مجلة الاقتصاد الزراعي والعلوم الاجتماعية

موقع المجلة & متاح على: www.jaess.journals.ekb.eg

الأمن السيبراني للعاملين بالقطاع الحكومي بريف محافظة الشرقية

خالد أنور علي لبن*

قسم الاقتصاد الزراعي - شعبة الاجتماع الريفي والإرشاد الزراعي (اجتماع ريفي) - كلية الزراعة – جامعة الزقازيق - مصر

Cross Mark

الملخص

استهدفت الدراسة التعرف على مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) للعاملين في القطاع الحكومي المبحوثين، التعرف على الأهمية النسبية لممارسات الأمن السيبراني للعاملين في القطاع الحكومي المبحوثين، اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً لنوع المبحوث، اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً لسن المبحوث، اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً للحالة الزواجية للمبحوث، اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً لعدد أفراد أسرة المبحوث. أجري البحث في ريف محافظة الشرقية اعتماداً على منهج المسح الاجتماعي، وذلك على العاملين في القطاع الحكومي، وذلك في قريتي أم الزين وانشاص البصل بمركز الزقازيق، وقريتي المناجاة الصغرى والصالحية الأحرار بمركز مشتول السوق، وبلغ إجمالي عدد المبحوثين ١٣٤ مبحوث، وتم جمع البيانات بداية من شهر مايو وحتى نهاية شهر يونيو عام ٢٠٢٣، عن طريق استمارة استبيان بالمقابلة الشخصية. واستخدمت الأساليب الإحصائية التكرارات والنسبة المئوية، المتوسط المرجح، اختبار "T-Test" للفروق، اختبار تحليل التباين أحادي الاتجاه "One Way ANOVA". وكانت أهم النتائج: أن إجمالي مستوى الأمن السيبراني لأكثرية المبحوثين منخفض بنسبة بلغت ٤١,٨%، ووجود فروق معنوية عند مستوى معنوية ٠,٠١ في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لسن المبحوث، وهذه الفروق لصالح الفئة السنية (٢٥-٣٦) سنة، ذات المتوسط الأعلى والذي بلغ ١٢٠,٤٨، ٦٨,٠٧، ٢٨,٦١، ٢٣,٨درجة على الترتيب، وعدم وجود أي فروق معنوية إحصائية في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً لنوع، والحالة الزواجية، وعدد أفراد الأسرة للمبحوث.

الكلمات الدالة: الأمن السيبراني؛ حماية الحسابات والأجهزة الإلكترونية؛ حماية المعاملات المصرفية.

المقدمة

يمثل التطور التقني الحادث في مجال المعلومات والاتصالات، أساس تحويل العالم الى قرية صغيرة، من خلال شبكة الإنترنت التي سمحت بتصميم وتطوير العديد من التطبيقات ومنصات التواصل الاجتماعي التي قلصت المسافة بين الأفراد وسمحت بالتواصل فيما بينهم بشكل آني وسريع وذلك من خلال تبادل الصور والرسائل والبيانات، وتوفير الخدمات الإلكترونية المختلفة التي تساعد في إنجاز المعاملات الإلكترونية بكافة أشكالها (لجنة دراسة المخاطر السيبرانية، ٢٠٢٠).

وعلى الرغم من الفوائد الهائلة التي تحققت بفضل تلك الثورة المعلوماتية، إلا أنه صاحب تلك التغيرات مجموعة من الانعكاسات السلبية الخطيرة نتيجة سوء الاستخدام، ومن بين تلك الانعكاسات المستحدثة ظهور الجريمة الرقمية، والتي زادت أخطارها بصورة كبيرة، مما أفرز نوعاً جديداً من الجرائم العابرة للقارات، التي لا تنحصر أخطارها وأثارها في نطاق دولة بعينها (احليل، ٢٠٢٤).

وتعتبر الجريمة السيبرانية هي أحد التحديات التي تواجه الأمن القومي للعديد من البلدان، فهي تشمل مجموعة كبيرة من الأنشطة الإجرامية مثل القرصنة الإلكترونية، وغسيل الأموال، والإرهاب الدولي، حيث تلحق الجريمة السيبرانية الدمار بالاقتصاد والأمن القومي والاستقرار الاجتماعي والمصالح الفردية، وتركز الجهود الحالية للدول على الحد من تهديدات الجرائم السيبرانية (Chen *et al.*, 2023).

وإدراكاً من الدولة المصرية لخطورة هذه التهديدات، فقد أولت اهتماماً بالغاً بهذا المجال ومحاولة اتخاذ مجوعة من التدابير والإجراءات لتنظيم الفضاء الإلكتروني وحماية البيانات في القطاع الحكومي، وذلك على كافة المستويات حتى تصبح قادرة على التصدي للتحديات والمخاطر العالمية الناجمة عن التهديدات السيبرانية، على النحو الذي يدعم جهود الدولة في بناء مصر الرقمية والتي يتم من خلالها تبني المعاملات الرقمية للعاملين وجمهور المستفيدين من الخدمات الحكومية (الهيئة العامة للاستعلامات، ٢٠٢٣).

المشكلة البحثية

تتنامى التهديدات والمخاطر العالمية المعاصرة، وتتنوع مصادرها الخارجية والداخلية، وتتسع دوائر تأثيراتها السلبية على النظم السياسية والاجتماعية، مما أدى إلى ظهور الجرائم الالكترونية التي أصبحت أخطر أنواع الجرائم والتي ترتكب عبر الشبكة الدولية للمعلومات (عبد الجواد، ٢٠٢٣)، فالجرائم السيبرانية تتسم بطابع سرية الهوية ولا تترك سوى القليل من الأثر، بالإضافة إلى ذلك لا تقف أمام الجرائم السيبرانية أي قيود إقليمية أو زمنية، ويمكن أن تسبب أضراراً لعدد لا يحصى من الضحايا، ويجدر الاشارة أن قضية الأمن السيبراني قد تجاوزت مفهومها التقني لتشمل الأبعاد الأمنية والدفاعية والاستراتيجية والاجتماعية، فضلاً عن أنها أصبحت جزءًا لا يتجزأ من خطط الأمن القومي لأي دولة (Adil, 2017)، وتظهر بيانات التقرير الرسمي للجرائم السيبرانية أن إجمالي أضرار الجرائم السيبرانية في جميع دول العالم هي ما يقارب ٨ تريليونات دولار لعام ٢٠٢٣ فقط (الانتربول، ٢٠٢٣)، كما تظهر البيانات إلى أن نسبة المشتركين في خدمات الانترنت في مصر حتى شهر يناير ٢٠٢٤ بلغت ٧٢,٢% من أجمالي عدد السكان، كما أن نسبة المشتركين في الريف في نفس الفترة بلغت ٦٤,٩% من أجمالي الريفيين في مصر (Datareportal,2024)، وهو ما قد يشير إلى زيادة فرص التعرض للجرائم السيبرانية في مصر نتيجة زيادة أعداد المشتركين في خدمات الانترنت، حيث تشير دراسة (اللبان وآخرون، ٢٠٢٣) أن نحو ٤١,٢٥% من عينة الدراسة تعرضوا لنوع واحد على الأقل من الجرائم السيبرانية، وهو ما يؤكد على انتشار وخطورة الجرائم السيبرانية، وما قد يترتب على ذلك من أضرار اقتصادية واجتماعية على مستوى الأفراد والمجتمع، وهو ما يستوجب التعرف على مستوى الأمن السيبراني لمواجهة والحد من تلك الجرائم، ومن العرض السابق تطرح الدراسة مجموعة من التساؤلات كما يلي: ما هو مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) للعاملين في القطاع الحكومي المبحوثين، ما هي الأهمية النسبية لممارسات الأمن السيبراني للعاملين في القطاع الحكومي المبحوثين، هل هناك فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً للنوع، هل هناك فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً للسن، هل هناك فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً للحالة الزواجية، هل هناك فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً لعدد أفراد الأسرة.

الأهداف البحثية:

وفقاً لما سبق عرضه في المشكلة البحثية يمكن تحديد أهداف البحث كما يلي:

1- التعرف على مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) للعاملين في القطاع الحكومي المبحوثين.
2- التعرف على الأهمية النسبية لممارسات الأمن السيبراني للعاملين في القطاع الحكومي المبحوثين.
3- اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً لنوع المبحوث.
4- اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً لسن المبحوث.

*الباحث المسئول عن التواصل
البريد الالكتروني: khaledlaban@yahoo.com
DOI: 10.21608/jaess.2024.324497.1341

5- اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً للحالة الزواجية للمبحوث.

6- اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً لعدد أفراد أسرة المبحوث.

الإطار النظري والمرجعي للدراسة

أولاً- مفهوم الأمن السيبراني: عرف المعهد القومي للمعايير والتقنية NIST (2019) الأمن السيبراني على أنه "حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها المعلومات التي تتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات". ويمكن تعريف الأمن السيبراني على أنه "أمن الشبكات والأنظمة المعلوماتية، وأي بيانات تتعلق بالأجهزة المتصلة بالإنترنت، وعليه فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها أو الالتزام بها لمواجهة التهديدات ومنع التعديات" (طالة، ٢٠٢٠). في حين يعرف على أنه "حماية المعلومات، وكل ما له صلة بتلك المعلومات من عمليات وخدمات وأجهزة وتقنيات، ضد أي شكل من أشكال الوصول غير المسموح به، أو استخدام تلك المعلومات بشكل سلبي، أو ما يمثل خطراً على الجهات أو الأفراد ذوي الصلة بتلك المعلومات لحماية سلامة الشبكات والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به، ويشمل ذلك حماية الأجهزة والبيانات" (سراج، ٢٠٢٢). كما يعرف على أنه مجموعة من الإجراءات التي تتخذ في الدفاع ضد الهجمات السيبرانية، وعواقبها، وتنفيذ التدابير المضادة المطلوبة (Ramirez *et al.*, 2022). في حين عرفه المري (٢٠٢٣) على أنه حماية الأفراد وبياناتهم وحساباتهم من الهجمات الالكترونية، بهدف الحفاظ على سلامة ونزاهة المعلومات المخزنة داخل هذه الأنظمة الالكترونية.

ويمكن أن تعرف الدراسة الأمن السيبراني على أنه "مجموعة من الإجراءات والقوانين والممارسات والاتفاقيات الدولية التي تهدف إلى حماية خصوصية الأفراد والمؤسسات المعلوماتية على شبكة الإنترنت، وحماية الفضاء الإلكتروني ضد أي مخاطر".

ثانياً- أهمية الأمن السيبراني: يلعب الأمن السيبراني أهمية كبيرة في حماية المجتمعات من خلال (القريطي، ٢٠٢٢):

1- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات.
2- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة وسد الثغرات في أنظمة أمن المعلومات.
3- مقاومة البرمجيات الخبيثة، وما تحدثه من أضرار بالغة للمستخدمين.
4- الحد من التجسس والتخريب الالكتروني على مستوى الحكومة والأفراد.

ثالثاً- الأبعاد الاجتماعية للأمن السيبراني: تسمح طبيعة الإنترنت المفتوحة عبر المدونات والشبكات الاجتماعية بشكل خاص لكل فرد بأن يعبر عن تطلعاته وطموحاته الاجتماعية، حيث تمثل مشاركة جميع شرائح المجتمع فرصة للاطلاع على الأفكار والمعلومات المختلفة وبما تكونه من حاجة لدى المجتمع في الحفاظ على استقرار الفضاء السيبراني والمجتمع الذي يرتكز إليه (احليل، ٢٠٢٤)، ويؤسس انفتاح مجتمع ما على مجتمع آخر لتبادل خبرات وأفكار، وتكوين حاجات جديدة وآفاق تعاون وتكامل، لكن في المقابل يعرض أخلاقيات المجتمع للخطر كالمواد الاباحية، والإرهاب، ونشر الفكر المتطرف، ومحاولة تجنيد الشباب والترويج للإتجار بالممنوعات، كما يعرض الهويات لعمليات اختراق خارجي، مما قد يسبب تهديد للسلم الاجتماعي للمجتمع (فرحان، ٢٠٢١)، وهو ما يشير إلى أهمية اتخاذ إجراءات تهدف للحماية من تلك المخاطر التي تهدد بناء المجتمع.

رابعاً- مجالات الأمن السيبراني: أصبح من الضروري أن تتطور وسائل الأمن السيبراني، لتواجه تطور طرق الاختراق والهجمات السيبرانية، ولذلك أصبح الأمن السيبراني يشمل العديد من المجالات كما يلي:

1- **الأمن السيبراني للحسابات والتطبيقات:** تشكل حماية كلمات المرور، حسابات مواقع التواصل الاجتماعي، البريد الإلكتروني جزءاً أساسياً من حماية المجتمع من المخاطر السيبرانية (لجنة دراسة المخاطر السيبرانية، ٢٠٢٠).
2- **الأمن السيبراني للأجهزة الإلكترونية:** نتيجة الاعتماد على الهواتف والحواسب المحمولة، قام العديد من الأشخاص بالتربص لاختراق خصوصية الآخرين، لذلك أصبح من الضروري تأمين هذه الأجهزة وتعزيز الأمن الخاص بها (سراج، ٢٠٢٢).
3- **الأمن السيبراني للمعاملات المصرفية الالكترونية:** نتج عن زيادة الاعتماد على الخدمات المصرفية الالكترونية، ارتفاع نسبة المخاطر والهجمات السيبرانية، وما ينتج عن ذلك من خسائر مالية كبيرة، مما يستدعى اتباع إجراءات أمن سيبرانية صارمة لحماية بيانات وحسابات الأفراد (Akhgar et *al.*, 2022).

وسوف تستعين الدراسة بمجالات الأمن السيبراني السابق ذكرها في قياس مستوى الأمن السيبراني للمبحوثين عينة البحث.

خامساً- الاستراتيجية الوطنية للأمن السيبراني: عززت الدولة المصرية جهودها لدعم الأمن القومي، ومجابهة المخاطر والتهديدات المتزايدة، وأنشأت المجلس الأعلى للأمن السيبراني التابع لرئاسة مجلس الوزراء، وكلف بوضع استراتيجية لتأمين البنى التحتية للاتصالات والمعلومات بشكل متكامل لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الإلكترونية المتكاملة، وعليه تم إعداد الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١)، وكذلك الاستراتيجية الوطنية للأمن السيبراني (٢٠٢٣-٢٠٢٧)، وتتمثل أهمية وجود استراتيجية وطنية للأمن السيبراني في التصدي للحوادث السيبرانية التي تزايدت من حيث عددها ومصادرها (مركز المعلومات ودعم اتخاذ القرار، ٢٠٢٤)، وتشمل الاستراتيجية الوطنية للأمن السيبراني (٢٠٢٣-٢٠٢٧) مجموعة من البرامج كما يلي: بناء إطار تشريعي متكامل، تعزيز الشراكة الوطنية، بناء دفاعات سيبرانية قوية وقادرة على الصمود، تعزيز التعاون الدولي، تغيير ثقافة المجتمع حول الأمن السيبراني، تشجيع البحث العلمي وتعزيز الابتكار والنمو(المجلس الأعلى للأمن السيبراني، ٢٠٢٤).

التوجهات النظرية للبحث:

هناك مجموعة من النظريات التي يمكن أن يعتمد البحث عليها في تناول موضوع الأمن السيبراني وهي كما يلي:

١- نظرية الممارسة الاجتماعية: تركز هذه النظرية على كيفية تشكيل الأفراد في المجتمعات والبيئة الثقافية التي يعيشون فيها وكيف يتأثرون بها ويؤثرون فيها. وما قد يصاحب تلك العمليات من ممارسات صحيحة أو خاطئة يمكن تناقلها بقصد أو دون قصد، وتمثل الممارسات الاجتماعية عنصراً أساسياً في الأمن السيبراني من خلال التزام الأفراد بمجموعة الممارسات الخاصة بالحسابات والأجهزة الالكترونية التي من شأنها الحفاظ على بياناتهم وخصوصيتهم على شبكة الانترنت (Nehme and Warkentin, 2022)، وبذلك فإن الأمن السيبراني يعتمد على مدى التزام الأفراد بمجموعة من الممارسات الاجتماعية، والتي تعمل بشكل أساسي على حمايتهم من الهجمات السيبرانية.

٢- نظرية تشكيل البنية: وهي تشير إلى أن البناءات الاجتماعية تتأسس من خلال الفعل البشرى، وفي الوقت نفسه تعد الوسيط الذي يحدث بواسطته هذا الفعل، وعند وجود أخطاء أو غياب للضوابط المنظمة للفعل البشري ينتج عن ذلك خلل في البناءات الاجتماعية، وعلى ذلك فإن الأمن السيبراني يعتبر فعل بنائي يشكله المجتمع والأفراد وقد يؤثر سلباً أو إيجاباً على البناء الاجتماعي الواقعي والافتراضي نتيجة ارتباطه بمدى وجود ضوابط منظمة له، لما لهذا الفعل "الأمن السيبراني" من تأثير قوي وفعال على الضبط الاجتماعي والاستقرار المجتمعي (جيدنز، ٢٠٠٠). وهنا ينظر للأمن السيبراني على أنه فعل بنائي، يرتبط ارتباطاً قوياً بالحفاظ على تماسك واستقرار المجتمع من خلال محاولة الحد من اختراق خصوصيتهم وقيمهم.

٣- نظرية مجتمع المخاطر: تعتبر من أول النظريات التي تناولت رصد وتحليل المخاطر، حيث تتناول الوجود المتزايد لانعدام اليقين المنتشر في ظل التغيرات التي تحدث في المجتمع (لطيف، ٢٠١٧)، حيث ظهرت مخاطر المجتمع التقني والتكنولوجي أو المجتمع المعلوماتي، وهو ما يطلق عليه منظور ما بعد الحداثة "عالم الفوضى" الذي تغيب معه أنماط الحياة المستقرة، وتنتشر فيه الأخطار عبر مجتمع عالمي في مختلف الأقطار يجعلها تنتشر وتتمدد دون القدرة علي إخضاعها أو التحكم فيها والسيطرة عليها من خلال العولمة وانسيابية التدفق وتخطي الحدود القومية التي عملت علي توسيع نطاق عدم الأمان (Beck, 1992)، وبذلك فإن العلاقات والأفعال الافتراضية ساعدت في تشكيل مجتمع المخاطر، فقد شكلت خطراً علي العلاقات الاجتماعية الواقعية باتساع شبكة العلاقات الإلكترونية والتي تزيد من مخاطر شبكة العلاقات الإجرامية وانعدام الأمن الافتراضي، مما يقلل من مستوي الأمن السيبراني.

٤- نظرية التفاعلية الرمزية: تتناول هذه النظرية عملية التفاعل الاجتماعي الرمزي، حيث يقوم الفرد بمحاولة الاتصال الفكري بالآخرين بغرض التعرف على احتياجاتهم ووسائل تحقيق أهدافهم (لطفي والزيات، ١٩٩٩)، وهو ما يشير إلى أنه يتم استغلال التفاعل الاجتماعي الرمزي في معرفة احتياجات الافراد ومحاولة استغلالها للوصول لمعلومات وبيانات خاصه بهم، كما يمكن الاستعانة بالتفاعل الاجتماعي الرمزي في الأمن السيبراني، من خلال معرفة أغراض المخترقين الحقيقية وعدم اتباعهم.

ومن العرض السابق للنظريات يتضح أن كل نظرية تناولت جانب هام في مفهوم الأمن السيبراني، وسوف يتم الاستعانة بالنظريات السابق ذكرها في محاولة تفسير النتائج التي سوف يتم التوصل إليها.

الدراسات السابقة ذات الصلة بالبحث:

توصلت دراسة (Mahabi, 2010) إلى أن هناك انخفاض في مستوى أمن المعلومات لدي المبحوثين العاملين في الجامعة، كما أن هناك حاجة إلى تقييم درجة وعي المبحوثين بأمن المعلومات وممارساته داخل بيئة العمل وخارجها. كما أظهرت نتائج دراسة (Martnez, 2013) وجود العديد من الثغرات التقنية التي تؤدي إلى حدوث اختراقات للبيانات، وينتج عن ذلك مشكلات في سلامة البيانات أو توافرها، والعديد من

المشكلات الاقتصادية والمجتمعية. وفي دراسة (زقوت وآخرون، ٢٠٢٢) تبين أن اتجاهات أفراد عينة الدراسة نحو متغير الأمن السيبراني كانت إيجابية بمتوسط بلغ ٣,٢١ درجة، كما أنهم كانوا على معرفة مرتفعة بمتغير انتهاكات ومخاطر الأمن السيبراني بمتوسط بلغ ٢,٨٣ درجة، كما تبين وجود علاقة ذات دلالة إحصائية بين وعى أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني والتحول الرقمي.

وتشير نتائج دراسة (اللبان وآخرون، ٢٠٢٣) إلى أن نحو ٢٦,٧٥% من المبحوثين تعرضوا للاختراق الالكتروني عبر مواقع التواصل الاجتماعي، وأن أهم أسباب الاختراق كانت الحصول على المال بنسبة بلغت ٣٢,٧٥%، كما أنه لا توجد فروق ذات دلالة إحصائية بين استجابات المبحوثين عينة الدراسة عن التعرض للاختراق الالكتروني تعزى لكل من متغيرات النوع، والمنطقة وعدد أفراد الأسرة. كما توصلت دراسة (سلامة، ٢٠٢٣) أن الجرائم السيبرانية الأكثر انتشاراً في المجتمع المصري من وجهة نظر أفراد عينة الدراسة هي الجرائم المالية الالكترونية وذلك بنسبة بلغت ٩١,٨%، وأن مستوى المعرفة بالجرائم السيبرانية متوسط بمتوسط بلغ ٦٨,٧ درجة، وكانت أهم مقترحات المبحوثين للحد من الجرائم السيبرانية هو تفعيل موقع الكتروني مختص بالجرائم الالكترونية يحتوي على العقوبات القانونية وآراء العلماء وأحكامها الشرعية بمتوسط حسابي ٢,٦٤ درجة.

وفي دراسة (عبد الجواد، ٢٠٢٣) تشير النتائج إلى أن أكثر أشكال الجريمة السيبرانية انتشاراً هي سرقة المعلومات والبيانات بنسبة ٣٩,٩%، وأن أهم الإجراءات التي يجب أن تتخذها الدولة لتأمين فضائها السيبراني هي التعاون بين الدول في هذا المجال بنسبة ٣٨%، يليها تأمين البنية التحتية الالكترونية بنسبة ٣٠,٨%. كما تشير نتائج دارسة (Shahrom, 2024) أن المؤسسات التي تقدم تدريباً للعاملين بها يكون مستوى الأمن السيبراني لديهم مرتفع، كما أن المبحوثين من العاملين الأصغر سناً يكون مستوى الأمن السيبراني لديهم مرتفع إذا ما قورن بالعاملين الأكبر سناً، وأن الوضع المالي للمؤسسة له تأثير كبير على مستوى الأمن السيبراني بها.

ومن العرض السابق للدراسات السابقة يتبين أن غالبية الدراسات التي أمكن الاطلاع عليها اهتمت بدرجة المعرفة ووجود الجريمة السيبرانية ودرجة تعرض المبحوثين لتلك الجرائم، كما تناولت بعض الدراسات مفهوم أمن المعلومات واتجاهات المبحوثين تجاهه، في حين تبن أن هناك قلة في عدد الدراسات التي تناولت الأمن السيبراني أو قياس مستوى الأمن السيبراني للأفراد بشكل مباشر، وهو ما سيحاول البحث دراسته وعرضه بالتفصيل.

الفروض البحثية:

لحقيق أهداف البحث تم صياغة مجموعة من الفروض الإحصائية وهي كما يلي:

1- لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لنوع المبحوث.

2- لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لسن المبحوث.

3- لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً الحالة الزواجية للمبحوث.

4- لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لعدد أفراد أسرة المبحوث.

وسوف يتم التحقق من صحة تلك الفروض من خلال اختبارها إحصائياً بالأساليب المناسبة لكل فرض.

الطريقة البحثية

أجري البحث في ريف محافظة الشرقية اعتماداً على منهج المسح الاجتماعي، وذلك على العاملين في القطاع الحكومي، حيث تبلغ نسبة العاملين في القطاع الحكومي في ريف جمهورية مصر العربية نحو ٥٢,١٩% من أجمالي العاملين في القطاع الحكومي، وتم اختيار محافظة الشرقية حيث تتصدر محافظات الجمهورية في إجمالي عدد العاملين في القطاع الحكومي حيث بلغ إجمالي عدد العاملين ٤٦٧,٨ ألف موظف، وبلغ إجمالي العاملين بالقطاع الحكومي في ريف محافظة الشرقية ٣١٧,٦ ألف موظف بنسبة ٦٧,٨٩% من إجمالي العاملين بالقطاع الحكومي بالمحافظة (CAPMAS, 2023)، ولتحديد مناطق الدراسة تم اختيار مركزين بأسلوب المعاينة العشوائية البسيطة، وهما مركز الزقازيق ومركز الحسينية، ثم تم اختيار قريتين من كل مركز بنفس الأسلوب، حيث اختيرت قريتي أم الزين وانشاص البصل بمركز الزقازيق، وقريتي المناجاة الصغرى والصالحية الأحرار بمركز مشتول السوق، ولتحديد عدد المبحوثين تم اختيار قطاعين من أكثر القطاعات الحكومية انتشاراً في الريف قطاعي التعليم والصحة، حيث تم اختيار مدرسة ووحدة صحية من كل قرية، وتم جمع البيانات من جميع المدرسين العاملين بالمدارس محل الدراسة، وجميع الأطباء والتمريض العاملين بالوحدات الصحية محل الدراسة، والجدول التالي يوضح توزيع المبحوثين على قري الدراسة:

جدول ١. توزيع المبحوثين على قري الدراسة.

مركز	قرية	مدرسة	وحدة صحية
الزقازيق	أم الزين	٢٤	١٠
	انشاص البصل	٢٩	١٢
الحسينية	المناجاة الصغرى	١٩	٩
	الصالحية الأحرار	٢٣	٨
الإجمالي		٩٥	٣٩
ن= ١٣٤			

ويتضح من الجدول رقم (١) أن عدد المبحوثين من المدارس بلغ ٩٥ مبحوث، في حين بلغ عدد المبحوثين من الوحدات الصحية ٣٩ مبحوث، وبذلك بلغ إجمالي عدد المبحوثين ١٣٤ مبحوث، وقد تم جمع البيانات بداية من شهر مايو وحتى نهاية شهر يونيو عام ٢٠٢٣، عن طريق استمارة استبيان بالمقابلة الشخصية.

الأساليب الإحصائية:

تم تحليل البيانات الميدانية باستخدام بعض الأساليب الإحصائية وهي: التكرارات والنسبة المئوية، المتوسط المرجح، اختبار "T-Test" للفروق، اختبار تحليل التباين أحادي الاتجاه "One Way ANOVA".

قياس المتغيرات البحثية:

يمكن عرض طريقة قياس المتغيرات المتعلقة بموضوع الدراسة الراهنة كما يلي:

١- **النوع:** تم قياس هذا المتغير بتحديد ما إذا المبحوث ذكر أم أنثى، وأعطيت الاستجابات ترميز هو: ذكر=١، أنثى= ٢، للتمييز الرقمي فقط.

٢- **السن:** تم قياس هذا المتغير كرقم مطلق، بإجمالي عدد سنوات عمر المبحوث وقت إجراء الدراسة.

٣- **الحالة الزواجية:** تم قياس هذا المتغير بسؤال المبحوث عن حالته الزواجية، وأعطيت الاستجابات ترميز هو: أعزب= ١، متزوج=٢، أرمل=٣، مطلق=٤، للتمييز الرقمي فقط.

٤- **عدد أفراد الأسرة المعيشية:** تم قياس هذا المتغير كرقم مطلق، بإجمالي عدد أفراد الأسرة أو الأقارب اللذين يعيشون في نفس منزل المبحوث.

٥- **الحصول على دورات في مجال الأمن السيبراني:** تم قياس هذا المتغير بسؤال المبحوث عن ما إذا كان قد اشترك في أي دورات تدريبية تخص مجال الأمن السيبراني، وأعطيت الاستجابات ترميز هو: لا= ١، نعم=٢، للتمييز الرقمي فقط.

٦- **مكان الحصول على الدورات:** تم قياس هذا المتغير بسؤال المبحوث عن جهة الحصول على الدورات التدريبية في مجال الأمن السيبراني، وأعطيت الاستجابات ترميز هو: خارج جهة العمل= ١، داخل جهة العمل=٢، للتمييز الرقمي فقط.

٧- **وجود إجراءات للأمن السيبراني داخل جهة العمل:** تم قياس هذا المتغير بسؤال المبحوث عن وجود نظام للأمن السيبراني متبع داخل جهة العمل، وأعطيت الاستجابات ترميز هو: لا توجد= ١، توجد=٢، للتمييز الرقمي فقط.

٨- **الأمن السيبراني للحسابات والتطبيقات:** تم قياس هذا المتغير بمجموع درجات ثلاثة متغيرات وهي: حماية كلمات المرور، حماية حسابات مواقع التواصل الاجتماعي، حماية حسابات البريد الإلكتروني، وبلغ المدي النظري لمتغير الأمن السيبراني للحسابات والتطبيقات (٢٢- ٨٨) درجة، وتم قياس الثلاثة متغيرات كما يلي:

أ- **حماية كلمات المرور:** تم قياس هذا المتغير بسؤال المبحوث عن سبع عبارات، تدور حول قدرته على اختيار كلمات قوية لحساباته، وتطبيق معايير حماية كلمات المرور، وأعطيت الاستجابات ترميز هو: دائماً=٤، أحياناً=٣، نادراً=٢، لا=١، وبلغ المدى النظري (٧-٢٨)، وقد بلغت قيمة معامل الثبات ألفا كرونباخ ٠,٨٩٩، وهو ما يشير لثبات المقياس.

ب- **حماية حسابات مواقع التواصل الاجتماعي:** تم قياس هذا المتغير بسؤال المبحوث عن سبع عبارات، تدور حول قدرته على اتباع إجراءات الحفاظ على بياناته وخصوصيته على مواقع التواصل الاجتماعي، وأعطيت الاستجابات ترميز هو: دائماً=٤، أحياناً=٣، نادراً=٢، لا=١، وبلغ المدى النظري (٧-٢٨)، وقد بلغت قيمة معامل الثبات ألفا كرونباخ ٠,٨٢٥، وهو ما يشير لثبات المقياس.

ج- **حماية حسابات البريد الالكتروني:** تم قياس هذا المتغير بسؤال المبحوث عن ثماني عبارات، تدور حول قدرته على تأمين حسابات البريد الالكتروني الخاصة به، وتطبيق مجموعة من إجراءات التأمين، وأعطيت الاستجابات ترميز هو: دائماً=٤، أحياناً=٣، نادراً=٢، لا=١، وبلغ المدى النظري (٨-٣٢)، وقد بلغت قيمة معامل الثبات ألفا كرونباخ ٠,٧٨٥، وهو ما يشير لثبات المقياس.

٩- **الأمن السيبراني للأجهزة الإلكترونية:** تم قياس هذا المتغير بسؤال المبحوث عن عشر عبارات، تدور حول قدرته على حماية الأجهزة الالكترونية سواء

تليفون محمول أو أجهزة كمبيوتر وما شابه، وأعطيت الاستجابات ترميز هو: دائماً=٤، أحياناً=٣، نادراً=٢، لا=١، وبلغ المدى النظري (١٠-٤٠)، وقد بلغت قيمة معامل الثبات ألفا كرونباخ ٠,٨٨١، وهو ما يشير لثبات المقياس.

١٠- الأمن السيبراني للمعاملات المصرفية الالكترونية: تم قياس هذا المتغير بسؤال المبحوث عن تسع عبارات، تدور حول تطبيقه لممارسات حماية الحسابات والبطاقات البنكية والتعاملات المصرفية الإلكترونية، وأعطيت الاستجابات ترميز هو: دائماً=٤، أحياناً=٣، نادراً=٢، لا=١، وبلغ المدى النظري (٩-٣٦)، وقد بلغت قيمة معامل الثبات ألفا كرونباخ ٠,٩١١، وهو ما يشير لثبات المقياس.

١١- إجمالي مستوى الأمن السيبراني: تم قياس هذا المتغير بمجموع درجات ثلاثة متغيرات وهي: الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية، وبلغ المدي النظري لمتغير الأمن السيبراني للحسابات والتطبيقات (٤١- ١٦٤) درجة.

توصيف عينة الدراسة:

١- الخصائص العامة للمبحوثين: تظهر نتائج جدول رقم (٢) إلى أن ما يقرب من ثلثي المبحوثين ذكور بنسبة بلغت ٦٣,٤%، كما أن ما يقرب من نصف المبحوثين يتراوح سنهم بين (٣٧-٤٨) سنة بنسبة بلغت ٤٧,٨%، وأن ما يقرب من ثلثي المبحوثين متزوجين بنسبة بلغت ٦٣,٤%، في حين أن ما يقرب من نصف المبحوثين يتراوح عدد أفراد أسرهم المعيشية بين (٤-٦) فرد بنسبة بلغت ٤٧,٨%، وتشير النتائج إلى أن غالبية المبحوثين لم يحصلوا على أي دورات في مجال الأمن السيبراني بنسبة بلغت ٩٣,٣%، وأن جميع من حصل على دورات في مجال الأمن السيبراني حصلوا عليها خارج جهة العمل بنسبة بلغت ١٠٠%، كما أن أكثرية المبحوثين أقروا بأنه لا توجد إجراءات للأمن السيبراني داخل جهة العمل بنسبة بلغت ٨٠,٦%.

جدول ٢. الخصائص العامة للمبحوثين

المتغير	أجمالي المبحوثين (ن=١٣٤)	
	عدد	٪
١- النوع:		
ذكر	٨٥	٦٣,٤
انثي	٤٩	٣٦,٦
٢- السن:		
(٢٥-٣٦) سنة	٤٤	٣٢,٨
(٣٧-٤٨) سنة	٦٤	٤٧,٨
(٤٩-٥٩) سنة	٢٦	١٩,٤
٣- الحالة الزواجية:		
أعزب	٢٢	١٦,٤
متزوج	٨٥	٦٣,٤
مطلق	١٧	١٢,٧
أرمل	١٠	٧,٥
٤- عدد افراد الأسرة المعيشية:		
(٢-٣) فرد	٣٢	٢٣,٩
(٤-٦) فرد	٦٤	٤٧,٨
(٧-٨) فرد	٣٨	٢٨,٣
٥- الحصول على دورات في مجال الأمن السيبراني		
لا	١٢٥	٩٣,٣
نعم	٩	٦,٧
٦- مكان الحصول على الدورات:		
خارج جهة العمل	٩	١٠٠
داخل جهة العمل	صفر	صفر
٧- وجود إجراءات للأمن السيبراني داخل جهة العمل:		
لا توجد	١٠٨	٨٠,٦
توجد	٢٦	١٩,٤

النتائج والمناقشات

أولاً- مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) المبحوثين:

لتحقيق الهدف الأول من البحث والذي ينص على التعرف على مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) للعاملين في القطاع الحكومي المبحوثين، تم حساب التكرارات والنسب المئوية لاستجابات المبحوثين لكل محور وتمثيلها بيانياً، وكانت النتائج كما يلي:

1- مستوى الأمن السيبراني للحسابات والتطبيقات للمبحوثين: يتضح من الشكل رقم (١) أن مستوى الأمن السيبراني لحسابات وتطبيقات أكثرية المبحوثين منخفض بنسبة بلغت ٣٧,٣%، وهو ما يشير إلى أن انخفاض مستوى حماية المبحوثين لحساباتهم سواء على مواقع التواصل الاجتماعي أو البريد الإلكتروني، وهو ما يرتبط مع أن مستوى حماية كلمات المرور ليس بالمستوى المطلوب، وربما يرجع ذلك أيضاً إلى عدم التزام المبحوثين بممارسات حماية حسابات البريد ومواقع التواصل الاجتماعي، وهو ما يتفق مع دراسة (اللبان وآخرون، ٢٠٢٣) أن أكثرية من تعرضوا للاختراق كان عبر مواقع التواصل الاجتماعي، كما تتفق مع دراسة (عبد الجواد، ٢٠٢٣) أن أكثر أشكال الجريمة السيبرانية انتشاراً هي سرقة المعلومات والبيانات.

أ- **مستوى حماية كلمات المرور:** ويظهر الشكل رقم (٢) أن مستوى حماية المبحوثين لكلمات المرور الخاصة بهم متوسط بنسبة بلغت ٤١%.

ب- **مستوى حماية حسابات مواقع التواصل الاجتماعي:** كما يشير الشكل رقم (٣) إلى أن مستوى حماية حسابات مواقع التواصل الاجتماعي لأكثرية المبحوثين متوسط بنسبة بلغت ٣٧,٣%.

ج- **مستوى حماية حسابات البريد الإلكتروني:** في حين يتضح من الشكل رقم (٤) أن مستوى حماية حسابات البريد الإلكتروني لأكثرية المبحوثين منخفض بنسبة بلغت ٤٤%.

2- مستوى الأمن السيبراني للأجهزة الإلكترونية للمبحوثين: يشير الشكل رقم (٥) إلى أن مستوى الأمن السيبراني للأجهزة الإلكترونية لأكثرية المبحوثين منخفض بنسبة بلغت ٤٢,٦%، وهو ما يظهر أن مستوى حماية المبحوثين لأجهزتهم الإلكترونية منخفض، وربما يرجع ذلك لانخفاض وعي المبحوثين بأهمية حماية أجهزتهم، ومدى خطورة الاختراق لتلك الأجهزة من فقدان للبيانات، وغياب الخصوصية، أو وجود ثغرات أمنية يمكن للمخترق استغلالها، وهو ما يتفق مع دراسة (Mahabi, 2010) و (Martnez, 2013) أن ووجود ثغرات تقنية يعمل على انخفاض مستوى الأمن السيبراني.

3- مستوى الأمن السيبراني للمعاملات المصرفية الالكترونية للمبحوثين: يتضح من الشكل رقم (٦) أن مستوى الأمن السيبراني للمعاملات المصرفية الإلكترونية لأكثر من نصف المبحوثين منخفض بنسبة بلغت ٥٤,٥%، وهذه النسبة تشير إلى أن أقل مستوى للأمن السيبراني يتمثل في محور الأمن السيبراني للمعاملات المصرفية الإلكترونية، بالرغم من أهميته وخطورته، وربما يرجع ذلك إلى أن غالبية الهجمات السيبرانية على مستوى الأفراد يكون الدافع الأساسي لها هو المال، وهو ما يتفق مع دراسة (سلامة، ٢٠٢٣) أن الجرائم السيبرانية الأكثر انتشاراً في المجتمع المصري هي الجرائم المالية الالكترونية

4- إجمالي مستوى الأمن السيبراني للمبحوثين: يظهر الشكل رقم (٧) أن إجمالي مستوى الأمن السيبراني لأكثرية المبحوثين منخفض بنسبة بلغت ٤١,٨%، وهو ما يشير إلى أن قدرة المبحوثين منخفضة لحماية أنفسهم والبيئة المحيطة بهم سواء أسرة أو عمل من الهجمات السيبرانية، وربما يرجع ذلك لعدم الالتزام بممارسات الأمن السيبراني أو عدم المعرفة بها، وهو ما يتفق مع نظريتي الممارسة الاجتماعية، تشكيل البنية، حيث أشارا إلى أن الحفاظ على البيانات والخصوصية مترابط بمدي التزام الأفراد بمجموعة الممارسات الخاصة بالحسابات والأجهزة الالكترونية.

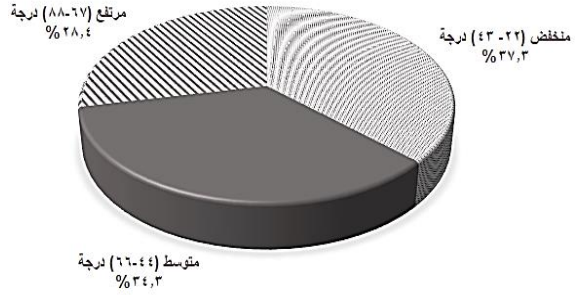
كما أن زيادة التفاعل والعلاقات الافتراضية على مواقع التواصل الاجتماعي، وانخفاض مستوى الخصوصية في نشر المعلومات، يزيد من فرص التعرض للهجمات السيبرانية، كما هو موضح في نظريتي مجتمع المخاطر، والتفاعلية الرمزية، وربما يرجع ذلك لانخفاض الوعي بأهمية الأمن السيبراني كما ذكر في دراستي Mahabi, 2010) و (Martnez, 2013)، أو نتيجة انخفاض مستوي تدريب العاملين بالمؤسسات كما ذكر المبحوثين في الدراسة الحالية، وهو ما يتفق مع نتائج دارسة (Shahrom, 2024) أن المؤسسات التي تقدم تدريباً للعاملين بها يكون مستوى الأمن السيبراني لديهم مرتفع.

ثانياً- الأهمية النسبية لممارسات الأمن السيبراني للعاملين في القطاع الحكومي:

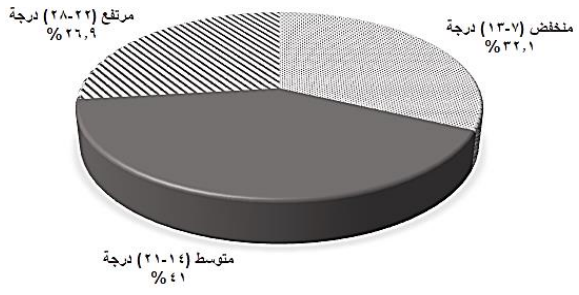
لتحقيق الهدف الثاني من البحث والذي ينص على التعرف على الأهمية النسبية لممارسات الأمن السيبراني للعاملين في القطاع الحكومي المبحوثين، تم حساب التكرارات والنسب المئوية، ثم تم الترتيب وفقاً للمتوسط المرجح لاستجابات المبحوثين لكل محور، وكانت النتائج كما يلي:

١- الأهمية النسبية لممارسات الأمن السيبراني للحسابات والتطبيقات: يمكن عرض ممارسات الأمن السيبراني للحسابات والتطبيقات من خلال ثلاثة متغيرات هي: حماية كلمات المرور، حماية حسابات مواقع التواصل الاجتماعي، حماية حسابات البريد الإلكتروني، كانت النتائج كما يلي:

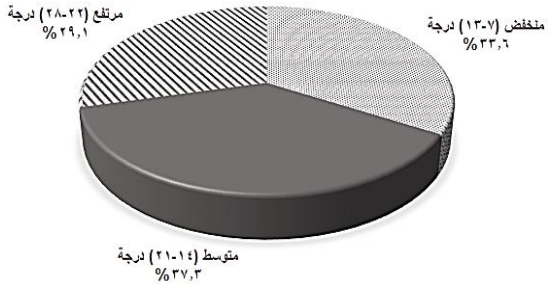
أ- **حماية كلمات المرور:** يتضح من جدول رقم (٣) أن أعلى ثلاث ممارسات للمبحوثين لحماية كلمات المرور الخاصة بهم هي: عدم مشاركة كلمات المرور الخاصة أو إدخالها بشكل مرئي أمام أي أحد بمتوسط مرجح ٤٠,٨ درجة، واستخدام كلمات مرور قوية ومعقدة تتضمن مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز بمتوسط مرجح ٣٨,٥ درجة، تجنب حفظ كلمات المرور جنباً الى جنب مع معلومات تفصيلية عن الحساب بمتوسط مرجح ٣٥,٨ درجة، في حين تأتي في المرتبة الأخيرة لممارسات المبحوثين لحماية كلمات المرور الخاصة بهم: تجنب استخدام نفس كلمة المرور لمختلف الحسابات والتطبيقات بمتوسط مرجح ٢٤,٥ درجة.



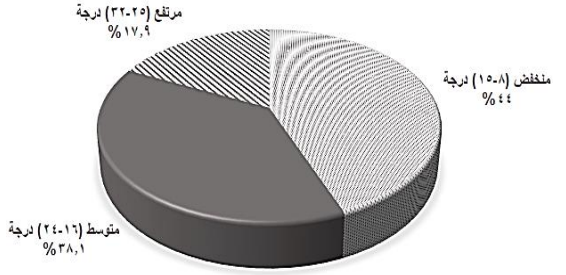
شكل ١. مستوى الأمن السيبراني للحسابات والتطبيقات للمبحوثين.



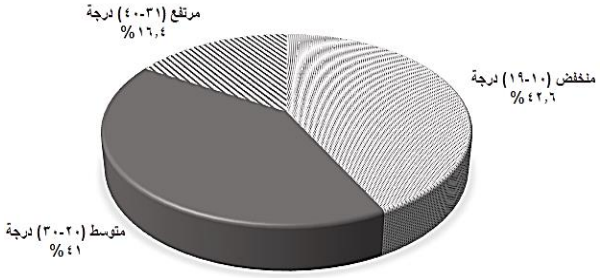
شكل ٢. مستوى حماية المبحوثين لكلمات المرور.



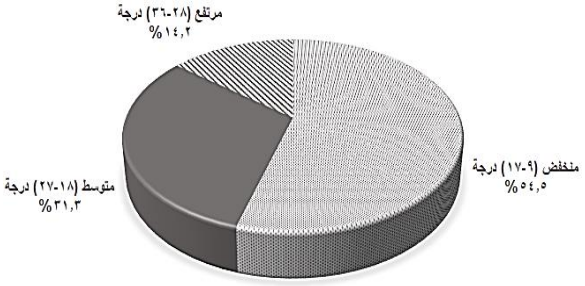
شكل ٣. مستوى حماية المبحوثين لحسابات مواقع التواصل الاجتماعي.



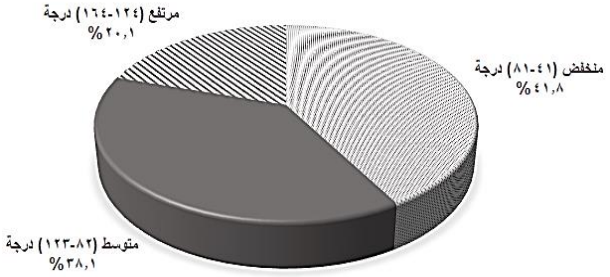
شكل ٤. مستوى حماية المبحوثين لحسابات البريد الإلكتروني.



شكل ٥. مستوى الأمن السيبراني للأجهزة الإلكترونية للمبحوثين.



شكل ٦. مستوى الأمن السيبراني للمعاملات المصرفية الالكترونية للمبحوثين.



شكل ٧. إجمالي مستوى الأمن السيبراني للمبحوثين.

جدول ٣. التوزيع العددي والنسبي للمبحوثين وفقاً لممارسات حماية كلمات المرور، وترتيبها وفقاً للمتوسط المرجح.

م	العبارة	دائما		أحياناً		نادراً		لا		المتوسط المرجح	الترتيب
		عدد	%	عدد	%	عدد	%	عدد	%		
١	عدم مشاركة كلمات المرور الخاصة أو إدخالها بشكل مرئي أمام أي أحد.	٤٤	٣٢,٨	٥٦	٤١,٨	٣٠	٢٢,٤	٤	٣	٤٠,٨	١
٢	استخدام كلمات مرور قوية ومعقدة تتضمن مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز.	٣٧	٢٧,٦	٤٧	٣٥,١	٤٦	٣٤,٣	٤	٣	٣٨,٥	٢
٣	تجنب حفظ كلمات المرور جنباً الى جنب مع معلومات تفصيلية عن الحساب.	٢٧	٢٠,١	٤٣	٣٢,١	٥٧	٤٢,٥	٧	٥,٣	٣٥,٨	٣
٤	تجنب استخدام حروف متسلسلة في لوحة المفاتيح.	٢٨	٢٠,٩	٤٠	٢٩,٨	٥٦	٤١,٨	١٠	٧,٥	٣٥,٤	٤
٥	تجنب استخدام المعلومات الشخصية في كلمات المرور.	٣١	٢٣,١	٢٠	١٤,٩	٤٢	٣١,٤	٤١	٣٠,٦	٣٠,٩	٥
٦	تغيير كلمة المرور الخاصة بالحسابات بشكل دوري.	٢١	١٥,٧	٣١	٢٣,١	٣٦	٢٦,٩	٤٦	٣٤,٣	٢٩,٥	٦
٧	تجنب استخدام نفس كلمة المرور لمختلف الحسابات والتطبيقات.	٦	٤,٥	١٥	١١,٢	٦٣	٤٧	٥٠	٣٧,٣	٢٤,٥	٧

ب- حماية حسابات مواقع التواصل الاجتماعي: يشير جدول رقم (٤) إلى أن أعلى ثلاث ممارسات للمبحوثين لحماية حساباتهم على مواقع التواصل الاجتماعي هي: عدم ارسال صور أو فيديوهات خاصة لأي شخص عبر أي تطبيق بمتوسط مرجح ٣٧,٨ درجة، الحذر من الرسائل مجهولة المصدر التي تطلب معلومات شخصية بمتوسط مرجح ٣٦,٣ درجة، عدم فتح الروابط المجهولة التي تصل عبر تطبيقات الدردشة بمتوسط مرجح ٣٥,٣

درجة، في حين تأتي في المرتبة الأخيرة لممارسات المبحوثين لحماية حساباتهم على مواقع التواصل الاجتماعي: تحميل كافة التطبيقات من المتاجر الرسمية فقط بمتوسط مرجح ٢٥,٧ درجة.

جدول ٤. التوزيع العددي والنسبي للمبحوثين وفقاً لممارسات حماية حسابات مواقع التواصل الاجتماعي، وترتيبها وفقاً للمتوسط المرجح.

م	العبارة	دائما		أحيانا		نادرا		لا		المتوسط المرجح	الترتيب
		عدد	%	عدد	%	عدد	%	عدد	%		
١	عدم ارسال صور او فيديوهات خاصة لاي شخص عبر اي تطبيق.	٣٩	٢٩,١	٥٧	٤٢,٥	١٣	٩,٧	٢٥	١٨,٧	٣٧,٨	١
٢	الحذر من الرسائل مجهولة المصدر التي تطلب معلومات شخصية.	٣٥	٢٦,١	٥٠	٣٧,٣	٢٤	١٧,٩	٢٥	١٨,٧	٣٦,٣	٢
٣	عدم فتح الروابط المجهولة التي تصل عبر تطبيقات الدردشة.	٢٧	٢٠,١	٣٨	٢٨,٤	٦٢	٤٦,٣	٧	٥,٢	٣٥,٣	٣
٤	عدم نشر معلومات شخصية مفصلة على مواقع التواصل الاجتماعي.	٢٩	٢١,٧	٣٠	٢٢,٤	٥٩	٤٤	١٦	١١,٩	٣٤	٤
٥	التواصل مع الاشخاص الموثوق بهم فقط.	٣٤	٢٥,٤	١٠	٧,٥	٧٧	٥٧,٥	١٣	٩,٦	٣٣,٣	٥
٦	عدم نشر اي معلومات قبل التأكد من صحتها وقانونيتها.	٢٨	٢٠,٩	١٦	١١,٩	٦١	٤٥,٥	٢٩	٢١,٧	٣١,١	٦
٧	تحميل كافة التطبيقات من المتاجر الرسمية فقط.	١٠	٧,٥	١٧	١٢,٧	٥٩	٤٤	٤٨	٣٥,٨	٢٥,٧	٧

ج- حماية حسابات البريد الإلكتروني: يتضح من جدول رقم (٥) أن أعلى ثلاث ممارسات للمبحوثين لحماية حسابات بريدهم الالكتروني هي: تجاهل رسائل البريد الالكتروني التي ترد من مصادر مجهولة أو غير معروفة بمتوسط مرجح ٣٨,٨ درجة، عدم فتح البريد الالكتروني أمام الآخرين أو في مكان عام بمتوسط مرجح ٣٦,٤ درجة، تجنب التفاعل مع الرسائل المغرية التي تزعم أنك ربحت جائزة أو مبلغاً من المال بمتوسط مرجح ٣٤,٣ درجة، في حين تأتي في المرتبة الأخيرة لممارسات المبحوثين لحماية حسابات بريدهم الالكتروني: تسجيل الخروج من حساب البريد الالكتروني عند الانتهاء من استخدامه بمتوسط مرجح ٢٥,٧ درجة.

جدول ٥. التوزيع العددي والنسبي للمبحوثين وفقاً لممارسات حماية حسابات البريد الإلكتروني، وترتيبها وفقاً للمتوسط المرجح.

م	العبارة	دائما		أحيانا		نادرا		لا		المتوسط المرجح	الترتيب
		عدد	%	عدد	%	عدد	%	عدد	%		
١	تجاهل رسائل البريد الالكتروني التي ترد من مصادر مجهولة أو غير معروفة.	٤٠	٢٩,٩	٥٥	٤١	٢٤	١٧,٩	١٥	١١,٢	٣٨,٨	١
٢	عدم فتح البريد الالكتروني أمام الآخرين أو في مكان عام.	٣١	٢٣,١	٤٩	٣٦,٦	٣٩	٢٩,١	١٥	١١,٢	٣٦,٤	٢
٣	تجنب التفاعل مع الرسائل المغرية التي تزعم أنك ربحت جائزة أو مبلغاً من المال.	٢٦	١٩,٤	٣٨	٢٨,٤	٥٥	٤١	١٥	١١,٢	٣٤,٣	٣
٤	مشاركة عنوان بريدك الالكتروني فقط مع الأشخاص الموثوقين فقط.	١٤	١٠,٤	٥٠	٣٧,٣	٦٦	٤٩,٣	٤	٣	٣٤,٢	٤
٥	عدم ترك عنوان البريد الإلكتروني مرئياً للجميع في شبكات التواصل الاجتماعي وغيرها من المواقع.	٢٥	١٨,٧	٢٧	٢٠,١	٥١	٣٨,١	٣١	٢٣,١	٣١,٤	٥
٦	إنشاء حساب البريد الإلكتروني الجديد دون الاستعانة بأي أحد.	١٨	١٣,٤	٣١	٢٣,١	٣٨	٢٨,٤	٤٧	٣٥,١	٢٨,٨	٦
٧	إنشاء عنوان بريد الكتروني إضافي لاستعادة الحساب الأساسي في حال تعرضه للقرصنة.	١٤	١٠,٤	٣٠	٢٢,٤	٤٢	٣١,٤	٤٨	٣٥,٨	٢٧,٨	٧
٨	تسجيل الخروج من حساب البريد الالكتروني عند الانتهاء من استخدامه.	٦	٤,٥	٢٤	١٧,٩	٣٩	٢٩,١	٦٥	٤٨,٥	٢٣,٩	٨

٢- الأهمية النسبية لممارسات الأمن السيبراني للأجهزة الإلكترونية: يظهر جدول رقم (٦) أن أعلى ثلاث ممارسات للأمن السيبراني للأجهزة الإلكترونية للمبحوثين هي: تفعيل خصائص الأمان المتقدمة مثل التعرف على الوجه، بصمات الأصابع، وبصمة العين بمتوسط مرجح ٣٦,٣ درجة، تفعيل ميزة إقفال الهاتف تلقائياً بعد فترة قصيرة من عدم الاستخدام بمتوسط مرجح ٣٥,٨ درجة، تفعيل خاصية التحديث الأوتوماتيكي للهاتف لسد الثغرات الأمنية بمتوسط مرجح ٣٢,٨ درجة، في حين تأتي في المرتبة الأخيرة لممارسات الأمن السيبراني للأجهزة الإلكترونية للمبحوثين: عدم منح أذونات للتطبيقات على الجهاز إذا كان مبالغ فيها أو غير منطقية بمتوسط مرجح ٢٣,٩ درجة.

جدول ٦. التوزيع العددي والنسبي للمبحوثين وفقاً لممارسات الأمن السيبراني للأجهزة الإلكترونية، وترتيبها وفقاً للمتوسط المرجح.

م	العبارة	دائما		أحيانا		نادرا		لا		المتوسط المرجح	الترتيب
		عدد	%	عدد	%	عدد	%	عدد	%		
١	تفعيل خصائص الأمان المتقدمة مثل التعرف على الوجه، بصمات الأصابع، وبصمة العين.	٢٧	٢٠,١	٦٠	٤٤,٨	٢٨	٢٠,٩	١٩	١٤,٢	٣٦,٣	١
٢	تفعيل ميزة إقفال الهاتف تلقائياً بعد فترة قصيرة من عدم الاستخدام.	٢٤	١٧,٩	٥٦	٤١,٨	٤٠	٢٩,٩	١٤	١٠,٤	٣٥,٨	٢
٣	تفعيل خاصية التحديث الأوتوماتيكي للهاتف لسد الثغرات الأمنية.	١٤	١٠,٤	٦٠	٤٤,٨	٣٢	٢٣,٩	٢٨	٢٠,٩	٣٢,٨	٣
٤	تحميل برنامج موثوق للحماية من الفيروسات والبرمجيات الخبيثة.	١٨	١٣,٤	٣٦	٢٦,٩	٦٠	٤٤,٨	٢٠	١٤,٩	٣٢	٤
٥	اغلاق وسائل اتصال الهاتف بالشبكات المختلفة في حال عدم استخدامها.	٢٣	١٧,٢	٣٤	٢٥,٤	٤٨	٣٥,٨	٢٩	٢١,٦	٣١,٩	٥
٦	عدم حفظ كلمات المرور أو المعلومات الحساسة على الجهاز.	٥	٣,٧	٤٩	٣٦,٦	٤٣	٣٢,١	٣٧	٢٧,٦	٢٩	٦
٧	استخدام شبكة موثوق بها للاتصال بالإنترنت وتجنّب شبكات الواي فاي العامة والمجانية.	٦	٤,٥	٤٣	٣٢,١	٤٣	٣٢,١	٤٢	٣١,٣	٢٨,١	٧
٨	تحميل التطبيقات التي تحتاج إليها فعلياً فقط من متاجرها الرسمية.	١٦	١١,٩	٣٠	٢٢,٤	٣٧	٢٧,٦	٥١	٣٨,١	٢٧,٩	٨
٩	الاحتفاظ بنسخ احتياطية من بيانات الجهاز على وحدات تخزين صلبة أو سحابية.	٥	٣,٧	٤١	٣٠,٦	٢٨	٢٠,٩	٦٠	٤٤,٨	٢٥,٩	٩
١٠	عدم منح أذونات للتطبيقات على الجهاز إذا كان مبالغ فيها أو غير منطقية.	٤	٣	٢٧	٢٠,١	٣٩	٢٩,١	٦٤	٤٧,٨	٢٣,٩	١٠

٣- الأهمية النسبية لممارسات الأمن السيبراني للمعاملات المصرفية الالكترونية: يظهر جدول رقم (٧) أن أعلى ثلاث ممارسات للأمن السيبراني للمعاملات المصرفية الالكترونية للمبحوثين هي: سرعة الغاء البطاقة البنكية عند سرقتها أو سرقة بياناتها بمتوسط مرجح ٣٥,٥ درجة، اتمام العمليات المصرفية الإلكترونية من خلال أجهزة موثوق فيها بمتوسط مرجح ٣٢,٨ درجة، عدم مشاركة بيانات البطاقات أو الحسابات البنكية إلا لمواقع موثوقة وللضرورة بمتوسط مرجح ٣٠,١ درجة، في حين تأتي في المرتبة الأخيرة لممارسات الأمن السيبراني للمعاملات المصرفية الالكترونية للمبحوثين: تحديد سقف معين على بطاقات الائتمان للمبالغ المسموح سحبها أو الشراء بها في وقت واحد بمتوسط مرجح ٢٢,١ درجة.

جدول ٧. التوزيع العددي والنسبي للمبحوثين وفقاً لممارسات الأمن السيبراني للمعاملات المصرفية الالكترونية، وترتيبها وفقاً للمتوسط المرجح.

م	العبارة	دائما		أحيانا		نادرا		لا		المتوسط المرجح	الترتيب
		عدد	%	عدد	%	عدد	%	عدد	%		
١	سرعة الغاء البطاقة البنكية عند سرقتها أو سرقة بياناتها.	٣٩	٢٩,١	٢٣	١٧,٢	٥٨	٤٣,٣	١٤	١٠,٤	٣٥,٥	١
٢	اتمام العمليات المصرفية الإلكترونية من خلال أجهزة موثوق فيها.	١٨	١٣,٤	٥٢	٣٨,٨	٣٦	٢٦,٩	٢٨	٢٠,٩	٣٢,٨	٢
٣	عدم مشاركة بيانات البطاقات أو الحسابات البنكية إلا لمواقع موثوقة وللضرورة.	١١	٨,٢	٥٤	٤٠,٣	٢٦	١٩,٤	٤٣	٣٢,١	٣٠,١	٣
٤	إجراء التدقيق والمصادقة الإضافية للعمليات من خلال ربط الحساب البنكي برقم الهاتف.	١٢	٩	٣٤	٢٥,٤	٥١	٣٨,١	٣٧	٢٧,٦	٢٨,٩	٤
٥	عدم توفير معلومات تتخطى المعلومات الضرورية لإنجاز عملية الشراء عبر الانترنت.	٧	٥,٢	٤١	٣٠,٦	٣٥	٢٦,١	٥١	٣٨,١	٢٧,٢	٥
٦	التأكد من المراسلات المصرفية أنها من جهة صحيحة وآمنة.	٣	٢,٢	٤٣	٣٢,١	٤١	٣٠,٦	٤٧	٣٥,١	٢٧	٦
٧	تجنب إجراء العمليات المصرفية الإلكترونية في حال كنت متصلا بشبكة واي فاي عامة.	٧	٥,٢	٤١	٣٠,٦	٢٧	٢٠,١	٥٩	٤٤	٢٦,٤	٧
٨	تسجيل الخروج فور الانتهاء من استخدام الخدمات المصرفية عبر الإنترنت.	٩	٦,٧	٢٧	٢٠,١	٣٤	٢٥,٤	٦٤	٤٧,٨	٢٤,٩	٨
٩	تحديد سقف معين على بطاقات الائتمان للمبالغ المسموح سحبها أو الشراء بها في وقت واحد.	٤	٣	٣٠	٢٢,٤	١٥	١١,٢	٨٥	٦٣,٤	٢٢,١	٩

ثالثاً- اختبار معنوية الفروق في مستوى الأمن السيبراني ومحاوره وفقاً لنوع المبحوث:

لتحقيق الهدف الثالث من البحث والذي ينص على اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً لنوع المبحوث، تم صياغة الفرض الإحصائي الصفري التالي "لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لنوع المبحوث"، ولاختبار صحة هذا الفرض تم استخدام اختبار "T-Test" للفروق، وكانت النتائج كما يلي:

تشير نتائج جدول رقم (٨) إلى عدم وجود أي فروق معنوية إحصائية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لنوع المبحوث، وهو ما يشير إلى أنه لا توجد فروق معنوية بين الذكور والإناث في مستوى الأمن السيبراني سواء أمن الحسابات والتطبيقات أو أمن الأجهزة الإلكترونية أو أمن المعاملات المصرفية، وهو ما يتفق مع دراسة (اللبان وآخرون، ٢٠٢٣) انه لا توجد فروق ذات دلالة إحصائية بين استجابات المبحوثين عينة الدراسة عن التعرض للاختراق الالكتروني تعزى لمتغير النوع.

وعلى ذلك يتم رفض الفرض البديل وقبول الفرض الإحصائي الصفري الذي ينص على "لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لنوع المبحوث".

جدول ٨. نتائج اختبار معنوية الفروق في محاور الأمن السيبراني للمبحوثين وفقاً للنوع.

المحور	المتوسط الحسابي للذكور	المتوسط الحسابي للإناث	قيمة "t"
١- إجمالي الأمن السيبراني.	١٠٠,٦٩	٩٣,٠٧	١,٤٧٠
٢- الأمن السيبراني للحسابات والتطبيقات.	٥٦,٩٤	٥٢,٥٩	١,٤٣٨
٣- الأمن السيبراني للأجهزة الإلكترونية.	٢٣,٧٣	٢٢,٠٤	١,٣٩٢
٤- الأمن السيبراني للمعاملات المصرفية الالكترونية.	٢٠,٠٢	١٨,٤٥	١,٦١٦

ن=١٣٤

رابعاً- اختبار معنوية الفروق في مستوى الأمن السيبراني ومحاوره وفقاً لسن المبحوث:

لتحقيق الهدف الرابع من البحث والذي ينص على اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً لسن المبحوث، تم صياغة الفرض الإحصائي الصفري التالي "لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لسن المبحوث"، ولاختبار صحة هذا الفرض تم استخدام اختبار تحليل التباين أحادي الاتجاه " One Way ANOVA"، وكانت النتائج كما يلي:

تظهر نتائج جدول (٩) وجود فروق معنوية عند مستوى معنوية ٠,٠١ في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لسن المبحوث، وهذه الفروق لصالح الفئة السنية (٢٥-٣٦) سنة، ذات المتوسط الأعلى والذي بلغ ١٢٠,٤٨، ٦٨,٠٧، ٢٨,٦١، ٢٣,٨درجة على الترتيب، أي أن الأفراد الأصغر سناً لديهم مستوى أعلي من الأمن السيبراني وذلك في أمن الحسابات والتطبيقات، وأمن الأجهزة الإلكترونية، وأمن المعاملات المصرفية، وهو ما يتفق مع دارسة (Shahrom, 2024) أن المبحوثين من العاملين الأصغر سناً يكون مستوى الأمن السيبراني لديهم مرتفع إذا ما قورن بالعاملين الأكبر سناً.

وبناءً على ما سبق يتم قبول الفرض البديل ورفض الفرض الإحصائي الصفري الذي ينص على "لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لسن المبحوث"

جدول ٩. نتائج اختبار معنوية الفروق في محاور الأمن السيبراني للمبحوثين وفقاً لسن المبحوث.

المحور	المتوسط الحسابي للفئة السنية (٢٥-٣٦) سنة	المتوسط الحسابي للفئة السنية (٣٧-٤٨) سنة	المتوسط الحسابي للفئة السنية (٤٩-٥٩) سنة	قيمة "F"
١- إجمالي الأمن السيبراني.	١٢٠,٤٨	٨٧,٩٢	٧٣,٧٣	٤١,٣٩٣**
٢- الأمن السيبراني للحسابات والتطبيقات.	٦٨,٠٧	٤٩,٣٨	٤٢,٥٠	٣٥,٩٣٧**
٣- الأمن السيبراني للأجهزة الإلكترونية.	٢٨,٦١	٢٠,٨٩	١٦,٩٢	٤٧,٧٧٠**
٤- الأمن السيبراني للمعاملات المصرفية الألكترونية.	٢٣,٨	١٧,٦٦	١٤,٣١	٤٩,١٠٩**

ن = ١٣٤ ** مستوى دلالة ٠,٠١

خامساً- اختبار معنوية الفروق في مستوى الأمن السيبراني ومحاوره وفقاً للحالة الزواجية للمبحوث:

لتحقيق الهدف الخامس من البحث والذي ينص على اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً للحالة الزواجية للمبحوث، تم صياغة الفرض الإحصائي الصفري التالي "لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً للحالة الزواجية للمبحوث"، ولاختبار صحة هذا الفرض تم استخدام اختبار تحليل التباين أحادي الاتجاه "One Way ANOVA"، وكانت النتائج كما يلي:

تشير نتائج جدول رقم (١٠) إلى عدم وجود أي فروق معنوية إحصائية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً للحالة الزواجية للمبحوث، وهو ما يشير إلى أنه لا توجد فروق معنوية في مستوى الأمن السيبراني سواء أمن الحسابات والتطبيقات أو أمن الأجهزة الإلكترونية أو أمن المعاملات المصرفية وفقاً للحالة الزواجية للفرد سواء كان أعزب أو متزوج أو مطلق أو أرمل، وعلى ذلك يتم رفض الفرض البديل وقبول الفرض الإحصائي الصفري الذي ينص على "لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً للحالة الزواجية للمبحوث".

جدول ١٠. نتائج اختبار معنوية الفروق في محاور الأمن السيبراني للمبحوثين وفقاً للحالة الزواجية.

المحور	المتوسط الحسابي لفئة أعزب	المتوسط الحسابي لفئة متزوج	المتوسط الحسابي لفئة مطلق	المتوسط الحسابي لفئة أرمل	قيمة "F"
١- إجمالي الأمن السيبراني.	١٠١,٨٨	٩٩,٣	٩٨,١٤	٩٣,٦٦	٠,٤٩٣
٢- الأمن السيبراني للحسابات والتطبيقات.	٥٧,٦٥	٥٦,١	٥٥,٥	٥٢,٩٢	٠,٤٧٧
٣- الأمن السيبراني للأجهزة الإلكترونية.	٢٤,١٢	٢٣,٩	٢٣,١٤	٢٢,٠٩	٠,٥٩٣
٤- الأمن السيبراني للمعاملات المصرفية الالكترونية.	٢٠,١٢	١٩,٥	١٩,٣	١٨,٦٥	٠,٤٢١

ن = ١٣٤

سادساً- اختبار معنوية الفروق في مستوى الأمن السيبراني ومحاوره وفقاً لعدد أفراد أسرة المبحوث:

لتحقيق الهدف الخامس من البحث والذي ينص على اختبار معنوية الفروق في إجمالي مستوى الأمن السيبراني ومحاوره وفقاً لعدد أفراد أسرة المبحوث، تم صياغة الفرض الإحصائي الصفري التالي "لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لعدد أفراد أسرة المبحوث"، ولاختبار صحة هذا الفرض تم استخدام اختبار تحليل التباين أحادي الاتجاه "One Way ANOVA"، وكانت النتائج كما يلي:

تشير نتائج جدول رقم (١١) إلى عدم وجود أي فروق معنوية إحصائية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لعدد أفراد أسرة المبحوث، وهو ما يشير إلى أنه لا توجد فروق معنوية في مستوى الأمن السيبراني سواء أمن الحسابات والتطبيقات أو أمن الأجهزة الإلكترونية أو أمن المعاملات المصرفية وفقاً لاختلاف حجم الأسرة سواء كانت الأسرة كبيرة أو صغيرة، وهو ما يتفق مع دراسة (اللبان وآخرون، ٢٠٢٣) بعدم وجود فروق معنوية في درجة التعرض للاختراق الالكتروني وفقاً لعدد أفراد الأسرة.

وعلى ذلك يتم رفض الفرض البديل وقبول الفرض الإحصائي الصفري الذي ينص على "لا توجد فروق معنوية في إجمالي مستوى الأمن السيبراني ومحاوره (الأمن السيبراني للحسابات والتطبيقات، الأمن السيبراني للأجهزة الإلكترونية، الأمن السيبراني للمعاملات المصرفية الالكترونية) وفقاً لعدد أفراد أسرة المبحوث".

جدول ١١. نتائج اختبار معنوية الفروق في محاور الأمن السيبراني للمبحوثين وفقاً لعدد أفراد الأسرة.

المحور	المتوسط الحسابي لفئة (٢-٣) فرد	المتوسط الحسابي لفئة (٤-٦) فرد	المتوسط الحسابي لفئة (٧-٨) فرد	قيمة "F"
١- إجمالي الأمن السيبراني.	١٠٠,٠٦	٩٩,٧٩	٩١,٤٢	١,٤٤٠
٢- الأمن السيبراني للحسابات والتطبيقات.	٥٦,٣٧	٥٦,٢٢	٥١,٨٦	١,١٥٣
٣- الأمن السيبراني للأجهزة الإلكترونية.	٢٣,٨٨	٢٣,٤٧	٢١,٥٦	١,٦١٨
٤- الأمن السيبراني للمعاملات المصرفية الالكترونية.	١٩,٩٧	١٩,٩٥	١٨	٢,١٨٥

ن = ١٣٤

توصيات البحث:

وفقاً للعرض السابق للنتائج يمكن أن توصي الدراسة بمجموعة توصيات كما يلي:

أولاً- توصيات تتعلق بالأمن السيبراني للحسابات والتطبيقات:

1- ضرورة قيام وزارة الاتصالات وتكنولوجيا المعلومات بالتعاون مع مؤسسات القطاع الحكومي بتقديم دورات تدريبية تهدف إلى تحسين قدرة العاملين في حماية حساباتهم ومعلوماتهم الإلكترونية، مع الاهتمام بصفة خاصة بالفئات الأكبر سناً.

2- التأكيد على أهمية عدم تحميل أي تطبيقات إلا من المتاجر الرسمية، والبعد عن التطبيقات المهكرة أو غير معلومة المصدر.

3- ضرورة قيام مؤسسات القطاع الحكومي بزيادة وعي العاملين به بأهمية تجنب استخدام نفس كلمات المرور للحسابات المختلفة وتغييرها بشكل دوري، والبعد عن استخدام المعلومات الشخصية فيها، والخروج من الحسابات عند الانتهاء من استخدامها.

ثانياً- توصيات تتعلق بالأمن السيبراني للأجهزة الإلكترونية:

1- ضرورة زيادة وعي العاملين بالقطاع الحكومي بممارسات حماية الأجهزة الإلكترونية، عدم إعطاء اذونات للتطبيقات تسمح باختراق بيانات الأجهزة، أو بيانات خاصة، الحرص على الاحتفاظ بنسخ احتياطية من بيانات الجهاز على وحدات تخزين صلبة أو سحابية.

2- ضرورة استخدام الأجهزة الإلكترونية لشبكات موثوقة للاتصال بالإنترنت، وإغلاق كافة وسائل اتصال الجهاز عند عدم استخدامها.

3- أهمية تحميل وتفعيل برامج لحماية الأجهزة الإلكترونية من الفيروسات والبرامج الخبيثة، أن تكون محدثة دائماً، وأن يتم تحميلها من مواقعها الرسمية.

ثالثاً- توصيات تتعلق بالأمن السيبراني للمعاملات المصرفية الالكترونية:

1- ضرورة قيام المؤسسات الحكومية بالتعاون مع اتحاد بنوك مصر بتقديم دورات تدريبية للعاملين بغرض رفع مستوى معرفتهم وتنفيذهم لممارسات حماية حساباتهم ومعاملاتهم المصرفية الإلكترونية، وكيفية اكتشاف عمليات الاحتيال في المعاملات المصرفية الإلكترونية.

2- ضرورة وضع قيمة محددة للمبالغ المسموح سحبها أو الشراء بها في نفس الوقت، وربط تلك العمليات بإذن من رقم هاتف محمول خاص.

3- عدم إعطاء أي بيانات مصرفية لأي جهة، أو الشراء عبر الإنترنت من مواقع غير موثوقة، والخروج من الحساب بعد الانتهاء من عمليات الشراء.

المراجع

احليل، كريم (٢٠٢٤). الأمن السيبراني، المجلة الإلكترونية الدولية، مجلد ٤، عدد (١٨)، المغرب.

الإنتربول (٢٠٢٣). تقرير الجريمة السيبرية، تقرير سنوي.

القريطي، دحان حزام (٢٠٢٢). الأمن السيبراني وحماية المعلومات، دار الفكر الجامعي، الإسكندرية، مصر.

اللبان، شريف درويش، صقر، غادة موسى إبراهيم، عوف، مروة محمد، الحضري، ياسمين محمد كمال (٢٠٢٣). تعرض الشباب الجامعي للجرائم الالكترونية عبر مواقع التواصل الاجتماعي ومستوى الوعي بخطورتها، المجلة العلمية لكلية التربية النوعية، جامعة دمياط، عدد (٨)، ص ص ١١٩-١٤٥، مصر.

المجلس الأعلى للأمن السيبراني (٢٠٢٤). الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٣-٢٠٢٧، رئاسة مجلس الوزراء، مصر.

المري، راشد محمد (٢٠٢٣). الأمن السيبراني وحماية الأنظمة الإلكترونية دراسة تحليلية تأصيلية، مجلة الدراسات القانونية والاقتصادية، مجلد ٩، عدد (١)، ص ص ٩٥٩-١٠٠٨.

الهيئة العامة للاستعلامات (٢٠٢٣). ملفات أمنية، بيان اعلامي، المركز الإعلامي، مصر.

جيدنز، أنتونى (٢٠٠٠). قواعد جديدة للمنهج في علم الاجتماع، ترجمة محمد محى الدين، المجلس الأعلى للثقافة، مصر.

زقوت، نشوه إسماعيل، السائح، سناء أحمد، العطاب، الصديق عبد القادر (٢٠٢٢). مدى وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي: دراسة تطبيقية بجامعة الزاوية، المؤتمر العلمي الأول لتقنية المعلومات وعلوم الحاسب، كلية تقنية المعلومات، جامعة الزاوية، ٢١-٢٢/٢/٢٠٢٢، ليبيا.

سراج، شيماء أحمد محمد أحمد (٢٠٢٢). التحليل البعدي لدراسات الأمن السيبراني في المجال التربوي، المجلة العربية للعلوم التربوية والنفسية، المؤسسة العربية للتربية والعلوم والآداب، مجلد ٦، عدد (٢٦)، مصر.

سلامة، نسرين سيد (٢٠٢٣). الجرائم الالكترونية وأثرها على المجتمع، مجلة القاهرة للخدمة الاجتماعية، عدد (٣٩)، مصر.

طالة، لامية (٢٠٢٠). التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، مجلة معالم للدراسات القانونية والسياسية، مجلد ٢، عدد (٤)، الجزائر.

عبد الجواد، نجوان أحمد عاصم (٢٠٢٣). الجريمة السيبرانية وتأثيرها على الأمن القومي المصري: دراسة سوسيو تحليلية، مجلة كلية الآداب، جامعة الفيوم، مجلد ١٥، عدد (١)، ص ص ٢٠٨٣-٢١٤٩، مصر.

فرحان، علاء الدين (٢٠٢١). من الردع النووي إلى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني، مجلة الفكر، جامعة بسكرة، مجلد ١٦، عدد (١)، الجزائر.

لجنة دراسة المخاطر السيبرانية (٢٠٢٠). دليل التوعية حول المخاطر السيبرانية، شعبة العلاقات العامة، قوى الأمن الداخلي، لبنان.

لطفي، طلعت إبراهيم وكمال عبد الحميد الزيات (١٩٩٩). النظرية المعاصرة في علم الاجتماع، دار غريب للطباعة والنشر والتوزيع، القاهرة.

مركز المعلومات ودعم اتخاذ القرار (٢٠٢٤). سبعة اتجاهات للأمن السيبراني في عام ٢٠٢٤، نشرة الكترونية، رئاسة مجلس الوزراء، مصر.

Adil Rasool (2017). Crimes and Laws Related to Internet users: an Overview, SSRG International Journal of Economics and Management Studies, 4(3), pp. 6-10.

Akhgar, B., Staniforth, A., Bosco, F. (2014) Cyber Crime and Cyber Terrorism Investigator's HandbooK, Elsevier.

Beck, U. (1992) Risk Society: Towards a New Modernity, translated by Mark Ritter, SAGE Publications, London.

CAPMAS (2023). Annual Bulletin of Labour Force 2022, Egypt.

Chen, S., Hao, M., Ding, F., Jiang, D. (2023). Exploring the global geography of cybercrime and its driving forces, Humanities and Social Sciences Communications, 10(1), pp 1-10.

Datareportal (2024). Digital 2024: Egypt, Simon Kemp, 23 February.

Mahabi, V. (2010) Information Security Awareness: System Administrators and End-User Perspectives at Florida State University, degree doctor of philosophy, Florida State University.

Martinez, D. (2013). Privacy and Confidentiality issues in Cloud Computing architectures, Master, Polytechnic University, Catalonia, Spain.

Nehme, A., Warkentin, M. (2022). "A Preliminary Look at Information Security through a Social Practice Theory Lens, MWAIS 2022 Proceedings.

NIST (2018). A Glossary of key information security terms National institute of standards and technology interagency or internal report, Revision 2.

Ramirez, M., Ariza, L., Miranda, M. (2022). The disclosure of information on security in listed companies in Latin America- proposal for a cyber-security disclosure index, journal of sustainability, 14(3), pp 1390-1403.

Shahrom M. (2024). Cyber Security Challenges Faced by Employees in the Digital Workplace, The African Journal of Information Systems, 15(3), pp 305-319.

Cybersecurity for Government Sector Employees in the Rural Areas of Sharkia Governorate

Laban, Kh. A. A.

Agric. Economic Dept., Branch of Rural Sociol., Fac. Agric., Zagazig Univ., Egypt

ABSTRACT

The study aimed to: Identify the level of cybersecurity and its dimensions (cybersecurity of accounts and applications, cybersecurity of electronic devices, cybersecurity of electronic banking transactions) for the employees in the government sector, and to identify the relative importance of cybersecurity practices for the employees in the government sector, Test the significance of differences for cybersecurity divide according to the variables (sex, age, marital status, and The number of family members). The study was conducted in the rural areas of Sharkia Governorate, based on the social survey approach, and the total number of respondents reached 134. This study resulted: the level of cybersecurity for the majority of respondents was low, with percentages of 41.8%. There are significant differences at a significance level of

0.01 in the total level of cybersecurity and its dimensions (cybersecurity of accounts and applications, cybersecurity of electronic devices, cybersecurity of electronic banking transactions) according to the age of the respondent, that is due to the age group (25-36) years, which has the highest average, that reached 120.48, 68.07, 28.61, and 23.8 degrees, respectively.

***Keywords*:** Cybersecurity; Electronic accounts and devices Protection; Banking transactions Protection.