"النمذجة التنبؤية لمسارات المحددات المؤثرة في زيادة وعي المجتمعات السكانية تجاه المخاطر السيبرانية: إطار تحليلي لدعم الأمن الرقمي المجتمعي في خورفكان"

"Predictive Modeling of the Determinants Influencing Community Awareness of Cyber Risks: An Analytical Framework for Community Digital Security in Khorfakkan"

أ.د/ محمد أحمد الخولى

أستاذ مشارك

أكاديمية السادات للعلوم الإدارية بالقاهره

mohkholy5@hotmail.com

مجلة الدراسات التجارية المعاصرة

كلية التجارة – جامعة كفر الشيخ

المجلد (١١) - العدد (٢٠) - الجزء الثاني

ابريل ٢٠٢٥م

رابط المجلة: https://csj.journals.ekb.eg

الملخص:

في العصر الرقمي الراهن، أصبحت المخاطر والتهديدات السيبرانية تشكل تهديدًا متزايدًا للمجتمعات السكانية على مستوى العالم في ظل التوسع المتزايد على تطبيق العديد من الأدوات والتقنيات الذكية والتكنولوجيا الرقمية والتي تتطلب تبادل بيانات بين المستخدمين بطرق لا تضمن الخصوصية أو الحفاظ على الأصول المعلوماتية، ولذا تواجه المجتمعات مجموعة متنوعة من التهديدات السيبرانية التي تتطلب استراتيجيات فعالة لتعزيز الوعي العام لدى أفراد المجتمع تحقيقا لمقومات الأمن الرقمي المجتمعي بشكل آمن ومستدام استعدادا للمستقبل. وتهدف هذه الدراسة إلى تحليل العوامل المؤثرة في زيادة وعي المجتمعات السكانية بالمخاطر السيبرانية استنادا إلى نمذجة تنبؤية لمسارات المحددات المؤثرة على زيادة الوعي بالأمن الرقمي المجتمعي لضمان استدامته في المستقبل، مع التركيز على مدينة خورفكان كحالة دراسية وبناء نموذج نظري يساهم في تحديد معاملات مسارات مجموعة من المحددات المحتمل تأثيرها على زيادة الوعي تجاه احتمالية التعرض للتهديدات السيبرانية في المستقبل، وقد كشفت نتائج الدراسة عن أهمية المحددات الثقافية والدينية، والبيئية، والتعليمية والتدريبية، والأخلاقية في تشكيل الوعي الرقمي المجتمعي بالمخاطر والتهديدات السيبرانية، حيث جاءت هذه المحددات في مقدمة المحددات الأكثر أهمية في التمييز بين مستويات الوعي المختلفة. كما أظهرت الدراسة أن المحددات الصناعية والابتكار لها التأثير الأكبر على الوعي بالمخاطر السيبرانية، حيث بلغت قيمة معامل التأثير ٠,٤١٤، تليها المحددات البيئية بقيمة ٠,٢٤١، وقد بلغت نسبة التصنيف الصحيح الإجمالية لنموذج تحليل التمايز ٨٨,٧% حيث حققت مجموعتا التأثير المحتمل المتوسط والعالي جداً دقة تصنيف مثالية (١٠٠٪)، بينما كانت مجموعة التأثير المحتمل العالي الأقل في دقة التصنيف (61.5%)، كما بلغت قيمة معامل التأثير للمحددات الصناعية والابتكار ٠,٤١٤، وللمحددات البيئية ٠,٢٤١، وللمحددات الأخلاقية ٠,٢١٠، وللمحددات الاجتماعية ٠,١٣٤. وقدمت الدراسة مجموعة من التوصيات والمقترحات الداعمة لصناع القرار والمخططين والجهات المعنية بالأمن السيبراني أو التوعية المجتمعية العامة بحيث يجب أن تشمل تطوير برامج توعية مستهدفة للفئات السكانية الأكثر احتياجا في مواجهة المخاطر السيبرانية مع تحديد الأولويات لضمان مجتمع سكاني آمن رقميا ومستدام، وتعزيز البعد الاجتماعي والثقافي في استراتيجيات وتشريعات الأمن السيبراني، وتطوير آليات تشخيصية لتقييم مستوى الوعي.

الكلمات الدالة: النمذجة التنبؤية، تحليل المسار، التهديدات والمخاطر السيبرانية، الأمن الرقمي المجتمعي، خورفكان.

Abstract:

In the current digital age, cyber risks and threats are escalating, posing a global threat to societies amidst the rapid expansion of smart tools, technologies, and digital platforms. These technologies often necessitate data exchange among users in ways that may compromise privacy or the security of information assets, exposing communities to a range of cyber threats. This situation calls for the development of effective strategies to enhance public awareness, ensuring a secure and sustainable community digital security framework for the future. This study aims to analyze the factors influencing cybersecurity awareness in communities, employing predictive modeling to map the determinants impacting community digital security awareness for future sustainability. Focusing on Khorfakkan City as a case study, the research proposes a theoretical model to identify the path coefficients of potential determinants that influence awareness of future cyber threat exposure. The findings highlight the significant role of cultural, religious, environmental, educational, training, and ethical determinants in shaping community digital awareness of cyber risks and threats. These determinants emerged as the most critical in distinguishing between different levels of awareness. The study also revealed that industrial and innovation determinants have the most substantial impact on cybersecurity awareness, with a path coefficient of 0.414, followed by environmental determinants at 0.241. The overall correct classification rate of the discriminant analysis model was 88.7%, with the medium and very high potential impact groups achieving perfect classification accuracy (100%), while the high potential impact group had the lowest accuracy (61.5%). The path coefficients were 0.414 for industrial and innovation determinants, 0.241 for environmental determinants, 0.210 for ethical determinants, and 0.134 for social determinants. The study provides a set of recommendations for

policymakers, planners, and stakeholders in cybersecurity and public awareness. These include developing targeted awareness programs for the most vulnerable populations, prioritizing initiatives to ensure a digitally secure and sustainable community, enhancing the social and cultural dimensions in cybersecurity strategies and legislation, and developing diagnostic mechanisms to assess awareness levels.

Keywords: Predictive Modeling, Path Analysis, Cyber Threats and Risks, Community Digital Security, Khorfakkan.

مقدمــة:

في ظل التحول الرقمي المتسارع الذي يشهده العالم، أصبحت الهجمات السيبرانية واحدة من أبرز التحديات التي تهدد المجتمعات الرقمية على مختلف الأصعدة. وبينما تركز معظم الدراسات السابقة على الجوانب التقنية للأمن السيبراني، تظل المحددات الديموغرافية والاجتماعية للتعرض للهجوم السيبراني مجالًا بحثيًا ناشئًا يستدعي استكشافًا أعمق. يشكل فهم العوامل الديموغرافية والاجتماعية التي تؤثر على احتمالية تعرض الأفراد للهجمات السيبرانية مدخلًا استشرافيًا لتعزيز الأمن الرقمي المجتمعي، خاصةً في المجتمعات السكانية ذات الخصوصية الثقافية والاجتماعية مثل مدينة خورفكان بإمارة الشارقة بدولة الامارات العربية المتحدة. والتوعية بالأمن السيبراني بمثابة درع المجتمعات الرقمية في العصر الرقمي الذي في طور الاعتماد كليا على التقنيات الذكية والرقمية، لتحصين الأفراد وحماية المؤسسات من الهجمات الإلكترونية المتزايدة يبدأ بترسيخ ثقافة الأمان الرقمي والاستثمار في البحث والتطوير للحد من الجرائم السيبرانية وتعزيز بيئة إلكترونية آمنة، والأمن السيبراني ليس خيارا، بل ضرورة لتحقيق تنمية مستدامة ومجتمع رقمي مزدهر (Cobos, 2024)، لذا تحدد الدافع لهذه الدراسة في الحاجة إلى بناء إطار تحليلي يدمج بين الخصائص الديموغرافية والاجتماعية والسياسية والاقتصادية والتكنولوجية والقانونية والثقافية والدينية لنمذجة المسارات التنبؤية (Path Analysis) في نموذج نظري شامل ومتكامل لفهم كيفية تأثير تلك المحددات في زيادة أو تقليل مستوى درجة الوعي الفردي أو المجتمعي تجاه احتمالية التعرض للهجوم السيبراني أو التهديدات الالكترونية والرقمية بشكل عام نتيجة التوسع في تطبيق تقنسات الذكاء الاصطناعي وفي ظل الثورة الصناعية وتنامي نظم الابتكار في جميع المؤسسات وعلى مستوى جميع الخدمات المتاحة لحصول المستخدمين عليها عبر المنصات الذكية والرقمية دعما لمقومات التنمية المستدامة.

فالأمن السيبراني ركيزة أساسية لحماية أفراد المجتمع من المخاطر والتهديدات الرقمية المتزايدة، والاستثمار في التوعية والتدريب على ممارسات الأمن الرقمي الآمن يعزز مناعـة المجتمعات ضد

الهجمات الإلكترونية (Alqahtani, 2022)، وأشارت هيئة الاتحاد الأوربية للأمن السيبراني أن التوعية بالأمن السيبراني حجر الأساس في بناء مجتمعات سكانية رقمية آمنة، حيث تعزز المرونة الرقمية وتحد من الجرائم الإلكترونية. من خلال استراتيجيات متكاملة تشمل التثقيف، التعاون المؤسسي، والتقييم المستمر للتهديدات، يمكن تحقيق بيئة سيبرانية محمية (ENISA, 2021)، وبالتالي فإن أي محاولات ومبادرات بحثية تساهم في تمكين الأفراد والمؤسسات بالمعرفة الرقمية يساهم في تنمية مستدامة ويعزز الثقة في الفضاء الرقمي، وأصبح يشكل ضعف الوعي بالأمن السيبراني في المجتمعات السكانية ولاسيما تزامنا مع التوسع في انشاء مدن ذكية حاجزًا خفيًا أمام التنمية الرقمية، مما يجعل الفئات الأقل حظًا أكثر عرضة للاستغلال الإلكتروني (Sultan, 2024). ولذا تمكين هذه المجتمعات من المعرفة الرقمية يعزز الثقة في التكنولوجيا ويفتح أبواب التنمية المستدامة عبر استراتيجيات توعوية ذكية وشراكات فاعلة، يمكن تحويل الأمن السيبراني من تحدٍ إلى فرصة للارتقاء المجتمعي

ومن شأن المقاربة الإحصائية التي سوف تنتهجها الدراسة الحالية باستخدام تحليل المسار لبناء النماذج التنبؤية أحادية الاتجاه Unidirectional أن تسهم في ترسيخ مفهوم الأمن الرقمي المجتمعي في إطار تعزيز أسس الأمن السيبراني باعتباره ظاهرة متعددة الأبعاد تتجاوز النطاق التقني لتشمل العوامل السكانية والسلوكيات الاجتماعية للأفراد. تهدف هذه الدراسة إلى تقديم نموذج إحصائي تنبؤي يستند إلى التحليل السببي لمسارات التأثير بين الخصائص الديموغرافية والاجتماعية واحتمالية التعرض للهجمات السيبرانية، مع تطبيقه على مجتمع مدينة خورفكان كمجتمع محلي يمثل نموذجًا للبيئة العربية بحيث يمكن تعميمه على مجتمعات سكانية مشابهة. ومن خلال هذه المقاربة، تسعى الدراسة إلى سد الفجوة البحثية في مجال الأمن السيبراني من خلال إدماج المنظور الديموغرافي والاجتماعي مع التوعية بالأمن الرقمي في النمذجة التنبؤية، بما يسهم في تطوير سياسات وتشريعات وقائية أو استباقية قائمة على معالجة البيانات وتحويلها إلى معلومات ومعارف يمكن توظيفها من خلال توظيف تقنيات وأدوات ومنصات ذكية لتزويد صناع القرار والمخططين والجهات المعنية السيادية ذات الصلة سواء الأمنية أو التكنولوجية أو المجتمعية تدعم التوجهات الاستراتيجية السكانية لبناء مجتمعات ذكية آمنة ومستدامة.

مشكلة الدراسة:

مع تزايد الاعتماد على التقنيات الرقمية في مختلف مجالات الحياة، أصبحت المجتمعات السكانية أكثر عرضة للهجمات السيبرانية، مما يشكل تهديدًا مستمرًا على أمن الأفراد والمجتمعات. وعلى الرغم من التركيز المتزايد على الجوانب التقنية للأمن السيبراني، إلا أن البعد الديموغرافي والاجتماعي لا يزال غير مستكشف بشكل كافٍ. تتمثل مشكلة الدراسة في وجود فجوة معرفية حول دور الخصائص الديموغرافية والاجتماعية في تحديد احتمالية تعرض الأفراد للهجوم السيبراني، مما يستدعي تطوير نموذج إحصائي يوضح مسارات التأثير بين هذه العوامل الاستباقية. فضلا عن وجود فجوة في الإحصاءات الرسمية التي تظهر انتشار الجرائم الإلكترونية والقاء الضوء على قياسات لمعدلات الوعي بين فئات السكان باختلاف أعمارهم، والتي تستكشف تأثير استخدام التكنولوجيا الرقمية على الإحساس بالضعف السيبراني والتعرض للتهديدات والمخاطر الرقمية (Bernik et al.,2022).

وتبرز مشكلة الدراسة في احصائيات الاختراقات والتهديدات الرقمية التي تعرض لها المستخدمين للمنصات والمواقع الالكترونية، ففي عام ٢٠٢٣، فقد شهد العالم زيادة بنسبة ٧٢٪ في خروقات سرية البيانات مقارنة بعام ٢٠٢١، حيث بلغ متوسط تكلفة خرق البيانات ٤,٨٨ مليون دولار أمريكي، وفي نفس العام أيضا تم تسليم ٣٥٪ من البرمجيات الخبيثة عبر البريد الإلكتروني، وأبلغت ٩٤٪ من المنظمات عن حوادث وتهديدات أمنية رقمية تتعلق بالبريد الإلكتروني (Forbes, 2024)، مما أصبحت تشكل مخاطر وتهديدات سيبرانية على الحسابات الشخصية والعامة للمستخدمين مما أصبحت تشكل مصدرا حرجا لتهديد الأمن الرقمي المجتمعي من أجل ضمان الحصول على جودة حياة رقمية آمنة، أما في منطقة الشرق الأوسط، فقد أبلغت ٦٧٪ من المؤسسات الحكومية والخاصة عن قلقها المتزايد من نقص الوعي بين أفراد المجتمع، وزادت ميزانيات الانفاق على الأمن السيبراني بنسبة ٥٣٪ منذ عام ٢٠١٩ (Moody's., 2024)، بالنسبة لدولة الإمارات العربية المتحدة فقد أبلغت ٧٠٪ من المنظمات عن نقص في الوعي المجتمعي تجاه مقومات الأمن الرقمي الأساسية بين أفراد المجتمع Fortinet, (2024)، مما يزيد من مخاطر التعرض للهجمات السيبرانية أو الرقمية التي يمكن مواجهتها في المستقبل مع التوسع في تطبيق تقنيات الذكاء الاصطناعي المتواكبة مع تنامي التطور الصناعي والابتكارات بشكل مستمر المنبثقة مع الثورة الصناعية الرابعة، أما بالنسبة لاحصائيات محلية تخص مدينة خورفكان، فلم يتوافر أية إحصائيات محددة لخورفكان تستند إليها في تعزيز الأمن الرقمي المجتمعي لدعم صناع القرار في هذا المجال الأمني تجاه مواكبة عوامل العموض المحتملة مع استشراف المستقبل داخل المجتمع.

وبالتالي أصبحت تواجه المجتمعات السكانية، وفي خورفكان تحديدا تحديات ملحوظة في مجال دعم الأمن السيبراني، في ظل عدم وجود برامج مخصصة لنشر الوعي بالمخاطر والتهديدات السيبرانية وطرق التعامل معها بشكل آمن. ولايوجد بيانات أو احصائيات لقياس الوعي تجاه احتمالية التعرض للهجمات السيبرانية، مما يستدعي تطوير استراتيجيات فعالة لتعزيز الوعي العام لتحقيق الأمن الرقمي المجتمعي. ولذا تهدف هذه الدراسة البحثية إلى تقديم إطار تحليلي لدعم الأمن الرقمي المجتمعي في خورفكان من خلال نمذجة التنبؤية لمسارات المحددات المؤثرة في زيادة الوعي بالمخاطر السيبرانية. وفي ضوء السياق أعلاه، فقد تمحورت المشكلة في أهمية التركيز على فحص العلاقات التفاعلية والديناميكية لمتغيرات أو محددات جديدة في إطار نمذجة تلك المسارات بتوظيف تقنيات إحصائية متقدمة لرصد وقياس وتقييم مسارات التأثير المباشرة أو غير المباشرة المحتملة فيما بينها كمتغير ات تفسيرية أو وسيطة للتنبؤ بمستوى الوعي الرقمي المجتمعي تجاه احتمالية التعرض لمخاطر وتهديدات سيبرانية، وذلك وفق تطبيق النموذج على بيانات مسحية بإحدى المدن العربية "خورفكان" في أحد الدول العربية المتقدمة في مجالات التوسع في استخدام التقنيات والأدوات الذكية مع انتشار توظيف المنصات الرقمية والالكترونية لتقديم مختلف الخدمات الأساسية والحيوية لجميع فئات السكان تعزيزا لجودة ورفاهية الحياة، وتحديدا دولة الامارات وفق استراتيجيتها الوطنية لجودة الحياة بحلول ٢٠٣١، وبالتالي يمكن أن تساهم نتائج ومخرجات هذه الدراسة بشكل عام في توليد قيمة مضافة جديدة لصناع القرار والمعنيين بتطوير السياسات السكانية والتنموية استعدادا للمستقبل من خلال طرح أهم التوصيات كمقومات داعمة لتطبيق مسارات ورؤى استشرافية بشكل استباقي لزيادة التوعية المبكرة بين أفراد المجتمع تجاه تعزيز الأمن الرقمي المجتمعي بشكل آمن ومستدام.

أهداف الدراسة:

- بناء نموذج نظري تنبؤي استنادا إلى الإطار النظري للدراسة يوضح مسارات التأثير لبعض المحددات المؤثرة المحتمل لها دور معنوي على زيادة الوعي تجاه احتمالية التعرض للهجوم السيبراني.
- فحص علاقات الارتباط المحتملة بين مجموعة من الخصائص الديموجرافية والخلفية للمبحوثين المستهدفة - قيد الدراسة الحالية - وبين حالة التعرض (نعم / لا) للهجمات السيبرانية والتهديدات الرقمية.
- فحص الاختلافات المعنوية الدال احصائيا في قيم المحددات المؤثرة قيد الدرسة نتيجة الوعي بالذكاء الاصطناعي أو الأمن الرقمي أو الاستخدام اليومي للتقنيات الذكية والرقمية.
- تطوير دالة التمايز للمتغيرات أو المحددات التي لها دور معنوي في التمييز والتصنيف لمستويات حالة الوعي المجتمعي أو الفردي المكتسب تجاه التعرض للتهديدات الإلكترونية.
- قياس معاملات تحليل المسارات ذات التأثير المباشر وغير المباشر لنمذجة النموذج النظري التنبؤي للمحددات او للمتغيرات الاجتماعية والاقتصادية والتكنولوجية والسياسية والقانونية والبيئية والتعليمية والتدريبية والاخلاقية والثقافية في تحديد مستويات زيادة الوعي للتعرض السيبراني.
- استكشاف العلاقات السببية التنبؤية بين مسارات المحددات المؤثرة على مستوي الوعي تجاه التعرض السيبراني على مستوى الفرد أو المجتمع في بيئة مدينة خورفكان بإمارة الشارقة.
- تقديم توصيات استشرافية لتعزيز الأمن الرقمي المجتمعي استنادًا إلى النتائج التنبؤية للنموذج الإحصائي.

تساؤلات وفرضيات الدراسة:

انبثقت من خلال استعراض مشكلة الدراسة وأهدافها مجموعة من التساؤلات والفروض البحثية التالية:

- ما هي المسارات السببية للمحددات المحتمل تأثيرها في نمذج نموذج نظري تنبؤي في التنبؤ بدرجة الوعي تجاه التعرض لمخاطر وتهديدات الهجمات السيبرانية تطبيقا على مدينة خورفكان؟
- توجد علاقة ارتباطية معنوية ذات دلالة احصائية بين بعض الخصائص الديموغرافية والخلفية للمبحوثين وبين حالة التعرض للهجوم السيبراني أو الجرائم الالكترونية (نعم / لآ)
- هل توجد فروق ذات دلالة معنوية احصائيا في قيم المحددات المؤثرة سواء كانت (السياسية، أو الاجتماعية، أو الاقتصادية، أو التكنولوجية، أو القانونية والتشريعية، أو البيئية، أو الثقافية، أو التدريبية والتعليمية، أو الأخلاقية) وفقًا للوعي بالذكاء الاصطناعي (نعم/ لا) أو الوعي بالأمن الرقمي (نعم/ لا) أو الاستخدام اليومي للتقنيات الذكية (نعم/لا)؟
- ما هي المحددات أو العوامل الأكثر تأثيرا باستخدام دالة التمايز في التنبؤ بتصنيفات مستويات الوعي لدى الفرد أو المجتمع تجاه احتمالية التعرض للتهديدات والمخاطر السيبرانية (عالي جدا/ عالي/ متوسط/ منخفض).

- يلعب كل من (محددات التطور الصناعي والابتكار، ومحددات الذكاء الاصطناعي) دورًا وسيطًا كمتغيرات وسيطة Intermediate Variables في نمذجة مسارات المحددات التفسيرية داخل النموذج النظري المقترح ذات التأثير المباشر أو غير المباشر للتنبؤ بمستوى الوعي تجاه احتمالية التعرض للهجوم السيبراني.
- تختلف مسارات التأثير المباشر وغير المباشر بين المتغيرات أو المحددات المؤثرة باختلاف معنوية معاملات ارتباطها المعيارية Beta مع المتغير التابع (الوعي باحتمالية التعرض للتهديدات السيبرانية في خورفكان)

أهميـة الدراسـة:

- قلة الدراسات والبحوث الاحصائية التي تناولت التركيز على تطبيق أساليب احصائية متقدمة كتحليل المسارات التنبؤية لمجموعة من المحددات أو العوامل المؤثرة على زيادة درجة الوعي بالأمن الرقمي المجتمعي بشكل آمن مع تحديد التفاعلات المتبادلة فيما بينها كتأثيرات مباشرة او غير مباشرة لصقل مقومات الوعي العام كتوجهات استراتيجية واستشرافية يتم تبنيها من قبل الجهات المهنية كاجراءات وقائية أو احترازية استباقية للحد من أو التحكم في انتشار التهديدات والمخاطر الرقمية على مستوى الفرد او المجتمع.
- تبرز أهمية الدراسة في تقديم مقاربة علمية تساهم في بناء إطار نظري حديث لفهم العلاقة التنبؤية بين مجموعة من المحددات المحتمل تأثيرها في زيادة درجة الوعي تجاه التعرض للهجمات والتهديدات السيبرانية.
- تكتسب الدراسة قيمتها من دورها المحور المحتمل في تمكين صناع القرار والمخططين في الجهات ذات العلاقة بالأمن السيبراني من تطوير سياسات استباقية وحلول ذكية قائمة على الأدلة والكشف المبكر لتعزيز مقومات وملامح الأمن الرقمي المجتمعي استعدادا للمستقبل بالمزيد من المرونة والرشاقة
- تسهم الدراسة في إثراء الأدبيات الأكاديمية من خلال إدماج المنظور الديموغرافي والاجتماعي والاقتصادي والتكنولوجي وغيرها في نمذجة التنبؤات السيبرانية، ما يعزز من تكامل الأبعاد السكانية مع استراتيجيات الأمن الرقمي المجتمعي ودعم آليات التخطيط الاستراتيجي والاستشرافية في مجالات السكان والتنمية المستدامة.

الأطراف المستفيدة من الدراسة

١. صناع القرار في مجال الأمن الرقمي والسياسات الاجتماعية.
٢. الهيئات الحكومية والمؤسسات المعنية بحماية الأمن السيبراني.
٣. الباحثون في مجالات الإحصاء الحيوي والدراسات السكانية.
٤. مؤسسات المجتمع المدني العاملة في التوعية بالأمن الرقمي.
٥. الأفراد والمجتمعات المحلية لتعزيز معرفتهم بآليات الحماية الرقمية.

الدراسـات السابقـة:

تشير الدراسات الحديثة إلى أن مجموعة من العوامل الديموغرافية، والاجتماعية، والاقتصادية، والتكنولوجية قد تلعب دورًا حاسمًا في تحديد احتمالية تعرض الأفراد للهجمات والمخاطر السيبرانية. يستعرض هذا القسم من الدراسة أحدث الأبحاث المنشورة التي تسلط الضوء على أهم المحددات الرئيسية المتوقع تأثيرها على المخاطر الأمن السيبراني، وذلك على النحو التالي:

- دور المعرفة والوعي المبكر بالأمن السيبراني: ذهبت دراسة (Lee & Chua, 2024) إلى أنه لا تزال هناك برامج محدودة وفعالة للوقاية المبكرة من الوقوع في الجرائم الإلكترونية وتعزيز الأمن السيبراني، وهدفت إلى التركيز على دور المعرفة والوعي بالأمن السيبراني في تشكيل نوايا وسلوكيات الأفراد فيما يتعلق بالأمن السيبراني في الولايات المتحدة. وكشف نتائج الدراسة إلى متغيرات تكنولوجيا المعلومات والاتصالات، والتعليم، والدخل، والجنس تعد من العوامل المؤثرة في مستوى المعرفة بالأمن السيبراني. وقد اكدت على أهمية الفهم الشامل للعوامل المختلفة معا لتعزيز المعرفة والتثقيف في مجال الأمن السيبراني.
- محددات التأثيرات الثقافية: أبرزت دراسة (de Bruin & Mersinas, 2024) دور الثقافة الوطنية على سلوكيات الأمان السيبراني في تشكيل السلوكيات الرقمية، حيث تزداد الممارسات غير الآمنة في المجتمعات التي تفتقر إلى التوعية الرقمية النظامية، وقد أشارت الدراسة إلى أن بعض الثقافات قد تكون أكثر عرضة لسلوكيات غير آمنة بسبب القيم والمعتقدات السائدة. شملت الدراسة ١٠ دول أوروبية
- تأثير العوامل الداخلية والخارجية: كشفت دراسة (Saleh, 2024) عن تأثير عوامل خفية على زيادة وعي الأفراد بالأمن السيبراني وتحسين سلوكياتهم، مستندة إلى تحليل نوعي لمجموعات نقاش إلكترونية. وقد حددت خمس محاور تشمل (التهديدات والتدابير الوقائية، الخبرات الأمنية، وأهمية التوعية، التكاليف، والثقة). وقد أكدت النتائج على ضرورة تعزيز التثقيف الأمني ودراسة تطبيقها في سياقات مختلفة لفهم المزيد من العوامل والمحددات المؤثرة على زيادة الوعي بالأمن السيبراني بعمق أكبر.
- محددات العوامل السلوكية: استعرضت دراسة (Longtchi et al., 2022) تأثير العوامل السلوكية على تعرض الأفراد ذوي الاستجابات العاطفية القوية يكونون أكثر عرضة لهجمات الهندسة الاجتماعية، مشيرة إلى أن الاستجابات العاطفية يمكن أن تزيد من الضعف أمام هذه الهجمات خاصة عند مواجهة رسائل احتيالية تستهدف استثارة مشاعرهم. وقد شملت الدراسة مراجعة لأكثر من ١٠٠ بحث أكاديمي سابق في هذا المجال.
- الوعي والتدريب لسلوكيات العنصر البشري: تطرقت دراسة (Al-Shanfari et al.,2022) إلى ان المسبب الرئيسي لمعظم انتهاكات الأمن السيبراني في العصر الرقمي هو تبني تطبيق الحلول التقنية بشكل مفرط دون التركيز الكافي على العنصر البشري، واقترحت الدراسة نموذجًا نظريًا شاملًا يعتمد على عدة نظريات نفسية وسلوكية لتحليل العوامل المؤثرة على وعي الموظفين في القطاع العام بسلوكيات الأمن المعلوماتي حيث أظهرت النتائج أن معظم العوامل المدروسة تعزز تبني السلوكيات الأمنية، باستثناء إدراك حتمية العقوبة. تؤكد الدراسة أن تعزيز الوعي والتدريب العملي على الأمن

السيبراني هو المفتاح لتحسين السلوكيات الأمنية في المؤسسات. وتوصي بضرورة تطوير برامج توعية أمنية متكاملة بفعالية.

- توصلت دراسة ميدانية في سلوفينيا (Bernik et al.,2022) اعتمدت على تحليل الفروقات بين سكان المناطق الحضرية والريفية من حيث أهداف استخدام الأجهزة الرقمية والإلكترونية وتأثيرها على التعرض للجرائم السيبرانية. وقد أظهرت النتائج اختلافات ملحوظة في الإدراك السيبراني للضحية، مع وجود ارتباط بين طبيعة استخدام التكنولوجيا ومستوى الشعور بالضعف في التعامل مع التهديدات السيبرانية، مما يشير إلى تباين هذه العلاقات بين الفضاء الرقمي والعالم المادي نتيجة انخفاض الوعي اللازم بالتعاملات الآمنة.
- التوسع الصناعي وانتشار التكنولوجيا: بحثت دراسة (Chizanga et al.,2022) في العوامل المؤثرة على الوعي بالأمن السيبراني في الجامعات الحكومية الكينية، نظراً لتزايد الهجمات الإلكترونية مع انتشار الثورة الصناعية والتحول نحو الاستخدام الرقمي. وقد أظهرت نتائج المسح أن معظم الأكاديميين يفتقرون للتدريب الكافي في الأمن السيبراني، إضافة إلى غياب سياسات إلزامية وبنية تحتية مناسبة لحماية أصول المعلومات في الجامعات. وأكدت على أهمية تعزيز الوعي والتدريب الأمني لحماية مختلف بيئات الأعمال للقطاعات الحيوية والأكاديمية تحديدا من التهديدات السيبرانية المتزايدة.
- الوعي الأمني والهجمات الالكترونية: سلطت دراسة (Dam & Deshpande, 2020) الضوء على تزايد التهديدات السيبرانية في ظل النمو المتسارع للمعاملات الإلكترونية، مؤكدة أن الوعي الأمني لدى الأفراد يعد عاملًا حاسمًا في الحد من المخاطر المالية الناجمة عن الاختراقات. وأوضحت الدراسة أن مستخدمي الخدمات والمعاملات الالكترونية معرضون بشدة للهجمات والتهديدات الإلكترونية، وهي لا تتأثر باختلاف متغيرات العمر أو المستوى التعليمي أو النوع الاجتماعي، مما يستدعي وجود أساليب توعية مبكرة أكثر فاعلية تتجاوز الرسائل الجماعية التقليدية. وتبرز أهمية دراسة العوامل والمحددات المؤثرة على سلوك الأفراد تجاه زيادة الوعي بالأمن السيبراني، لتطوير تشريعات واستراتيجيات تعزز الحماية الرقمية للفرد والمجتمع ككل.
- محددات المعرفة الرقمية في التصيد الإلكتروني: أشارت (Díaz & Joshi, 2018) في ضوء إجراء الدراسة المسحية في مجتمع أكاديمي جامعي إلى أن محددات التطور التكنولوجي لقدرات الأفراد الذين لديهم معرفة سابقة بالتصيد الإلكتروني قد يكونون أقل عرضة للوقوع ضحية لهذه الهجمات الالكترونية.
- التدريب والتوعية بالأمن السيبراني: كشفت دراسة (McCrohan et al.,2010) عن تأثير التوعية بالأمن السيبراني على سلوك المستخدمين، حيث قُسم المشاركون إلى مجموعتين حيث أظهرت المجموعة التي تلقت معلومات متقدمة وبرامج تدريبية عن الأمن الرقمي والتهديدات الرقمية تحسنًا في أدائها للحفاظ على سرية المعلومات والبيانات استنادا إلى قوة كلمات المرور مقارنة بالمجموعة الأخرى. وأكدت النتائج أن التعليم الموجه حول التوعية بالتهديدات الإلكترونية يعزز الممارسات الأمنية بشكل ملموس. وأوصت بضرورة الاستثمار في برامج توعوية هادفة للكشف المبكر والحد من المخاطر السيبرانية على الأفراد والمؤسسات.

التعقيب على الدراسات السابقة:

تكشف الدراسات السابقة عن ثراء معرفي في تناول الجوانب المختلفة للهجمات السيبرانية من قبل عوامل ومحددات متعددة، إلا أنها غالبًا ما تعالج العوامل أو تلك المحددات بشكل منفصل أو فردي دون استكشاف العلاقات التفاعلية المباشرة أو غير المباشرة بين تلك العوامل ، والتي تمثل الجوانب الديموغرافية، الاجتماعية، الاقتصادية، النفسية، والثقافية، وغيرها، وتشير بعض الدراسات إلى أن هناك تداخلًا بين هذه العوامل في التأثير المحتمل في التعرض إلى الوقوع في المخاطر الالكترونية، ما يستلزم الحاجة إلى توليد أو تطوير إطار نظري تكاملي يعكس التفاعل الديناميكي بين المتغيرات أو المحددات المؤثرة على تهديدات الأمن السيبراني.، وقد يعكس ذلك أهمية تبني تطبيق النهج المتعدد الأبعاد في تحليل الأمن الرقمي. على سبيل المثال، قد أشارت إلى احتمالية أن الأفراد ذوو المستويات التعليمية والتدريبية العالية أكثر وعيًا بالمخاطر الرقمية، بينما تؤثر العوامل الاجتماعية والاقتصادية مثل مستوى استخدام التكنولوجيا أو الوعي بتقنيات الذكاء الاصطناعي على تبني تدابير استباقية أو وقائية لتعزيز مقومات الأمان الرقمي. ومن ناحية أخرى، أظهرت الدراسات أن الثقافة الرقمية للأفراد تتطور بشكل تدريجي عبر مراحل الحياة المختلفة، مما يعزز الحاجة إلى برامج توعية للأمن الرقمي بشكل مستمر.

أوجه القصور في الدراسات السابقة:

- ندرة الأبحاث والدراسات التي تربط بين تطبيقات الذكاء الاصطناعي والاستراتيجيات الوقائية للأمن السيبراني في العالم العربي.
- قلة الدراسات التحليلية المتعمقة التي تعتمد نموذجًا نظريا تفاعليًا يعكس التأثير المشترك لمجموعة متنوعة من العوامل والمحددات المؤثرة على رفع مقومات الوعي باحتمالية التعرض للتهديدات السيبرانية التي تؤثر على مقومات الأمن الرقمي المجتمعي مع تطبيقه في أحد المدن الممثلة لثقافة البيئة العربية وتحدياتها.
- قلة وجود نماذج تنبؤية لقياس مستوى الوعي الرقمي المجتمعي وتأثيره على الحد من التهديدات السيبرانية.
- تركيز معظم الأبحاث على مجتمعات غربية وآسيوية، مع نقص في الدراسات التي تستهدف البيئات العربية.

القيمة المضافة للدراسة الحالية

تُبرز الدراسة الحالية أهمية تقديم نموذج نظري تنبؤي وتكاملي يجمع بين مجموعة من العوامل والمحددات، ولاسيما المؤثرة على البيئة الخارجية في التخطيط بعيد المدى وفقا لمصفوفة (بيستل) والتي تتضمن المحددات الديموجرافية والاجتماعية والاقتصادية والسياسية والتكنولوجية والبيئية والتعليمية والثقافية والدينية في فحص احتمالية التاثير المباشر وغير المباشر على رفع مستوى الوعي الرقمي تجاه الكشف المبكر عن احتمالية التعرض للتهديدات والمخاطرالسيبرانية سواء على مستوى الفرد أو المجتمع

لتطوير رؤية جديدة لتطوير قياسات وسياسات ومنهجيات وآليات عمل ذكية تعزز الأمن الرقمي المجتمعي الذكي بالشكل الأمثل، وهذا من شأنه قد يساهم نوعا كقيمة بحثية جديدة في سد الفجوة البحثية الحالية ويساهم في تعزيز مقومات الأمن الرقمي المجتمعي في الدول العربية في ظل التوسع في تطبيقات تقنيات الذكاء الاصطناعي المصاحبة لسرعة التطورات الصناعية والتكنولوجية وثقافة الابتكار والابداع على مستوى المجالات الحيوية في معظم بقاع دول العالم، وسوف يسعى نمذجة هذا النموذج النظري التنبؤي في دمج مختلف هذه المحددات والعوامل الديموغرافية والاجتماعية والاقتصادية وغيرها ضمن إطار تحليلي متعمق وشامل لتحديد مستوى الوعي الرقمي المجتمعي وقياس تأثيره على الحد من الجرائم الإلكترونية. ويُعد هذا النموذج خطوة متقدمة نحو تطوير سياسات أمنية استباقية قائمة على البيانات الذكية، مما يعزز من استدامة الأمن الرقمي في المجتمعات العربية.

جدول فجوة الدراسات السابقة والقيمة المضافة:

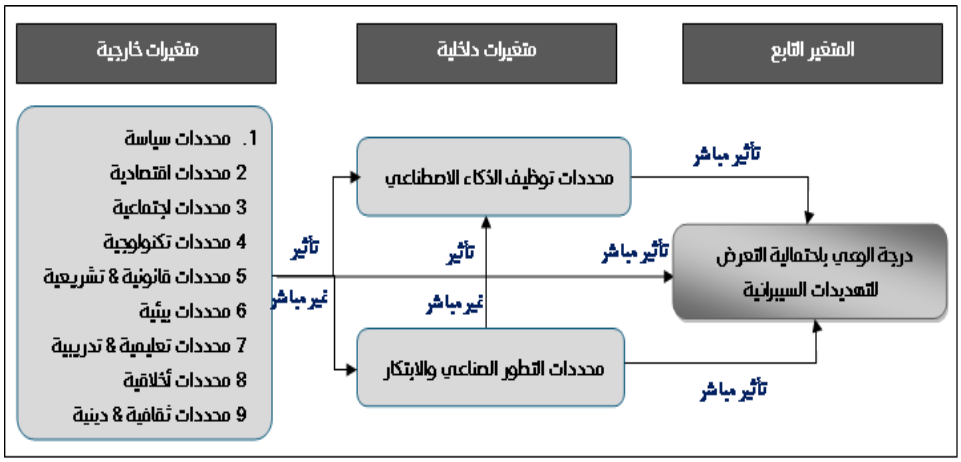
مجال الدراسة	الدراسات السابقة	الفجوة البحثية	القيمة المضافة للدراسة الحالية
المحددات الاجتماعية أو الديموغرافية أو غيرها	تم تناولها بشكل فردي	عدم دراسة التداخل بين العوامل أو المحددات المختلفة في إطار بناء نموذج تفاعلي للعلاقات	نموذج تكاملي يجمع يعكس العلاقات التفاعلية فيما بين المحددات والعوامل المقترحة من قبل الدراسة الحالية
الوعي الرقمي	تأثير محدود على التعرض للهجمات	نقص الدراسات التي تعتمده كمتغير وسيط	اعتماد الوعي الرقمي سواء تطبيقات الذكاء الاصطناعي أو التطور الصناعي والابتكار كمتغيرات وسيطة
الأمن السيبراني في المجتمعات العربية	أبحاث قليلة ومحدودة	قلة الدراسات التي تركز على هذا المجال في الدول العربية	تركيز الدراسة على المجتمع العربي مع تقديم نموذج مصمم خصيصًا لأحد المدن في البيئة العربية
نموذج أمان رقمي	غياب النماذج التنبؤية	عدم وجود إطار قياسي لتقييم الوعي أو الأمن الرقمي في مجتمعاتنا العربية	بناء نموذج سببي يعتمد على رؤية تحليلية لفحص العلاقات التنبؤية فيما بين متغيرات الدراسة

الإطار النظري للدراسة:

يتمثل الإطار العام للدراسة الحالية في التركيز على اظهار بناء نموذج نظري تنبؤي للعلاقات المتوقعة فيما مجموعة من المحددات المؤثرة أو المتغيرات الخارجية والداخلية وأخرى التي لايمكن أن تكون قيد الدراسة الحالية (وما يسمي بالبواقي) لفحص تأثيراتها المباشرة وغير المباشرة على مستوى الوعي الرقمي المجتمعي لاحتمالية التعرض للتهديدات والمخاطر السيبرانية، بما يضمن تعزيز مقومات الاستعداد الأمني السيبراني.

مخطط إطار النموذج التنبؤي للعلاقات بين المتغيرات الخارجية والداخلية

في التأثير في المتغير التابع (درجة مقياس الوعي باحتمالية التهديدات السيبرانية)



سوف يتيح هذا الإطار النظري نمذجة نموذج تنبؤي قادر على إجراء تحليلًا شاملًا للعوامل أو المحددات المحتمل تأثيرها على زيادة رفع مستوى درجة الوعي الفردي أو المجتمعي بالأمن الرقمي من خلال احتمالية التعرض للتهديدات والمخاطر السيرابنية، مما يمكّن من تطوير استراتيجيات استباقية لمكافحة الجرائم الإلكترونية وتعزيز الأمان الرقمي في المجتمعات المستهدفة.

منهجية الدراسة:

اعتمدت الدراسة على الإحصاء الوصفي والاستدلالي من خلال المسح بعينة عشوائية بسيطة بلغت ١٥٩ مبحوث استهدفت مجتمع مدينة خورفكان التي تقع في المنطقة الشرقية لإمارة الشارقة بدولة الامارات العربية المتحدة، كما تم تصميم أداة استبيان الكترونين لجمع البيانات المتعلقة بالخصائص الديموغرافية والاجتماعية والممارسات الرقمية للأفراد مقسمة إلى مجموعة من المحددات قيد الدراسة وفق النموذج النظري التنبؤي المفترض والمؤثرة على مستويات درجة الوعي الوعي الفردي أو المجتمعي تجاه احتمالية التعرض للهجمات السيبرانية أو المخاطر الرقمية. ويتم تطبيق التحليل

الإحصائي باستخدام النماذج السببية التنبؤية لتحديد المسارات التأثيرية والتفاعلات فيما بين المتغيرات أو المحددات المؤثرة قيد الدراسة حاليا، وقد تم مراعاة تقسيم أداة الاستبيان في التصميم على جزئين بحيث الجزء الأول يمثل الخصاص الديموغرافية والخلفية للمبحوثين المشمولين في عينة الدراسة المسحية، أما المجموعة الثانية فقد تضمنت عدد (٥٥) بند يمثلون أبعاد التأثير المحتمل لعدد (١١) من المحددات المتوقع تأثيرها على مستوى درجة الوعي العام لدى الفرد أو المجتمع تجاه احتمالية التعرض للتهديدات السيبرانية أو المخاطر الرقمية على ان يتم قياس كل محدد من خلال ٥ بنود لقياس التأثير المحتمل من وجدهة نظر المبحوثين، وقد تم مراعاة ما توصلت اليه الدراسة الحالية من خلال الاطلاع على الأدبيات والتقارير المختصة بتعزيز التوجه الاستشرافي نحو الأمن الرقمي المجتمعي وفقا التطور الآمن في التقنيات الذكية بشكل مستدام يضمن حجودة ورفاهية الحياة الرقمية للمستخدمين قدر المستطاع في ظل التهديات والتحديات الرقمية التي يشهدها التطورات المتلاحقة في بيئة الأعمال الدولية، وقد تم اختبار مدى توفر الخصائص الأساسية لصلاحية تطبيق أداة القياس المستخدمة في الدراسة البحثية بقياس كل من:

صـدق الأداة: تم التحقق بالطرق الإحصائية بإيجاد صدق التجانس الداخلي (Internal Contingency) عن طريق إيجاد العلاقة الارتباطية بين كل بعد في الاستبيان والدرجة الكلية للمقياس الكلي من خلال حساب معامل الارتباط لسبيرمان، وكانت جميعها دال إحصائيا عند مستوى الدلالة (α = ٠,٠١ أو ٠,٠٥)، مما يشير إلى تجانسها مع الأداة ككل وملاءمتها لقياس الأهداف أو الغرض الذي وضعت من أجله.

ثبـات الأداة: قامت الدراسة بالتحقق من ثبات الأداة على جميع أفراد عينة الدراسة المسحية المؤلفة من (١٥٩) مبحوث يمثلون وجهة نظر المبحوثين في مجتمع مدينة خورفكان لدور الذكاء الاصطناعي في تحقيق الأمن الرقمي وقياس وتقييم تأثير المحددات على الجرائم الالكترونية، وذلك باستخراج معامل الثبات لتقدير درجة التجانس والانسجام بين مكونات الأداة باستخدام Cronbach's alpha الذي يقيس الاتساق الداخلي للعناصر أو البنود التي يتكون منها المقياس، وقد أسفرت نتائج تحليل الاختبار بأن معامل الثبات لبنود الاستبيان بلغت ٠,٩٩٤، وبالتالي فهو يعكس مستوى جيد لثبات أداة الاستبيان بحيث يشير إلى أنه معامل ذو دلالة مرتفعة في الاستدلال على استقرار الاستبانة مما يعني إمكانية الاعتماد على استخدام الأداة تجاه تحقيق أهداف الدراسة المسحية ومن ثم الوثوق بنتائجها، ولاسيما أنه كلما كانت قيمة معامل الثبات أكبر من ٠,٦ كلما دل ذلك على وجود اتساق بين بنود الاستبيان وبالتالي يمكن وضعها في دليل (Index) أو مقياس واحد، وعموما فإن نتائج الصدق والثبات تدعم صلاحية اداة الاستبيان المستخدمة للقياس والاعتماد عليها من قبل الدراسة المسحية.

الأساليب الإحصائية المستخدمة:

المقاييس الأساسية للبيانات باستخدام النسب المئوية والتكرارات.

- استخدام اختبار كاي تربيع لفحص العلاقة الارتباطية بين حالة التعرض للهجمات والتهديدات الرقمية (نعم / لا) وبين مجموعة من الخصائص الديموجرافية والخلفية للمبحوثين المستهدفة.

- استخدام اختبار t للعينات المستقلة (T-Test for Independent Samples)، لفحص الفروق أو الاختلافات النسبية في قيم المحددات المؤثرة قيد الدرسة نتيجة أثر بعض الخصائص الديموجرافية المتاحة للمبحوثين المتمثلة في: (النوع الاجتماعي، والجنسية، والفئة العمرية، والمستوى التعليمي، والحالة الاجتماعية، والحالة الوظيفية، وطبيعة الوظيفة)، حيث إن:

الفرض العدمي (H0): متوسط المجموعة الأولى μ1= متوسط المجموعة الثانية μ2

الفرض العدمي (Ha): متوسط المجموعة الأولى μ1 ≠ متوسط المجموعة الثانية μ2

- استخدام أسلوب تحليل التمايز Discrimination analysis لاشتقاق الدالة التمييزية التي يمكنها التمييز والتنبؤ بتصنيف حالات المتغير التابع (تأثير الوعي العام تجاه احتمالية التعرض للتهديدات والمخاطر السيبرانية) اعتمادا على بعض المتغيرات محل اهتمام الدراسة الحالية حيث تم تقسيم المتغير التابع إلى أربع مجموعات (تأثير عالي جدا/ تأثير عالي/ تأثير متوسط / تأثير منخفض) حيث تقوم دالة التمايز بالتنبؤ برقم المجموعة التي ينتمي لها حالة الوعي للفرد او المجتمع، ويهدف تحليل التمايز بشكل عام إلى إجراء الآتي:
  - تصميم التوليفات الخطية للمتغيرات الأفضل تنبؤا أو تمييزا محل اهتمام الدراسة.
  - التحقق من مدى وجود فروق معنوية بين المجموعات فيما يتعلق بتلك المتغيرات.
  - تحديد المتغيرات التي تسهم بأكبر قدر في تفسير الاختلاف بين فئات المتغير التابع (حالة الوعي المجتمعي أو الفردي).
  - تقسيم الحالات بين فئات المتغير التابع وفقا لقيم المتغيرات المستقلة الداخلة في دالة التمايز.
  - تقييم دقة وقدرة النموذج المقترح (الدالة المشتقة) على التصنيف أو التقسيم كنسبة مئوية.
  - وبافتراض أن دالة التمايز خطية، فإن النموذج المقترح الذي يمثل دالة التمايز يكون كالآتي:

$$D = B_1X_1 + B_2X_2 + B_3X_3 + \ldots\ldots + B_nX_n$$

حيث إن: كل من $B_1, B_2, B_3, \ldots\ldots Bn$ هي معالم مجهولة مطلوب تقديرها، وبشرط الوصول إلى أفضل التقديرات لمعالم النموذج التي تضمن أقل احتمال لخطا التمييز أو التقسيم.

- استخدام أسلوب تحليل المسار لتحديد الارتباط والسببية بين مسارات المحددات المؤثرة على زيادة الوعي باحتمالية التعرض للتهديدات السيبرانية. ويستخدم لتحديد قيمة معاملات المسارات Path coefficients لتحديد الأثر المباشر وغير المباشر لعلاقة السبب والنتيجة Cause-Effect بين المتغيرات دون الحاجة إلى تثبيت أو عزل المتغيرات الأخرى، أي يعتمد على علاقة التأثير والتأثر من خلال البناء التخطيطي لنموذج سببي يتضمن تصنيف مجموعة من المتغيرات إلى خارجية "مستقلة" وداخلية "تابعة" وفق نظام مغلق لاستخراج مجموعة من المعادلات تعبر عن العلاقة فيما بينها وكذلك متغيرات البواقي التي تؤثر تأثير مباشر على المتغيرات الداخلية المراد تفسيرها ولكنها غير موجودة قيد البحث الحالي (Abbasi, n.d.)

نتائج الدراسة المسحية ومناقشتها:

يستهدف هذا الجزء من الدراسة إلقاء الضوء عن كثب على أهم الخصائص الخلفية الأساسية لعينة المسح وفق المشاركين البالغ عددهم (١٥٩) حيث يقدم الجدول رقم (١) التالي تحليلًا دقيقًا للخصائص الخلفية موزعًا إياهم حسب تصنيف تعرضهم للتهديدات والمخاطر الإلكترونية أو السيبرانية. من خلال هذا التوزيع، نسعى إلى فهم العوامل الديموغرافية والاجتماعية التي قد تزيد أو تقلل من احتمالية التعرض لهذه المخاطر، مما يوفر رؤى قيمة لتطوير استراتيجيات وقائية فعالة، وذلك وفقا لمعطيات الجدول التالي:

جدول (١): الخصائص الخلفية لعينة المسح المستهدفة موزعين نسبيا

حسب تصنيف حالة تعرضهم للتهديدات والمخاطر الالكترونية من واقع تجربة المبحوثين الفعلية

المتغيرات الخلفية (الديموجرافية والاجتماعية)		حالة التعرض للتهديدات والمخاطر السيبرانية			
		لا (n=١٠٢)		نعم (n=٥٧)	
		العدد	%	العدد	%
النوع الاجتماعي	ذكور	٢٦	٢٥,٥	١٨	٣١,٦
	إناث	٧٦	٧٤,٥	٣٩	٦٨,٤
الجنسية	مواطنين	٨٧	٨٥,٣	٤٧	٨٢,٥
	غير مواطنين	١٥	١٤,٧	١٠	١٧,٥
الحالة الاجتماعية	متزوج	٢١	٢٠,٦	١٥	٢٦,٣
	غير متزوج	٨١	٧٩,٤	٤٢	٧٣,٧
الفئة العمرية	٢٤ سنة فأقل (فئة الشباب والمراهقين)	66	64.7	33	57.9
	٢٥ سنة فأكثر (فئة البالغين)	36	35.3	24	42.1
الحالة التعليمية	تعليم عالي فمافوق	٧٣	٧١,٦	٤٤	٧٧,٢
	تعليم دون الجامعي	٢٩	٢٨,٤	١٣	٢٢,٨
الحالة الوظيفية	يعمل	35	34.3	21	36.8
	لايعمل	67	65.7	36	63.2
طبيعة الوظيفة	وظيفة رقمية	47	46.1	26	45.6
	وظيفة غير رقمية	55	53.9	31	54.4

كشفت نتائج التحليل في الجدول رقم (١) عن توزيع متقارب نسبيًا بين المجموعتين (تعرضوا للتهديدات ولم يتعرضوا) في معظم الخصائص الديموغرافية والاجتماعية. ومع ذلك، يمكن ملاحظة بعض الفروق الطفيفة التي تستحق التنويه، فاالنوع الاجتماعي نجد أن الإناث يمثلن نسبة أعلى في كلتا المجموعتين،

ولكن النسبة أعلى قليلاً في مجموعة "لم يتعرضوا" (٧٤,٥٪ مقابل ٦٨,٤٪). أما الجنسية فنجد أن الغالبية العظمى من المبحوثين هم مواطنون في كلتا المجموعتين، مع تقارب كبير في النسب، والفئة العمرية :الشباب والمراهقون (٢٤ سنة فأقل) يمثلون نسبة أعلى في مجموعة "لم يتعرضوا" (٦٤,٧٪ مقابل ٥٧,٩٪)، والحالة التعليمية نجد أن الحاصلون على تعليم عالي فما فوق يمثلون نسبة أعلى في مجموعة "تعرضوا" (٧٧,٢٪ مقابل ٧١,٦٪)، وبالنسبة الحالة الوظيفية فنجد أن العاطلون عن العمل يمثلون نسبة أعلى في كلتا المجموعتين، مع تقارب في النسب، أما بالنسبة لطبيعة الوظيفة فنجد هناك تقارب كبير في نسب أصحاب الوظائف الرقمية وغير الرقمية في كلتا المجموعتين.

وبشكل عام التقارب الكبير في النسب بين المجموعتين يشير إلى أن التعرض للتهديدات والمخاطر الإلكترونية لا يقتصر على فئة ديموغرافية أو اجتماعية معينة، بل هو تحدٍ يواجه جميع الفئات، والنسبة الأعلى قليلاً للشباب والمراهقين في مجموعة "لم يتعرضوا" قد تشير إلى زيادة وعي هذه الفئة بالمخاطر الإلكترونية أو اتخاذهم إجراءات وقائية أفضل، والنسبة الأعلى من الحاصلين على تعليم عالي في مجموعة "تعرضوا" قد تدل علي انهم الاكثر استخداما للتقنيات الرقمية، وفي نهاية المطاق تظهر نتائج الجدول رقم (١) رؤى جديدة لصناع القرار حول الخصائص الخلفية للمبحوثين وعلاقتها بالتعرض للتهديدات والمخاطر الإلكترونية، مما يساعدهم في اتخاذ قرارات مستنيرة لتعزيز الأمن السيبراني في المجتمع من خلال سياسات وبرامج توعية فعالة.

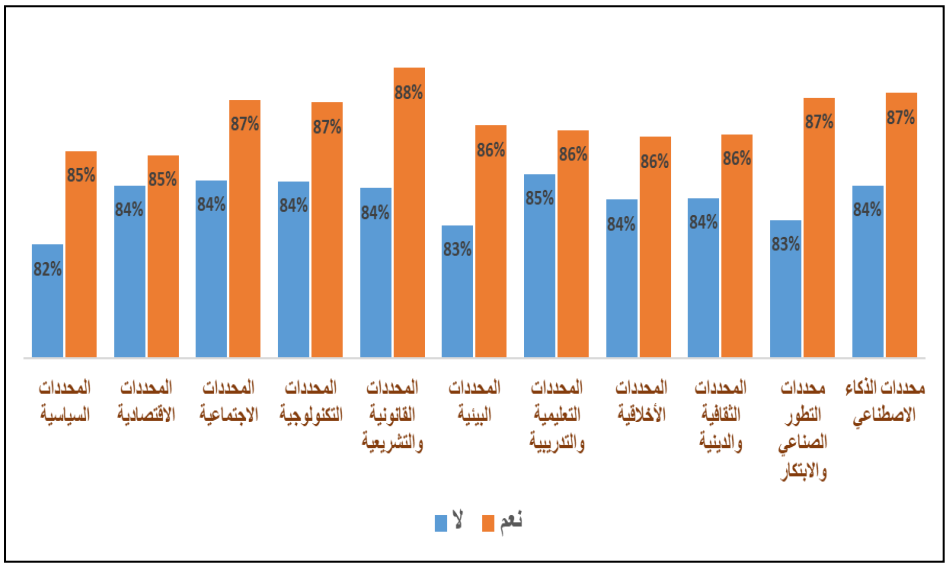
كما أن الجدول رقم (٢) يقدم تحليلًا للأهمية النسبية للمحددات المؤثرة المتضمنة في نمذجة النموذج التنبؤي وفق الإطار النظري للدراسة على قياس الوعي بالتهديدات والمخاطر السيبرانية، مصنفًا إياها حسب حالة تعرض المبحوثين لهذه التهديدات. من خلال هذا التحليل، نسعى إلى فهم الفروق في إدراك أهمية هذه المحددات بين المجموعتين، مما قد تساهم في توليد أنشطة ومبادرات لتطوير استراتيجيات توعية وتدريب فعالة، وقد جاءت النتائج موضحة كما في الجدول التالي:

جدول (٢): الأهمية النسبية للمحددات المؤثرة على زيادة الوعي تجاه احتمالية التعرض للتهديدات والمخاطر السيبرانية حسب تصنيف حالة تعرضهم للتهديدات والمخاطر الالكترونية من واقع تجربة المبحوثين الفعلية

المحددات المؤثرة	حالة التعرض للتهديدات والمخاطر السيبرانية	
	الذين لم يتعرضوا	الذين تعرضوا فعلا
المحددات السياسية	82.5%	85.3%
المحددات الاقتصادية	84.3%	85.2%
المحددات الاجتماعية	84.4%	86.9%
المحددات التكنولوجية	84.4%	86.8%
المحددات القانونية والتشريعية	84.2%	87.9%
المحددات البيئية	83.1%	86.1%

المحددات التعليمية والتدريبية	84.6%	86.0%
المحددات الأخلاقية	83.8%	85.8%
المحددات الثقافية والدينية	83.9%	85.8%
محددات التطور الصناعي والابتكار	83.2%	86.9%
محددات الذكاء الاصطناعي	84.3%	87.1%

وقد أظهرت تحليل النتائج في الجدول رقم (٢) تقارب كبير في الأهمية النسبية للمحددات المؤثرة بين المجموعتين، مع وجود فروق طفيفة تشير إلى بعض الاتجاهات الهامة، ومنها ارتفاع الأهمية النسبية لدى الذين تعرضوا فعلا. وبشكل عام، تظهر المجموعة التي تعرضت فعليًا للتهديدات والمخاطر السيبرانية تقديرًا أعلى لأهمية جميع المحددات المؤثرة مقارنة بالمجموعة التي لم تتعرض. وبالإضافة إلى ذلك تبرز المحددات القانونية والتشريعية، ومحددات الذكاء الاصطناعي، والمحددات الاجتماعية، ومحددات التطور الصناعي والابتكار كأكثر المحددات التي يرى فيها الذين تعرضوا للتهديدات أهمية نسبية. كما بينت نتائج الجدول وجود تقارب في الأهمية النسبية للمحددات، وعلى الرغم من الفروق الطفيفة، إلا أن الأهمية النسبية لجميع المحددات تتراوح بين ٨٢,٥٪ و٨٧,٩٪، مما يشير إلى أن كلتا المجموعتين تدرك أهمية هذه المحددات في زيادة الوعي بالمخاطر السيبرانية، وللمزيد من التوضيح فقد يعكس الشكل التالي رقم (١) ملخص الأهمية النسبية للمحددات المؤثرة من واقع تجربة المبحوثين الذين تعرضوا لهجمات ومخاطر سيبرانية في مقابل الذين لم يتعرضوا لمثل هذه التهديدات، كما يلي:



شكل (١): الأهمية النسبية للمحددات المؤثرة حسب تصنيف حالة التعرض للتهديدات والمخاطر السيبرانية (نعم / لا)

وقد أظهر الشكل رقم (١) وجود التقارب الكبير في الأهمية النسبية مما يشير إلى أن المحددات المؤثرة المتضمنة في النموذج النظري تعتبر ذات أهمية عالية لدى جميع المبحوثين، سواء تعرضوا للتهديدات أم لا مع ارتفاع طفيف في الأهمية النسبية لدى المجموعة التي تعرضت للتهديدات بحيث يشير إلى أن التجربة الفعلية تزيد من إدراك أهمية هذه المحددات من قبل المستخدمين الرقميين لرفع مقومات الوعي بالأمن الرقمي المجتمعي الآمن من التهديدات والمخاطر السيبرانية، وهذا الوعي يساهم في تعزيز استدامة التنمية الرقمية.

وفي إطار استخدام اختبارt لفحص مدى وجود الاختلافات أو الفروق النسبية الدالة احصائيا في تقييم المحددات المؤثرة على زيادة الوعي العام تجاه احتمالية التعرض للهجمات السيبرانية وفقا لتأثير وعي المبحوثين بالذكاء الاصطناعي أو الأمن الرقمي أو الاستخدام اليومي، وقد أسفرت نتائج الجدول التالي عن وجود تأثيرات متباينة، ولكنها جوهرية لدور وعي المبحوثين بالذكاء الاصطناعي والأمن الرقمي والاستخدام اليومي للتقنيات الرقمية على تقييمهم للمحددات المؤثرة على الوعي بالهجمات السيبرانية. باستخدام اختبار t للعينات المستقلة، نهدف إلى تحديد الفروق المعنوية التي تكشف عن ديناميكيات تفاعلية في إدراك هذه المحددات.

جدول (٣): اختبار t للعينات المستقلة لفحص الاختلافات النسبية في تقييم المحددات المؤثرة على زيادة الوعي العام تجاه التعرض للهجمات السيبرانية وفقا لتأثير وعي المبحوثين بالذكاء الاصطناعي أو الأمن الرقمي أو الاستخدام اليومي

المحددات المؤثرة	الوعي بالذكاء الاصطناعي			الوعي بالأمن الرقمي			الاستخدام اليومي للتقنيات الرقمية والذكية		
	العدد	المتوسط	T-test	العدد	المتوسط	T-test	العدد	المتوسط	T-test
المحددات السياسية	نعم	109	21.16	96	21.39	2.187*	139	20.96	.745
	لا	50	20.26	63	20.10		20	20.30	
				1.430					
المحددات الاقتصادية	نعم	109	21.49	96	21.76	2.886*	139	21.41	2.608*
	لا	50	20.42	63	20.22		20	19.35	
				1.871					
المحددات الاجتماعية	نعم	109	21.80	96	22.08	3.594*	139	21.58	2.545*
	لا	50	20.30	63	20.17		20	19.55	
				2.630*					
المحددات التكنولوجية	نعم	109	21.71	96	21.99	3.144*	139	21.53	2.132*
	لا	50	20.46	63	20.29		20	19.80	
				2.149*					
المحددات القانونية والتشريعية	نعم	109	21.80	96	22.08	3.020*	139	21.58	1.778
	لا	50	20.46	63	20.30		20	20.00	
				2.123*					

المحددات البيئية	نعم	109	21.54	2.497*	96	21.94	3.824*	139	21.26	1.944
	لا	50	19.94		63	19.67		20	19.50	
المحددات الثقافية والدينية	نعم	109	21.76	3.049*	96	22.07	3.904*	139	21.42	2.444*
	لا	50	19.80		63	19.73		20	19.20	
المحددات التعليمية والتدريبية	نعم	109	21.76	2.488*	96	22.04	3.331*	139	21.55	2.474*
	لا	50	20.22		63	20.11		20	19.40	
المحددات الأخلاقية	نعم	109	21.65	2.683*	96	21.86	3.193*	139	21.41	2.559*
	لا	50	20.00		63	20.02		20	19.20	

(*) معنوية عند مستوى دلالة أقل من ٠,٠٥.

في ضوء نتائج الجدول رقم (٣)، تبين أن الوعي المسبق بمفاهيم وأسس الذكاء الاصطناعي والأمن الرقمي والاستخدام اليومي للتقنيات الرقمية والذكية لهما تأثيرات معنوية على تقييم المبحوثين لمعظم المحددات المؤثرة على الوعي بالهجمات السيبرانية، وفيما يخص الوعي بالأمن الرقمي، فقد أظهرت النتائج بالجدول وجود تأثيرًا معنويًا على جميع المحددات، مما يشير إلى أن الأفراد الذين لديهم وعي بالأمن الرقمي يقدرون أهمية هذه المحددات بشكل أكبر مقارنة بما ليس لديهم وعي استنادا إلى قيم المتوسطات لكلا المجموعتين. وهذا يعكس فهمًا أعمق لأبعاد الأمن السيبراني وأهمية العوامل المختلفة في تعزيز الوعي الرقمي المجتمعي بشكل عام. أما بالنسبة للاستخدام اليومي للتقنيات الرقمية والذكية فقد أظهرت النتائج وجود تأثيرًا معنويًا على المحددات الاقتصادية، الاجتماعية، التكنولوجية، الثقافية والدينية، التعليمية والتدريبية، والأخلاقية. وهذا يشير إلى أن الاستخدام المتكرر للتقنيات الرقمية يزيد من إدراك الأفراد لأهمية هذه المحددات في مواجهة التهديدات السيبرانية. وأيضا بالنسبة للوعي بالذكاء الاصطناعي، فقدأوضحت النتائج وجود تأثيرًا معنويًا على المحددات الاجتماعية، التكنولوجية، القانونية والتشريعية، البيئية، الثقافية والدينية، التعليمية والتدريبية، والأخلاقية. ومع ذلك، لا يظهر تأثيرًا معنويًا على المحددات السياسية والاقتصادية. وهذه النتائج تسلط الضوء على أهمية تعزيز الوعي بالأمن الرقمي وتشجيع الاستخدام الآمن للتقنيات الرقمية. لذا يجب على صناع القرار تطوير برامج توعية وتدريب تستهدف جميع الفئات، مع التركيز على الجوانب التي تظهر تأثيرًا معنويًا في هذه الدراسة. بالإضافة إلى ذلك، يجب إجراء المزيد من الدراسات لفهم الأسباب التي تجعل الوعي بالأمن الرقمي والاستخدام اليومي للتقنيات الرقمية يؤثران بشكل كبير على تقييم المحددات المؤثرة على الوعي بالهجمات السيبرانية.

وسوف تكشف نتائج الجدول التالي فحص العلاقات الارتباطية بين حالة التعرض للهجمات والتهديدات السيبرانية من خلال تجربة المبحوثين مع مجموعة من الخصائص الديموغرافية والاجتماعية. باستخدام اختبار كاي تربيع، نهدف إلى تحديد مصادر الاختلاف المعنوي التي تلقي الضوء

على الفئات الأكثر عرضة لهذه التهديدات، مما يساعد في تطوير استراتيجيات وقائية فعالة من قبل الجهات المعنية. كما إن النتائج المعروضة هنا لا تقدم فقط صورة إحصائية، بل تكشف عن أنماط سلوكية واجتماعية حاسمة يجب أخذها في الاعتبار في استراتيجيات الأمن السيبراني، وذلك على النحو الآتي

جدول (٤): التوزيع العددي والنسبي لحالة التعرض للهجمات السيبرانية أو الالكترونية (نعم / لا) وعلاقتها ببعض المتغيرات الأساسية محل اهتمام الدراسة الحالية

الخصائص للمبحوثين	الخلفية	التعرض للهجمات السيبرانية أو الالكترونية				الإجمالي	المعنوية لـ(X^2) Sig.
		نعم		لا			
		العدد	%	العدد	%		
النوع	ذكور	١٨	٤٠,٩٪	٢٦	٥٩,١٪	٤٤	٠.411
	اناث	٣٩	٣٣,٩٪	٧٦	٦٦,١٪	١١٥	
الجنسية	مواطن	٤٧	٣٥,١٪	٨٧	٦٤,٩٪	١٣٤	0.637
	غير مواطن	١٠	٤٠,٠٪	١٥	٦٠,٠٪	٢٥	
الحالة الاجتماعية	متزوج	١٥	41.7%	٢١	58.3%	٣٦	0.408
	غير متزوج	٤٢	34.1%	٨١	65.9%	١٢٣	
الحالة التعليمية	تعليم جامعي فمافوق	٤٤	٣٧,٦٪	٧٣	٦٢,٤٪	١١٧	٠,٤٤٠
	تعليم دون الجامعي	١٣	٣١,٠٪	٢٩	٦٩,٠٪	٤٢	
الفئة العمرية	٢٤ سنة فأقل	33	33.3%	66	66.7%	99	0.395
	٢٥ سنة فأكثر	24	40.0%	36	60.0%	60	
الحالة الوظيفية	يعمل	21	37.5%	35	62.5%	56	0.749
	لا يعمل	36	35.0%	67	65.0%	103	
طبيعة الوظيفة	وظيفة رقمية	26	35.6%	47	٦٤,٤٪	73	0.955
	وظيفة غير رقمية	31	٣٦,٠٪	55	٦٤,٠٪	86	
الوعي بالذكاء الاصطناعي	نعم	41	٣٧,٦٪	68	٦٢,٤٪	109	0.439
	لا	16	٣٢,٠٪	34	٦٨,٠٪	50	
الوعي بالأمن الرقمي	نعم	36	٣٧,٥٪	60	٦٢,٥٪	96	0.592
	لا	21	٣٣,٣٪	42	٦٦,٧٪	63	
الاستخدام اليومي	نعم	53	38.1%	86	61.9%	139	0.014*
	لا	5	25.0%	15	75.0%	20	

للتقنيات الرقمية والذكية						
قلق من انتشارتطبيق الذكاء الاصطناعي في المستقبل	نعم	48	38.1%	78	61.9%	126	0.248
	لا	9	27.3%	24	72.7%	33	
الإجمالي		٥٧	٣٥,٨٪	102	٦٤,٢٪	159	

(*) قيمة Chi-Square معنوية عند مستوى 0.05.

(**) قيمة Chi-Square معنوية عند مستوى 0.01.

كشفت نتائج تحليل النتائج في الجدول رقم (٤) أن المتغير الوحيد الذي يرتبط بشكل معنوي بالتعرض للهجمات السيبرانية هو الاستخدام اليومي للتقنيات الرقمية والذكية (Sig. = 0.014) وهي دالة احصائيا عند مستوى أقل من ٠,٠٥، وهذه النتيجة تشير إلى أن الأفراد الذين يستخدمون التقنيات الرقمية والذكية بشكل يومي هم أكثر عرضة للتعرض للهجمات السيبرانية. وفي المقابل، نجد ان المتغيرات الأخرى مثل النوع، الجنسية، الحالة الاجتماعية، الحالة التعليمية، الفئة العمرية، الحالة الوظيفية، طبيعة الوظيفة، الوعي بالذكاء الاصطناعي، والوعي بالأمن الرقمي لا تظهر علاقة معنوية بالتعرض للهجمات السيبرانية، وهذه النتائج تسلط الضوء على أهمية اعتبار الاستخدام اليومي للتقنيات الرقمية والذكية كعامل خطر محتمل للتعرض للهجمات السيبرانية. لذا يجب على صناع القرار التركيز على توفير تدريب وتوعية للأفراد الذين يستخدمون هذه التقنيات بشكل يومي لتقليل خطر تعرضهم للهجمات، في ظل التوسع في استخدام تقنيات الذكاء الاصطناعي المتزامن مع التطور الصناعي وأنظمة الابتكار في مختلف القطاعات والخدمات، بالإضافة إلى ذلك، يجب إجراء المزيد من الدراسات لفهم الأسباب التي تجعل الأفراد الذين يستخدمون الذكاء الاصطناعي بشكل يومي أكثر عرضة للهجمات السيبرانية، وتطوير استراتيجيات وقائية فعالة بناءً على هذه الأسباب. وبشكل عام هذه النتائج تقدم رؤى قيمة لصناع القرار حول العوامل المرتبطة بالتعرض للهجمات السيبرانية، وتساعدهم في اتخاذ قرارات مستنيرة لحماية الأفراد من هذه التهديدات.

يهدف هذا الجزء من البحث إلى تطوير نموذج تنبؤي استشرافي يعتمد توظيف أسلوب تحليل التمايز لتمييز العوامل أو المحددات الأكثر تأثيرًا في التنبؤ بتصنيف مستوى التوعية المكتسبة على مستوى الفرد أو المجتمع ككل تجاه احتمالية التعرض أو الوقوع في الجرائم الإلكترونية. من خلال استثمار التحليل الإحصائي العميق للبيانات المستمدة من الدراسة المسحية، وبحيث يتيح النموذج رؤية استباقية لصناع القرار يمكنهم من تبنّي استراتيجيات وقائية فاعلة لتعزيز الأمن الرقمي مع تطوير أدوات الذكاء الاصطناعي كوسائل وتقنيات دفاعية أكثر دقة ومرونة في تطبيق سيناريوهات الاستجابة المناسبة لمواجهة مختلف المخاطر والتهديدات السيبرانية المتطورة بذكاء وفعالية، وسوف يوفر النموذج إطارًا عمليًا لتنفيذ آليات رقابة استباقية

جدول (٥): توزيع عينة الدراسة حسب مستوى التأثير المحتمل للتعرض للمخاطر والتهديدات السيبرانية

مستوى التأثير المحتمل	العدد	(%)
ضعيف	39	24.5
متوسط	40	25.2
عالي	39	24.5
عالي جداً	41	25.8
المجموع	159	100.0

يُظهر الجدول رقم (٥) توزيع عينة الدراسة البالغة ١٥٩ مبحوث حسب مستوى التأثير المحتمل للتعرض للمخاطر والتهديدات السيبرانية، ونلاحظ أن هناك توزيعاً متوازناً نسبياً بين المجموعات الأربع، حيث تتراوح النسب بين ٢٤,٥٪ و٢٥,٨٪، مما يعزز من موثوقية التحليل الإحصائي في تطبيق أسلوب تحليل التمايز نظراً لعدم وجود تحيز في حجم المجموعات.

جدول (٦): متوسطات المحددات حسب مجموعات مستوى التأثير المحتمل

المحددات	تأثير محتمل ضعيف	تأثير محتمل متوسط	تأثير محتمل عالي	تأثير محتمل عالي جداً
المحددات القانونية والتشريعية	16.51	20.38	23.79	25.00
المحددات التعليمية والتدريبية	17.05	21.15	25.03	27.24
المحددات الثقافية والدينية	14.56	18.65	23.10	25.68
المحددات البيئية	15.10	19.45	23.74	25.83
المحددات الاقتصادية	16.82	20.70	24.18	26.05
المحددات الأخلاقية	15.51	19.83	23.51	25.78
محددات التطور الصناعي والابتكار	16.41	20.55	24.69	26.32

يوضح الجدول رقم (٦) متوسطات المحددات المختلفة لكل مجموعة من مجموعات مستوى التأثير المحتمل، ونلاحظ تبايناً واضحاً في المتوسطات بين المجموعات الأربع، حيث تزداد قيم المتوسطات تدريجياً مع ارتفاع مستوى التأثير المحتمل. على سبيل المثال، نجد أن متوسط "المحددات الثقافية والدينية" يتراوح من ١٤,٥٦ للمجموعة ذات التأثير الضعيف إلى ٢٥,٦٨ للمجموعة ذات التأثير العالي جداً، مما يشير إلى أهمية هذا المحدد في التمييز بين المجموعات. هذا النمط المتدرج في المتوسطات يظهر بوضوح في جميع المحددات، مما يدعم فرضية وجود علاقة طردية بين قيم هذه المحددات ومستوى الوعي باحتمالية التعرض للجرائم الإلكترونية.

جدول (٧): اختبار تساوي متوسطات المجموعات (Tests of Equality of Group Means)

المحددات	Wilks' Lambda	F	درجات الحرية ١	درجات الحرية ٢	مستوى الدلالة
المحددات الثقافية والدينية	0.131	342.708	3	155	0.000
المحددات البيئية	0.163	266.135	3	155	0.000
المحددات التعليمية والتدريبية	0.166	259.744	3	155	0.000
المحددات الأخلاقية	0.182	232.204	3	155	0.000
محددات التطور الصناعي والابتكار	0.233	169.822	3	155	0.000
المحددات الاقتصادية	0.244	160.202	3	155	0.000
المحددات القانونية والتشريعية	0.405	75.884	3	155	0.000

يعرض الجدول رقم (٧) نتائج اختبار تساوي متوسطات المجموعات، وقد تم ترتيب المحددات تنازلياً حسب قدرتها التمييزية (من الأعلى إلى الأدنى) بناءً على قيم Wilks' Lambda. جميع المحددات أظهرت قدرة تمييزية عالية ودالة إحصائياً ($p < 0.001$)، حيث كانت قيم Wilks' Lambda منخفضة (تتراوح بين ٠,١٣١ و٠,٤٠٥)، ومن الملاحظ أن "المحددات الثقافية والدينية" تأتي في المرتبة الأولى من حيث القدرة التمييزي (Wilks' Lambda = 0.131، F = 342.708)، وتليها "المحددات البيئية" (Wilks' Lambda = 0.163، F = 266.135)، ثم "المحددات التعليمية والتدريبية" (Wilks'

Lambda = 0.166، F = 259.744) هذه النتائج تشير إلى أن العوامل الثقافية والبيئية والتعليمية هي الأكثر أهمية في التمييز بين مستويات الوعي المختلفة باحتمالية التعرض للجرائم الإلكترونية أو التهديدات السيبرانية بشكل عام.

جدول (٨): نتائج اختبار Box's M لتجانس مصفوفات التباين والتغاير

الإحصائية	القيمة
Box's M	668.366
F Approx.	9.348
درجات الحرية ١	56
درجات الحرية ٢	42241.147
مستوى الدلالة	0.000

يوضح الجدول رقم (٨) نتائج اختبار Box's M لتجانس مصفوفات التباين والتغاير بين المجموعات، وقد أظهر الاختبار قيمة ٦٦٨,٣٦٦ ودلالة إحصائية عالية ($p < 0.001$)، مما يشير إلى عدم تجانس مصفوفات التباين والتغاير بين المجموعات، وعلى الرغم من أن هذه النتيجة قد تشكل انتهاكاً لأحد افتراضات تحليل التمايز، إلا أن هذا الأسلوب الإحصائي معروف بمرونته تجاه انتهاك هذا الافتراض، خاصةً مع تساوي حجم المجموعات تقريباً كما هو موضح في الجدول (١). تم التعامل مع هذه المشكلة من خلال استخدام إجراء خاص حيث تم اختبار المجموعات غير المتفردة مقابل مصفوفة التباين والتغاير المجمعة الخاصة بها.

جدول (٩): القيم الذاتية والنسبة المئوية للتباين المفسر للدوال التمييزية

الدالة	القيمة الذاتية	%من التباين	%التراكمي	الارتباط القانوني
1	14.583	97.8	97.8	0.967
2	0.209	1.4	99.2	0.416
3	0.122	0.8	100.0	0.330

يعرض الجدول رقم (٩) القيم الذاتية والنسبة المئوية للتباين المفسر للدوال التمييزية الثلاث حيث نلاحظ أن الدالة الأولى تفسر النسبة الأكبر من التباين (٩٧,٨٪)، بقيمة ذاتية مرتفعة جداً (١٤,٥٨٣) وارتباط قانوني قوي (٠,٩٦٧). في المقابل، تفسر الدالتان الثانية والثالثة نسباً ضئيلة من التباين (١,٤٪ و٠,٨٪ على التوالي)، وبالتالي فإن هذه النتائج تشير إلى أن الدالة الأولى هي الأكثر أهمية في التمييز بين المجموعات، وأنها كافية تقريباً لتفسير الاختلافات بين مستويات الوعي المختلفة باحتمالية التعرض للجرائم الالكترونية أو المخاطر السيبرانية.

جدول (١٠): اختبار Wilks' Lambda للدوال التمييزية

اختبار الدوال	Wilks' Lambda	Chi-square	درجات الحرية	مستوى الدلالة
1خلال ٣	0.045	478.523	21	0.000
2خلال ٣	0.705	53.726	12	0.000
3	0.891	17.574	5	0.142

كما يوضح الجدول رقم (١٠) نتائج اختبار Wilks' Lambda للدلالة الإحصائية للدوال التمييزية حيث أظهرت النتائج أن الدالتين الأولى والثانية دالتان إحصائياً($p < 0.001$) ، بينما الدالة الثالثة ليست دالة إحصائياً($p = 0.142$) غير معنوية عند مستوى أقل من ٠,٠٥، كما أوضحت أن قيمة 'Wilks Lambdaتعتبر منخفضة جداً للدالة الأولى (٠,٠٤٥) ، وهذا يؤكد قدرتها التمييزية العالية، مقارنة بالدالتين الثانية والثالثة اللتين لهما قيم أعلى (٠,٧٠٥ و٠,٨٩١ على التوالي) ، وبصورة عامة فإن هذه النتائج تتفق مع ما تم عرضه في الجدول رقم (٩) السابق بحيث تؤكد أن الدالة الأولى هي الأكثر أهمية في نموذج التصنيف، بينما يمكن الاعتماد على الدالة الثانية كعامل مساعد، وإهمال الدالة الثالثة لعدم دلالتها الإحصائية.

جدول (١١): المعاملات المعيارية للدوال التمييزية القانونية

المحددات	الدالة ١	الدالة ٢	الدالة ٣
المحددات القانونية والتشريعية	0.035	0.309	0.614
المحددات التعليمية والتدريبية	0.239	0.282	-0.521
المحددات الثقافية والدينية	0.449	-0.675	0.149
المحددات البيئية	0.337	0.057	0.147
المحددات الاقتصادية	0.318	0.351	0.113
المحددات الأخلاقية	0.061	0.529	-0.287
محددات التطور الصناعي والابتكار	0.388	-0.257	0.258

يبين الجدول رقم (١١) المعاملات المعيارية للدوال التمييزية القانونية الثلاث. فنجد بالنسبة للدالة الأولى (الأكثر أهمية) أن "المحددات الثقافية والدينية" لها أعلى معامل معياري (٠,٤٤٩)، تليها "محددات التطور الصناعي والابتكار" (٠,٣٨٨)، ثم "المحددات البيئية" (٠,٣٣٧)، و"المحددات الاقتصادية" (٠,٣١٨). وهذا يشير إلى أن هذه المحددات هي الأكثر مساهمة في التمييز بين المجموعات المختلفة من خلال الدالة الأولى. أما في الدالة الثانية، فنجد أن "المحددات الأخلاقية " و"المحددات الثقافية والدينية" لهما المعاملات الأعلى (٠,٥٢٩ و-٠,٦٧٥ على التوالي)، كما يشير المعامل السلبي للمحددات الثقافية والدينية إلى تأثير معاكس لتأثيرها في الدالة الأولى.

جدول (١٢): مصفوفة البنية (Structure Matrix)

المحددات	الدالة ١	الدالة ٢	الدالة ٣
المحددات الثقافية والدينية	0.673*	-0.407	0.115
المحددات البيئية	0.594*	0.153	0.193
المحددات التعليمية والتدريبية	0.586*	0.246	-0.261
المحددات الأخلاقية	0.571*	0.372	-0.098
محددات التطور الصناعي والابتكار	0.470*	-0.090	0.302
المحددات الاقتصادية	0.460*	0.341	0.170
المحددات القانونية والتشريعية	0.312*	0.308	0.580

*** الارتباط الأكبر بين المتغير والدالة التمييزية.**

يوضح الجدول (١٢) مصفوفة البنية التي تعرض الارتباطات بين المتغيرات والدوال التمييزية. نلاحظ أن جميع المحددات ترتبط بشكل أقوى مع الدالة الأولى، كما هو مشار إليه بالعلامة (*). بالنسبة للدالة الأولى، نجد أن أقوى الارتباطات كانت مع "المحددات الثقافية والدينية" (٠,٦٧٣)، تليها "المحددات البيئية" (٠,٥٩٤)، ثم "المحددات التعليمية والتدريبية" (٠,٥٨٦)، و"المحددات الأخلاقية " (٠,٥٧١). وهذه النتائج الموضحة في جدول (١٢) تؤكد ما تم استنتاجه من الجدول (١١) حول أهمية هذه المحددات في التمييز بين المجموعات، وتقدم صورة أوضح عن ترتيب أهمية المحددات في النموذج التمييزي.

جدول (١٣): مراكز ثقل المجموعات (Functions at Group Centroids)

مستوى التأثير المحتمل	الدالة ١	الدالة ٢	الدالة ٣
ضعيف	-5.489	0.089	0.121
متوسط	-1.460	-0.492	-0.324
عالي	2.435	0.557	-0.144
عالي جداً	4.330	-0.126	0.342

يعرض الجدول رقم (١٣) مراكز ثقل المجموعات على الدوال التمييزية الثلاث حيث نلاحظ تباعداً واضحاً بين المجموعات الأربع على امتداد الدالة الأولى، حيث تتراوح القيم من -٥,٤٨٩ للمجموعة ذات التأثير المحتمل الضعيف إلى ٤,٣٣٠ للمجموعة ذات التأثير المحتمل العالي جداً، ولذا فإن هذا التباعد الواضح يؤكد قدرة الدالة الأولى العالية على التمييز بين المجموعات المختلفة، وبالإضافة إلى ذلك نلاحظ أن هناك تدرجاً منتظماً في قيم مراكز ثقل المجموعات على امتداد الدالة الأولى يتناسب مع مستوى التأثير المحتمل، مما يدعم صلاحية النموذج التمييزي في تصنيف مستويات الوعي باحتمالية التعرض للمخاطر السيبرانية أو للجرائم الإلكترونية.

جدول (١٤): نتائج التصنيف (Classification Results)

مستوى التأثير المحتمل الفعلي	تصنيف ضعيف	تصنيف متوسط	تصنيف عالي	تصنيف عالي جدًا	المجموع	الملاحظات
ضعيف	92.3% (36)	7.7% (3)	0.0% (0)	0.0% (0)	100% (39)	تصنيف دقيق جدًا مع نسبة خطأ منخفضة
متوسط	0.0% (0)	100.0% (40)	0.0% (0)	0.0% (0)	100% (40)	تصنيف مثالي بلا أخطاء.
عالي	0.0% (0)	12.8% (5)	61.5% (24)	25.6% (10)	100% (39)	تقليل أو تضخيم مستوى التأثير
عالي جدًا	0.0% (0)	0.0% (0)	0.0% (0)	100.0% (41)	100% (41)	تصنيف دقيق جدًا بلا أخطاء.

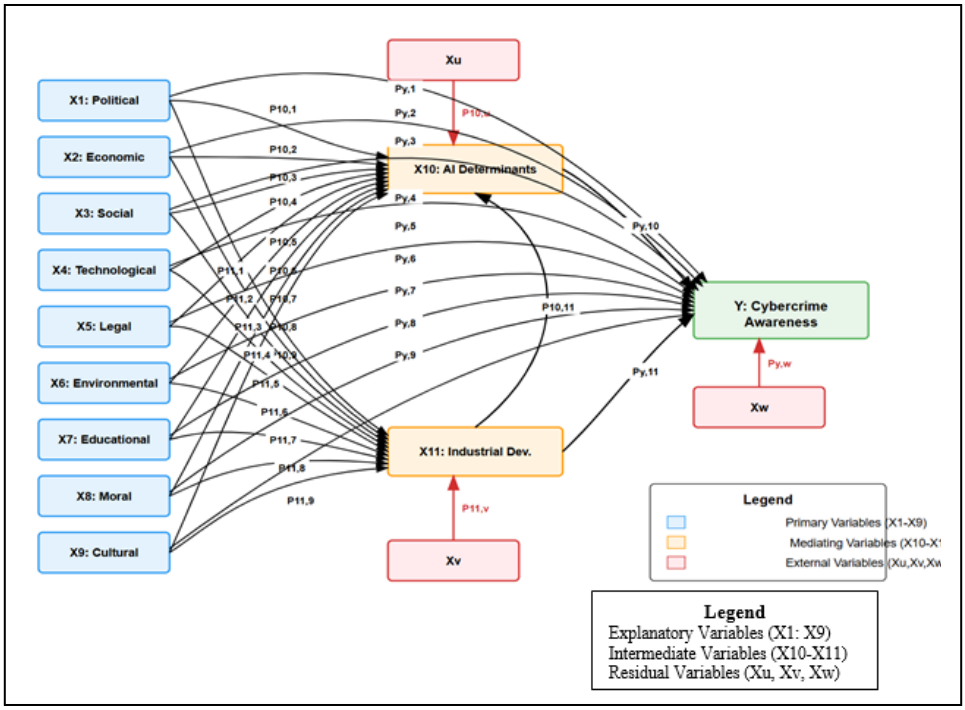
نسبة التصنيف الصحيح الإجمالية: ٨٨,٧%

استعرض الجدول رقم (١٤) نتائج التصنيف باستخدام النموذج التمييزي، ويظهر قدرة تنبؤية عالية للنموذج، حيث بلغت نسبة التصنيف الصحيح الإجمالية ٨٨,٧٪، وقد تباينت دقة التصنيف بين المجموعات المختلفة، حيث حققت مجموعتا التأثير المحتمل المتوسط والعالي جداً دقة تصنيف مثالية (١٠٠٪)، وقد حققت مجموعة التأثير المحتمل الضعيف دقة تصنيف عالية (٩٢,٣٪) مع نسبة خطأ صغيرة (7.7%). وفي المقابل، كانت مجموعة التأثير المحتمل العالي الأقل في دقة التصنيف (٦١,٥٪)، حيث تم تصنيف ١٢,٨٪ منها خطأً ضمن التأثير المتوسط و٢٥,٦٪ ضمن التأثير العالي جداً. وهذا التداخل يشير إلى وجود تشابه في بعض خصائص هذه المجموعة مع المجموعات المجاورة لها، وقد يستدعي إجراء تحليل إضافي لفهم طبيعة هذا التداخل وأسبابه لإعادة تقييم معايير التصنيف لتحسين دقة الفئة "عالي"، مع الحاجة إلى استخدام تقنيات تحليل إضافية لضمان عدم التقليل أو التضخيم

في تقدير مستوى التأثير، وباختصار نجد أن فعالية النموذج التصنيف لنموذج التنبؤ بمستوى الوعي يمتلك دقة عالية (٨٨,٧٪)، مما يجعله أداة فعالة لدى الجهات المعنية في مدينة خورفكان من أجل استهداف تقييم مستوى الوعي لدى الأفراد وتحديد الفئات الأكثر عرضة للمخاطر السيبرانية، وقد تمثلت المجموعات الأكثر تحدياً لمواجهة تلك التهديدات الرقمية في الأفراد ذوو مستوى التأثير المحتمل العالي يمثلون تحدياً في التصنيف، مما يشير إلى ضرورة التركيز على هذه الفئة في برامج التوعية.

تم استخدام طريقة تحليل المسار لقياس التأثيرات كمنهج احصائي لاختبار نموذج سببي فرضي بهدف الوصول إلى تقديرات كمية للتأثيرات السببية "إن وجدت"، وذلك لتحديد الأثر غير المباشر إلى جانب الأثر المباشر ومن ثم تحديد الأثر الكلي للمتغيرات ذات التأثير المعنوي دون الحاجة إلى تثبيت أو عزل المتغيرات الأخرى، وهو ما نسميه العلاقة السبب-النتيجة (Cause-Effect).

أولا: تم بناء النمذجة للنموذج النظري بناء على تصميم الباحث وفي ضوء الاستناد إلى ما أسفر عنه تحليل أهم النتائج التي توصلت إليها الدراسة السابقة والأخذ بعين الاعتبار مكونات أسلوب PESTLE التي تمثل مكونات تحليل البيئة الخارجية (سياسية P، واقتصادية E، واجتماعية S، وتكنولوجية T، وقانونية L، وبيئية E) المحتمل تأثيرها في المستقبل على الظاهرة محل الدراسة الحالية من خلال تحديد العلاقات والتفاعلات بين المتغيرات وفقا لمكونات الإطار النظري باعتبار أن (X1 to X9) متغيرات تفسيرية تؤثر على درجة الوعي لاحتمالية التعرض للتهديدات السيبرانية (Y)، وذلك من خلال متغيرات وسيطة، وهي على الترتيب (X10) التي تمثل محددات الذكاء الاصطناعي، و(X11) التي تمثل محددات التطور الصناعي والابتكار، كما هو موضح بالشكل التالي:



الشكل رقم (٢) نمذجة الإطار النظري للدراسة في نموذج تنبؤي باستخدام تحليل المسار

ثانيا: تم بناء معادلات النظام بفرض أنها خطية من نمذجة النموذج السابق التنبؤي المعتمد على الإطار النظري:

$$\mathbf{X_{10}} = p_{101} X_1 + p_{102} X_2 + p_{103} X_3 + p_{104} X_4 + p_{105} X_5 + p_{106} X_6 + p_{107} X_7 + p_{108} X_8 + p_{109} X_9 + p_{10u} X_u \ldots..(1)$$

$$\mathbf{X_{11}} = p_{111} X_1 + p_{112} X_2 + p_{113} X_3 + p_{114} X_4 + p_{115} X_5 + p_{116} X_6 + p_{117} X_7 + p_{118} X_8 + p_{119} X_9 + p_{11v} X_v \ldots.(2)$$

$$\mathbf{Y} = p_{y1} X_1 + p_{y2} X_2 + p_{y3} X_3 + p_{y4} X_4 + p_{y5} X_5 + p_{y6} X_6 + p_{y7} X_7 + p_{y8} X_8 + p_{y9} X_9 + p_{y10} X_{10} + p_{y11} X_{11} + p_{yw} X_w..(3)$$

ثالثاً: تطبيق طريقة الانحدار المتعدد Multi-Regression، باستخدام طريقة Stepwise لاختبار العلاقات المفروضة وفق كل معادلة من معادلات النظام المقترحة الخطية لاستبعاد المتغيرات غير المعنوية (ليس لها دلالة إحصائية) من معادلات النظام، ويتم من خلال مستوى المعنوية (α) تحديد معنوية العلاقات لكل متغير في النموذج حسب كل معادلة من معادلات النظام الثلاثة السابقة فيما يخص قيم معاملات Beta المناظرة لقيم معاملات الانحدار الأصلية (β_i)، وذلك لفحص سؤال الدراسة الذي يهدف إلى تحديد ما هي اهم المسارات السببية المؤثرة ذات التأثير المباشر او غير المباشر عبر دراسة التفاعلات والعلاقات بين مجموعة من المحددات السياسية والاجتماعية والاقتصادية والتكنولوجية والقانونية والبيئية وغيرها من المحددات ذات الصلة ، وبين زيادة رفع مستويات الوعي على مستوى الفرد او المجتمع باحتمالية التعرض للمخاطر والتهديدات السيبرانية باستخدام النمذجة لنموذج نظري يعتمد على المقاربة الإحصائية في إطار تحليلي متعمق، وبتطبيق قوانين الانحدارلاحتساب قيمة معامل التحديد R–Square على مستوى كل معادلة من معادلات النظام المقترحة في الشكل رقم (٢) أعلاه حيث أثبتت جميعها مقدرة أو نسبة ما تساهم به المتغيرات المستقلة التى دخلت كل معادلة انحدار مقترحة في النظام المفترض وفق الإطار النظري للدراسة (المحددات المؤثرة) في تفسير تباين المتغير التابع (مستوى درجة الوعي باحتمالية التعرض للتهديدات او المخاطر السيبرانية في خورفكان) أوالتنبؤ به وهى ذات دلالة إحصائية عند مستوى أقل من ٠,٠٥، وهى تدل على مدى ملاءمة معادلات الانحدار فيما بين المتغيرات التي دخلت النموذج في ضوء الاعتبارات الإحصائية. كما حققت قيم خطأ التقدير لنماذج معادلات الانحدار المتضمنة في النظام حسب الإطار الزمني (Std. Error of the Estimate) للتقديرات مستوى دقة مرتفع في تقديرات النموذج. كما يتضح من نتائج تحليل الانحدار مدى معنوية معادلة الانحدار باستخدام اختبار تحليل التباين ANOVA حيث كانت قيم F ذات دلالة إحصائية عند مستوى أقل من ٠,٠٥، وهذا دليل على معنوية علاقة الانحدار والتأكيد على وجود علاقة ما بين المتغيرات المستقلة (المحددات المؤثرة)، وبين المتغير التابع (مقياس مستوى الوعي باحتمالية التعرض

للتهديدات والمخاطر السيبرانية)، ما يعكس وجود تأثير جوهري لهذه المحددات في تشكيل مستوى الوعي الرقمي المجتمعي بشكل أمثل.

وبناءا على معاملات التحديد R^2 يتم احتساب معاملات البواقي بالتعويض في العلاقة التالية $\boldsymbol{Pij = \sqrt{1 - R^2}}$، وقد جاءت النتائج في ضوء احتساب الثلاث دوال السابقة من خلال نماذج الانحدار، وذلك على النحو التالي:

- احتساب دالة الانحدار الأولي لمعادلة الخطية

جدول (١٥) نتائج تحليل الانحدارالمتعدد لفحص أهم المتغيرات المؤثرة على التنبؤ بقيمة التأثير لمحددات الذكاء الاصطناعي

(X10: متغير محددات الذكاء الاصطناعي)

المتغيرات المؤثرة في النموذج	B	Std. Error	Beta	t-test	Sig.
(Constant)	.947	.828	-	1.143	.255
المحددات التعليمية والتدريبية (X_7)	.816	.054	.802	15.157	.000
المحددات التكنولوجية (X_4)	.142	.058	.130	2.450	.015
Power of the derived model (r = 905 | R^2 = 0.819| Adjusted R^2 = 0.817 | F = 352.930*) Dependent Variable: X10- محددات الذكاء الاصطناعي					

- **المصدر**: مخرجات برنامج SPSS

(*) معنوية عند مستوى دلالة أقل من ٠,٠٥.

- احتساب دالة الانحدار الثانية لمعادلة الخطية

جدول (١٦) نتائج تحليل الانحدارالمتعدد لفحص أهم المتغيرات المؤثرة على التنبؤ بقيمة التأثير لمحددات التطور الصناعي والابتكار

(X11: متغير محددات التطور الصناعي والابتكار)

المتغيرات المؤثرة في النموذج	B	Std. Error	Beta	t-test	Sig.
(Constant)	-.706	.888	-	-.795	.428
المحددات التعليمية والتدريبية (X_7)	.804	.068	.740	11.912	.000
المحددات الاجتماعية (X_3)	.222	.073	.188	3.024	.003
Power of the derived model (r = 903 | R^2 = 0.815| Adjusted R^2 = 0.812 = 343.030*) Dependent Variable: X11- محددات التطور الصناعي والابتكار					

- **المصدر**: مخرجات برنامج SPSS

(*) معنوية عند مستوى دلالة أقل من ٠,٠٥.

- احتساب دالة الانحدار الثالثة لمعادلة الخطية

جدول (١٧) نتائج تحليل الانحدارالمتعدد لفحص أهم المتغيرات المؤثرة على التنبؤ بقيمة التأثير لدرجة المتغير التابع

(Y: درجة الوعي في خورفكان لاحتمالية التعرض للتهديدات السيبرانية)

المتغيرات المؤثرة في النموذج	B	Std. Error	Beta	t-test	Sig.
(Constant)	.021	.682		.030	.976
محددات التطور الصناعي والابتكار (X_{11})	.391	.053	.414	7.388	.000
المحددات البيئية (X_6)	.239	.063	.241	3.792	.000
المحددات الأخلاقية (X_8)	.216	.078	.210	2.782	.006
المحددات الاجتماعية (X_3)	.149	.066	.134	2.267	.025

Power of the derived model (r = 937 | R2 = 0.878| Adjusted R2 = 0.874 = 276.090*) Dependent Variable: Y- درجة الوعي في خورفكان لاحتمالية التعرض للتهديدات السيبرانية

- **المصدر**: مخرجات برنامج SPSS

(*) معنوية عند مستوى دلالة أقل من ٠,٠٥.

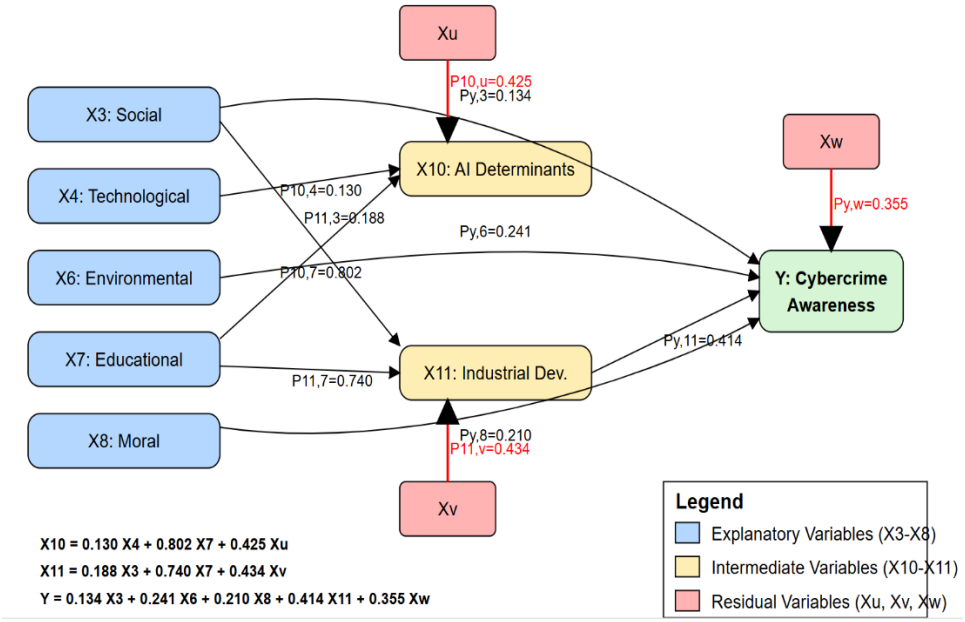
رابعا: تم تحديد معاملات المسارات في نمذجة النموذج التنؤي النظري على النحو التالي:

$\mathbf{X_{10}}$ = ٠,١٣٠ X_4 + 0.802 X_7 +0.425 X_u

$\mathbf{X_{11}}$ = 0.188 X_3 +0.740 X_7 + 0.434 X_v

$\mathbf{Y}$ = 0.134 X_3+ 0.241 X_6 + 0.210 X_8 + 0.414 X_{11} +0.355 X_w

وقد تبين من خلال النتائج الموضحة في جدول (١٧) أنه تم حساب العلامة المعيارية Z-Score للمتغيرات التي دخلت معادلة نموذج الانحدار التنبؤي، وهو ما يسمي بمعامل Beta بحيث يكون المعامل في هذه الحالة مساويا لقيمة معامل الارتباط بين كل متغير مستقل من المتغيرات التي دخلت المعادلة (أي المحددات المؤثرة) مع المتغير التابع (مستوى الوعي باحتمالية التهديدات والمخاطر السيبرانية) وتستخدم للتنبؤ بالقيم المعيارية للمتغير التابع من خلال القيم المعيارية للمتغيرات المستقلة حيث تبرز كل من المحددات (التطور الصناعي والابتكار X_{11}، البيئية X_6، الأخلاقية X_8، ومن ثم الاجتماعية X_3) كأهم العوامل أو المتغيرات المؤثرة في النموذج ومعاملات انحدارها ذات دلالة إحصائية عند مستوى أقل من ٠,٠٥، حيث كانت محددات التطور الصناعي والابتكار لها النصيب الأكبر في تفسير التباين بواقع 0.414، وقد تلتها المحددات البيئية بمقدار٠,٢٤١، وهو ما يعكس الدور المحوري الذي تلعبه العوامل والمحددات البيئية في تشكيل إدراك مستوى الوعي العام على مستوى الأفراد أو المجتمع لاحتمالية التعرض للتهديدات والمخاطر السيبرانية.



الشكل رقم (٣) استخراج معاملات المسارات المتضمنة في النموذج النظري التنبؤي باستخدام تحليل المسار

١) تحليل مسارات المحددات الاجتماعية:

- الأثر المباشر لـ X_3 (المحددات الاجتماعية) على Y (الوعي بالتهديدات السيبرانية) = 0.134
- الأثر غير المباشر لـ X_3 (المحددات الاجتماعية) على Y (الوعي بالتهديدات السيبرانية) من خلال X_{11} (التطور الصناعي والابتكار) = 0.078

٢) تحليل مسارات المحددات التكنولوجية:

- الأثر المباشر لـ X_4 (المحددات التكنولوجية) على Y (الوعي بالتهديدات السيبرانية) = ٠
- الأثر المباشر لـ X_4 (المحددات التكنولوجية) على X_{10} (محددات الذكاء الاصطناعي) = 0.130

٣) تحليل مسارات المحددات البيئية:

- الأثر المباشر لـ X_6 (المحددات البيئية) على Y (الوعي بالتهديدات السيبرانية) = ٠,٢٤١
- الأثر غير المباشر لـ X_6 (المحددات البيئية) على Y (الوعي بالتهديدات السيبرانية) = 0

٤) تحليل مسارات المحددات التعليمية والتدريبية:

- الأثر المباشر لـ X_7 (المحددات التعليمية والتدريبية) على Y (الوعي بالتهديدات السيبرانية) = 0
- الأثر غير المباشر لـ X_7 (المحددات التعليمية والتدريبية) على Y (الوعي بالتهديدات السيبرانية) من خلال X_{11} (التطور الصناعي والابتكار) = ٠,٣٠٦
- الأثر المباشر لـ X_7 (المحددات التعليمية والتدريبية) على X_{10} (محددات الذكاء الاصطناعي) = 0.802

٥) تحليل مسارات المحددات الأخلاقية:

- الأثر المباشر لـ X_8 (المحددات الأخلاقية) على Y (الوعي بالتهديدات السيبرانية) = ٠,٢١٠
- الأثر غير المباشر لـ X_8 (المحددات الأخلاقية) على Y (الوعي بالتهديدات السيبرانية) = ٠

النتائج المستخلصة من تحليل التمايز تؤكد الدور الحاسم لمجموعة من العوامل أو المحددات التي تساهم في تشكيل مستوى الوعي الرقمي المجتمعي بالتهديدات السيبرانية، حيث أظهرت المحددات الصناعية والابتكار ((X11 أعلى تأثير بواقع 0.414، مما يعكس مدى ارتباط التطور التكنولوجي بمستوى الإدراك الرقمي للمخاطر السيبرانية. كما احتلت المحددات البيئية (X6) المرتبة الثانية بواقع 0.241، مما يبرز تأثير البيئة الرقمية المحيطة في تعزيز الوعي السيبراني، سواء عبر التشريعات، أو الممارسات الأمنية، أو الثقافة الرقمية العامة. أما المحددات الأخلاقية (X8) والاجتماعية (X3) فقد سجلت تأثيرات مباشرة ملحوظة (0.210 و٠,١٣٤ على التوالي)، مما يشير إلى أن القيم المجتمعية والسلوكيات الأخلاقية تشكل عاملاً رئيسيًا في تقليل المخاطر السيبرانية. ومن اللافت أن المحددات التكنولوجية (X4) لم يكن لها أثر مباشر على الوعي بالتهديدات، لكنها أثرت في محددات الذكاء الاصطناعي (X10) بواقع ٠,١٣٠، مما يشير إلى دور غير مباشر للتكنولوجيا في تعزيز الأمن السيبراني من خلال الابتكار الذكي. كما يؤكد التحليل أن التعليم والتدريب (X7) لم يكن له أثر مباشر، ولكنه لعب دورًا وسيطًا قويًا عبر تأثيره على التطور الصناعي والابتكار (0.306) والذكاء الاصطناعي (0.802)، مما يبرز أهمية الاستثمار في التدريب السيبراني كوسيلة لرفع مستوى الحماية الرقمية بشكل غير مباشر. تعكس هذه النتائج الحاجة إلى استراتيجية شاملة تعزز الابتكار، وترسخ الثقافة الأخلاقية، وتدعم البيئة الرقمية لرفع مستوى الوعي السيبراني وتحقيق حماية مستدامة للمجتمع الرقمي.

وعموما فإن محصلة النتائج والمخرجات التي توصلت إليها الدراسة الحالية من خلال أهداف واضحة سعت إلى تحقيقها باستخدام الأساليب والتقنيات الإحصائية المناسبة لطبيعة البيانات وكيفية تحقيق كل هدف بشكل مستقل إلى تقديم إطاراً علمياً متيناً لفهم العوامل والمحددات المؤثرة في التاثير على درجة مستوى الوعي بالأمن الرقمي المجتمعي تجاه احتمالية التعرض للجرائم الإلكترونية أو التهديدات السيبرانية، وبالتالي سوف تعتبر خارطة طريق للمزيد من الدراسات المستقبلية لاضافة المزيد من المحددات المتوقعة في التأثير والتي يمكن أن تنطبق على بيئات ومجتمعات سكانية مختلفة لدراسة الظاهرة بشكل عام توفر، وهذا سوف يساهم في الوصول إلى تشكيل أساساً قوياً لاتخاذ القرارات المستنيرة في مجال الأمن السيبراني والتوعية المجتمعية الرقمية بشكل آمن ومستدام.

التوصيات والمقترحات:

- ضرورة تبني صناع القرار والمخططين والجهات السيادية ذات الصلة بتعزيز مقومات الأمن الرقمي المجتمعي من تطوير مجموعة متنوعة من برامج التوعية والتدريب المتخصص والمهني التي يجب أن يستهدف جميع الفئات، مع التركيز على تعزيز الوعي بالمخاطر الإلكترونية والتهديدات السيبرانية بشكل عام، وهذا يستلزم توفير القنوات اللازم للدعم والتوعية من قبل متخصصين لديهم الأدوات والمهارات اللازمة للحماية منها من خلال سيناريوهات استجابة فعالة.
- ضرورة إجراء المزيد من الدراسات والبحوث المتخصصة لفهم الأسباب الجذرية التي تجعل بعض الفئات أكثر عرضة للتهديدات والمخاطر الإلكترونية من غيرها، وكذلك التي تجعل بعض المحددات أكثر أهمية من غيرها، وهذا من شانه يساهم في تطوير استراتيجيات وقائية مخصصة بناءً على هذه الأسباب من خلال التوسع في دراسة الكثير من المتغيرات والمحددات التي يحتمل تأثيرها على زيادة الوعي بالأمن المجتمعي بشكل آمن ومستدام بدراسة جميع عوامل الغموض والتحديات والتهديدات والمخاطر المحتملة لكي تكون مجتمعاتنا السكانية أكثر استعداد للمستقبل من خلال توجهات تعتمد على استراتيجيات اكثر رشاقة ومرونة دعما لفرص التنمية المستدامة في مدن ذكية تتمتع بمقومات رفاهية الحياة الرقمية الآمنة.
- تبني المبادرات والاستراتيجيات والتشريعات التي تعزز التركيز على جميع المحددات المؤثرة عند تطوير برامج التوعية والتدريب، مع إيلاء اهتمام خاص للمحددات التي تظهر أهمية أكبر لدى المجموعة التي تعرضت للتهديدات والمخاطر السيبرانية من واقع الاستفادة من التجارب الفعلية في تطوير سيناريوهات استجابة مناسبة لديها تدابير وإجراءات فعالة في التحكم في تلك المخاطر او الحد منها تعزيز لمقومات التنمية الرقمية المستدامة.
- ضرورة توليد استراتيجيات التوعية والتثقيف عناصر تركز على التجارب الواقعية وأثرها في زيادة الوعي مع ربطها بمخرجات الأهمية النسبية للمحددات المؤثرة في زيادة الوعي بالأمن الرقمي المجتمعي تجاه احتمالية التعرض للتهديدات والمخاطر السيبرانية وطرق الوقاية المبكرة منها بشكل استباقي، مما يساعدهم في اتخاذ قرارات مستنيرة لتعزيز الأمن السيبراني في المجتمع.
- العمل على تركيز برامج التوعية المبكرة على محددات الوعي الرئيسية (المحددات الثقافية والدينية، والبيئية، والتعليمية، والأخلاقية باعتبارها الأكثر أهمية في التمييز بين مستويات الوعي العام سواء على مستوى الفرد او المجتمع باحتمالية التعرض للمخاطر والتهديدات السيبرانية أو الرقمية.
- يستوجب أهمية مراعاة خصوصية محددات البيئة المحلية في مدينة خورفكان في التمييز بين الفئات الأشد احتياجا في برامج التوعية المبكرة بشكل وقائي أو استباقي عند صياغة وتنفيذ وإدارة استراتيجيات الأمن السيبراني داخل المجتمعات السكانية، والتي يمكن ان تتبناها إمارة الشارقة او دولة الإمارات عموما أو المناطق المشابهة في المجتمعات المحلية المماثلة لمجتمع مدينة خورفكان.
- تطوير برامج توعية مستهدفة استناداً إلى المحددات الأكثر تأثيراً في التمييز بحيث يمكن تصميم برامج توعية مستهدفة تركز على الجوانب الثقافية والتعليمية والبيئية مع أمكانية استخدام النموذج التمييزي كأداة تشخيصية لتقييم مستوى الوعي العام لدى مجموعات مختلفة من السكان وتوجيه موارد التوعية

بشكل أكثر فعالية.

- تعزيز البعد الاجتماعي والثقافي في استراتيجيات الأمن السيبراني من حيث الاهتمام بالمحددات الاجتماعية والثقافية والدينية التي أثبتت أهميتها القصوى في التمييز بين مستويات الوعي العام مع إجراء دراسات تتبعية لمتابعة تطور مستويات الوعي بعد تنفيذ برامج التوعية، لتقييم فعاليتها وتعديلها حسب الحاجة في ضوء آليات التحسين المستمر التي تتبناها الجهات المعنية مجتمعيا وأمنيا وتكنولوجيا في مدينة خورفكان.

- المراجـع والمصادر:

- Longtchi, T., Rodriguez, R. M., Al-Shawaf, L., Atyabi, A., & Xu, S. (2022). Internet-based social engineering attacks, defenses, and psychology: A survey. arXiv preprint arXiv:2203.08302. *https://arxiv.org/abs/2203.08302*
- de Bruin, M., & Mersinas, K. (2024). Individual and Contextual Variables of Cyber Security Behaviour - An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour, arXiv preprint arXiv:2405.16215,https://arxiv.org/abs/2405.16215
- Díaz, A., Sherman, A. T., & Joshi, A. (2018). Phishing in an Academic Community: A Study of User Susceptibility and Behavior. arXiv preprint arXiv:1811.06078, https://arxiv.org/abs/1811.06078
- Dam, L. & Deshpande, K. (2020). Relationship Between Demographic Variables and Awareness on Cybersecurity Threats: An Empirical Analysis. Orissa Journal of Commerce, Volume XXXXI, April- June-2020, Issue No-II 113.
- Lee, C. S., & Chua, Y. T. (2024). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, *70*(9), 2250-2277. https://doi.org/10.1177/00111287231180093
- McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce*, *9*(1), 23–41, https://doi.org/10.1080/ 15332861.2010. 487415.
- Al-Shanfari, I., Yassin, W., Tabook, N., Ismail, R., & Ismail, A. (2022). Determinants of information security awareness and behaviour strategies in public sector organizations among employees. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *13*(8), 479.
- Saleh, T. (2024). *Factors affecting cybersecurity awareness: A qualitative study in Saudi Arabia* (Doctoral dissertation, Westcliff University).
- Bernik, I., Prislan, K., & Mihelič, A. (2022). Country life in the digital era: Comparison of technology use and cybercrime victimization between residents of rural and urban environments in Slovenia. *Sustainability*,

14(21), 14487. https://doi.org/10.3390/ su142114487.

- Abbasi, A. H. (n.d.). Path *analysis: Applications in social sciences using computers*. Graduate School of Statistical Sciences.
- Chizanga, M. K., Agola, J., & Rodrigues, A. (2022). Factors affecting cyber security awareness in combating cyber crime in Kenyan public universities. *International Research Journal of Innovations in Engineering and Technology (IRJIET), 6*(1), 54–57. https://doi.org/10.47001/IRJIET/2022.601011
- Forbes Advisor. (2024). *Cybersecurity stats: Facts and figures you should know*. Retrieved from https://www.forbes.com/sites/chuckbrooks/2024/06/05/alarming-cybersecurity-stats-what-you-need-to-know-in-2024/
- *Fortinet. (2024). Global* research report 2024: Security awareness and training. Retrieved from https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2024-security-awareness-and-training.pdf
- Moody's. (2024). Cyber awareness grows, but basic risk mitigation practices still trail other sectors. Retrieved from https://www.moodys.com/research/Moodys-Cyber-awareness-grows-but-basic-risk-mitigation-practices-still--PBC_1329045
- European Union Agency for Cybersecurity (ENISA). (2021). Raising awareness of cybersecurity: A key element of national cybersecurity strategies. https://doi.org/10.2824/363629.
- Sultan, A. (٢٠٢٤). *Improving cybersecurity awareness in underserved populations*. Center for Long-Term Cybersecurity (CLTC) White Paper Series. Retrieved from https://cltc.berkeley.edu.
- Cobos, E. V. (2024). Cybersecurity economics for emerging markets. International Bank for Reconstruction & Development / The World Bank. https://doi.org/10.1596/978-1-4648-2120-2.

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences, 12*(5), 2589. https://doi.org/10.3390/app12052589 .