العلاقة بين معرفة مستخدمى الإنترنت بسياسات وإجراءات أمن المعلومات وسلوكيات حماية أمنهم السيبرانى

د. هدير محمود عبد الله أحمد*

ملخص

هدفت الدراسة إلى التعرف على مدى وجود علاقة ارتباطية بين معرفة مستخدمي الإنترنت بسياسات وإجراءات أمن المعلومات وسلوك حماية أمنهم السيبراني. وتم تطبيق الدراسة على عينة قوامها ٤٠٠ مبحوثا من مستخدمي الإنترنت ممن تبلغ أعمارهم ١٨ سنة فأكثر. وتوصلت النتائج إلى أنه كلما زادت معرفة الأفراد بسياسات وإجراءات أمن المعلومات زاد التزامهم بسلوكيات الحماية لأمنهم السيبراني. كما حددت النتائج بعض المتغيرات التي تؤثر على العلاقة بين المعرفة والسلوك السيبراني للأفراد.

كلمات مفتاحية: الأمن السيبراني، أمن المعلومات، سلوكيات الحماية، ممارسات الأمن السيبراني، مستخدمي الإنترنت

The relationship between Internet users' knowledge of information security policies and procedures and their cybersecurity protective behaviours

Hadeer Mahmoud Abdullah

Abstract

This study focuses on the relationship between information security knowledge and cybersecurity protective behaviour among internet users. Results show that there is a correlation between higher levels of information security knowledge and cybersecurity safe practices. In addition knowledge is also connected to positive attitude towards cybersecurity protection. Lastly, findings defined some factors that affect the correlation between knowledge and behaviour.

* **مدرس الإذاعة والتليفزيون بكلية الإعلام- جامعة القاهرة**

Key Words: information security, cybersecurity, cybersecurity behaviours, cybersecurity practices, Internet users.

مقدمة

الأمن هو الركن الركين لأى نشاط يقوم به البشر، والأمن السيبراني مصطلح حديث نسبيا فهو سلاح استراتيجي في يد الحكومات والأفراد حيث يمس الثروة الرقمية والهوية الثقافية للمجتمعات فالغرض منه هو حماية موارد وأصول المنظمات والهيئات من النواحي التنظيمية المالية البشرية، التقنية والمعلوماتية، بحيث تقوم بأداء مهما الموكولة بها بأمان تام، كما يضمن حماية المعلومات والبيانات الشخصية للأفراد.[١]

والأمن السيبراني هو أمن المعلومات على أجهزة وشبكات الحاسب الآلي الذي يستخدم مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصال والمعلومات التي تحتويها.[٢]

ويعد أمن المعلومات ضرورة ملحة، فهو العلم الذى يعنى بحماية المعلومات من المخاطر، فلقد أفسح هذا الفضاء السيبرانى الواسع والمتعدد والمتشعب المجالات عن محاور جديدة للصراع المعلوماتي، كما بات يشكل منظومة اجتماعية تقنية واقتصادية ذات تأثير على الأمن بأبعاده.[٣]

ولا شك أن الإنترنت وتكنولوجيا المعلومات قد أثرت بشكل كبير في حياة الإنسان. ومع ذلك، لا يزال أمن المعلومات مصدر قلق مهم لكل من المستخدمين والمؤسسات. فلا يمكن للتكنولوجيا وحدها أن تضمن بيئة آمنة للمعلومات؛ حيث يجب مراعاة الجوانب الإنسانية لأمن المعلومات، إلى جانب الجوانب التكنولوجية. فقلة الوعي بأمن المعلومات والجهل والإهمال واللامبالاة والأذى والمقاومة هي أصل أخطاء المستخدمين.[٤]

وبناء على ما سبق فإن الأمن السيبراني هو ظاهرة عالمية تمثل تحديًا اجتماعيًا وتقنيًا معقدًا للحكومات، ولكنها تتطلب إشراك الأفراد.[٥] فمن المعروف أن الحلقة الأضعف في سلسلة الأمان السيبرانية هي مستخدم الكمبيوتر. فهجمات الهندسة الاجتماعية تُستخدم عادةً لخداع مستخدمي الكمبيوتر للقيام بأشياء يمكن أن تؤدي إلى تسريب معلومات خاصة. ومثل هذه الهجمات تتلاعب نفسيا بمستخدمي الكمبيوتر للكشف عن معلوماتهم السرية.[٦]

ففى ظل انتشار الأجهزة الذكية التى تتمتع بتقنيات عالية تمكنها من حماية بيانات مستخدميها أصبح اعتماد الجرائم الإلكترونية فى الوقت الحالى على ما يطلق عليه الهندسة الاجتماعية لخداع المستخدمين والوصول لهم عبر منتديات النقاش ورسائل البريد الإلكتروني وخداعهم بإرسال الروابط التى يتسبب فتحها اختراق الأجهزة وسرقة أو تدمير البيانات الشخصية.

وقد أظهرت التقارير أن غالبية حوادث الأمن السيبراني تحدث بسبب فشل المستخدمين في

التصرف بشكل آمن؛ لذا فعلى الرغم من أن الأمن السيبراني هو أحد أهم التحديات التي تواجهها الحكومات اليوم؛ لا تزال الرؤية والوعي العام محدودة. فلقد سمع الجميع تقريبًا عن الأمن السيبراني، ومع ذلك، فإن أولويات وسلوكيات الأشخاص لا يعكسان مستوى عالٍ من الوعي.[٧]

وفى ضوء ما سبق تتحدد **مشكلة الدراسة** فى التعرف على مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات، ومدى تأثير هذه المعرفة على التزامهم بسلوكيات حماية أمنهم السيبرانى، وكذلك اختبار تأثير بعض المتغيرات على العلاقة بين المعرفة والسلوك.

أولا: أهداف الدراسة

١. قياس مستوى معرفة مستخدمى الإنترنت بسياسات وإجراءات أمن المعلومات ومدى تأثير هذه المعرفة على اتجاهاتهم وسلوكيات حمايتهم لأمنهم السيبرانى.
٢. الوقوف على مدى تأثير الاتجاه، درجة ميل الأشخاص للمخاطرة، وسمات الشخصية الخمس الكبرى (الانبساط، القبول أو المسايرة، الضمير، العصابية، الانفتاح) على العلاقة بين مستوى معرفة مستخدمى الإنترنت بسياسات وإجراءات أمن المعلومات وسلوكيات حمايتهم لأمنهم السيبرانى.
٣. التعرف على مدى تأثير العوامل الديموغرافية (النوع، السن، المستوى التعليمى) على مستوى معرفة مستخدمى الإنترنت بسياسات وإجراءات أمن المعلومات وكذلك على سلوكيات حمايتهم لأمنهم السيبرانى.

ثانيا: أهمية الدراسة

أ- من الناحية البحثية

- يعد موضوع الأمن السيبراني واحدا من الموضوعات التي تلقي اهتماما واسعا فى العصر الحالي، نظرا لما أصبحت تتمع به الوسائل التقنية والرقمية من شعبية واسعة لدي جميع الناس على اختلاف متغيراتهم الديموغرافية، بالإضافة إلى دعم الحكومات فى مختلف الدول للتحول الرقمي والتوجه إلى رقمنة معظم الوثائق والخدمات الحكومية؛ فأصبحت هذه الوسائل جزءا لا يتجزأ من حياتنا اليومية بما تحمله من مزايا وعيوب.
- قلة الأبحاث العربية فى مجال الأمن السيبراني نظرا للحداثة النسبية لمفهوم وموضوع الأمن السيبراني وخاصة تلك الأبحاث التى تناولت السلوكيات التى يقوم بها المستخدمين لحماية أمنهم السيبراني.
- ندرة الاستعانة بالإطار النظرى المستخدم فى الدراسة فى الدراسات العربية (نموذج

المعرفة- الاتجاه- السلوك)، وكذلك مقياس (HAIS-Q) رغم اعتماد الدراسات الأجنبية عليه كمقياسا موثوقا للوعى بأمن المعلومات.

- إدراج متغيرات بحثية جديدة على مجال دراسات الأمن السيبرانى العربية كمتغير سمات الشخصية الخمس الكبرى، و متغير الميل للمخاطرة.

ب- من الناحية المجتمعية

توفير معلومات مبنية على دراسة علمية حول مستوى معرفة مستخدمى الإنترنت بسياسات وإجراءات الأمن السيبرانى واتجاهاتهم نحوها للوقوف على جوانب القصور فى هذه المعرفة، وكذلك تحديد مدى ارتباط هذه المعرفة بسلوكيات حماية المستخدمين لأمنهم السيبرانى لتوظيف هذه المعلومات فى تصميم حملات توعية لمستخدمى الإنترنت لزيادة مستوى وعيهم السيبرانى، وتبصيرهم بخطورة بعض الممارسات التى قد تهدد أمنهم السيبرانى وتجعلهم عرضة للجرائم والانتهاكات الإلكترونية.

ثالثا: دراسات سابقة

مع تزايد الاهتمام بالأمن السيبرانى وخطورته تزايد الاهتمام البحثي بدراسة سلوكيات الأمن السيبرانى لمستخدمىالإنترنت والعوامل المؤثرة فيها، وفيما يلى عرض لبعض الدراسات من التراث العلمى التى وجدت الباحثة ارتباطا مباشرا بينها وبين موضوع ومتغيرات الدراسة:

المعرفة والسلوك

قامت بعض الدراسة بقياس مستوى المعرفة الجمهور بالأمن السيبرانى كدراسة Kleij et al (2021)[٨] حول سلوك الأمن السيبراني للمواطنين الهولنديين، والتى أشارت نتائجها إلى أن الأشخاص الذين لديهم معرفة ذات صلة ولديهم الدافع لحماية أنفسهم، يبلغون عن سلوك أكثر أمانًا عبر الإنترنت. وأن الفرصة المتاحة للأفراد لحماية أنفسهم مرتبطة جزئيًا فقط بسلوك الأمن السيبراني المبلغ عنه ذاتيًا.

وبالمثل هدفت دراسة Alharbi& Tassaddiq (٢٠٢١)[٩] إلى تقييم المعرفة بالأمن السيبراني بين طلاب الجامعات في المملكة العربية السعودية، وتوصلت الدراسة إلى أن معظم المشاركين في الاستطلاع لم يكونوا على دراية بأساسيات مفهوم الأمن السيبراني ولم يعرفوا كيف يديرون بياناتهم رغم أن ٩٢٪ منهم كانوا قد حضروا برنامج رسمي للتوعية الأمنية.

وركزت دراسة Zwilling et al (2020)[١٠] على العلاقات بين الوعي الأمني السيبراني والمعرفة والسلوك فى أربع دول: إسرائيل وسلوفينيا وبولندا وتركيا. وأظهرت

النتائج أن مستخدمي الإنترنت يمتلكون وعيًا كافيًا بالتهديدات السيبرانية لكنهم يطبقون فقط الحد الأدنى من التدابير الوقائية الشائعة نسبيًا وبسيطة، وارتباط المعرفة السيبرانية الأعلى بمستوى الوعي السيبراني على اختلاف البلد أو نوع المبحوثين. بالإضافة إلى ارتباط الوعي بأدوات الحماية، ولكن ليس بالمعلومات التي كانوا على استعداد للإفصاح عنها. كما تشير النتائج إلى التفاعل بين الوعي والمعرفة والسلوكيات يختلف باختلاف البلدان.

وبالتطبيق على بعض الموظفين وجدت دراسة Li et al (٢٠١٩) [١١] أنه عندما يكون الموظفون على دراية بسياسة أمن معلومات لشركتهم وإجراءاتها، فهم أكثر كفاءة لإدارة مهام الأمن السيبراني من أولئك الذين ليسوا على دراية بها. كما تشير الدراسة إلى أن المعلومات التنظيمية تؤثر على البيئة الأمنية بشكل إيجابي على تقييم التهديدات للموظفين وقدراتهم على التكيف، والتي تسهم بدورها بشكل إيجابي في سلوك الامتثال للأمن السيبراني.

بينما هدفت دراسة الصحفي وعسكول (٢٠١٩)[١٢] للكشف عن مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي بالمملكة السعودية، وتوصلت إلى وجود ضعف وقصور لدى معلمات الحاسب الآلي في مستوي الوعي بالأمن السيبراني، ولم تجد فروق ذات دلالة إحصائية في درجة وعي معلمات الحاسب الآلي بالأمن السيبراني تعزي لمتغيري سنوات الخبرة المستوي التعليمي.

وقامت دراسة نوره القحطانى (٢٠١٩)[١٣] بمحاولة قياس الوعى بالأمن السيبرانى لدى الجمهور من خلال التعرف على مفهوم الأمن السيبرانى بالتطبيق على طلاب وطالبات الجامعات السعودية التى توصلت إلى أن أقرب مفهوم للأمن السيبرانى من وجهة نظر عينة الدراسة هو "استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التى تحتويها".

وقام المعلم Moallem (٢٠١٨) [١٤] بدراسة مواقف الطلاب تجاه الأمن السيبراني في وادي السيليكون في ولاية كاليفورنيا بالولايات المتحدة الأمريكية، وركزت الدراسة على تقييم مستوى الأمن السيبراني بين الطلاب في البيئة التكنولوجية الأكثر تقدمًا في العالم. وتوصلت النتائج إلى أن الطلاب لم يكونوا على دراية بسلامة معلوماتهم، على الرغم من أنهم كانوا على علم بأن أنشطتهم تمت مراقبتها، ولم يتم نقل بياناتهم بشكل آمن عبر شبكات الجامعة.

كما تشير نتائج دراسة Raytheon (2017) [١٥] على ٣,٣٥٩ مبحوثا تتراوح أعمارهم بين ١٨:٢٦ عاما من تسع دول مختلفة قيام المبحوثين ببعض سلوكيات الأمن السيبراني المحفوفة بالمخاطر؛ حيث أن ٦٦٪ قاموا بالاتصال بشبكة Wi-Fi عامة، وشارك ٤٢٪ كلمة

مرور مع فرد من خارج العائلة في عام ٢٠١٦. كما لم يغير٢٠٪ منهم كلمة المرور الخاصة بالخدمات المصرفية عبر الإنترنت أبدًا، وكذلك يستخدم الكثير منهم نفس كلمة المرور لتسجيل الدخول إلى حسابات أو مواقع ويب مختلفة.

كما أجرى Senthilkumar and Easwaramoorthy (2017)[١٦] دراستهما على طلاب إحدى الجامعات بالهند لقياس درجة وعيهم بالأمن السيبرانى، وتوصلت النتائج إلى أن الطلاب لديهم مستوى أعلى من المتوسط من الوعي بقضايا التهديد السيبراني الذى يمكن أن يساعدهم فى حماية أنفسهم من الهجمات الإلكترونية حيث ظهر أن ٧٠٪ من المستجيبين لديهم معرفة أساسية بتهديدات الأمن السيبراني، وتذهب الدراسة إلى أن الوعي السيبراني الكامل سيجعل الطلاب يحمون أنفسهم من المتسللين ومن ثم يجب خلق مستوي أعلى من الوعي.

وأشارت نتائج دراسة Parsons et al. (2014) [١٧] أن المعرفة بسياسات وإجراءات أمن المعلومات تُحدث تباينا فى اتجاهات المستخدمين بنسبة ٦٦٪، بينما المعرفة والاتجاه سويًا يحدثان تباينا فى السلوك المبلغ عنه ذاتيًا بنسبة ٧٨٪، حتى عند التحكم في الموقف ظلت المعرفة والاتجاه من أهم المنبئات بالسلوك.

وقارنت دراسة Hoggard (٢٠١٤) [١٨] بين الوعى السيبراني للمواطنين الأمريكيين والكنديين، وأظهرت النتائج تقارب في مستويات الوعى بالأمن السيبراني بين المواطنين الأمريكيين والكنديين، وإدراكهم لوجود تهديدات عبر الإنترنت يجب تخفيفها بأفضل ممارسات الأمن السيبراني ومع ذلك أظهرت الاستطلاعات أن غالبية الكنديين والأمريكيين لم يتبعوا أفضل الممارسات حتى مع علمهم بأنهم يجب أن يفعلوا ذلك.

وهدفت دراسة Slusky and Partow-Navid (2012) [19] إلى تقييم الوعي الأمني لدى مجموعة من الطلاب في كلية الأعمال والاقتصاد في جامعة ولاية كاليفورنيا، لوس أنجلوس، الولايات المتحدة الأمريكية إلى أن المشكلة الرئيسية في الوعي الأمني لا ترجع إلى نقص المعرفة الأمنية، ولكن في الطريقة التي يطبق بها الأشخاص تلك المعرفة في مواقف العالم الحقيقي.

السمات الشخصية

ولاشك أنه عند الحديث عن الوعى السيبرانى من المهم النظر في التأثير المحتمل للفروق للفردية بين مستخدمى الإنترنت؛ حيث يعد فهم التباين بين الأفراد أمرًا ضروريًا لفهم الآليات النفسية الأساسية التي قد تؤثر على وعي المستخدم فيما يتعلق بالأمن السيبرانى.

وفى هذا السياق هدفت بعض الدراسات إلى اختبار العلاقة بين السمات الشخصية لمستخدمى الإنترنت وسلوكيات الأمن السيبرانى كدراسة Kennison et al. (2021) [20] على

مجموعة من الطلاب الجامعيين والعاملين التي توصلت إلى وجود فروق فردية بين المبحوثين من حيث قوة كلمة المرور وفقا لمتغيرات السمات الشخصية (كالضمير والاستقرار العاطفي)، والحاجة إلى الإدراك، ومعرفة كلمة المرور الآمنة المبلغ عنها ذاتيًا والاتجاه والسلوك والمخاطرة العامة). كما كان لدى العاملين مستويات أعلى من المعرفة بالأمن السيبراني وأنشأوا كلمات مرور أقوى من طلاب الجامعات. بينما لم تؤدِ رسائل التنبيه إلى كلمات مرور أقوى.

كما أشارت نتائج دراسة [21] M. Kennison & Chan-Tin (2020) علي مجموعة من الطلاب الجامعيين إلى تأثير المعرفة بالأمن السيبراني المبلغ عنها ذاتيًا وكذلك الخصائص الشخصية (السمات الشخصية وسلوك المخاطرة العام غير المرتبط باستخدام التكنولوجيا كالانبساط، والضمير، والوفاق، والانفتاح، وعدم استقرار الحالة المزاجية) علي الاختلافات الفردية في سلوكيات الأمن السيبراني المحفوفة بالمخاطر (كاستخدام شبكة Wi-Fi غير آمنة، وعدم تسجيل الخروج من الحسابات على أجهزة الكمبيوتر المشتركة، وما إلى ذلك).

كذلك تشير نتائج دراسة Alohali et al. (2018) [٢٢] إلى أن سمات الشخصية تلعب دورًا مهمًا في التأثير على مستويات مخاطر السلوك الأمني للمستخدمين. علاوة على ذلك ، تشير النتائج إلى أن نتيجة السمات الشخصية الخمس الكبري لها تأثير كبير حيث ترتبط شخصية المستخدمين عبر الإنترنت بشخصيتهم غير المتصلة بالإنترنت، لا سيما في سمة شخصية الضمير. بالإضافة إلى ذلك، كان هذا التأثير أقوى عندما ارتبطت الشخصية بعوامل إتقان تكنولوجيا المعلومات والجنس والعمر والنشاط عبر الإنترنت..

وفى هذا السياق وجد McCormac et al (2017) [23] فى دراستهم على موظفين إستراليين أن متغيرات الضمير، والموافقة، والاستقرار العاطفي، والميل للمخاطرة تحدث تباينا كبيرا الوعى بأمن المعلومات، في حين أن العمر والجنس لم يفعلوا ذلك.

العوامل الديموغرافية

وقامت بعض الدراسات بقياس تأثير المتغيرات الديموغرافية على سلوكيات ووعى المبحوثين بالأمن السيبرانى كدراسة سماح حمدان (٢٠٢١)[٢٤] التى تشير نتائجها إلى وجود فروق ذات دلالة إحصائية فى مستوى الوعي بالهجمات الإلكترونية والإجراءات الاحترازية التى تتخذها الأسرة للحماية منها وفقا لمتغيري المستوى التعليمي ودخل الأسرة، بينما ثبت عدم وجود فروق ترجع لمتغيرات (النوع، العمر، العمل).

كما وجدت دراسة السواط وآخرين (٢٠٢٠)[٢٥] فروقا في معرفة التلاميذ بالأمن السيبراني والقيم تعزي لمتغير المرحلة الدراسية لصالح أفراد المرحلة الابتدائية، وكذلك في متغير دخل

الأسرة لصالح الدخل العالي، في حين لم توجد فروق ذات دلالة إحصائية تعزي لمتغير الجنس ونوع المدرسة.

كما توصلت دراسة (٢٠١٩) Fatokun et al[26] التى أجريت على طلاب الجامعات بماليزيا إلى أن سلوكيات الأمن السيبراني للطلاب تختلف بناءً على العمر لعوامل مثل: الشدة المتصورة، سلوك الأقران، الإلمام بالتهديدات السيبرانية، وفعالية الاستجابة والضعف المتصور. وكانت الاختلافات على أساس النوع الاجتماعي موجودة في الكفاءة الأمنية الذاتية، ومهارات الكمبيوتر، وسلوكيات الأمن السيبراني، والشدة المتصورة، والقليل من التأثيرات في التجارب السابقة مع ممارسات أمان الكمبيوتر. بينما الفروق في المستوى التعليمي كانت موجودة في إشارات إلى العمل والإلمام بالتهديدات السيبرانية. وكان العمر والجنس والمستوى التعليم عوامل مهمة في التوسط في سلوكيات الأمن السيبراني للطلاب.

وأشارت نتائج دراسة الصائغ (٢٠١٨)[٢٧] إلى وجود علاقة بين وعي أفراد الأسرة بمفهوم الأمن السيبراني وبين دخل الأسرة، فيما لم تجد فروقا في درجة وعي أفراد الأسرة بمفهوم الأمن السيبراني تعزى إلى متغيرات النوع والعمل والعمر.

كما قامت دراسة Anwar et al. (2017)[٢٨] بتقييم تأثير دور النوع الاجتماعي في سلوكيات ومعتقدات الأمن السيبراني بالتطبيق علي موظفي مؤسسات متنوعة، وأظهرت النتائج وجود اختلافات كبيرة بين الذكور والإناث من حيث مهارات الكمبيوتر، الخبرة السابقة، الكفاءة الذاتية للأمن، بينما تتضاءل الفروق بينهما في سلوك الأمن السيبراني المبلغ عنه ذاتيًا.

وفحصت دراسة Pattinson et al (2015)[٢٩] المكون السلوكي للجوانب البشرية لاستقصاء أمن المعلومات، وتوصلت إلى عدم وجود فروق ذات دلالة إحصائية بين الجنسين. ومع ذلك، وجدوا علاقة إيجابية ذات دلالة بين العمر وسلوك أمن المعلومات، مما يشير أن كبار السن قد يكون لديهم سلوك أمن معلوماتى أفضل. وبفحص العلاقة بين سلوكيات المستخدمين غير الضارة والعوامل السلوكية والفردية التي تتضمن عمر الموظف، مستوى التعليم، والإلمام بأجهزة الكمبيوتر، وطبيعة الشخصية وُجِد أن سلوك الموظفين العرضى الساذج محتمل أن يكون أقل خطورة إذا كانوا أكثر وعيًا، وأكثر قبولًا، وأقل إندفاعا، وأكثر انفتاحًا، وأقل دراية بأجهزة الكمبيوتر.

أما دراسة الصانع (٢٠٢٠)[٣٠] التى أجريت على عينة من معلمى ومعلمات بعض المدارس السعودية لمعرفة درجة وعيهم بالأمن السيبراني وعلاقته بتطبيق أساليب حديثة لحماية الطلبة من مخاطر الإنترنت فلم تجد فروقا ذات دلالة إحصائية بين استجابات المعلمين حول الوعي بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وأساليب تعزيز القيم والهوية الوطنية تبعا للجنس وللتخصص وللمؤهل العلمي ولسنوات الخبرة في التدريس.

أوجه الاستفادة من الدراسات السابقة

بعد مراجعة التراث العلمى العربى والأجنبى المرتبط بموضوع ومتغيرات الدراسة يمكن تحديد أوجه الاستفادة من هذه المراجعة فى النقاط التالية:

- ساعدت الدراسات السابقة الباحثة فى تحديد الإطار النظرى الأمثل للاستخدام فى الدراسة وهو نموذج المعرفة- الاتجاه- السلوك Knowledge, Attitude, Behavior (KAB).
- إضافة بعض المتغيرات غير المتضمنة فى نموذج (KAB) كمتغير الميل للمخاطرة، والسمات الشخصية الخمس الكبرى واختبارها كمتغيرات وسيطة قد تؤثر على شدة العلاقة بين المعرفة بسياسات وإجراءات أمن المعلومات وسلوكيات حماية أمنهم السيبرانى.
- صياغة فروض الدراسة بالبناء على الإطار النظرى الذى تم اختياره، والمتغيرات الأخرى التى تم إضافتها.
- بناء مقاييس الدراسة بالاعتماد على مقاييس تم استخدامها واختبار صدقها وثباتها فى الدراسات السابقة كمقياس HAIS-Q لقياس المعرفة-الاتجاه-السلوك، ومقياس الميل للمخاطرة، ومقياس سمات الشخصية BFI مع قيام الباحثة ببعض التعديلات فى عبارات المقاييس بما يتناسب وموضوع الدراسة الحالية ومجتمعها.

رابعا: الإطار المعرفي

- **نشأة الأمن السيبراني**

ارتبطت نشأة الأمن السيبراني باعتماد الأفراد على الإنترنت في كافة أعمالهم، من تنمية تجارتهم، وحساباتهم البنكية، والتعليم، والتواصل الاجتماعي، وإنهاء إجراءاتهم الحكومية ومهام عديدة ومختلفة، فالمعلومات التى يستخدمونها بالغة الحساسية والأهمية وأصبحت معرضة للخطر والاختراق والاستيلاء، فنشأ مجال الأمن السيبراني لتأمين الأجهزة التقنية على كافة أشكالها وأنواعها بما تحتويه من أنظمة وبيانات ومعلومات يتم تداولها من خلال شبكة الإنترنت وبات من أهم العلوم في عصر التكنولوجيا التي تستخدم للحفاظ على هذه الثروة المعلوماتية المهمة لكلا من الجهات الحكومية والأهلية والأفراد في الفضاء السيبراني الذي يعد أعم وأشمل من شبكة الانترنت؛ لارتباطه باستخدام العديد من الشبكات حول العالم من خلال شبكة الألياف البصرية والشبكات اللاسلكية.[٣١]

وقد حاز الأمن السيبراني على المزيد من الاهتمام على المستوي الدولي والوطني نتيجة ارتفاع عدد الهجمات والتهديدات الناجمة عنها، حيث شهدت الكثير من دول العالم اختراقات أمنية عديدة استهدفت مؤسسات وشركات كبرى تمثلت في سرقة البيانات والمعلومات والتجسس والنصب والاحتيال والإرهاب الإلكتروني،

وهو ما كشفت عنه تقرير المفوضية الأوروبية فى خطتها الاستراتيجية (إبريل ٢٠٢١) والتي تقوم على تعزيز الأمن السيبراني ومكافحة الإرهاب والجريمة الإلكترونية.[٣٢]

- **مفهوم الأمن السيبرانى**

عرَّف التقرير الصادر عن الاتحاد الدولي للاتصالات عام ٢٠١١ الأمن السيبراني بأنه "مجموعة من المهمات مثل (تجميع وسائل وسياسات وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات) يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين".[٣٣]

ويرتبط الأمن السيبرانى ارتباطا وثيقا بأمن المعلومات؛ فالوصول إلى أمن المعلومات أو بثها أو الإطلاع عليها والمتاجرة بها، أو تشهويهها واستغلالها هو ما يقف غالب الأحيان وراء عمليات الاعتداء على الشبكات والإنترنت.[٣٤]

- **الفرق بين الأمن السيبرانى وأمن المعلومات[٣٥]**

– مفهوم الأمن السيبرانى Cyber Security: هو مفهوم أوسع من أمن المعلومات ويتضمن تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية أو الخارجية والتي يتم تخزينها في خوادم داخل أو خارج الشركة من الاختراقات.

– مفهوم أمن المعلومات Information Security: هو حماية المعلومات أو أنظمة المعلومات من النفاذ غير المصرح أو السرقة أو التعديل أو التشهير لحفظ سرية وخصوصية العملاء وبقاء المعلومات محفوظة وفقاً لنهج CIA.

– وترمز CIA للسرية والكمال والتوفر، وهي جزء أساس في جميع مراجع أمن المعلومات وتعتبر مثلث الكمال لأخصائي أمن المعلومات وعلى أساسها يتم بناء منظومة كبيرة لتأمين البنية التحتية للمنشآت الخاصة أو الحكومية. ويعتبر الهدف الأساس هو الحفاظ على معلومات العميل وعدم تسريبها لأن ضمان بقائها يؤدي لرضا العميل وعدم الإخلال بأمنه الاجتماعى.

- **أبعاد الأمن السيبراني**

تتعدد أبعاد الأمن السيبراني لتشمل الجوانب الاقتصادية والإنسانية والسياسية والاجتماعية، فهو يتميز بقدرته على حماية جميع مؤسسات الدولة وأبنائها من أي خطر يهدد اختراق معلوماتهم، ومن هذه الأبعاد: الأبعاد العسكرية والاقتصادية والقانونية والاجتماعية والسياسية.[٣٦]

- **أهداف الأمن السيبراني**

يهدف الأمن السيبراني إلى عدة أمور منها ما يلي:[٣٧]

- الحرص على تعزيز حماية أنظمة التشغيل في الحواسيب وما تقدمه من خدمات وما تشمله من بيانات
- معرفة كيفية التصدي لهجمات وحوادث أمن المعلومات التي تستهدف أجهزة مؤسسات القطاع العام والخاص.
- توفير بيئة آمنة وموثوقة في التعاملات في المجتمع المعلوماتي
- مقاومة البنية التحتية وتصديها للهجمات الإلكترونية.
- السعي إلى معرفة نقاط الضعف في أنظمه تشغيل الحواسيب والأجهزة الإلكترونية بكافة أشكالها والتخلص منها.
- مقاومة البرمجيات الخبيثة وما تحتويه من فيروسات تستهدف إلحاق الأضرار بالمستخدمين.
- الحد من التجسس والتخريب الإلكتروني على المستوى الحكومي والأفراد.
- أخذ جميع الاحتياطات والتدابير اللازمة لحماية المستخدمين من المخاطر المحتملة في مجالات استخدام الإنترنت المتنوعة.
- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد إحداث الضرر بمعلوماتهم الشخصية سواء بإتلاف أو بقصد السرقة.

- **الوعى الأمنى السيبرانى**

ظهرت الأبحاث السابقة أن الوعي بأمن المعلومات (ISA) أمر حيوي في التخفيف من المخاطر المرتبطة بانتهاكات أمن المعلومات، ويشار إلى الأشخاص مرارًا وتكرارًا باسم "خط الدفاع الأول" ضد تهديدات أمن المعلومات المختلفة.[٣٨]

فالوعى الأمنى السيبرانى عامل رئيسي فى مخاطر الأمن السيبراني، ويمكن تصنيف الوعى الأمنى السيبرانى إلى منخفض، متوسط، وعال. وتشتمل سلوكيات الوعى القليل على: عدم الانتباه أو إهمال التنبيهات الأمنية التي ترسلها التطبيقات بشكل تلقائي فى معظم الحالات كالدخول على الشبكات المفتوحة بدون مقابل (كشبكات الإنترنت اللاسكلية Wi-fi) بأجهزة الهاتف المحمول والكمبيوتر المحمول، أما الوعى المتوسط فيتجسد فى الإهمال المعبر عنه فى عمليه تقنية غير لائقة، أم الوعي العالٍ فيتضمن معرفة التهديدات السيبرانية والإجراءات اللازم اتخاذها الوقاية منها.[٣٩]

ويعرف Shaw et al (2009)[40] مصطلح الوعي الأمني السيبراني بالفعل بواسطة على أنه "درجة فهم المستخدمين لأهمية أمن المعلومات ومسؤولياتهم وتصرفاتهم لممارسة مستويات كافية من مراقبة أمن المعلومات لحماية بيانات منظمتهم وشبكتهم".

ويشير التراث العلمى أنه بالرغم من اعتماد الأفراد في الواقع على تقنيات الإنترنت في مهامهم اليومية بشكل متزايد نتيجة سهولة الاستخدام التى يسرت المشاركة في الأنشطة المتعلقة بالإنترنت على نطاق واسع إلا أن المعرفة بالأدوات اللازمة للحماية من التهديدات الإلكترونية عند المستخدمين لازالت منخفضة.[٤١]

وقد لاحظ Abawajy [٤٢] أن حتى المستوى الأساسي السيبراني قد لا يُترجم الوعي الأمني إلى معرفة كافية أو مناسبة لحماية الأمن السيبراني للتخفيف من حدة المخاطر والأخطار لذا اقترح زيادة المعرفة الأمنية من خلال برامج التدريب على الأمن السيبراني، واستخدام المحاضرات والمحاكاة النظرية لتقديم عروض لأدوات حماية الأمن السيبراني تركز على الجوانب التشغيلية والاستخدام والعملية لتحسين معرفة المستخدم والتى ستؤدى بدورها سلوك فعال لحماية الأمن السيبراني.

خامسا: الإطار النظرى

نموذج المعرفة- الاتجاه- السلوك Knowledge, Attitude, Behavior (KAB)

تقوم الدراسة باختبار العلاقة بين ثلاثة عوامل إنسانية معقدة وهى: المعرفة، الاتجاه، والسلوك من خلال الاعتماد على نموذج المعرفة- الاتجاه- السلوك Knowledge, Attitude, Behavior (KAB) الذى تم وضعه فى الأساس لاختبار عناصر أكثر تعقيدا مرتبطة بالسلوك الإنساني.

وفي عام ٢٠١٨، كروجرو Kearney نموذجًا يعتمد على مجال علم النفس الاجتماعي لتحديد الوعي بأمن المعلومات من خلال عوامل مختلفة المعرفة والموقف والسلوك (KAB) والنسخة المكررة من نموذج كاب هو HAIS-Q.

ويركز نموذج KAB بشكل أساسي على الجانب المعرفي للإنسان، وبحسب النموذج فإن المعرفة تتراكم وتظهر في سلوك ذى صلة، فعلى سبيل المثال ، أمن المعلومات، الصحة، البيئة، التعليم وما إلى ذلك، بدأت التغييرات في المواقف. ففي الأساس يشرح النموذج دور المعرفة في تغيير السلوك وتراكم المعرفة، ووفقا للنموذج فإن هذا التراكم فى المعرفة يؤدي إلى تغيير في اتجاه وأخيرًا التغيير السلوكي.[٤٣]

قام بارسونز وآخرون بوضع مقياس The Human Aspects of Information Security Questionnaire (HAIS-Q) بشكل شامل كأداة قياس للوعي بأمن المعلومات

تركز على الجانب الإنساني؛ حيث أن الإنسان هو أحد جوانب الضعف في أمن المعلومات، ويتكون الوعي بأمن المعلومات من عاملين، الأول هو فهم السلوك الآمن للأمن المعلوماتى، والثانى هو الالتزام الفردى وسلوك تنفيذ أمن المعلومات بشكل صحيح ويتوافق ذلك مع نموذج المعرفة- الاتجاه- السلوك (KAB).[٤٤]

ويتكون مقياس HAIS-Q من سبعة مجالات أساسية: إدارة الكلمات المفتاحية، واستخدام البريد الإلكتروني، واستخدام الإنترنت، استخدام مواقع التواصل الاجتماعي، ونظام الأجهزة، ومعالجة المعلومات، والإبلاغ عن الحوادث. يتكون كل مجال من ثلاثة مجالات فرعية. مما أنتج ٢١ مجال اهتمام ، يتم قياس كل منها من خلال عنصر معرفة واتجاه وسلوك منفصل.[٤٥]

وقد استخدم العديد من الباحثين هذا النموذج كإطار نظرى في عديد من الدراسات، وقاموا باختبار صدقه وثباته، وأصبح نموذج HAIS-Q مقياسا موثوقا للوعى بأمن المعلومات.[٤٦]

سادسا: تساؤلات الدراسة وفروضها

- **تساؤلات الدراسة**

- ما مستوى معرفة المبحوثين عينة الدراسة بسياسات وإجراءات أمن المعلومات؟
- ما اتجاهات المبحوثين نحو حماية أمنهم السيبرانى؟
- ما مدى التزام المبحوثين بسلوكيات حماية أمنهم السيبرانى؟
- ما مدى ميل المبحوثين عينة الدراسة للمخاطرة؟
- ما مدى اتسام المبحوثين بسمات الشخصية الخمس الكبرى؟

- **فروض الدراسة**

فى ضوء تحديد مشكلة الدراسة وأهدافها وإطارها النظرى، وفى ضوء استعراض الدراسات السابقة تمت صياغة فروض الدراسة على النحو التالى:

١. توجد علاقة ارتباطية بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات، وسلوكيات حماية أمنهم السيبرانى.
٢. توجد علاقة ارتباطية بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات، واتجاهاتهم نحو حماية أمنهم السيبرانى.
٣. تؤثر متغيرات (اتجاهات المبحوثين نحو حماية أمنهم السيبرانى، الميل للمخاطرة، سمات الشخصية) على العلاقة بين معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكيات حماية أمنهم السيبرانى.
٤. توجد فروق ذات دلالة إحصائية بين المبحوثين فى مستوى المعرفة بسياسات وإجراءات

أمن المعلومات تعزى إلى متغيرات (النوع، السن، المستوى التعليمى).

٥. توجد فروق ذات دلالة إحصائية بين المبحوثين فى سلوكيات حماية أمنهم السيبرانى تعزى إلى متغيرات (النوع، السن، المستوى التعليمى).

سابعا: التعريفات الإجرائية لمفاهيم الدراسة

- **المعرفة:** معرفة الأفراد بالسياسات والإجراءات التي يجب عليهم إتباعها لحماية أنفسهم إلكترونيا.
- **سياسات وإجراءات أمن المعلومات**: هى ما يجب أن يفعل الفرد لحماية أمنه السيبرانى، ولماذا؟ ومتى؟ وأين؟ يجب أن يفعل. كالسياسات والإجراءات الخاصة بكلمات المرور واستخدام البريد الإلكترونى ومواقع التواصل الاجتماعى وطرق حفظ وتخزين البيانات.
- **الاتجاه نحو حماية الأمن السيبرانى:** يشير إلى كيف يشعر المستخدمون تجاه ما يمتلكونه من معرفة ومعلومات بسياسات وإجراءات أمن المعلومات.
- **سلوك حماية الأمن السيبرانى:** ما يقوم به مستخدمو الإنترنت لحماية أنفسهم أثناء استخدام شبكة الإنترنت لضمان الأمان وعدم التعرض للجرائم والانتهاكات الإلكترونية.
- **الأمن السيبراني:** الأمن المرتبط بتقنيات الاتصالات والمعلومات للحد من الخسائر والأضرار.
- **الميل للمخاطرة:** مدى ميل الفرد إلى أن يخاطر أو يتجنب المخاطرة فى حياته بوجه عام.
- **سمات الشخصية:** هى السمات التى حددها علم النفس بخمس سمات رئيسية (الانبساط، القبول أو المسايرة، الضمير، العصابية، الانفتاح).

ثامنا: الإجراءات المنهجية

أ- منهج الدراسة

تعتمد الدراسة الحالية على منهج المسح، من خلال عمل دراسة ميدانية على عينة من مستخدمى الإنترنت؛ للتعرف على مستوى معرفتهم بسياسات وإجراءات الأمن السيبرانى، ومدى تأثير هذه المعرفة على ما يقومون به من سلوكيات لحماية أمنهم السيبرانى.

ب- مجتمع البحث والعينة

يتمثل مجتمع البحث فى جميع مستخدمى الإنترنت فى المجتمع المصرى ممن تبلغ أعمارهم ١٨ عاما فأكثر، وقد تم تطبيق الدراسة على عينة عمدية قوامها (٤٠٠) مبحوثا من مستخدمى الإنترنت الذين تتراوح أعمارهم من ١٨ سنة فأكثر.

وقد جاءت خصائص العينة كالتالى:

جدول رقم (١)

خصائص عينة الدراسة

المتغيرات		ك	%
النوع	ذكور	٢٠٤	%٥١
	إناث	١٩٦	%٤٩
السن	من ١٨ إلى ٣٥ سنة	٣٣٩	%٨٤,٧
	من ٣٦ إلى ٥٠ سنة	٥٢	%١٣
	أكثر من ٥٠ سنة	٩	%٢,٣
المستوى التعليمي	مؤهل متوسط وما يعادله (ثانوية أو دبلوم)	٣٦	%٩
	مؤهل عال	٢٩٢	%٧٣
	دراسات عليا (ماجستير ودكتوراه)	٧٢	%١٨

يتضح من بيانات الجدول السابق أن عينة الدراسة تتوزع بين ٥١% ذكور مقابل ٤٩% من الإناث، أما حسب متغير السن فقد توزعت فئات الدراسة إل ثلاث فئات، كان أكبرها القيمة فئة من ١٨ إلى ٣٥ سنة حيث بلغت نسبتها ٨٤,٧%، تلتها فئة من ٣٦ إلى ٥٠ سنة التى بلغت نسبتها ١٣%، ثم فئة أكثر من ٥٠ سنة بنسبة ٩%، وحسب متغير المستوى التعليمى توزعت عينة الدراسة على ثلاث فئات فان ٧٣% ممن يحملون مؤهل عال، و١٨% منهم حملة ماجستير ودكتوراه، بينما ٩% كانوا ممن يحملون مؤهل متوسط وما يعادله (ثانوية أو دبلوم).

ج- أداة جمع البيانات

اعتمدت الدراسة على أداة (استمارة الاستبيان) لاستطلاع آراء مستخدمى الإنترنت إلكترونيا باستخدام نماذج جوجل google forms، وقد تكونت الاستمارة من مجموعة من المقاييس التى تم اقتباسها من بعض الدراسات السابقة مع إدخال تعديلات فى بعضها لتتناسب مع موضوع ومجتمع الدراسة، كما تم عرض الاستمارة على الأساتذة المحكمين[٤٧] لاختبار الصدق الظاهرى للاستمارة، وفيما يلى عرض لمقاييس المستخدمة فى الدراسة وكيفية احتساب درجاتها:

- **مقاييس المعرفة- الاتجاه- السلوك**

تم الاعتماد على استبيان الجوانب البشرية لأمن المعلومات (HAIS-Q) الذى وضعه بارسونز وآخرون[٤٨]، والذى يتكون من ٦٣ عبارة لقياس المعرفة الفردية والاتجاهات والسلوك المتعلق بـأمن المعلومات، كل ٢١ عبارة منهم تشكل مقياسا لأحد المتغيرات الثلاثة (المعرفة،الاتجاه، السلوك)، يحدد المبحوث موقفه منها على مقياس ليكرت ثلاثى (موافق، محايد، معارض)، وتم وضع درجة لكل اختيار كما يلى: (موافق ٣ درجات)، (محايد درجتين)، (معارض درجة واحدة)، وتراوحت درجات كل مقياس منهم بين (٢١-٦٣)، وكانت درجات

المقياس عل النحو التالى:

- منخفض (٢١-٣٤).
- متوسط (٣٥-٤٩).
- مرتفع (٥٠-٦٣).

- **مقياس الميل للمخاطرة**

تم اقتباس مقياس الميل للمخاطرة الذى يقيس ميل الفرد لتحمل المخاطر من دراسة (Pan & Zinkhan، 2006)،[٤٩] يتكوَّن المقياس من ٥ عبارات، يحدد المبحوث موقفه منها على مقياس ليكرت ثلاثى (موافق، محايد، معارض)، وتم وضع درجة لكل اختيار كما يلى: (موافق ٣ درجات)، (محايد درجتين)، (معارض درجة واحدة)، وتراوحت درجات المقياس بين (٥-١٥)، وكانت درجات المقياس على النحو التالى:

- منخفض (٥-٨).
- متوسط (٩-١١).
- مرتفع (١٢-١٥).

- **مقاييس سمات الشخصية الخمس الكبرى Big five(BFI)**

تم اقتباس المقياس من (بينيت مارتينيز وجون ،١٩٩٨ ؛ جون وسريفاستافا ، ١٩٩٩)، وهو مقياس مكون من ٤٤ عبارة لقياس الأبعاد الخمسة الكبرى للشخصية (الانبساط، القبول أو المسايرة، الضمير، العصابية، الانفتاح).

* **الانبساط:** تكوَّن المقياس من ٨ عبارات يحدد المبحوث موقفه منها على مقياس ليكرت ثلاثى (إلى حد كبير، إلى حد ما، لا)، وتم وضع درجة لكل اختيار كما يلى: (إلى حد كبير ٣ درجات)، (إلى حد ما درجتين)، (لا درجة واحدة)، وتراوحت درجات المقياس بين (٨-٢٤) ، وكانت درجات المقياس عل النحو التالى:
  - منخفض (٨-١٣)
  - متوسط (١٤-١٨)
  - مرتفع (١٩-٢٤)
* **القبول أو المسايرة:** تكوَّن المقياس من ٩عبارات يحدد المبحوث موقفه منها على مقياس ليكرت ثلاثى (إلى حد كبير، إلى حد ما، لا)، وتم وضع درجة لكل اختيار كما يلى: (إلى حد كبير ٣ درجات)، (إلى حد ما درجتين)، (لا درجة واحدة)، وتراوحت درجات المقياس بين (٩-٢٧)، وكانت درجات المقياس عل النحو التالى:

- منخفض (٩-١٤)
- متوسط (١٥-٢١)
- مرتفع (٢٢-٢٧)

* **الضمير:** تكوَّن المقياس من ٩عبارات يحدد المبحوث موقفه منها على مقياس ليكرت ثلاثى (إلى حد كبير، إلى حد ما، لا)، وتم وضع درجة لكل اختيار كما يلى: (إلى حد كبير ٣ درجات)، (إلى حد ما درجتين)، (لا درجة واحدة)، وتراوحت درجات المقياس بين (٩-٢٧)، وكانت درجات المقياس عل النحو التالى:
  - منخفض (٩-١٤)
  - متوسط (١٥-٢١)
  - مرتفع (٢٢-٢٧)
* **العصابية:** تكوَّن المقياس من ٨ عبارات يحدد المبحوث موقفه منها على مقياس ليكرت ثلاثى (إلى حد كبير، إلى حد ما، لا)، وتم وضع درجة لكل اختيار كما يلى: (إلى حد كبير ٣ درجات)، (إلى حد ما درجتين)، (لا درجة واحدة)، وتراوحت درجات المقياس بين (٨-٢٤) ، وكانت درجات المقياس عل النحو التالى:
  - منخفض (٨-١٣)
  - متوسط (١٤-١٨)
  - مرتفع (١٩-٢٤)
* **الانفتاح:** تكوَّن المقياس من ١٠ عبارات يحدد المبحوث موقفه منها على مقياس ليكرت ثلاثى (إلى حد كبير، إلى حد ما، لا)، وتم وضع درجة لكل اختيار كما يلى: (إلى حد كبير ٣ درجات)، (إلى حد ما درجتين)، (لا درجة واحدة)، وتراوحت درجات المقياس بين (١٠-٣٠)، وكانت درجات المقياس عل النحو التالى:
  - منخفض (١٠-١٦)
  - متوسط (١٧-٢٣)
  - مرتفع (٢٤-٣٠)

تاسعا: المعالجة الإحصائية للبيانات

بعد الانتهاء من جمع البيانات اللازمة للدراسة، تم إدخالها -بعد ترميزها- إلى الحاسب الآلي، ثم جرت معالجتها وتحليلها واستخراج النتائج الإحصائية باستخدام برنامج "الحزمة الإحصائية للعلوم الاجتماعية" والمعروف باسم SPSS اختصاراً لـ: Statistical Package

(Version 23) for the Social Sciences)، وذلك باللجوء إلى المعاملات والاختبارات والمعالجات الإحصائية التالية:

١- التكرارات البسيطة والنسب المئوية.

٢- المتوسطات الحسابية والانحرافات المعيارية.

٣- حساب الوزن النسبي للبنود المُقاسه على مقياس ليكرت، وذلك عن طريق حساب المتوسط الحسابي لها، ثم ضرب النتائج X ١٠٠، ثم قسمة النتائج على الحد الأقصي لدرجات المقياس.

٤- معامل ارتباط بيرسون (Pearson Correlation Coefficient) لدراسة شدة واتجاه العلاقة الارتباطية بين متغيرين من مستوى المسافة أو النسبة (Interval Or Ratio). وقد اعتبرت العلاقة ضعيفة إذا كانت قيمة المعامل أقل من ٠,٤ ، ومتوسطة ما بين ٠,٤-٠,٧ ، وقوية إذا بلغت ٠,٧ فأكثر.

٥- معامل الارتباط الجزئي (Partial Correlation Coefficient) لدراسة العلاقة الارتباطية بين متغيرين من مستوى المسافة أو النسبة (Interval Or Ratio) بعد عزل متغير ثالث.

٦- اختبار (ت) للمجموعات المستقلة (Independent-Samples T-Test) لدراسة الدلالة الإحصائية للفروق بين متوسطين حسابيين لمجموعتين مستقلتين من الحالات المدروسة في أحد المتغيرات من نوع المسافة أو النسبة (Interval Or Ratio).

٧- تحليل التباين ذو البعد الواحد (One way Analysis of Variance) المعروف اختصاراً باسم ANOVA لدراسة الدلالة الإحصائية للفروق بين المتوسطات الحسابية لأكثر من مجموعتين من الحالات المدروسة في أحد المتغيرات من نوع المسافة أو النسبة (Interval Or Ratio).

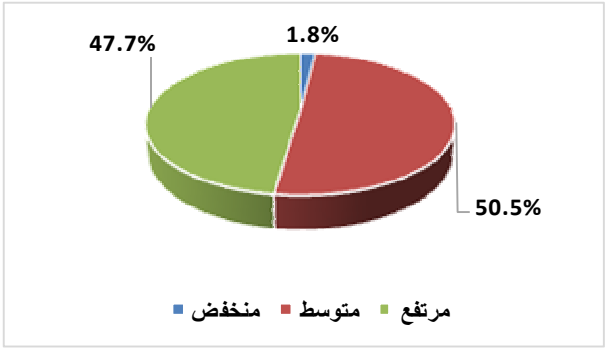
٨- الاختبارات البعدية (Post Hoc Tests) بطريقة أقل فرق معنوي (LSD: Least Significance Difference) لمعرفة مصدر التباين وإجراء المقارنات الثنائية بين المجموعات التي يثبت ANOVA وجود فروق دالة إحصائياً بينها.

وقد تم قبول نتائج الاختبارات الإحصائية عند درجة ثقة ٩٥% فأكثر، أي عند مستوى معنوية ٠,٠٥ فأقل.

عاشرا: نتائج الدراسة

- **النتائج العامة للدراسة**

١. مستوى معرفة المبحوثين عينة الدراسة بسياسات وإجراءات أمن المعلومات



شكل رقم (١)

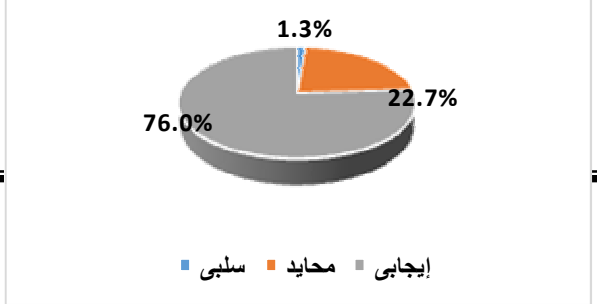
المعرفة بسياسات وإجراءات أمن المعلومات

يوضح الشكل السابق أن نصف حجم عينة الدراسة تقريبا (٥٠,٥%) كان لديهم مستوى متوسط من المعرفة بسياسات وإجراءات أمن المعلومات، بينما (٤٧,٧%) منهم كان لديهم مستوى مرتفع من المعرفة، بينما نسبة (١,٨%) فقط هم من كان مستوى معرفتهم منخفضا. وإجمالا يمكن القول أن معرفة المبحوثين عينة الدراسة بأمن المعلومات تتراوح ما بين متوسطة إلى مرتفعة.

وحول موقف المبحوثين من العبارات الخاصة بمقياس المعرفة بسياسات وإجراءات أمن المعلومات، فقد حازت بعض العبارات التى تشير إلى مستوى مرتفع من المعرفة على أعلى أوزان نسبية وهى: عبارة "عند فتح دردشات أو صور أو ملفات خاصة يجب أن أتأكد من عدم تمكن الغرباء حولي من رؤية شاشة الموبايل أو الكمبيوتر المحمول" بوزن نسبى (٩٥,٢%)، وعبارة "يجب أن أراجع إعدادات الخصوصية على حسابات وسائل التواصل الاجتماعي الخاصة بي بشكل دوري" بوزن نسبى (٩١,٢%)، وعبارة "يجب أن أبلغ مباحث الإنترنت إذا تعرضت لأحد الجرائم الإلكترونية" بوزن نسبى (٩٠,٧%).

بينما حازت بعض العبارات تم صياغتها بشكل معكوس والتى تشير إلى مستوى منخفض من المعرفة على أوزان نسبية عالية وهى: عبارة " يمكنني تنزيل أي ملفات على الكمبيوتر الخاص بي إذا كنت أحتاجها" بوزن نسبى (٨٣,٣%)، وعبارة "يمكن استخدام كلمة مرور واحدة لأكثر من موقع" بوزن نسبى (٧٩,٩%)، وعبارة "يمكنني فتح أي روابط في رسائل البريد الإلكتروني الواردة من أشخاص أعرفه" بوزن نسبى (٧٠,٨%).

٢. اتجاه المبحوثين نحو حماية أمنهم السيبرانى



شكل رقم (٢)

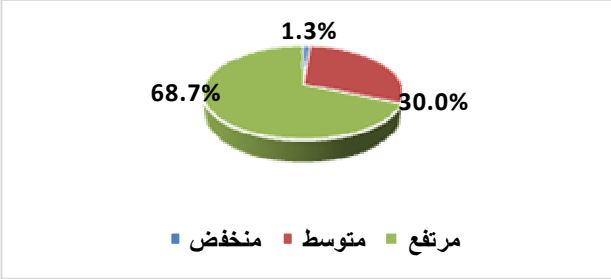
الاتجاه نحو حماية الأمن السيبرانى

يوضح الشكل السابق أن نسبة (76%) من المبحوثين عينة الدراسة كان اتجاههم إيجابى نحو حماية أمنهم السيبرانى، بينما ٢٢,٧% منهم كانوا محايدون الاتجاه، بينما نسبة ١,٣% فقط هم من كان اتجاههم نحو حماية أمنهم السيبرانى سلبيا.

وحول استجابات المبحوثين على العبارات الخاصة بمقياس الاتجاه نحو حماية الأمن السيبرانى؛ فقد حازت العبارات التالية على أعلى الأوزان النسبية من بين عبارات المقياس: عبارة "من الخطر فتح دردشات أو صور أو ملفات خاصة على الموبايل أو الكمبيوتر المحمول إذا كان الغرباء حولي يتمكنون من رؤية شاشتي" بوزن نسبى (٩٣,٨%)، وعبارة "من المهم مراجعة إعدادات الخصوصية لحسابات وسائل التواصل الاجتماعي الخاصة بي بانتظام" بوزن نسبي (٩٣,٣%)، وعبارة " من الخطر فتح ملف مرفق ببريد إلكتروني من مرسل غير معروف" بوزن نسبى (٩٢,٥%)، وعبارة "من الخطر نشر معلومات معينة عن نفسي على وسائل التواصل الاجتماعي" بوزن نسبى (٩٢,٢%).

وفى المقابل حازت بعض العبارات الت تم صياغتها بشكل عكسى على أوزان نسبية عالية مما يدل على انخفاض الاتجاه نحو حماية الأمن السيبرانى، وهذه العبارات هى: عبارة "من الآمن دائمًا فتح الروابط في رسائل البريد الإلكتروني الواردة مادامت من أشخاص أعرفهم" بوزن نسبى (٧٠,٨%)، وعبارة "من الآمن استخدام نفس كلمة المرور لأكثر من موقع" بوزن نسبى (٦٢,٩%)، وعبارة "لا يهم ما هي البيانات التي أضعها على موقع الإنترنت إذا كان ذلك سيحقق لي منفعة أو سيساعدني على إنجاز مهمة" بوزن نسبى (٥٦,٩%)، وعبارة "لن يحدث شيء سيء إذا قمت بتوصيل الفلاشة (يو اس بي) الخاصة بي في أى جهاز لنقل البيانات" بوزن نسبى (٥٦,٨%).

٣. مدى التزام المبحوثين بسلوكيات حماية أمنهم السيبرانى



شكل رقم (٣)

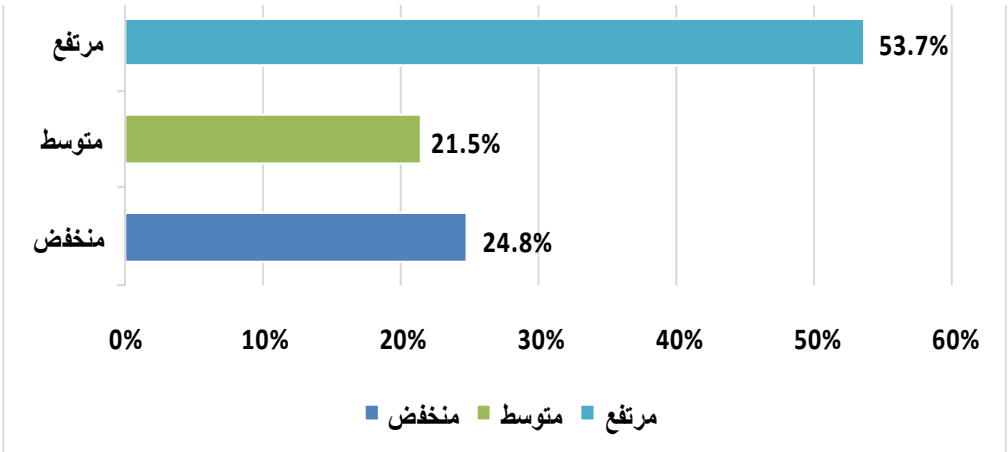
سلوكيات حماية الأمن السيبرانى

يوضح الشكل السابق أن نسبة (68.7%) من المبحوثين عينة الدراسة كان لديهم مستوى مرتفع من الالتزام بسلوكيات حماية الأمن السيبرانى، بينما (30.0%) منهم من كانوا يلتزمون بها بدرجة متوسطة، ونسبة (١,٣%) فقط هم من يتسم التزامهم بسلوكيات حماية الأمن السيبرانى بالانخفاض.

وقد حازت العبارات التالية على أعلى الأوزان النسبية من بين عبارات مقياس سلوك حماية الأمن السيبرانى: عبارة "أتأكد من أن الغرباء حولي لا يمكنهم رؤية شاشة الموبايل أو الكمبيوتر المحمول إذا كنت أفتح دردشات أو صور أو ملفات خاصة" بوزن نسبى (٩٥,٦%)، وعبارة " لا أقوم بفتح مرفقات البريد الإلكتروني إذا كان المرسل غير معروف بالنسبة لي" بوزن نسبى (٩٢,٥%)، وعبارة "لا أنشر أي شيء على وسائل التواصل الاجتماعي قبل التفكير في أي عواقب سلبية" بوزن نسبى (٩٠,٨%).

عبارات عبارة "عند تصفح الإنترنت أزور أي موقع إلكتروني أريده" بوزن نسبى (٧٦,٨%)، وعبارة "أقوم بتنزيل أي ملفات قد احتاجها على الكمبيوتر الخاص بي" بوزن نسبى (٧٦,٣%)، وعبارة "استخدم شبكات الواي فاي المفتوحة في الأماكن عامة" بوزن نسبى (٦٠,٣%).

٤. مستوى ميل المبحوثين للمخاطرة



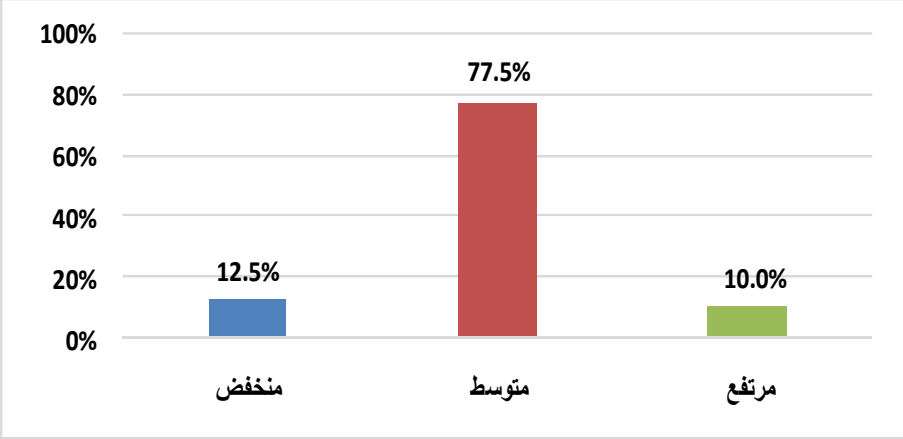
شكل رقم (٤) الميل للمخاطرة

تشير بيانات الشكل السابق أن أكثر من نصف المبحوثين عينة الدراسة (53.7%) كان لديهم مستوى مرتفع من الميل للمخاطرة، بينما (24.8%) منهم كانوا من منخفضي الميل للمخاطرة، وفى المرتبة الأخيرة جاء من لديهم نزعة متوسطة للمخاطرة بنسبة (٢١,٥%).

وحازت عبارة "تعتبر المخاطرة المعتدلة من أهم المهارات الإدارية" على أعلى استجابات للمبحوثين على مقياس الميل للمخاطرة بوزن نسبى (٨٢,٨%)، تلتها عبارة " لتحقيق شيء ما في الحياة، على المرء أن يجازف" بوزن نسبى (٨١,٦%)، ثم عبارة (إذا كانت هناك فرصة كبيرة للحصول على مكافأة؛ سأقدم على المخاطرة) بوزن نسبى (٧٢,٨%).

٥. السمات الشخصية الخمس الكبرى للمبحوثين

أ- الانبساط

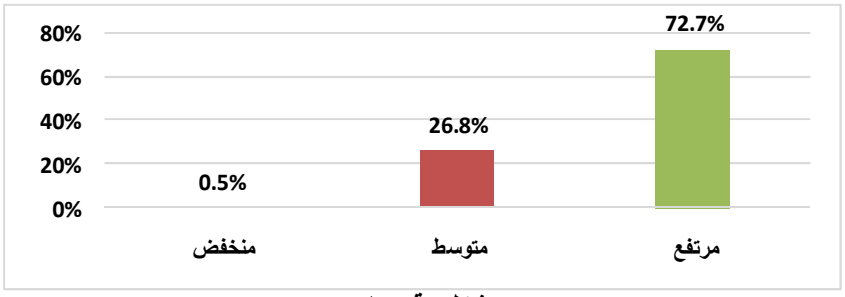


شكل رقم (٥) الانبساط

توضح بيانات الشكل السابق أن (77.5%) من المبحوثين عينة الدراسة يتسمون بسمة الانبساط بنسبة متوسطة، بينما (12.5%) منهم يتسمون بمستوى منخفض من الانبساط، و(10.0%) فقط منهم يتسمون بالانبساط بدرجة مرتفعة.

وقد حازت صفات (مليء بالطاقة)، (لديه الكثير من الحماس أو حماسي)، (يحب الخروج والاختلاط بالناس)، (يحب أن يفتح أحاديث مع الآخرين) على أعلى أوزان نسبية على مقياس الانبساط؛ حيث بلغت الأوزان النسبية لها: (٨٤,١%)، (٧٩,٤%)، (٧٤,٨%)، (٧٢,١%) على الترتيب.

ب- القبول أو المسايرة



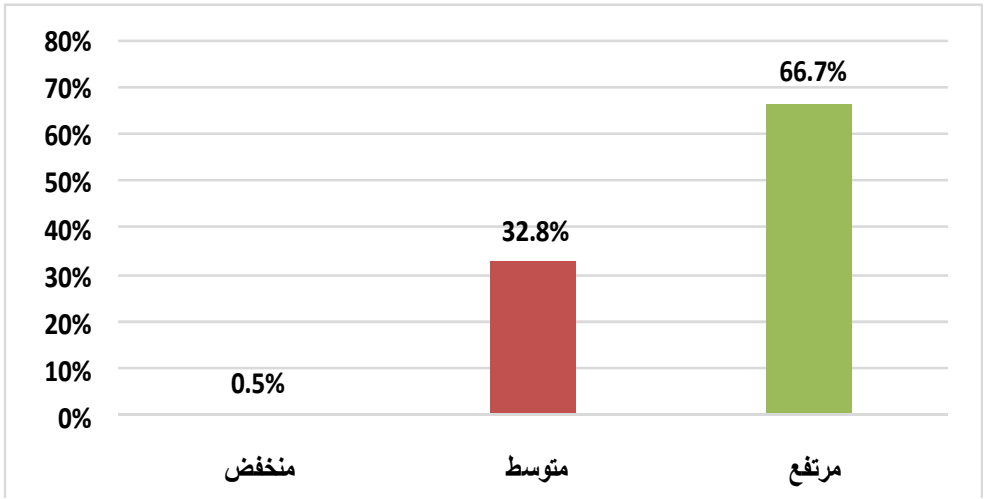
شكل رقم (٦)

القبول أو المسايرة

تشير بيانات الشكل السابق أن غالبية المبحوثين عينة الدراسة (72.7%) كانوا يتسمون بمستوى مرتفع من القبول أو المسايرة، بينما (26.8%) منهم كان لديهم مستوى متوسط من القبول أو المسايرة، وكانت نسبة ضئيلة جدا منهم (**0.5%**) هم من كانت سمة القبول أو المسايرة منخفضة لديهم.

وقد حازت صفة (يؤتمن وأهل للثقة) على أعلى وزن نسبى على مقياس القبول أو المسايرة بنسبة (٩٦,٨%)، تلتها (يحب التعاون مع الآخرين) بوزن نسبى (٩١,٢%)، ثم (متفهم ولطيف مع الجميع تقريبًا) بوزن نسبى (٨٩,٨%)، ثم (يساعد وغير أناني مع الآخرين) بوزن نسبى (٨٨,٧%).

ج- الضمير

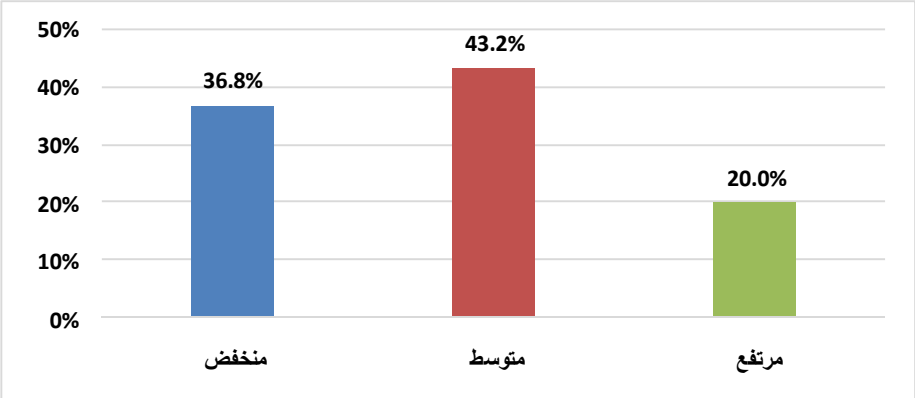


شكل رقم (٧) الضمير

وتشير نتائج استجابات المبحوثين على مقياس الضمير أن نسبة (٦٦,٧%) منهم يتسم بارتفاع سمة الضمير، بينما (٣٢,٨%) لديهم مستوى متوسط من هذه السمة، و نسبة (0.5%) فقط هم من كانوا يرون أنفسهم يتسمون بسمة الضمير بنسبة منخفضة.

وقد سجلت استجابات المبحوثين على صفات (شخص يعتمد عليه في العمل)، (يثابر حتى ينهى العمل المطلوب منه)، (يعمل بجد)، (يؤدى عمله بكفاءة)، (يضع الخطط وينفذها) أعلى أوزان نسبية على مقياس الضمير؛ حيث بلغت أوزانها: (٩٢,٣%)، (٩٠,٨%)، (٨٩%)، (٨٧,٢%)، و(٨٠,٧%) على الترتيب.

د- العصابية



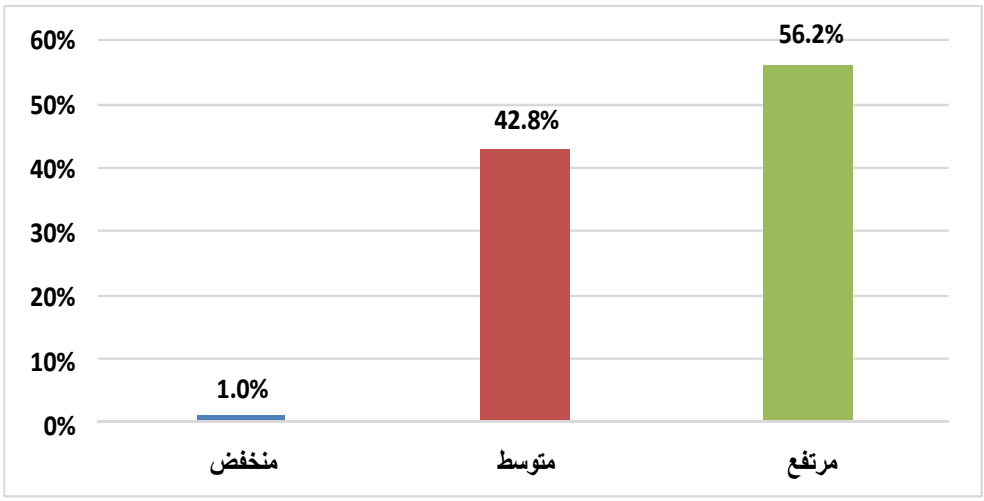
شكل رقم (٨)

العصابية

وتوضح نتائج مقياس العصابية أن (43.2%) من المبحوثين عينة الدراسة يرون أنهم لديهم مستوى متوسط من العصابية، بينما (36.8%) منهم يرون أنهم يتسمون بالعصابية بنسبة منخفضة، ويرى(**20.0%**) منهم أنهم مرتفعو العصابية.

وعلى مقياس العصابية حازت صفة (متقلب المزاج) عل أعلى وزن نسبي بلغ (٧١,٩%)، ثم (يقلق كثيرا) بوزن نسبى (٦٩,٦%)، ثم (ينفعل بسهولة) بوزن (٦٣,٢%)، ثم (يميل إلى التوتر) بنسبة (٦١,٨%).

ه- الانفتاح



شكل رقم (٩)

الانفتاح

وكما يوضح الشكل السابق؛ سجل أكثر من نصف المبحوثين عينة الدراسة (٥٦,٢%) مستوى مرتفع على مقياس الانفتاح، بينما سجل (٤٢,٨%) منهم مستوى متوسط، فى حين أن (١,٠%) فقط هم من سجلوا مستوى منخفض من الانفتاح.

وقد حازت صفات (لديه خيال نشط)، (يأتي بأفكار جديدة)، (يحب التفكير)، (يقدر الفن والأدب) على أعلى أوزان نسبية على مقياس الانفتاح كالتالى: (٨٥,١%)، (٨٤,٥%)، (٨٣,٤%)، (٧٩,٨%).

- **نتائج اختبار فروض الدراسة**

الفرض الأول: توجد علاقة ارتباطية بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكيات حماية أمنهم السيبراني.

جدول رقم (٢)

معنوية العلاقة الارتباطية بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكيات حماية أمنهم السيبراني

معامل بيرسون	مستوى المعنوية
**٠,٦٦٦	٠,٠٠٠
** دال عند مستوى معنوية ٠,٠١	

توضح بيانات الجدول السابق باستخدام معامل ارتباط بيرسون معنوية العلاقة الارتباطية ما بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات والسلوكيات التى يقومون بها لحماية أمنهم السيبراني حيث بلغت قيمة معامل بيرسون (٠,٦٦٦) وهى قيمة دالة إحصائيا عند مستوى معنوية أقل من (٠,٠١)، وهى علاقة طردية متوسطة الشدة أى أنه كلما زاد مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات زادت التزامهم بسلوكيات الحماية لأمنهم السيبراني والعكس صحيح.

وتتفق هذه النتيجة مع نتائج دراسات (Kleij et al, 2021[50]; Li et al, 2019[51]) التى تشير إلى أن الأشخاص الذين لديهم معرفة بالامن السيبرانى يبلغون عن سلوك أكثر أمانًا عبر الإنترنت.

بينما تختلف مع دراسة (Hoggard, ٢٠١٤)[٥٢] التى أشارت أن المبحوثين لم يتبعوا أفضل الممارسات حتى مع علمهم بأنهم يجب أن يفعلوا ذلك

وبذلك ثبتت صحة الفرض الأول القائل بوجود علاقة ارتباطية بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكياتهم نحو حماية أمنهم السيبراني.

الفرض الثاني: توجد علاقة ارتباطية بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات واتجاهاتهم نحو حماية أمنهم السيبراني.

جدول رقم (٣)

معنوية العلاقة الارتباطية بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات واتجاهاتهم نحو حماية أمنهم السيبراني

معامل بيرسون	مستوى المعنوية
**٠,٦٩١	٠,٠٠٠
** دال عند مستوى معنوية ٠,٠١	

توضح بيانات الجدول السابق باستخدام معامل ارتباط بيرسون معنوية العلاقة الارتباطية ما بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات واتجاهاتهم نحو حماية أمنهم السيبراني حيث بلغت قيمة معامل بيرسون (٠,٦٩١) وهى قيمة دالة إحصائيا عند مستوى معنوية(٠,٠١)، وهى علاقة طردية أى أنه كلما زاد مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات زاد اتجاههم الإيجابى نحو حماية أمنهم السيبراني والعكس صحيح. وهى علاقة متوسطة الشدة.

وتتفق هذه النتيجة مع دراسة (Parsons et al., 2014) [٥٣] التى أشارت نتائجها أن المعرفة بسياسات وإجراءات أمن المعلومات تُحدث تباينا فى اتجاهات المستخدمين.

وبذلك ثبتت صحة الفرض الثانى القائل بوجود علاقة ارتباطية بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات واتجاهاتهم نحو حماية أمنهم السيبراني.

الفرض الثالث: تؤثر متغيرات (اتجاهات المبحوثين نحو حماية أمنهم السيبرانى، الميل للمخاطرة، سمات الشخصية) على العلاقة بين معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكيات حماية أمنهم السيبرانى.

جدول رقم (٤)

معنوية تأثير(الاتجاه، الميل للمخاطرة، سمات الشخصية) على العلاقة بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكيات حماية أمنهم السيبراني

المتغيرات		معامل الارتباط الجزئي	مستوى المعنوية
الاتجاه		**٠,٣٥٣	٠,٠٠٠
الميل للمخاطرة		**٠,٦٤٩	٠,٠٠٠
سمات الشخصية	الانبساط	٠,٦٢٤	٠,٠٠٠
	القبول أو المسايرة	٠,٦٤٦	٠,٠٠٠
	الضمير	٠,٦٦١	٠,٠٠٠
	العصابية	٠,٦٧٤	٠,٠٠٠
	الانفتاح	٠,٦٧٤	٠,٠٠٠
** دال عند مستوى معنوية ٠,٠١			

توضح بيانات الجدول السابق باستخدام معامل الارتباط الجزئي معنوية تأثير **الاتجاه نحو حماية الأمن السيبراني** على العلاقة بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات والسلوكيات التى يقومون بها لحماية أمنهم السيبراني حيث بلغت قيمة معامل الارتباط الجزئي (٠,٣٥٣) وهى قيمة دالة إحصائيا عند مستوى معنوية(٠,٠١).

ويتضح من هذه النتيجة أنه عند عزل متغير الاتجاه نحو حماية الأمن السيبرانى فإن شدة العلاقة بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكياتهم نحو حماية أمنهم السيبراني قد قلت حيث بلغت قيمة معامل بيرسون قبل عزل متغير الاتجاه (٠,٦٦٦) وأصبحت قيمة معامل الارتباط الجزئي بعد عزله (٠,٣٥٣)؛ لذا يمكن القول أن اتجاه الفرد نحو حماية الأمن السيبرانى يزيد من شدة العلاقة بين مستوى معرفته بسياسات وإجراءات أمن المعلومات وسلوكياته نحو حماية أمنه السيبراني.

وتتفق هذه النتيجة مع ما توصلت إليه دراسة (Parsons et al. 2014)[٥٤] من نتائج؛ حيث أشارت إلى أن المعرفة والاتجاه سويًا يحدثان تباينا أكبر فى السلوك المبلغ عنه ذاتيًا.

كما توضح بيانات الجدول السابق معنوية تأثير **الميل للمخاطرة** على العلاقة بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكياتهم في حماية أمنهم السيبراني

حيث بلغت قيمة معامل الارتباط الجزئي (٠,٦٤٩) وهى قيمة دالة إحصائيا عند مستوى معنوية (٠,٠١).

ويتضح من هذه النتيجة أن تأثير الميل للمخاطرة على العلاقة بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكياتهم نحو حماية أمنهم السيبراني موجود ولكن بنسبة ضئيلة حيث بلغت قيمة معامل بيرسون قبل عزل هذا المتغير (٠,٦٦٦)، بينما بلغت قيمة معامل الارتباط الجزئي بعد عزله (٠,٦٤٩).

ووتفق هذه النتيجة مع نتائج دراسة (McCormac et al, 2017) [55] التى تشير إلى أن الميل للمخاطرة يحدث تباينا كبيرا فى الوعى بأمن المعلومات.

وفيما يخص متغير **سمات الشخصية** تشير بيانات الجدول إلى معنوية تأثير سمات الشخصية الخمس الكبرى على العلاقة بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكياتهم في حماية أمنهم السيبراني حيث بلغت قيمة معامل الارتباط الجزئي لسمة الانبساط (٠,٦٢٤)، ولسمة القبول أو المسايرة (٠,٦٤٦)، ولسمة الضمير (٠,٦٦١)، ولسمة العصابية (٠,٦٧٤) ولسمة الانفتاح (٠,٦٧٤) وهى جميعها قيم دالة إحصائيا عند مستوى معنوية(٠,٠١).

ولقياس شدة تأثير سمات الشخصية الخمس الكبرى على شدة العلاقة بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكياتهم نحو حماية أمنهم السيبراني قارنا بين قيمة معامل بيرسون للعلاقة قبل عزل هذه المتغيرت (٠,٦٦٦) ومعامل الارتباط الجزئى بعد عزل كل سمة من هذه السمات على حدة، وتشير النتائج إلى أن تأثير كل من: سمة الانبساط، وسمة القبول أو المسايرة ، ولسمة الضمير على شدة العلاقة بين المعرفة والسلوك ولكن بنسب طفيفة حيث أصبح معامل الارتباط الجزئي بعد عزل هذه السمات: (٠,٦٢٤)، (٠,٦٤٦)، (٠,٦٦١) على الترتيب.

أما فيما يخص سمتى العصابية والانفتاح فقد أصبحت العلاقة بين المعرفة والسلوك أكثر قوة بعد عزل هاتين السمتين ولكن بنسب ضئيلة جدا؛ حيث أصبح معامل الارتباط الجزئى بعد عزل سمتى العصابية والانفتاح: (٠,٦٧٤)، و (٠,٦٧٤) على الترتيب.

وتتفق هذه النتيجة مع نتائج دراسات (Kennison et al., 2021 [56]; M. Kennison [57]; Chan-Tin, 2020 & التى Alohali et al., 2018 [58]; McCormac et al., 2017 [59]) تشير إلى أن السمات الشخصية تحدث تبيانا فى وعى الأفراد بالأمن السيبرانى وسلوكياتهم فى حمايته.

وبالبناء على ما سبق ثبتت صحة الفرض الثالث القائل بتأثير متغيرات (اتجاهات المبحوثين نحو حماية أمنهم السيبرانى، الميل للمخاطرة، سمات الشخصية) على العلاقة بين

معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكيات حماية أمنهم السيبرانى.

الفرض الرابع: توجد فروق ذات دلالة إحصائية بين المبحوثين فى مستوى المعرفة بسياسات وإجراءات أمن المعلومات تعزى إلى متغيرات (النوع، السن، المستوى التعليمى).

جدول رقم (٥)

معنوية الفروق بين المبحوثين عينة الدراسة بحسب خصائصهم الديموغرافية (النوع، والسن، والمستوى التعليمي) في مستوى معرفتهم بسياسات وإجراءات الأمن السيبراني

المتغيرات		العدد	المتوسط الحسابي	الانحراف المعياري	إحصائي الاختبار	درجة الحرية	مستوى المعنوية
النوع	ذكور	٢٠٤	٤٧,٤٨	٦,١٥٦	T= ٥,٥٦-	٣٩٨	٠,٠٠٠
	إناث	١٩٦	٥٠,٦٩	٥,٣٥٥			
السن	من ١٨ إلى ٣٥ سنة	٣٣٩	٤٨,٥٧	٦,٠١٣	F= ٨,٠٩٩	٢ ٣٩٧	٠,٠٠٠
	من ٣٦ إلى ٥٠ سنة	٥٢	٥٢,١٠	٥,٣٧٣			
	أكثر من ٥٠ سنة	٩	٤٩,٤٤	٢,٨٣٣			
المستوى التعليمي	مؤهل متوسط وما يعادله (ثانوية أو دبلوم)	٣٦	٤٢,٥٠	٥,٥٣٢	F= ٣٥,٥١	٢ ٣٩٧	٠,٠٠٠
	مؤهل عال	٢٩٢	٤٩,١٣	٥,٤٩٩			
	دراسات عليا (ماجستير ودكتوراه)	٧٢	٥٢,٠٠	٥,٦٥٩			

تشير بيانات الجدول السابق إلى ثبوت معنوية الفروق بين المبحوثين عينة الدراسة في مستوى معرفتهم بسياسات وإجراءات الأمن السيبراني تعزى إلى **متغير النوع** حيث بلغت قيمة (T) ٥,٥٦- وهى قيمة دالة إحصائيا عند مستوى معنوية (٠,٠٠٠)، وتشير النتائج إلى أن الفروق لصالح الإناث حيث بلغ المتوسط الحسابى للذكور (٤٧,٤٨) مقابل (٥٠,٦٩) للإناث،لذا يمكن القول أن الإناث لديهم مستوى أعلى من المعرفة بسياسات وإجراءات الأمن السيبراني مقارنة بالذكور.

وتختلف هذه النتيجة مع نتائج دراسات (McCormac et al, 2017[60]، سماح حمدان٢٠٢١[٦١]، السواط وآخرين ٢٠٢٠[٦٢]، الصائغ ٢٠١٨[٦٣]) التى لم تجد نتائجها فروقا في درجة الوعي بالأمن السيبراني تعزى إلى متغيرات النوع.

كما تشير النتائج إلى معنوية الفروق بين المبحوثين عينة الدراسة في مستوى معرفتهم بسياسات وإجراءات الأمن السيبراني تعزى إلى **متغير السن** حيث بلغت قيمة F (٨,٠٩٩) وهى قيمة دالة إحصائيا عند مستوى معنوية (٠,٠٠٠).

وتختلف هذه النتيجة مع نتائج دراسة (سماح حمدان ٢٠٢١[٦٤]، السواط وآخرين ٢٠٢٠[٦٥]،

الصائغ ٢٠١٨[٦٦] ; McCormac et al, 2017;[٦٧]) التى تذهب نتائجها إلى عدم وجود فروق ذات دلالة إحصائية فى وعى المبحوثين بالأمن السيبرانى ترجع إلى متغير العمر.

كذلك تشير النتائج إلى ثبوت معنوية الفروق بين المبحوثين فى مستوى معرفتهم بسياسات وإجراءات الأمن السيبراني تعزى إلى **متغير المستوى التعليمي** لصالح من هم أكثر تعليما حيث بلغ المتوسط الحسابى لحملة الماجستير والدكتوراه (٥٢,٠٠)، وبلغ المتوسط الحسابى لأصحاب المؤهل العالى (٤٩,١٣)، بينما بلغ المتوسط الحسابى لأصحاب المؤهل المتوسط وما يعادله (ثانوية أو دبلوم) (٤٢,٥٠)؛ ما يمكن معه القول أنه كلما زاد المستوى التعليمى للفرد أصبح أكثر معرفة بسياسات وإجراءات الأمن السيبراني.

تتفق هذه النتيجة مع نتائج دراسة (سماح حمدان٢٠٢١، ٦٨ ,Fatokun et al, ٢٠١٩[69]) التى تشير نتائجها إلى وجود فروق في الإلمام بالتهديدات السيبرانية تعزى إلى المستوى التعليمي.

تختلف هذه النتيجة مع دراسة (الصحفي وعسكول ٢٠١٩)٧٠ التى لم تجد نتائجها فروقا ذات دلالة إحصائية في درجة الوعي بالأمن السيبراني تعزي لمتغير المستوي التعليمي.

وبناء على ما سبق فقد ثبتت صحة الفرض الرابع القائل بوجود فروق ذات دلالة إحصائية بين المبحوثين عينة الدراسة في مستوى معرفتهم بسياسات وإجراءات الأمن السيبراني بحسب خصائصهم الديموغرافية (النوع، والسن، والمستوى التعليمي).

ولاختبار مصدر الفروق بين المبحوثين عينة الدراسة بحسب السن والمستوى التعليمي في مستوى معرفتهم بسياسات وإجراءات الأمن السيبراني، قامت الباحثة بإجراء اختبار بعدي بطريقة LSD، وقد أسفر عن النتائج التالية:

جدول رقم (٦)

مصدر الفروق بين المبحوثين عينة الدراسة بحسب السن والمستوى التعليمي في مستوى معرفتهم بسياسات وإجراءات الأمن السيبراني

المتغيرات	المجموعة	المجموعة المقارنة	الفرق بين المتوسطين	الخطأ المعياري	مستوى المعنوية
السن	من ١٨ إلى ٣٥ سنة	من ٣٦ إلى ٥٠ سنة	-٣,٥٢٤*	٠,٨٧٧	٠,٠٠٠
		أكثر من ٥٠ سنة	-٠,٨٧٢	١,٩٨٨	٠,٦٦١
	من ٣٦ إلى ٥٠ سنة	أكثر من ٥٠ سنة	٢,٦٥٢	٢,١٢٥	٠,٢١٣
المستوى التعليمي	مؤهل متوسط وما يعادله (ثانوية أو دبلوم)	مؤهل عال	-٦,٦٣٠*	٠,٩٧٧	٠,٠٠٠
		دراسات عليا (ماجستير ودكتوراه)	-٩,٥٠٠*	١,١٢٩	٠,٠٠٠
	مؤهل عال	دراسات عليا (ماجستير ودكتوراه)	-٢,٨٧٠*	٠,٧٢٨	٠,٠٠٠
* دال عند مستوى معنوية ٠,٠٥					

يتضح من الجدول السابق أنه فيما يخص متغير السن فإن فئة من ١٨ إلى ٣٥ سنة هى مصدر الفروق بين المبحوثين عينة الدراسة في مستوى معرفتهم بسياسات وإجراءات الأمن السيبراني؛ حيث عند المقارنة بين فئتى من ١٨ إلى ٣٥ سنة و من ٣٦ إلى ٥٠ سنة بلغت قيمة الفرق بين المتوسطين (-٣,٥٢٤) وهى قيمة دالة إحصائيا عند مستوى معنوية (٠,٠٥)، بينما عند المقارنة بين فئتى من ١٨ إلى ٣٥ سنة و أكثر من ٥٠ سنة بلغت قيمة الفرق بين المتوسطين (-٠,٨٧٢) وهى قيمة غير دالة إحصائيا عند مستوى معنوية (٠,٠٥). كذلك عند المقارنة بين فئتى من ٣٦ إلى ٥٠ سنة و أكثر من ٥٠ سنة نجد أن قيمة الفرق بين المتوسطين (٢,٦٥٢) وهى قيمة غير دالة إحصائيا عند مستوى معنوية (٠,٠٥).

أما فيما يخص مصدر الفروق بين المبحوثين عينة الدراسة فى المستوى التعليمى فعند المقارنة بين المجموعات المختلفة نجد فروقا ذات دلالة بين جميع المجموعات كالتالى:

عند المقارنة بين فئة مؤهل متوسط وما يعادله وفئة مؤهل عال نجد الفرق بين المتوسطين (-٦,٦٣٠)، وعند المقارنة بين فئة مؤهل متوسط وما يعادله وفئة دراسات عليا نجد الفرق بين المتوسطين (-٩,٥٠٠)، أما الفرق بين متوسطين فئتى مؤهل عال ودراسات عليا فقد بلغ (-٢,٨٧٠) وهى جميعها قيم دالة إحصائيا عند مستوى معنوية (٠,٠٥).

الفرض الخامس: توجد فروق ذات دلالة إحصائية بين المبحوثين فى سلوكيات حماية أمنهم السيبرانى تعزى إلى متغيرات (النوع، السن، المستوى التعليمى).

جدول رقم (٧)

معنوية الفروق بين المبحوثين عينة الدراسة بحسب خصائهم الديموغرافية (النوع، والسن، والمستوى التعليمي) في سلوكياتهم في حماية أمنهم السيبراني

المتغيرات		العدد	المتوسط الحسابي	الانحراف المعياري	إحصائي الاختبار	درجة الحرية	مستوى المعنوية
النوع	ذكور	٢٠٤	٤٩,٧٢	٦,٢٥٣	T= -٤,٤٦	٣٩٨	٠,٠٠٠
	إناث	١٩٦	٥٢,٤٠	٥,٧٣٥			
السن	من ١٨ إلى ٣٥ سنة	٣٣٩	٥٠,٨٦	٦,٤٨٠	F= ١,٧٧١	٣ ٣٩٦	٠,١٧٢
	من ٣٦ إلى ٥٠ سنة	٥٢	٥٢,٤٤	٣,٥٥٦			
	أكثر من ٥٠ سنة	٩	٤٩,٥٦	٣,٥٣٩			
المستوى التعليمي	مؤهل متوسط وما يعادله (ثانوية أو دبلوم)	٣٦	٤٥,٣٩	٦,٥٩١	F= ١٩,٥١	٢ ٣٩٧	٠,٠٠٠
	مؤهل عال	٢٩٢	٥١,٣٥	٥,٩٥٨			
	دراسات عليا (ماجستير ودكتوراه)	٧٢	٥٢,٥٨	٥,١٣١			

تشير بيانات الجدول السابق إلى ثبوت معنوية الفروق بين المبحوثين عينة الدراسة في

سلوكيات حماية أمنهم السيبراني تعزى إلى **متغير النوع** حيث بلغت قيمة (T) -٤,٤٦ وهى قيمة دالة إحصائيا عند مستوى معنوية ٠,٠٠٠، وتشير النتائج إلى أن الفروق لصالح الإناث حيث بلغ المتوسط الحسابى للذكور (٤٩,٧٢) مقابل (٥٢,٤٠) للإناث، ما يعنى أن الإناث يسلكون سلوكيات أكثر أمانا لحماية أمنهم السيبرانى مقارنة بالذكور.

وتتفق هذه النتيجة مع نتائج دراسات (Fatokun et al, 2019;[71] Anwar et al.,[72] 2017) التى تشير إلى أن وجود فروق بين الذكور والإناث فى سلوكيات الأمن السيبرانى.

بينما تختلف هذه النتيجة مع نتائج دراسات (Pattinson et al, 2015[73]، الصانع ٢٠٢٠[٧٤])التى تشير أن متغير النوع لا يحدث فروقا فى سلوكيات المبحوثين لحماية أمنهم السيبرانى.

كما تشير النتائج إلى ثبوت معنوية الفروق بين المبحوثين عينة الدراسة فى ما يقومون به من سلوكيات لحماية أمنهم السيبرانى تعزى إلى **متغير المستوى التعليمي** لصالح من هم أكثر تعليما حيث بلغ المتوسط الحسابى لحملة الماجستير والدكتوراه (٥٢,٥٨)، وجاء فى المرتبة الثانية أصحاب المؤهل العالى بمتوسط حسابى (٥١,٣٥)، وفى المرتبة الأخيرة جاء أصحاب المؤهل المتوسط وما يعادله (ثانوية أو دبلوم) بمتوسط حسابى (٤٥,٣٩)؛ ما يعنى أنه كلما زاد المستوى التعليمى للفرد أصبح أكثر ميلا للقيام بسلوكيات تحمى أمنه السيبرانى.

بينما تشير بيانات الجدول إلى عدم معنوية الفروق بين المبحوثين عينة الدراسة في سلوكيات حماية أمنهم السيبراني تعزى إلى **متغير السن** حيث بلغت قيمة F (١,٧٧١) وهى قيمة غير دالة إحصائيا عند مستوى معنوية (٠,١٧٢).

وتختلف هذه النتيجة مع نتائج دراسات (Pattinson et al, 2015[٧٥]) التى تشير إلى وجود فروق بين المبحوثين فى سلوكيات حماية أمنهم السيبرانى باختلاف أعمارهم.

وبناء على ماسبق فقد ثبتت صحة الفرض الخامس القائل بوجود فروق ذات دلالة إحصائية بين المبحوثين عينة الدراسة في سلوكيات حماية أمنهم السيبراني بحسب خصائهم الديموغرافية جزئيا؛ حيث ثبت معنوية الفروق التى تعزى إلى متغيرى النوع والمستوى التعليمي بينما لم تثبت معنوية الفروق التى تعزى إلى متغير السن.

ولاختبار مصدر الفروق بين المبحوثين عينة الدراسة بحسب المستوى التعليمي في سلوكياتهم لحماية أمنهم السيبراني، قامت الباحثة بإجراء اختبار بعدي بطريقة LSD، وقد أسفر عن النتائج التالية:

جدول رقم (٨)

مصدر الفروق بين المبحوثين عينة الدراسة بحسب المستوى التعليمي في سلوكياتهم لحماية أمنهم السيبراني

المجموعة	المجموعة المقارنة	الفرق بين المتوسطين	الخطأ المعياري	مستوى المعنوية
مؤهل متوسط وما يعادله (ثانوية أو دبلوم)	مؤهل عال	-٥,٩٦٠*	١,٠٣٨	٠,٠٠٠
	دراسات عليا (ماجستير ودكتوراه)	-٧,١٩٤*	١,٢٠٠	٠,٠٠٠
مؤهل عال	دراسات عليا (ماجستير ودكتوراه)	-١,٢٣٤	٠,٧٧٤	٠,١١١
* دال عند مستوى معنوية ٠,٠٥				

يتضح من بيانات الجدول السابق أن فئة مؤهل متوسط وما يعادله (ثانوية أو دبلوم) هى مصدر الفروق بين المبحوثين عينة الدراسة في سلوكياتهم لحماية أمنهم السيبراني بحسب المستوى التعليمي.

حيث عند المقارنة بين فئة المؤهل المتوسط والمؤهل العالى بلغت قيمة الفرق بين المتوسطين (-٥,٩٦٠) وهى قيمة دالة إحصائيا عند مستوى معنوية (٠,٠٥)، كذلك عند المقارنة بين فئة المؤهل المتوسط والدراسات العليا بلغت قيمة الفرق بين المتوسطين (-٧,١٩٤) وهى قيمة دالة إحصائيا عند مستوى معنوية (٠,٠٥).

بينما عند المقارنة بين فئتى المؤهل العالى والدراسات العليا (ماجستير ودكتوراه) نجد أن قيمة الفرق بين المتوسطين (-١,٢٣ ٤) وهى قيمة غير دالة إحصائيا عند مستوى معنوية (٠,٠٥).

الخلاصة

سعت الدراسة الحالية إلى التعرف على العلاقة بين معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوك حماية أمنهم السيبرانى، واختبار مدى تأثير بعض المتغيرات الوسيطة على هذه العلاقة.

وكان من أهم نتائج الدراسة ما يلي:

- أن درجة معرفة المبحوثين عينة الدراسة بسياسات وإجراءات أمن المعلومات تتراوح ما بين متوسطة إلى مرتفعة حيث أن نسبة (٥٠,٥%) كان لديهم مستوى متوسط من المعرفة، بينما (٤٧,٧%) منهم كان لديهم مستوى مرتفع من المعرفة، ونسبة (١,٨%) فقط هم من كان مستوى معرفتهم منخفضا. ويمكن تفسير ذلك فى ضوء خصائص المبحوثين عينة الدراسة الذين اتسم معظمهم بارتفاع المستوى التعليمى، حيث كان ٩١% منهم من أصحاب المؤهلات العليا وحملة درجتى الماجستير والدكتوراه، و٩% فقط منهم من أصحاب

المؤهل المتوسط.

- أن نسبة (76%) من المبحوثين عينة الدراسة لديهم اتجاه إيجابى نحو حماية أمنهم السيبرانى، بينما(٢٢,٧%) اتجاههم محايد، ونسبة (١,٣%) فقط هم من كان يتسم اتجاههم بالسلبية، ويمكن أن يرجع ذلك إلى ارتفاع المعرفة بأمن المعلومات لدى عينة الدراسة، حيث تشير نتائج هذه الدراسة وبعض الدراسات السابقة إلى وجود علاقة ارتباطية بين مستوى معرفة الفرد بسياسات وإجراءات أمن المعلومات واتجاهه نحو حماية أمنه السيبرانى.
- أن نسبة (68.7%) من المبحوثين عينة الدراسة كان لديهم مستوى مرتفع من الالتزام بسلوكيات حماية الأمن السيبرانى، بينما (30.0%) منهم من كانوا يلتزمون بها بدرجة متوسطة، ونسبة (١,٣%) فقط هم من يتسم التزامهم بسلوكيات حماية الأمن السيبرانى بالانخفاض. ويمكن تفسير ذلك أيضا فى ضوء نتائج هذه الدراسة وبعض الدراسات السابقة إلى تشير إلى أن ارتفاع مستوى معرفة الأفراد بسياسات وإجراءات أمن المعلومات تجعلهم يميلون إلى سلوكيات الحماية لأمنهم السيبرانى أثناء استخدام الإنترنت والكمبيوتر.
- أن أكثر من نصف المبحوثين (53.7%) يمتلكون مستوى مرتفع من الميل للمخاطرة، بينما كان (24.8%) لديهم ميلا منخفضا للمخاطرة، ونسبة (٢١,٥%) من كانوا متوسطى الميل للمخاطرة ومع ذلك بلّغ (68.7%) من المبحوثين عينة الدراسة عن مستوى مرتفع من الالتزام بسلوكيات حماية الأمن السيبرانى؛ ما يعنى أن درجة ميل الأشخاص للمخاطرة في الحياة العامة لاينعكس بالضرورة على سلوكياتهم عبر الإنترنت.
- أما فيما يخص السمات الشخصية للمبحوثين عينة الدراسة لمبلغ عنها ذاتيا فنجد أن:

أن غالبية المبحوثين عينة الدراسة يرون أنهم يتسمون بسمات القبول أو المسايرة، الضمير، الانفتاح التالية بنسب مرتفعة، حيث سجل أكثر من نصف المبحوثين مستويات مرتفعة على مقاييس هذه بنسب: (72.7%)، (66.7%)، (56.2%) على الترتيب.

بينما كانت النسب المتوسطة هى الأعلى فى استجابات مقاييس سمات: الانبساط، من العصابية؛ حيث جاءت نسبها (77.5%)، (43.2%) على الترتيب.

- وجود علاقة طردية بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وإلتزامهم بسلوكيات الحماية لأمنهم السيبراني والعكس صحيح.
- وجود علاقة طردية بين مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات واتجاهاتهم نحو حماية أمنهم السيبراني، أى أنه كلما زاد مستوى معرفة المبحوثين بسياسات وإجراءات أمن المعلومات زاد اتجاههم الإيجابى نحو حماية أمنهم السيبراني والعكس صحيح.

- تأثير متغيرات (اتجاهات المبحوثين نحو حماية أمنهم السيبرانى، الميل للمخاطرة، سمات الشخصية) على العلاقة بين معرفة المبحوثين بسياسات وإجراءات أمن المعلومات وسلوكيات حماية أمنهم السيبرانى.
- ثبتت معنوية وجود فروق ذات دلالة إحصائية بين المبحوثين عينة الدراسة في مستوى معرفتهم بسياسات وإجراءات الأمن السيبراني بحسب خصائصهم الديموغرافية (النوع، والسن، والمستوى التعليمي).
- ثبتت معنوية الفروق التى تعزى إلى متغيرى النوع والمستوى التعليمي في سلوكيات حماية المبحوثين عينة الدراسة أمنهم السيبراني بينما لم تثبت معنوية الفروق وفقا لمتغير السن.

وفي ضوء ما تم عرضه وبالبناء على نتائج الدراسة، ولما كانت المعرفة بالأمن السيبرانى مؤثرة على اتجاهات الأفراد وسلوكياتهم لحماية أمنهم السيبراني؛ فيتوجب الاهتمام بالوعى السيبرانى ومعرفة الجمهور العام فى مجال أمن المعلومات بغية تحسين ممارساتهم وسلوكياتهم عبر الإنترنت بما يضمن أمنهم وسلامتهم وعدم تعرضهم للجرائم والانتهاكات لإلكترونية.

توصيات الدراسة

- يجب على وزارة الاتصالات وتكنولوجيا المعلومات أن تقوم بتطوير سياسة ومخطط وطنى لرفع الوعي حول قضايا الأمن السيبراني لدى الجمهور العام وذلك من خلال تزويده بالمعرفة الأساسية للأمن السيبراني وتبصيره بخطورة ما قد يقوم به من سلوكيات إلكترونية على أمنه السيبرانى مع التركيز على الفئات الأقل حظا من التعليم الذين قد تتسم معارفهم بالضعف فى هذا الجانب من خلال تصميم حملات للتوعية على اعتبار أن مجال الأمن السيبرانى أصبح جزءًا لا يتجزأ من الأمن القومي.
- ضررة التعاون بين وزارتى التربية والتعليم والتعليم العالي لإدراج المعلومات والمعارف ذات الصلة بأمن المعلومات والأمن السيبرانى ضمن المناهج الدراسية للمدارس والجامعات المصرية حيث أصبحت هذه المعرفة ضرورة ملحة ولا غنى عنها فى العصر الحالى (عصر تكنولوجيا المعلومات والبيانات الضخمة).
- أصبح من الضرورى على قطاعات الأعمال المختلفة العامة والخاصة الاهتمام بتوعية وتدريب العاملين بها على سياسات وإجراءات أمن المعلومات والأمن السيبرانى والتى قد يشكل اختراقها ضررا بالغا لأى منظمة.

مراجع الدراسة

1 الدفاع الوطني كتب القائد أكاديمية الدفاع الكندية، (٢٠١٦): الأمن السيبرانى منهج مرجعى عام
https://www.nato.int/nato%20static_12014/assets/pdf/pdf%202016%2010/20170908%201610-cybersecurity-curriculum-ar.pdf

2 الربيعة، صالح بن علي. (2017). **"الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت"**، (هيئة الاتصالات وتقنية المعلومات: الرياض). ص٦

3 الباروك، إبراهيم. (٢٠١٧) . "وزارة الدفاع ، التعان مع الوزارات والقطاع الخاص في مجال الأمن السيبرانى"، **ورقة عمل مقدمة لمؤتمر الأمن السيبرانى والدفاع السيبرانى**، الجامعة اللبنانية والوكالة الجامعية للفرنكوفرنية AUF ، ص ٤٨.

4 N. Safa, S.; V. Solms, R.; Furnell, S. (2016). "Information security policy compliance model in organizations". **Computers& Security**. Vol.56, pp.70–82.

5 D. Bruijn, H.& Janssen, M. (2017). "Building Cybersecurity Awareness: The need for evidence-based framing strategies", **Government Information Quarterly**. Vol. 34, Iss. 1, pp. 1-7.

6 Darwish, A.; El Zarka, A. and A. Aloul, F. (2012). "Towards understanding phishing victims' profile," **International Conference on Computer Systems and Industrial Informatics**, 2012, pp. 1-5.

7 D. Bruijn, H.& Janssen, M. (2017). "Building Cybersecurity Awareness: The need for evidence-based framing strategies", **Government Information Quarterly**. Vol. 34, Iss. 1, pp. 1-7.

8 V.D. Kleij, R.; Goede, S.; V.D. Weijer, S. and R. Leukfeldt, E. (2021). "How Safely Do We Behave Online? An Explanatory Study into the Cybersecurity Behaviors of Dutch Citizens". In: Zallio M., Raymundo Ibañez C., Hernandez J.H. (eds) **Advances in Human Factors in Robots, Unmanned Systems and Cybersecurity**. AHFE 2021. Lecture Notes in Networks and Systems, Vol. 268. Springer, Cham.

9 **Ibid**.

10 Zwilling, M. et al, **Op.Cit**

11 LingLi, Wu He, Li Xu, Ivan Ash, Mohd Anwar, Xiaohong Yuan. (2019). "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior". **International Journal of Information Management.** Vol.45, Iss. C, pp. 13-24.

12 الصحفى، مصباح؛ وعسكول، سناء. (٢٠١٩). "مستوى الوعى بالأمن السيبرانى لدى معلمات الحاسب الآلى للمرحلة الثانوية بمدينة جدة"، **مجلة البحث العلمى فى التربية**، مجلد ١٠، ع٢٠، ص.ص ٤٩٣-٥٣٤.

13 القحطانى، نورة بنت ناصر. (٢٠١٩). "مدى توافر الوعي بالأمن السيبرانى لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية" .**شؤون اجتماعية**. مج٣٦ , ع١٤٤ ،ص.ص.٨٥ – ١.

14 Moallem, A. (2018). "Cyber Security Awareness Among College Students". In: **International Conference on Applied Human Factors and Ergonomics**; Springer: Berlin/Heidelberg, Germany, 2018; pp.79–87.

15 Raytheon. (2017). "Securing our future: Cybersecurity and the millennial workforce". Retrieved from:

https://www.raytheon.com/sites/default/files/201712/2017_cyber_report_rev1.pdf

16 Senthilkumar, K.; Easwaramoorthy, S. (2017). "A Survey on Cyber Security awareness among college students in Tamil Nadu". In**: IOP Conference Series: Materials Science and Engineering**; IOP Publishing: Bristol, UK; Vol. 263, p. 042043.

17 Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M.; Jerram, C. (2014). "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", **Computers & Security**, Vol. 42, pp. 165-176.

18 Hoggard, A. (2014). "Comparing Canadian and American cybersecurity awareness levels: educational strategies to increases public awareness" **Partial Fulfillment of the Requirements for the Degree of Master of Science in Cybersecurity**, the Faculty of Utica College

19 Slusky, L. and Partow-Navid, P. (2012). "Students Information Security Practices and Awareness". **Journal of Information Privacy and Security**, Vol. 8, Iss. 4, pp.3-26.

20 Kennison, S.; T. Jones I.; H. Spooner, V. and Chan-Tin, D.E. (2021). "Who creates strong passwords when nudging fails, **Computers in Human Behavior Reports**, Vol. 4, No.12, p.100123.

21 M. Kennison, S. and Chan-Tin, E. (2020). "Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors", **MEDLINE**, Vol. 11, pp. 546-546.

22 Alohali, M.; Clarke, N.; Li, F. and Furnell, S.(2018). "Identifying and predicting the factors affecting end-users' risk-taking behavior", **Information and Computer Security**, Vol. 26, No. 3, pp. 306-326.

23 McCormac, A.; Zwaans T.; Parsons, K.; Calic, D.; Butavicius, M.; Pattinson, M. (2017). "Individual differences and Information Security Awareness". **Computers in Human Behavior**, Vol. 69, pp. 151-156.

24 حمدان، سماح. (٢٠٢١). "وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته بالإجراءات الاحترازية للحماية من الهجمات الإلكترونية فى ظل جائحة كورونا". **المجلة العربية للعلوم الاجتماعية**. ع١٩، ج١، ص.ص١٨-٦٩.

25 السواط، حمد والصانع، نورة وأبو عيشة، زاهدة وسليمان، إيناس وعسران، عواطف. (٢٠٢٠). "العلاقة بين الوعى بالأمن السيبرانى والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف". **مجلة البحث العلمي فى التربية**، مجلد ٢١، ع٤، ص.ص ٢٧٨-٣٠٦.

26 F B Fatokun *et al* (2019). "The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities". **Journal of Physics: Conference Series**, Volume 1339, International Conference Computer Science and Engineering (IC2SE) 26–27 April 2019, Padang, Indonesia.

27 الصائغ، وفاء حسن. (٢٠١٨). "وعى أفراد الأسرة بمفهوم الأمن السيبرانى وعلاقته باحتياطاتهم الأمنية من الجرائم الإليكترونية"، **المجلة العربية للعلوم الاجتماعية**، مجلد ١٤، ع٣، ص.ص ١٨-٧٠

28 Anwar, M.; Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, Li Xu (2017). "Gender difference and employees' cybersecurity behaviors". **Computers in Human Behavior**, Vol. 69, pp. 437-443.

29 Pattinson, M.; Butavicius, M.; Parsons, K.; McCormac, A. and Calic, D. (2015). "Factors that Influence Information Security Behavior: An Australian Web-Based Study**".** International Conference on Human Aspects of Information Security, Privacy, and Trust. **Part of the Lecture Notes in Computer Science book series** (LNISA, volume 9190) . Springer, Cham. Pp. 231–241.

30 الصانع، نورة عمر أحمد.(٢٠٢٠). "وعى المعلمين والمعلمات بالأمن السيبرانى وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم"، **المجلة العلمية لكلية التربية- جامعة أسيوط**، مجلد ٣٦، ع٦، ص ص. ٤١-٩٠.

31 مجمع البحوث والدراسات بأكاديمية السلطان قابوس. (٢٠١٦). الجريمة الإليكترونية فى المجتمع الخليجي وكيفية مواجهتها

32 https.//:www.linkedin.com/pulse/how-netflix-uses-ai-data-conquer-world-mario-gavira/

33 الاتحاد الدولي للاتصالات (٢٠١١) تقرير الاتجاهات في مجال الاتصالات تمكين عالم الغد الرقمي 2010-SUM-PDF-E.pdf-https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-TTR.12

34 عبد الفتاح، فاطمة الزهراء. (٢٠١٢). **المدونات الالكترونية والمشاركة السياسية**، دار العالم العربي، القاهرة، ص١٢

35 المبارك، عبد الله. (٢٠١٦). ما الفرق ما بين Cyer security و Information Security؟ متاح على الرابط التالى:

https://sa.linkedin.com/in/aaalmubarak?trk=pulse-article_main-author-card

36 السواط وآخرين، **مرجع سابق**

37 الصائغ، **مرجع سابق**.

38 Kleij et al, **Op.Cit.**

39 Zwilling, M.; G. Klien, Lesjak, D.; Wiechetek, Ł.; Cetin, F. and H. N. Basim, H. (2022) "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study", **Journal of Computer Information Systems**, Vol.62, Iss.1, pp.82-97.

40 Shaw, RS.; C. Chen, C.; L. Harris, A. and Huang, HJ. (2009). "The impact of information richness on information security awareness training effectiveness". **Computers& Education**. Vol.52, Iss. 1, pp.92–100.

41 Zwilling et al., **Op.Cit**.

42 Abawajy, J. (2014). "User preference of cyber security awareness delivery methods". **Behavior& Information Technolog**, Vol.33, Issu 3, pp.237–48.

43 Khan, B.; S. Alghathbar, K.; I. Nabi, S. and K. Khan, M. (2011). "Effectiveness of information security awareness methods based on psychological theories". **African Journal of Business Management**, Vol. 5, Iss.26, pp. 10862-10868.

44 S. Saridewi, V.& F. Sari, R. (2021) "Implentation of machine learning for human aspect in information security awareness". **Journal of Applied Engineering Science**, Vol.19. Issu. 4, pp.1126-1142.

45 Parsons, K.; Calic, D.; Pattinson, M.; Butavicius, M; McCormac, A.; and Zwaans, T.(2017) "The Human Aspects of Information Security Questionnaire

(HAIS-Q): Two further validation studies," **Computers & Security**, vol.66, pp. 40-51.

46 D. Dharmawansa, A.& Madhuwanthi, R.(2022). "Evaluating the Information Security Awareness (ISA) of Employees in the Banking Sector: A Case Study", **13th International Research Conference**. General Sir John Kotelawala Defence University.

47 **أسماء السادة المحكمين حسب الترتيب الأبجدى:**

د. اسماء أبو زيد، أستاذ مساعد الصحافة بكلية الإعلام جامعة القاهرة.

أ.د.حسن عماد مكاوى، أستاذ الإذاعة والتليفزيون بكلية الإعلام جامعة القاهرة.

أ.د.محمد المرسي، أستاذ الإذاعة والتليفزيون بكلية الإعلام جامعة القاهرة.

أ.د.هويدا مصطفى، أستاذ الإذاعة والتليفزيون بكلية الإعلام جامعة القاهرة.

48 Parsons et al., **Op.Cit.**

49 Pan, Y. & M. Zinkhan, G. (2006). "Exploring the impact of online privacy disclosures on consumer trust". **Journal of Retailing**, Vol. 82, Issue 4, pp.331-338.

50 Kleij et al, **Op.Cit.**

51 Li et al, **Op.Cit.**

52 Hoggard,A., **Op.Cit.**

53 Parsons et al. **Op.Cit.**

54 **Ibid**

55 McCormac et al., **Op.Cit**.

56 Kennison et al., **Op.Cit**

57 M.Kennison& Chan-Tin**, Op.Cit.**

58 Alohali et al, **Op.Cit**.

59 McCormac et al., **Op.Cit**.

60 McCormac et al., **Op.Cit**.

61 حمدان، **مرجع سابق**.

62 السواط وآخرين، **مرجع سابق**

63 الصائغ، **مرجع سابق**.

64 حمدان، **مرجع سابق**.

65 السواط وآخرين، **مرجع سابق**.

66 الصائغ، **مرجع سابق.**

67 McCormac et al., **Op.Cit**.

68 حمدان، **مرجع سابق**.

69 Fatokun et al, **Op.Cit.**

70 الصحفي وعسكول، **مرجع سابق.**

71 Fatokun et al, **Op.Cit.**

72 Anwar et al., **Op.Cit.**

73 Pattinson et al., **Op.Cit.**

74 الصانع، **مرجع سابق.**

75 Pattinson et al., **Op.Cit.**