrahim, N. H. A. (2024). Cyberspace: Concepts and dimensions. The Scientific Journal for Research and Commercial Studies, 38(2), 711–746. http://search.mandumah.com/Record/1505737

Ibn Halima, M. (2021). The impact of values on social behavior in the university environment. Journal of Human and Social Studies, 10(2, Suppl.), 317–330. https://search.emarefa.net/detail/BIM-1199914

International Telecommunication Union. (2002). Cybersecurity guidelines for developing countries. ITU.

Ahleihal, K. (2024). Cybersecurity. International Electronic Journal for Publishing Legal Research, 4(18), 48–74. http://search.mandumah.com/Record/1464912

Adheem, A. H. A., & Al-Ma'aytah, M. (2018). The impact of social media site attributes on the customer purchasing process: E-trust as a mediating variable—A field study of university students in Amman (Unpublished master's thesis). Al-Balqa Applied University, Al-Salt. http://search.mandumah.com/Record/1296730

Belfred, L. L., & Barqouq, A. (2024). Cyberspace: Actors and threats. Afaq for Sciences Journal, 9(3), 621–631. http://search.mandumah.com/Record/1480129

UAE Government Portal. (2024). Government services and digital transformation strategies. https://u.ae/ar-AE/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation

Boumediene, M. (2019). Mechanisms for building digital trust in Morocco. Al-Manara Journal for Legal and Administrative Studies (Special Issue), 87–106. http://search.mandumah.com/Record/1058632

Boumediene, B., Abdelkader, S., Souaq, A., & Dahou, S. (2021). Structural modeling of the contribution of data-cybersecurity dimensions to achieving e-consumer satisfaction through strengthening trust as a mediating variable: A field study on users of BDL e-payment cards in Ghardaïa Province. Journal of Business Administration and Economic Studies, 7(1), 829–852. http://search.mandumah.com/Record/1202298

Al Bishi, M. A. M. (2021). Cybersecurity in Saudi universities and its impact on enhancing digital trust from the perspective of faculty members: A study at the University of Bisha. Islamic University

Journal for Educational and Psychological Studies, 29(6), 353–372. http://search.mandumah.com/Record/1196627

Touati, N., & Maataoui, M. (2024). Youth social behavior between socialization norms and the space of electronic platforms. Maaref, 19(1), 823–841. https://search.emarefa.net/detail/BIM-1565651

Jarboua, A., & Boutmine, A. (2023). The digital space and cybersecurity. Journal of Human Sciences, 34(3), 453–464. http://search.mandumah.com/Record/1418616

Al Hamiri, S. A. N. (2023). The role of cybersecurity and digital safety in the United Arab Emirates. Al-Bahith Journal for Legal and Judicial Studies, (58), 517–538. http://search.mandumah.com/Record/1414178

Khadem, N., & Moqaddem, A. S. (2021). The role of trust-building in developing digital transactions: France as a model. Journal of Legal and Political Thought, 5(1), 141–154. http://search.mandumah.com/Record/1200915

Khreisan, B. A. (2020). Cyberspace: The inevitability of connection and the challenge of communicating with the other. Tikrit Journal of Political Science, (22), 3–24. http://search.mandumah.com/Record/1205584

Al Dakroury, M. I. M., Abdelghaffar, M. S., & Al-Satouhi, A. M. S. A. (2018). The effect of e-selling ethics on e-trust: An applied study on e-shopping site customers. Egyptian Journal of Commercial Studies, 42(1), 214–239. http://search.mandumah.com/Record/958530

Al Dakroury, M. S. A. (2023). The mediating role of brand love and e-trust in the relationship between online brand experience and electronic word-of-mouth: An applied study on e-shopping customers. The Scientific Journal for Research and Commercial Studies, 37(2), 715–803. http://search.mandumah.com/Record/1505946

International Telecommunication Union. (2002). Cybersecurity guidelines for developing countries. ITU. (Duplicate entry in source list—kept once above.)

Sabaa, S. M. A. (2023). Mediating e-trust in the relationship between content marketing and customer retention: An applied study on e-shopping site users. The Scientific Journal of Financial and Commercial Studies and Research, 4(1), 1281–1313. https://doi.org/10.21608/cfdj.2023.259997

Al Dmour, A. M. (2024). Cybercrimes and their impact on community security in the United Arab Emirates. Fikr Al-Shurti (Police Thought), 33(131), 19–64. http://search.mandumah.com/Record/1521685

Abdel-Ati, A. M. (2022). Levels of trust in health websites to which youth are exposed and their relationship to their online vigilance: A field study. Egyptian Journal of Public Opinion Research, 21(2, Part 1), 51–87. https://search.emarefa.net/detail/BIM-1399375

Abdelmaksoud, R. (2024). Exploring the role of cybersecurity in enhancing digital trust of Egyptian travel and tourism agencies. Arab Universities Journal of Tourism and Hospitality, 26(1), 185–204. https://doi.org/10.21608/jaauth.2024.269299.1553

Telecommunications and Digital Government Regulatory Authority. (2023). UAE Trust List. https://tdra.gov.ae

Qandil, A. A. (2023). Mechanisms for achieving information security in the United Arab Emirates. Fikr Al-Shurti (Police Thought), 32(126), 185–229. http://search.mandumah.com/Record/1393339

Qandil, R. H. M. (2025). The impact of digital transformation projects on improving the digital trust balanced scorecard: Application to the Egyptian Ministry of Education and Technical Education. Arab Journal of Administration, 45(1), 43–66. https://doi.org/10.21608/aja.2022.109881.1186

Koukash, T. J., & Al Badri, F. A. (2019). The moderating effect of perceived risk on the relationship between online trust and purchase intention among Jordanian e-shopping sites (Unpublished master's thesis). Middle East University, Amman. http://search.mandumah.com/Record/1013815

Al Mazrouei, N. A. S. (2024). The importance of the role of cybersecurity in achieving electronic security in the United Arab Emirates. Al-Bahith Journal for Legal and Economic Research and Human and Sharia Sciences, (71), 128–142. http://search.mandumah.com/Record/1502303

Al Mutairi, B. A. (2025). Requirements for developing cybersecurity awareness among public secondary-school students: A proposed vision. Journal of the College of Education, 13(42), 234–282. http://search.mandumah.com/Record/1560444

Makkawi, K. (2009). The concept of "trace" in Jacques Derrida's philosophy. Journal of Arts and Social Sciences, 6(3), 96–109. https://asjp.cerist.dz/en/article/39866

Al Muhairi, A. A. (2023). The role of the United Arab Emirates in achieving electronic security. Readings in Legal and Administrative Research Journal, (20), 441–471. http://search.mandumah.com/Record/1434464

Al Neyadi, M. S. S. (2024). Cybersecurity in the United Arab Emirates: An analytical study. Al-Bahith Journal for Legal and Judicial Studies, (69), 368–380. http://search.mandumah.com/Record/1481293

ثانياً: المصادر الأجنبية

Elmetwaly, M., Amin, M., Shehata, S., Elshorbagy, A., Mohamed, E. & Elbialy, B., (2020), Relationship between Saudi customers' electronic-trust and electronic-loyalty, Journal of Advanced Pharmacy Education & Research, 10 (3), 160-166.

Goliath, S., Tsibolane, P., & Snyman, D. (2024). Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviors in higher education. arXiv. https://doi.org/10.48550/arXiv.2411.03219

López Mendoza, A., Ventura Roque Hernández, R., Prieto Quezada, M. T., & Salazar Hernández, R. (2025). Cybersecurity among university students from Generation Z: A comparative study of the undergraduate programs in administration and public accounting in two Mexican universities. UIKTEN - Association for Information Communication Technology Education and Science. https://www.ceeol.com/search/article-detail?id=1103864

Syahidah, A. A., & Aransyah, M. F. (2023). Pengaruh E-Service Quality dan E-Trust terhadap E-Customer Loyalty pada pengguna dompet digital DANA melalui E-Satisfaction sebagai variabel intervening. SISFOKOM (Journal of Information Systems, Informatics and Computing), 12(1). https://doi.org/10.32736/sisfokom.v12i1.1593

الجدول ١ معاملات الثبات الداخلي (كرونباخ ألفا) لمحور الاستبانة وأداة الدراسة ككل

المحور	عدد البنود	معامل كرونباخ ألفا (α)	مستوى الثبات
دور التوعية والتثقيف السيبراني في تعزيز الثقة في الأمن الإلكتروني لدى طلاب جامعة الشارقة في البيئة الرقمية	10	0.88	جيد جداً

الجدول ٢ توزيع أفراد العينة حسب الجنس .

الجنس	التكرار	النسبة المئوية
أنثى	186	62.0%
ذكر	114	38.0%
المجموع	300	100%

الجدول ٣ توزيع أفراد العينة حسب التخصص الدراسي.

التخصص	التكرار	النسبة المئوية
التخصصات الإنسانية والاجتماعية (مثل: الإعلام، علم الاجتماع، التاريخ)	103	34.3%
التخصصات الصحية (مثل: الطب، التمريض، الصيدلة)	43	14.3%
التخصصات العلمية (مثل: الهندسة، العلوم، الحوسبة)	80	26.7%
التخصصات القانونية والإدارية (مثل: القانون، إدارة الأعمال)	74	24.7%
المجموع	300	100%

الجدول ٤ توزيع أفراد العينة حسب السنة الدراسية.

السنة الدراسية	التكرار	النسبة المئوية
الأولى	65	21.7%
الثانية	48	16.0%
الثالثة	59	19.6%
الرابعة	60	20.0%
الخامسة فما فوق	68	22.7%
المجموع	300	100%

الجدول ٥ توزيع أفراد العينة حسب الأجهزة الإلكترونية المستخدمة.

الأجهزة	التكرار	النسبة المئوية
الهاتف الذكي	78	26.0%
الهاتف + الحاسوب المحمول (اللابتوب)	46	15.3%
الهاتف + اللابتوب + التابلت	41	13.7%
الحاسوب المكتبي	31	10.3%
الجهاز اللوحي (التابلت)	23	7.7%
الهاتف + اللابتوب + المكتبي + التابلت	18	6.0%
الهاتف + التابلت	17	5.6%
الهاتف + اللابتوب + المكتبي	16	5.3%
الهاتف + المكتبي	15	5%
الهاتف + اللابتوب + التابلت + أخرى	15	5%
المجموع	300	100%

الجدول ٦ يوضح مدى تعرض أفراد العينة لمحاولات اختراق إلكتروني.

محاولة اختراق	التكرار	النسبة المئوية
نعم	89	29.7%
لا	211	70.3%
المجموع	300	100%

الجدول ٧ يوضح مدى تعرض أفراد العينة لمحاولات احتيال إلكتروني.

محاولة احتيال	التكرار	النسبة المئوية
نعم	154	51.3%
لا	146	48.7%
المجموع	300	100%

الجدول ٨ يوضح مدى حصول أفراد العينة على تدريب في مجال الأمن السيبراني.

التدريب	التكرار	النسبة المئوية
نعم	129	43.0%
لا	171	57.0%
المجموع	300	100%

الجدول ٩ يوضح نوع التدريب أو المعرفة المكتسبة من قبل أفراد العينة.

نوع التدريب	التكرار	النسبة المئوية
معرفة ذاتية (من الانترنت/كتب)	90	30.0%
تدريب رسمي خارج الجامعة	32	10.7%
تدريب رسمي ومعرفة ذاتية	32	10.7%
تدريب رسمي داخل الجامعة	23	7.6%
أخرى	123	41.0%
المجموع	300	100%

الجدول ١٠

توزيع استجابات الطلبة حول مدى ثقتهم في المواقع الإلكترونية التي تطلب معلومات شخصية.

الاستجابة	التكرار	النسبة المئوية
لا أثق بها أبداً	73	%24.3
أثق بها قليلاً	188	%62.7
أثق بها كثيراً	39	%13.0
المجموع	300	100%

الجدول ١١ توزيع استجابات الطلبة حول التحقق من مؤشرات الأمان (https، رمز القفل) عند الدخول إلى المواقع الإلكترونية.

الاستجابة	التكرار	النسبة المئوية
دائماً	125	%41.7
أحياناً	115	%38.3
نادراً	40	%13.3
لا أهتم إطلاقاً	20	%6.7
المجموع	300	100%

الجدول ١٢ توزيع استجابات الطلبة حول استخدامهم لوسائل الدفع الإلكتروني (البطاقات المصرفية والمحافظ الرقمية).

الاستجابة	التكرار	النسبة المئوية
نعم	257	%85.7
لا	43	%14.3
المجموع	300	100%

الجدول ١٣ توزيع استجابات الطلبة حول تعاملهم مع الرسائل المجهولة التي تتضمن روابط إلكترونية.

الاستجابة	التكرار	النسبة المئوية
أتجاهل الرسالة	151	%50.3
أتحقق من المصدر أولاً	105	%35.0
أبلغ عنها واحتيال	26	%8.7
أفتح الرابط مباشرة	18	%6.0
المجموع	300	100%

الجدول ١٤

توزيع استجابات الطلبة حول دور التوعية والتثقيف السيبراني في تعزيز الثقة بالأمن الإلكتروني.

رقم العبارة	نص العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري	الدرجة	الترتيب
1	أشارك في ورش العمل التوعوية حول الأمن السيبراني	47 (15.7%)	50 (16.7%)	90 (30.0%)	55 (18.3%)	58 (19.3%)	2.91	1.32	متوسط	10
2	أتابع الحملات التثقيفية حول الأمان الرقمي	57 (19.0%)	66 (22.0%)	108 (36.0%)	38 (12.7%)	31 (10.3%)	3.27	1.21	متوسط	9
3	أستفيد من المنشورات التوعوية التي تقدم نصائح حول الأمان الرقمي	82 (27.3%)	87 (29.0%)	90 (30.0%)	21 (7.0%)	20 (6.7%)	3.63	1.15	متوسط	7
4	أطبق ما أتعلمه من دورات التثقيف السيبراني لتحسين سلوكي الرقمي	87 (29.0%)	82 (27.3%)	91 (30.3%)	21 (7.0%)	19 (6.3%)	3.66	1.15	مرتفع	6
5	أُنبه الآخرين عند اكتشاف خطر إلكتروني أو تهديد أمني	112 (37.3%)	94 (31.3%)	71 (23.7%)	16 (5.3%)	7 (2.3%)	3.96	1.02	مرتفع	2
6	أطرح الأسئلة حول كيفية حماية بياناتي الشخصية عند الحاجة	92 (30.7%)	79 (26.3%)	94 (31.3%)	22 (7.3%)	13 (4.3%)	3.72	1.11	مرتفع	5
7	أُطالع محتوى تدريبياً متخصصاً حول الأمن الإلكتروني	76 (25.3%)	58 (19.3%)	99 (33.0%)	47 (15.7%)	20 (6.7%)	3.41	1.21	متوسط	8
8	أدعم الجهود المجتمعية التي تهدف إلى تعزيز الثقافة الأمنية	111 (37.0%)	79 (26.3%)	79 (26.3%)	20 (6.7%)	11 (3.7%)	3.86	1.10	مرتفع	4
9	أُدرك أهمية حماية الخصوصية الرقمية في كافة تعاملاته	131 (43.7%)	77 (25.7%)	70 (23.3%)	19 (6.3%)	3 (1.0%)	4.05	1.01	مرتفع	1
10	أبحث دائماً عن أفضل الممارسات لتعزيز الأمان الرقمي	114 (38.0%)	90 (30.0%)	73 (24.3%)	15 (5.0%)	8 (2.7%)	3.96	1.03	مرتفع	3
	الكلي						3.64	1.13	مرتفع	

الجدول ١٥ نتائج تحليل التباين الأحادي (One-Way ANOVA) لاختبار الفروق في المحور باختلاف النوع الاجتماعي

مجموع المربعات (بين)	درجات الحرية (بين)	متوسط المربعات (بين)	مجموع المربعات (داخل)	درجات الحرية (داخل)	متوسط المربعات (داخل)	قيمة F	مستوى الدلالة (Sig)
0.063	1	0.063	213.728	298	0.717	0.088	0.767

الجدول ١٦ نتائج تحليل التباين الأحادي (One-Way ANOVA) لاختبار الفروق في المحور باختلاف التخصص الدراسي

مجموع المربعات (بين)	درجات الحرية (بين)	متوسط المربعات (بين)	مجموع المربعات (داخل)	درجات الحرية (داخل)	متوسط المربعات (داخل)	قيمة F	مستوى الدلالة (Sig)
3.788	3	1.263	210.003	296	0.709	1.780	0.151

الجدول ١٧ نتائج اختبار Scheffé للفروق بين متوسطات استجابات أفراد العينة في محور المعوقات الثقافية والمجتمعية حسب التخصص الدراسي

المقارنة	الفرق في المتوسطات	القيمة الاحتمالية (p)	مجال الثقة ٩٥%	الدلالة
التخصصات الإنسانية والاجتماعية × التخصصات الصحية	−0.3606	0.0537	[−0.725, 0.004]	غير دالة
التخصصات الإنسانية والاجتماعية × التخصصات العلمية	−0.0466	0.9780	[−0.346, 0.253]	غير دالة
التخصصات الإنسانية والاجتماعية × التخصصات القانونية والإدارية	−0.0153	0.9992	[−0.321, 0.291]	غير دالة
التخصصات الصحية × التخصصات العلمية	0.3141	0.1437	[−0.066, 0.694]	غير دالة
التخصصات الصحية × التخصصات القانونية والإدارية	0.3453	0.0964	[−0.040, 0.730]	غير دالة
التخصصات العلمية × التخصصات القانونية والإدارية	0.0312	0.9946	[−0.293, 0.355]	غير دالة

الجدول ١٨ نتائج ANOVA لاختبار الفروق في المحور باختلاف نوع الأجهزة الإلكترونية المستخدمة

مجموع المربعات (بين)	درجات الحرية (بين)	متوسط المربعات (بين)	مجموع المربعات (داخل)	درجات الحرية (داخل)	متوسط المربعات (داخل)	F	Sig
27.341	23	1.189	186.450	276	0.676	1.760	0.019

الجدول ١٩ نتائج اختبار Scheffé للمقارنات البَعدية بين الأجهزة الإلكترونية في المحور

المقارنة	الفرق في المتوسطات	القيمة الاحتمالية (p)	مجال الثقة ٩٥%	الدلالة
الهاتف الذكي × اللابتوب	0.042	0.912	[−0.315, 0.399]	غير دالة
الهاتف الذكي × التابلت	−0.087	0.801	[−0.451, 0.278]	غير دالة
الهاتف الذكي × الهاتف + اللابتوب	0.156	0.650	[−0.243, 0.555]	غير دالة
الهاتف + اللابتوب × اللابتوب	−0.198	0.532	[−0.587, 0.191]	غير دالة
اللابتوب × التابلت	0.135	0.712	[−0.311, 0.581]	غير دالة
الهاتف + التابلت × الهاتف الذكي	−0.178	0.578	[−0.622, 0.266]	غير دالة