"إدراك مُستخدمي مواقع التَّواصل الاجتماعي لأهميَّة الأمن السيبراني ودوره في الأمن المعلوماتي

دِرَاسَةِ ميدانية"

د. آيَةُ طَارِقَ عَبْدُ الهَادِي سِيدَ*

الملخص:

تَمَثَّلَتْ مُشْكِلَةُ الدِّرَاسَةِ فِي "الحاجة إلى دِرَاسَةِ العلاقة بين استخدام مواقع التَّواصل الاجتماعي والوعي بأهميَّة الأمن السيبراني... وإدراكهم لدوره في الحفاظ على أمن المعلومات الخاصة بهم"، ولذلك تَتَمَحْوَرُ أَهْدَافُ الدِّرَاسَةِ حول هدف رئيسي وهو "الكشف عن العلاقة بين استخدام مواقع التَّواصل الاجتماعي وإدراك أهميَّة الأمن السيبراني ودوره في الأمن المعلوماتي"، وقد اِعْتَمَدْتُ البَاحِثَةَ فِي هَذِهِ الدِّرَاسَةُ على عينة عمدية قوامها (440 مُفردة) من مُستخدمي مواقع التَّواصل الاجتماعي من مختلف الأعمار والمُستويات (التعليمية، الاقتصادية، الاجتماعية).

نتائج الدراسة:

- ظهر أن أغلبية مُستخدمي مواقع التَّواصل الاجتماعي (عينة الدِرَاسَةِ) يتراوحون بين أنهم يدركون الأمن السيبراني وطرق المُحافظة على نظامه بدرجة مُتوسطة ومُرتفعة.
- أغلبية مُستخدمي مواقع التَّواصل الاجتماعي (عينة الدِرَاسَةِ) يتراوحون بين أنهم يدركون مخاطر الأمن السيبراني وانتهاكاته بدرجة مُرتفعة ومتوسطة.
- هناك علاقة ارتباطية دالة إحصائيًا بين مُعدلات استخدام مواقع التَّواصل الاجتماعي والمتغيرات التالية: (دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).
- هناك علاقة ارتباطية دالة إحصائيًا بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني وإدراكهم لطرق المحافظة على نظامه ومخاطره وانتهاكاته، وأن هناك علاقة ارتباطية دالة إحصائيًا بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني وإدراكهم لمخاطره وانتهاكاته، وأن هناك علاقة ارتباطية دالة إحصائيًا بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني وإدراكهم لانتهاكات الأمن السيبراني.

* دكتوراه في الإعلام من قسم الإذاعة والتليفزيون بكلية الإعلام - جامعة القاهرة

The Perecption of Social Media Users of Cyber Security and Its Role IN Information Security: Field Study

Dr. Aya Tarek

Abstract

- The problem of studying was represented in the need to study the relationship between using the social media and perception of the importance of cyber security and consciousness of its role of maintaining of security their privacy information security. The objectives of the study revolve around a main goal, which is "to reveal the relationship between the use of social networking sites and the perception of the importance of cyber security and its role in information security. A set of sub_ goals is emerged from this target and this goals is (the Recognition of the rates of using of social media and its motivates, knowing the extent of perception of users the social network sites of cyber security, its risks and violations, and Detection of the degree of the perception of the users of social media in ways to maintain cyber security system).
- The researcher in this study depend on quantitative survey method using the online questionnaire form (Electronic questionnaire) as tool to collect data intentional sample (440 individual) from the users of social media of different ages and levels (educational, economical, social) as well as the researcher based on theoretical framework of the study Public Sphere theory in order to reveal the relationship between the users of social media and the perception of the importance of cyber security and its role in information security. so the social media provide field in dialogues and discussion on various topics which create a kind of public field thus shapes individuals' perception about this topic.
- The study found that: The majority of users of the social media (the study sample) ranges between that they percept the cyber security and the ways to maintain its system with high and medium degree, The majority of users of social media (the study sample) its ranges between that they percept the risks of cyber security and its violation with high and medium degree, There is a statistically significant correlation between the rates of using of social media and the following variables: (the motivates of using the social media/ perception of users of social

media of cyber security/ perception of users of social networking sites of ways to maintain the cyber security system/ perception of users of social networking sites of cyber security risks/ perception of users of social media of cyber security violations), that There is a statistically significant correlation between users of social media sites' perception of cyber security and their perception of ways to maintain its system, its risks and violations, that There is a statistically significant correlation between users of social media sites' perception of ways to maintain the cyber security system and their perception of its risks and violations, that that There is a statistically significant correlation between the perception of social media users of cyber security risks and their perception of cyber security violations.

مُقَدِّمَةً:

أدت الثورة الرقمية المُعاصرة إلى إيجاد أفاق غير مسبوقة للتَّواصل وتبادل المعلومات والأفكار والآراء بين ملايين المُستخدمين لشبكة الإنترنت حول العالم وانعكس هذا الأمر على كافة مجالات النشاط الإنساني، ومع انتشار الهواتف الذكية والأجهزة المحمولة، فقد أصبح استخدام شبكة الإنترنت أمرًا متاحًا لجميع أفراد المجتمع على اختلاف فئاتهم العمرية، وأهداف هذا الاستخدام. وعلى الجانب الآخر، ومع التدفق المُستمر والهائل للمعلومات، واعتماد الملايين حول العالم من أفراد ومؤسسات خاصة وحكومية على استخدام شبكة الإنترنت للتَّواصل الاجتماعي أو إنجاز العديد من المعاملات، فقد ظهر تهديد جديد لهؤلاء المُستخدمين، حيث اتجه البعض إلى اختراق شبكات المعلومات، والتلاعب بالمعلومات وإيذاء المُستخدمين بأساليب مُتعددة، وذلك فيما يعرف بالجريمة السيبرانية Cyber Crime.

لذلك قد أصبح الأمن السيبراني حديث العالم بأسره، بل وأصبح جزءًا أساسيًا من أي سياسات أمنية أو اقتصادية أو سياسية أخرى، حيث أصبح صناع القرار في مختلف الدول يضعون مسائل الأمن السيبراني كأولوية في سياستهم.

وعليه فإن البحث في مدى إدراك مُستخدمي مواقع التَّواصل الاجتماعي لأهميَّة الأمن السيبراني ودوره في الأمن المعلوماتي له مبرراته في ظل الاهتمام الدولي بتعزيز الأمن السيبراني في ظل الثورة الرقمية والمعلوماتية المُعاصرة، وذلك لمواجهة الجرائم السيبرانية التي تُشكل تهديدًا جديًا لكافة فئات المجتمع، والمقدرات الاقتصادية والمادية لكافة دول العالم.

مُشْكِلَةُ الدِرَاسَةِ:

يُعتبر الأمن الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور نمو أي نشاط بعيدًا عن تحققه، سواء كان ذلك على المُستوى التقني أو القانوني، وقد تحول الأمن – مع بروز مجتمع المعلومات والفضاء السيبراني – إلى واحد من قطاع الخدمات التي تشكل قيمة مُضافة ودعامة أساسية لأنشطة الحكومات والأفراد على السواء، كما هي الحال مع التطبيقات الخاصة بـــــ (الحكومة الإلكترونية، والصحة الإلكترونية، والتعليم عن بعد، والتجارة الإلكترونية.... وغيرها)، إلا أن الوجوه المُتعددة لجرائم الفضاء السيبراني، ومضاعفاتها الخطيرة التي لا تقف عند حدود الإساءة إلى الأفراد والمؤسسات بل تتعداها إلى تعريض سلامة الدول والحكومات، ولهذا تصبح مهمة القائمين علية أكثر تعقيدًا وصعوبة لمواجهة التحديات التي يطرحها الفضاء السيبراني، فتحقيق الأمن وبناء الثقة في الفضاء السيبراني من أساسيات تسخير تقنيات المعلومات والاتصالات في مجالات التنمية لخدمة المجتمعات الإنسانية [1].

فقد اتجهت العديد من الدول المُتقدمة إلى تبني مُبادرات هادفة إلى توفير الأمن السيبراني لجميع مُستخدمي الإنترنت، ومنها (مبادرة دول الاتحاد الأوروبي لوضع مبادئ الاستخدام الآمن لشبكات المعلومات، والإطار الأوروبي للاستخدام الآمن للأجهزة المحمولة)، وفي عام 2009 تم إدراج مفاهيم الأمن السيبراني ضمن المناهج الدراسية في 24 دولة أوروبية، وفي الولايات المُتحدة تولت وزارة الأمن الداخلي مسؤولية تعزيز ونشر الوعي بالأمن السيبراني، وفي إطار هذا الاهتمام تم تأسيس التحالف الوطني للآمن السيبراني [2]. كما أطلقت الحكومة الأمريكية المبادرة الوطنية للتربية السيبرانية National Initiative for Cyber Security Education (NICE)، وقد جاءت هذه المُبادرة نتيجة للتعاون بين وزارة الأمن الداخلي والمعهد القومي للمعايير التكنولوجيا National Institute for Standrads and Technology (NIST) بهدف إعداد قوى عاملة في مجال الأمن السيبراني [3].

وكذلك سعت بعض الدول النامية إلى اتخاذ إجراءات مماثلة لضمان الأمن السيبراني، وقد واجهت تلك الدول بعض المُشكلات تتمثل في عدم وجود مبادرة شاملة للأمن السيبراني، ونقص الدعم الكافي، وعدم وجود مبادرات تعليمية قادرة على مواكبة التطورات الحاصلة في مجال الاتصالات وتكنولوجيا المعلومات، وقد انعكس هذا الأمر في تراجع مُستوى الأمن السيبراني لدى مُستخدمي شبكات الإنترنت وشبكات التَّواصل الاجتماعي في تلك الدول، مما جعلهم أكثر عرضه للهجمات والجرائم السيبرانية [4].

وبناء على ذلك فقد حددت الباحثة مُشكلة الدِرَاسَةِ في **"الحاجة إلى دِرَاسَةِ العلاقة بين استخدام مواقع التَّواصل الاجتماعي والوعي بأهميَّة الأمن السيبراني... وإدراكهم لدوره في الحفاظ على أمن المعلومات الخاصة بهم"**.

أَهْدَافُ الدِرَاسَةِ:

تسعي الدِرَاسَةِ إلي تحقيق هدف رئيسي وهو **"الكشف عن العلاقة بين استخدام مواقع التَّواصل الاجتماعي وإدراك أهميَّة الأمن السيبراني ودوره في الأمن المعلوماتي"**، وينبثق من هذا الهدف عددً مِن الأهداف الفرعية يُمكن إجمالها علي النَّحو التَّالي:

- التعرف على مُعدلات استخدام مواقع التَّواصل الاجتماعي ودوافعه.
- معرفة مدى إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني ومخاطره وانتهاكاته.
- الكشف عن درجة إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني.

أهميَّة الدِرَاسَةِ:

إن أهميَّة التعرف على مدى إدراك مُستخدمي مواقع التَّواصل الاجتماعي لأهميَّة الأمن السيبراني ودوره في الأمن المعلوماتي، تنبع من أمرين وهما:

1) **أهميَّة علمية تتمثل في النقاط التَّالية:**

- هذه الدِرَاسَةِ تُعد من الدِرَاسَاتُ العربية القليلة في مجال الأمن السيبراني، والتي يُمكن أن تُثري الإنتاج الفكري في هذا المجال.
- تسليط الضوء على أهميَّة الأمن السيبراني ودوره الحيوي والهام في الأمن المعلوماتي.
- إتاحة الفرصة للباحثين للاستفادة من هذه الدِرَاسَةِ في توسيع دائرة دِرَاسَةِ أهميَّة الأمن السيبراني ليشمل كافة فئات المُجتمع.
- تزويد المكتبة العربية بإطار نظري وتطبيقي عن مفهوم الأمن السيبراني وأهميته وأبعاده.
- توعية مُستخدمي مواقع التَّواصل الاجتماعي بأهميَّة الأمن السيبراني في الحفاظ على معلوماتهم الشخصية.

2) **أهميَّة عملية وتتمثل في التَّالي:**

من خلال نتائج هذه الدِرَاسَةِ يُمكننا الإلمام بالأمن السيبراني كركن حيوي ليس فقط على الصعيد الشخصي للفرد والمجتمع بل مهم لأمن الدولة، مما يُمكن مُتخذي القرار في مؤسسات الدولة بإعداد برامج توعية للأفراد ودورات تدريبية لإدراك أهميَّة الأمن السيبراني.

الدِّرَاسَاتُ السَّابقةُ:

تُمثل الدِّرَاسَاتُ السَّابقة الإطار المرجعي الأساسي لمُشكلة الدِرَاسَةِ، لذا فهي تحظي بأهميَّة لإسهامها في تحديد معالم المُشكلة البحثية وبيدو ضروريًا في هذا الشأن الإشارة إلى بعض الدِّرَاسَاتُ المهمة التي التقت من حيث موضوعيتها البحثية أو خياراتها المنهجية مع دراستنا الحالية.

فمما لاشك فيه أن الأمن السيبراني أصبح مهيمنًا على عرش البحوث والدِّرَاسَاتُ، وذلك لظهور الاهتمام الدولي بتعزيز الأمن السيبراني في ظل الثورة الرقمية والمعلوماتية المعاصر، بهدف التخفيف من مخاطر اختراق المعلومات والهجمات الإلكترونية، وأيضًا بهدف حماية وتأمين البيانات والمعلومات الشخصية التي يتم تداولها عبر شبكة الإنترنت. ولذلك ستقوم الباحثة فيما يلي بعرض الدِّرَاسَاتُ التي تناولت الأمن السيبراني من زوايا ومُتغيرات مُختلفة.

فمن منظور **درجة الوعي بالأمن السيبراني لدى فئات مُعينة** وعلاقة هذا الوعي بالقيم لدي هذه الفئات وأساليب حماية معلوماتهم، نجد **دِرَاسَةِ (فاطمة يوسف المنتشري، رندة حريري ، 2020)** (5) والتي أظهرت أن معلمات المرحلة المُتوسطة على درجة مُتوسطة من الوعي بكل من مفاهيم الأمن السيبراني، ومخاطر الأمن السيبراني، وانتهاكات الأمن السيبراني، وأنه لا يوجد فروق ذات دلالة إحصائية عند مُستوى (0,05) وتُعزى إلى مُتغيري المؤهل الدراسي وعدد سنوات الخبرة بين استجابات المعلمات، وأنه يوجد فروق ذات دلالة إحصائية عند دلالة (0,05) تُعزى إلى مُتغير دورات تدريب الأمن السيبراني.

أما **دِرَاسَةِ (حمد بن حمود بن حميد السواط، وآخرون ، 2020)** (6) فقد توصلت إلى أن درجة الوعي بالأمن السيبراني لدى التلاميذ مُرتفعة بدرجة كبيرة جدًا في مجال التعامل الآمن مع خدمات تصفح الإنترنت لدى تلاميذ المرحلتين الابتدائية والمُتوسطة بمدينة الطائف كما أن القيم الوطنية والأخلاقية والدينية مُتوفرة لديهم بدرجة عالية جدًا، وأن هناك علاقة قوية بين الوعي بالأمن السيبراني والقيم لدى أفراد العينة وقد اتضح إمكانية التنبؤ بالقيم الوطنية والأخلاقية والدينية من خلال الوعي بالأمن السيبراني، وأن هناك فروق في معرفة التلاميذ بالأمن السيبراني والقيم تُعزى لمتغير المرحلة الدراسية ولصالح أفراد المرحلة الابتدائية وكذلك في متغير دخل الأسرة ولصالح الدخل العالي، وأخيرًا أنه لا توجد فروق ذات دلالة إحصائية في مُتغير الجنس (ذكر/أنثى) ونوع المدرسة (حكومية/لغات).

وكذلك أفادت **دِرَاسَةِ (نورة عمر الصانع، وآخرون ، 2020)** (7) بارتفاع وعي المعلمين بالأمن السيبراني في مجال حماية الأجهزة الخاصة والمحمولة من مخاطر الاختراق الإلكتروني والهجمات السيبرانية، وفي درجة استخدامهم لأساليب حماية

الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية بمدينة الطائف من وجهة نظرهم في مجالات الأهداف الدراسية، وطرق التدريس، والأنشطة والمشاريع، وأساليب التقويم، كما ووجدت علاقة ارتباطية موجبة ومُتوسطة بين وعي المعلمين بالأمن السيبراني واستخدامهم لأساليب حماية الطلبة من مخاطر الإنترنت، ولأساليب تعزيز القيم والهوية الوطنية .

كما أوضحت **دِرَاسَةِ (وفاء بنت حسن عبد الوهاب صائغ ، 2018)** [8] أن هناك علاقة ذات دلالة إحصائية بين وعي أفراد الأسرة بمفهوم الأمن السيبراني وبين الاحتياطات الأمنية التي يتخذونها للوقاية من الجرائم الالكترونية، بينما لم توجد فروق ذات دلالة إحصائية في درجة وعي أفراد الأسرة بمفهوم الأمن السيبراني وبين مُتغير النوع أو مُتغير العمل أو العمر، في حين وجدت فروق دالة إحصائيًا بين وعي أفراد الأسرة بمفهوم الأمن السيبراني وبين دخل الأسرة.

بينما بينت **دِرَاسَةِ (مصباح أحمد حامد الصحفي، سناء صالح عسكول، 2019)** [9] وجود ضعف وقصور لدى معلمات الحاسب الآلي في الوعي بمفاهيم الأمن السيبراني، ووجود ضعف لدى معلمات الحاسب الآلي في الوعي بمُستوى الأمن السيبراني، وعدم وجود فروق ذات دلالة إحصائية بين مُتوسطات استجابات المبحوثين (عينة الدِرَاسَةِ) عند مُستوى الدلالة (0,05) في درجة وعي معلمات الحاسب بالأمن السيبراني تُعزى لمتغيرات الدِرَاسَةِ الحالية (سنوات الخبرة، المؤهل العلمي، الدورات التدريبية).

وكذلك أفادت نتائج **دِرَاسَةِ (Elmarie Kritzinger , 2017)** [10] بوجود نقص كبير في الوعي بالأمن السيبراني والذي من خلاله حثت الدراسة على ضرورة توعية وتثقيف الطلبة بالتهديدات المُتعلقة بالتكنولوجيا لضمان معرفتهم واكتسابهم للمهارات المطلوبة للتعامل مع مواقف الحياة، وتبين أن هذا النقص سببه قلة المحتوى في المناهج الدراسية، والتي يجب أن يكون لها دورًا في التوعية والتثقيف، لذلك حثت الدِرَاسَةِ على التنمية المُستدامة بين البيئة المدرسية والأمن السيبراني.

في حين أشارت **دِرَاسَةِ (نورة بنت ناصر القحطاني ، 2019)** [11] إلى أن أقرب مفهوم للأمن السيبراني من وجهة نظر (عينة الدِرَاسَةِ) هو "استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعاملات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها"، في حين جاءت جريمة "الاحتيال الإلكتروني/النصب الإلكتروني" كأكثر جريمة يتعامل معها الأمن السيبراني؛ في حين تعتبر التوعية الإعلامية للمجتمع حول طرقه هي أهم طرق الوقاية المجتمعية لمُشكلات الفضاء السيبراني، كما جاءت النتائج بوجود معوقات اجتماعية له في تحقيق الوقاية للمجتمع السعودي، وأن أهم هذه

المعوقات هو التطور الهائل في نظم المعلومات، ووسائل التكنولوجيا التي يتعامل معها أفراد الأسرة دون المعرفة الكاملة لمُشكلات هذه الوسائل وكيفية تجنبها.

وهناك منظور أخر تتطرقت إليه الدِّرَاسَاتُ وهو **دور القادة والمؤسسات في تعزيز الأمن السيبراني**، فنجد **دِرَاسَةِ (فاطمة يوسف المنتشري، 2020)** [12] والتي أوضحت أن دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلومات ولدى طالبات المدرسة يتحقق بدرجة موافقة قليلة من وجهة نظر المعلمات.

وأيضًا أظهرت نتائج **دِرَاسَةِ (Lauren K. Mark, Thanh Truc T. Nguyen, 2017)** [13] أهميَّة التوعية بالأمن السيبراني من وجهة نظر المبحوثين، وضرورة التعاون بين المنزل والمدرسة لتوفير بيئة إنترنت أكثر أمانًا للطلبة، كما أنها أظهرت الدور الهام للمعلمين ومديري المدارس في تعزيز الأمن السيبراني.

بينما أفادت نتائج **دِرَاسَةِ (Arjen Spiering , 2013)** [14] بوجود أكثر من (20 مُشكلة) ناتجة عن نقص الوعي بالأمن السيبراني ومنها (تعرض الطلبة لحالات الاستمالة، والتحرش الجنسي، والتنمر الإلكتروني، وبث مُحتوى غير أخلاقي، والتهديدات المُختلفة، والإيذاء الجسدي)، وقد أرجع أفراد العينة تلك المُشكلات إلى عاملين رئيسين وهما (غياب رؤية واضحة للتوعية بالأمن السيبراني، وندرة عدد المعلمين المختصين في مجال الأمن السيبراني).

وهناك دراسات تتطرقت إلى **الجانب القانوني للأمن السيبراني**، فنجد **دِرَاسَةِ (ماجدة غريب، حسن الأمير ، 2017)** [15] والتي توصلت إلى أن نصف أفراد العينة لديهم وعي بالممارسات غير الشرعية عند استخدام الأجهزة الإلكترونية، وأن معرفة الأنظمة والعقوبات الخاصة بمُكافحة الجرائم المعلوماتية كان لها دور كبير في الحد من الممارسات السلبية في تقنيات المعلومات.

وأخيرًا هناك دراسات تناولت الأمن السيبراني من منظور آخر وهو **الأمن السيبراني ومشكلاته على مواقع التَّواصل الاجتماعي والحلول المُقترحة للحفاظ على المعلومات**، فنجد **دِرَاسَةِ (Rituparna Das, Mayank Patel , 2017)** [16] والتي أوضحت أن مع تزايد شعبية مواقع التَّواصل الاجتماعي، حيث أصبحت هذه المواقع هدفًا رئيسيًا للجرائم والهجمات الإلكترونية. وأصبحت الجريمة الإلكترونية منتشرة على نطاق واسع وتشكل تهديدًا كبيرًا للأمن القومي والاقتصادي مما يؤدي إلى تعرض المؤسسات العامة والخاصة في قطاعات الصحة العامة والمعلومات والاتصالات والدفاع والمصارف والتمويل للخطر. لذلك يجب على المؤسسات اتخاذ تدابير أمنية مناسبة لتكون آمنة من الجرائم الإلكترونية ويجب على المُستخدمين حماية معلوماتهم الشخصية لتجنب سرقة الهوية أو إساءة الاستخدام، فقد أصبح الفضاء الإلكتروني مجالًا مهمًا للجرائم الإلكترونية والإرهابيين للهجوم على المعلومات

المهمة. لذلك، هناك حاجة إلى تعاون عالمي بين الدول للعمل معًا للحد من التهديد السيبراني المتزايد باستمرار.

التَّعْلِيقُ عَلَى الدِّرَاسَاتُ السَّابقةُ والاستفادة منها:

من المُلاحظ تركيز معظم الدِّرَاسَاتُ السَّابقة التي تم عرضها على التعرف على درجة الوعي بالأمن السيبراني لفئات مُحددة من المُجتمع، والوعي يقتصر على المعرفة العامة بالأمن السيبراني، ولذلك سعت الباحثة في هذه الدِرَاسَةِ لدرسة ما هو أبعد من الوعي بالأمن السيبراني حيث أنها هدفت إلى قياس مدى الإدراك، وهناك جزء من الدِّرَاسَاتُ السَّابقة كانت تهدف للتعرف على الوعي بمخاطر الإنترنت، لهذا كانت الفئة التي اختارتها الباحثة للدِرَاسَةِ هي فئة مُستخدمي مواقع التَّواصل الاجتماعي لتعرف على مدى إدراكهم لمخاطر وانتهاكات الأمن السيبراني.

الإطار النظري للدِرَاسَةِ (نظرية المجال العام public sphere):

أثار العالم الألماني غورين هابرماس Jurgen Habermas المناقشات العلمية حول فكرة "المجال العام Public Sphere" والتي صاغ مفهومها الفيلسوف الألماني (كانط) من خلال نشر كتابه "التحول البنائي للمجال العام Structural Transformation of the Public Sphere" وذلك عام 1989، وكان قد سبق نشر هذا الكتاب باللغة الألمانية عام 1961، ولكن ذيوع المفهوم وانتشاره ارتبط بالترجمة الإنجليزية التي صدرت عام 1989 (17).

ومن ثم أصبح مصطلح المجال العام للفليسوف الألماني غورين هابرماس Jurgen Habermas من أكثر المفاهيم تداولاً في مجال الدِّرَاسَاتُ الإعلامية في العقد الأخير، والذي يُعد ركيزة أساسية للمجتمعات الديموقراطية، حيث يفترض أن فكرة التَّواصل هي توصيف دقيق للديمقراطية باعتبارها التشكيل الحر للإرادة الشعبية، والتي نراها عبر وسائل التَّواصل المُختلفة التي تقود إلى الحوار من دون إكراه وتسلط، بل من خلال التفاهم المُستمر بين (الأنا والآخر) دون اللجوء إلى العنف، وهو ما يعمل على تكوين مجال عام يعتبره غورين هابرماس Jurgen Habermas صمام الديمقراطية الذي يكون دائرة التوسط بين المجتمع المدني والدولة (18).

ولقد حدد "هابرماس" ثلاث معايير مؤسسية يُمكن أن تعمل كشروط للمجال العام وهي على النحو التَّالي:

- **تجاهل المكانة Disregard of Status:** حيث يتم إغفال دور المكانة والتسلسل الهرمي داخل المجتمع وتأكيد انسجام الأفراد، ومن ثم يُنظر إلى المجال العام باعتباره منتدى موضوعيًا Objective Forum مستقلاً عن سلطة المنزلة والمكانة.

- **مجال الاهتمام المُشترك Domain of Common Concerns:** فيما بين الأفراد، ويمكن القول إنه قبل ظهور المجال العام كانت سلطة التفسير تقع في أيدي الدولة والكنيسة، وكانت هاتان المؤسستان لديهما سلطة احتكار التفسير في مجالات الأدب والفلسفة والفن، ومع تطور المجتمعات، فإن الأعمال الفلسفية والأدبية، وكذلك الأعمال الفنية أصبحت تتسم بالطابع التجاري وأصبحت مُتاحة للمواطنين، ومن ثم أصبح الإنتاج الثقافي ونقل المعلومات وتداولها بمنزلة اهتمام شائع للمواطنين، ومن ثم تمهيد الطريق لقضايا أخرى لتكون محل اهتمام مشترك.
- **الاندماجية Inclusivity:** فالمجال العام يتيح الفرصة لجميع الأفراد دون استبعاد أحد للمُشاركة بصورة متساوية في المناقشات، ومن ثم ضمان التنوع في الرؤى ووجهات النظر والبعد عن التحيزات الشخصية [19].

ويُعرف المفكر هابرماس المجال العام بأنه "هو شبكة اتصالية في مجتمع افتراضي أو خيالي ليس من الضروري أن يتواجد في مكان معروف أو مميز ويتكون من مجموعة من الأفراد لهم سمات مشتركة واهتمامات مشتركة مجتمعين مع بعضهم كجمهور دون أي قيود أو إجبار، يتفاعلون مع بعضهم حول قضايا ذات اهتمام مشترك حيث يتحدثون عن الشئون العامة، ويحددون حاجات المجتمع مع الدولة والتي يمكن فيها الوصول إلى مواقفة عامة على قيم ومعايير تعمل كميكانزمات لحل المشكلات الاجتماعية والسياسية، وهو المجال الذي يتشكل فيه الرأي العام غير المحكوم، دون اعتبار للفروق الاجتماعية التي تكون بينهم" [20]، ولذلك يعتبر المجال العام المثالي من وجهة نظر "هابرماس" ساحة للنقاش الحر والمستقل وغير المقيد، ويكون فيه الأفراد أحرارًا متساويين في نقاشهم للشئون العامة، ويعد المجال العام وسيلة للعمل الجماعي تمنع هيمنه أى طرف بالمجتمع على باقي الأطراف؛ حيث يتيح المجال العام حرية تداول الآراء للمواطنيين العاديين ويجعلهم أكثر تفاعلاً في قضايا مجتمعهم، ويجعل لهم أدوارًا اجتماعية، ويدعم التنافس لإظهار الكفاءة في الفضاء العام الاجتماعي؛ بما يجعله أكثر تعددية وتميزًا وأكثر إفادة للمجتمع [21]، وبناء على ذلك افترض هابرماس وجود أربع سمات رئيسية تميز بها الاتصال في المجال العام وسيتم عرض هذه السمات فيما يلي:

- إمكانية الوصول إلى دائرة الاتصال بيسر.
- حرية الأفراد في الاتصال داخل هذه الدائرة.
- بنية المُناقشة.
- طرح خطاب مبرر بأدلة وشواهد إقناعية محددة [22].

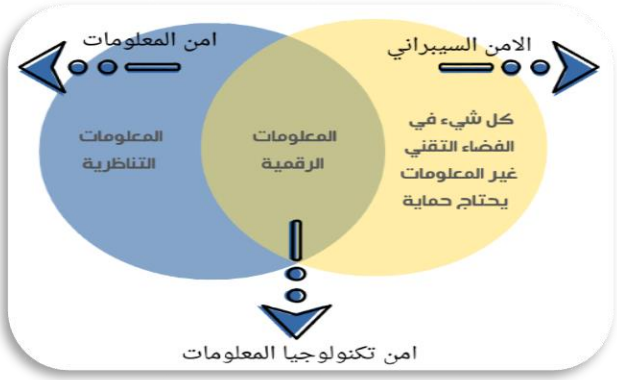
تستفيد الدِرَاسَةِ الحالية من نظرية المجال العام في الكشف عن العلاقة بين استخدام مواقع التَّواصل الاجتماعي وإدراك أهميَّة الأمن السيبراني ودوره في الأمن المعلوماتي، فمواقع

التَّواصل الاجتماعي تتيح مجالًا للحوارات والنقاشات حول الموضوعات المُختلفة مما يخلق نوعًا من المجال العام حول الموضوع الذي يتم مُناقشته وبالتَّالي تُشكل إدراك الأفراد حول هذا الموضوع، ولذلك ستقوم الباحثة بمعرفة مُعدلات استخدام مواقع التَّواصل الاجتماعي ودوافع هذا الاستخدام، ومدى إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني وطرق المُحافظة على نظامه ومخاطره وانتهاكاته.

الإطار المعرفي الدِرَاسَةِ:

يُعرف الأمن السيبراني بأنه "الحماية المادية للأجهزة والبرمجيات والمعلومات الشخصية والتكنولوجيا من الوصول غير المصرح به عبر الوسائل التكنولوجيا" [23].
كما أن هناك من يُعرفه على أنه "النشاط أو العملية أو القدرة أو الحالة التي يتم بموجبها تنظيم المعلومات والاتصالات والمعلومات الواردة فيها، ويحمي من الضرر أو الاستخدام أو التعديل غير المصرح به أو الاستغلال" [24].
وهناك **فرق بين مفهوم أمن المعلومات والأمن السيبراني**: حيث يتقاطع مجالي أمن المعلومات والأمن السيبراني من جهة الاهتمام بأمن المعلومات الإلكترونية "السايبري"، فالأمن السيبراني يعتني بأمن كل ما يوجد بالسايبر ومن ضمنه "أمن المعلومات" بينما يهتم مجال أمن المعلومات بأمن المعلومات وإن كانت على السايبر، وعلى الرغم من الاتفاق المذكور إلا أن هناك نقاط اختلاف جوهرية بين المجالين وبصورة أكثر تحديدًا تستطيع أن تُلاحظ الفروق فيما يلي:

- **الأمن السيبراني**: يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لاتهتم بذلك.
- **أمن المعلومات**: يهتم بأمن المعلومات الفيزيائية "الورقية" بينما لا يهتم الأمن السيبراني بذلك [25].



شكل رقم (1) يوضِّح الفرق بين الأمن السيبراني وأمن المعلومات

وارتبطت نشأة الأمن السيبراني باعتماد الأفراد على الإنترنت في كافة أعمالهم، مما جعل معلوماتهم تتعرض للخطر والاختراق، ومن هنا نشأ مجال الأمن السيبراني بهدف تأمين الأجهزة التقنية بكافة أنواعها وأشكالها وبما تحتويه من أنظمة وبيانات يتم تداولها عبر الإنترنت، وأصبح من أهم العلوم التي تحافظ على المعلومات الشخصية والحكومية الهامة [26]. وقد ظهر هذا المفهوم بعد الحرب الباردة استجابة للمزيد من الإبتكارات التكنولوجية والظروف الجيوسياسية المُتغيرة، وقد تم استخدامه لأول مرة من قبل علماء الكمبيوتر في أوائل التسعينات للتأكيد على سلسلة من حالات عدم الأمان المُرتبطة بأجهزة الكمبيوتر لكنه تجاوز مفهومه التقني لأمن الكمبيوتر عندما حث المؤيدين على أن التهديدات الناشئة عن التقنيات الرقمية يُمكن أن يكون لها أثار اجتماعية مُدمرة [27].

ويهدف الأمن السيبراني إلى المحافظة على أمن بيئة الاتصالات ومعرفة كل ما يستجد من أمور من خلال الرقابة والتحسين المُستمر للمعلومات، فلا بد من وضع نظام حماية عالي المُستوى، وكلمات مرور قوية ذات حماية عالية للمعلومات والموارد المخزنة، وهذا يقلل من فرص تخمين واكتشاف المعلومات خاصةً المهمة منها، وكذلك استخدام برامج مكافحة الفيروسات والتجسس، والتحديث المُستمر لكلمات المرور وللحسابات الشخصية، وتشفير أو اتلاف المعلومات الهامة بشكل آمن، واستخدام أجهزة آمنة [28].

وتتعدد أبعاد الأمن السبراني 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) [29].

وهناك مجموعة من **العناصر يجب أن تتوافر في الأمن السيبراني** لضمان الحماية الكافية للمعلومات، وسنوضح هذه العناصر فيما يلي:

- **السرية والأمن Confidentiality**: وتعني التأكد من أن المعلومات لا تكشف ولا بتطلع عليها من قبل أشخاص غير مخولين بذلك.
- **التكاملية Integration وسلامة المحتوى Content Integrity**: وهو التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله، وعلى نحو خاص لم يتم تدميره أو تغييره أو العبث به في آية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.
- **استمرارية توفر المعلومات أو الخدمة Continuation**: إذ يجب التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات

وتقديم الخدمة لمواقع المعلوماتية، وأن المُستخدم لن يتعرض إلى منع الاستخدام أو الدخول إلى النظام.

- **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به**: ويُقصد به ضمان عدم إنكار الشخص المتصل بالمعلومات أو مواقعها بقيامه بتصرف ما، بحيث تتوافر قدرة إثبات هذا التصرف وأن شخصًا ما في وقت معين قد قام به، كذلك عدم قدرة مستلم رسالة معينة على إنكار استلامه لهذه الرسالة (30).

وهناك مجموعة من **العوامل تؤثر على الأمن السيبراني**، سنقوم هنا بعرضها بشكل موجز ومُختصر فيما يلي:

- **الإبتزاز الإلكتروني**: والذي يتمثل في استخدام وسائل التقنية الحديثة للحصول على مكاسب مادية أو معنوية عن طريق الإكراه من شخص أو أشخاص أو حتى مؤسسات، ويكون ذلك الإكراه بالتهديد بفضح سر من أسرار المبتز بعد أن ينشب الجاني أنيابه على الضحية ويتمكن من جمع صور قد تكون فاضحة أو حتي مقاطع مصورة يكون مقابل عدم الفضيحة مبلغ مالي ضخم وإلا نشر الصور والفيديوهات (31).
- **التنمر الإلكتروني** Cyber – **Bullying**: والذي يكون عادة عن طريق مواقع التَّواصل الاجتماعي والذي يهدف للإيذاء من خلال شبكات تكنولوجيا المعلومات بطريقة مُتكررة ومتعمدة، ويُعرفه القانون الأمريكي بأنه قد يحدث عن طريق إرسال الشائعات عن شخص ما في الإنترنت بقصد تكريه الناس به أو ربما يصل لدرجة انتقاء ضحايا ونشر مواد لتشوية سمعتهم وإهانتهم. يُمكن عمل ذلك من خلال "الرسائل النصية، الصور والرسومات، مقاطع الفيديو، المكالمات الهاتفية، البريد الإلكتروني غرف المحادثة، المحادثة الفورية والمواقع الإلكترونية ومواقع التَّواصل الاجتماعي) (32).
- **الجرائم الإلكترونية**: وتُعتبر الجريمة الإلكترونية مظهرًا جديدًا من مظاهر السلوك الإجرامي لا يُمكن تصورها إلا من خلال ثلاث مظاهر وهي (إما أن تتجسد في شكل جريمة تقليدية يتم اقترافها بوسائل إلكترونية أو معلوماتية، أو في شكل استهداف للوسائل المعلوماتية ذاتها وعلى رأسها قاعدة المعطيات والبيانات أو البرامج المعلوماتية، أو أن يتم اقتراف الجرائم العادية في بيئة إلكترونية كما هو الأمر بالنسبة لجرائم الصحف) (33).

أما عن **الانتهاكات السيبرانية** فهي كل نشاط خبيث يسعى إلى الحصول على تنازلات من جهة ما، أو يتسبب في إضعاف السرية، أو النزاهة أو تعطيل توافر نظم الحواسيب، أو المعلومات، أو الاتصالات، أو الشبكات، أو البنية التحتية المادية، أو الافتراضية التي تتحكم فيها أجهزة الحواسيب، أو أنظمة المعلومات، أو المعلومات الموجودة فيها (34)، وسنعرض فيما يلي أنواع الانتهاكات السيبرانية:

- **انتهاك الخصوصية Violation of Privacy**: حيث تُعتبر من الحقوق الفردية التي نصت عليها التشريعات الداخلية والاتفاقات الدولية، والحياة الخاصة، والأحاديث الخاصة، والمحادثات الهاتفية، والمراسلات، والحقوق المالية، والمعتقدات الدينية، والمسكن، والأسم، والمهنة، وللفرد الحق الكامل في الحفاظ على خصوصية معلوماته وبياناته وترشيد استخدامها، ومن صور انتهاك الخصوصية في الفضاء السيبراني (إدخال معلومات وهمية وانتحال الشخصية بهدف حصول المعتدي على مبالغ مالية، التجسس الإلكتروني بتتبع العيوب واصطياد الأخطاء، التصنت ومحاولة الوصول إلى السجلات الخاصة والاعتداء على الحياة الخاصة) (35).
- **انتهاك أمن المعلومات Information Security Violation**: وهي مجموعة البيانات التي تخضع للمعالجة والتحليل والتفسير والاستخدام المنظم لأغراض معينة؛ لتحقيق زيادة المعرفة، وتشمل الانتهاكات المعلوماتية جرائم الدخول إلى نظام المعلوماتي، وسرقة المعلومات وتزيفها وتضليلها وإعاقة العمل المعلوماتي وتغيير المعلومات السرية وتعطيل الأنظمة وحجب الخدمة (36).
- **انتهاك الملكية الفكرية Violation of Intellectual property**: وتشمل تلك الانتهاكات وضع أسم المختلس على عمل، وانتهاك تقليد ختم المؤلف، والاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة (37).
- **انتهاك المواقع Violation of Sites**: ويُقصد بالمواقع الإلكترونية بمجموعة من صفحات إلكترونية ومصادر للمعلومات يُمكن التفاعل معها ومُشاهدتها عبر الحواسيب، أو الأجهزة النقالة، ويمكن للمجرمين انتهاك وتدمير هذه المواقع، والتلاعب بالبيانات والمعلومات الموجودة عليها والإضرار بها، وتهديدها بالفيروسات والبرامج الخبيثة والاختراقات (38).

تُعرف **مخاطر الأمن السيبراني** باعتبارها "المخاطر التي تمس عمليات أعمال الجهة بما في ذلك من (رؤية الجهة، أو رسالتها، أو إدارتها، أو صورتها، أو سمعتها)، أو أصول الجهة أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية الوصول غير المصرح به، أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات، أو نظم المعلومات" (39). وتتخذ مخاطر الأمن السيبراني العديد من الأشكال التي تستهدف إلحاق الأذي بالأفراد والمؤسسات، وأن تلك المخاطر تمتد لتشمل العديد من مكونات وقيم المجتمع وتؤثر على مُستخدمي الفضاء السيبراني بصورة خطيرة جدًا، ومن تلك المخاطر ما يتصل بالجوانب التَّالية:

- **الجانب الديني**: حيث تُسهم بعض مواقع الإنترنت، وصفحات التَّواصل الاجتماعي في التأثير سلبيًا على الفرد من خلال زعزعة بعض الثوابت والمعتقدات الدينية التي يؤمن بها، وتروج لبعض الأفكار السلبية بشكل مكثف لتحيل الأفراد إلى نوع من التناقض في العقيدة، مما يوقع بعض الأفراد في حبائل التطرف الديني، وقد

تعمد بعض المواقع إلى التشكيك في المعتقدات الدينية وبث بعض الأفكار الواهية التي تبعد الأفراد عن الالتزام بتعاليم الدين الحنيف (40).

- **الجانب الأخلاقي**: وذلك من خلال نشر قيم وثقافات ضارة بالمجتمع بواسطة دول ومؤسسات ذات أغراض تتعارض مع القيم الثقافية السائدة، ويُلاحظ ذلك من خلال مواقع الإنترنت التي تحتوى مواد تخرج عن حدود الأدب والأخلاق واللياقة، ولها تأثير سلبي على الأفراد حيث انتشار الكذب والأفعال الفاضحة والرذيلة، والتي تُسهم في الانحلال الأخلاقي للمجتمعات (41).
- **الجانب الوطني**: فقد أدى شيوع النقل الرقمي إلى خلق مُشكلة أمنية وطنية، حيث أصبح من السهل استراق السمع والتجسس الإلكتروني، بما يشمل الكثير من المجالات التعليمية والأمنية والاقتصادية والاجتماعية، بالإضافة إلى مخاطر تعطيل الأعمال الحكومية، أو العبث بالمعلومات أو إتلافها أو إخفائها (42).

الأطار المَنْهَجِيُّ:

- **نَوْعُ الدِرَاسَةِ وَمَنْهَجُهَا:**

تُعد هذه الدِرَاسَةِ من الدِّرَاسَاتُ الوصفية وتعتمد على المنهج المسحي survey الكمي، فالمسح ينصب على دِرَاسَةِ أشياء موجودة بالفعل وقت إجراء الدِرَاسَةِ، في مكان معين وزمان معين، بما يُساعد على فهمها أو إصدار الأحكام بشأنها، وقد تم اعتماد المسح الوصفي التفسيري.

- **أَدَوَاتُ الدِرَاسَةِ:**

استخدمت الباحثة استمارة الاستبيان عبر الإنترنت (الاستبيان الإلكتروني) كأداة لجمع البيانات، باعتبار أن الاستبيان أحد الأساليب التي تستخدم في جمع بيانات مُباشرة من العينة المُختارة، وذلك عن طريق توجيه مجموعة من الأسئلة المُحددة، وذلك بهدف التعرف على حقائق مُعينة أو وجهات نظر المبحوثين واتجاهاتهم أو الدوافع والمؤثرات التي تدفعهم إلى تصرفات سلوكية مُعينة.

ولتأكد من مدى صلاحية هذه الأداة في جمع بيانات الدِرَاسَةِ قامت الباحثة باختبار صدق مقاييس الدِرَاسَةِ، حيث اعتمدت الباحثة على الصدق الظاهري لقياس مدى صدق أداة جمع البيانات (الاستبيان الإلكتروني) لمعرفة ما إذا كانت الأداة تقيس ما ينبغي أن تقيسه وذلك من خلال الفحص المدقق لكل بند/سؤال والتأكد من أن البنود سليمة من حيث المحتوى والصياغة، بحيث تقيس الجوانب المطلوب قياسه في إطار الموضوع الأساسي.

كما قامت الباحثة بعرض الاستمارة على عدد من المُحكمين والمُتخصصين في مجال الإعلام والإحصاء (43)، للتحقق من صدق الأداة ومدى صلاحيتها لتحقيق أهداف الدِرَاسَةِ الميدانية واختبار فروضها، وقد قام السادة المحكمون بتعديل الاستمارة وصياغة الأسئلة وترتيبها وتنظيمها، وتم تعديل الاستمارة وفقًا لهذه التعديلات والمُقترحات التي اتفق عليها معظم الأساتذة المحكمين، وتم صياغة الاستمارة في صورتها النهائية.

- **مُجْتَمَعَ الدِرَاسَةِ:**

يتمثل مجتمع الدِرَاسَةِ في مُستخدمي مواقع التَّواصل الاجتماعي من مختلف الأعمار والمُستويات التعليمية والاقتصادية والاجتماعية.

- **عَيِّنَةُ الدِرَاسَةِ:**

تم تطبيق الدِرَاسَةِ الميدانية من خلال استمارة استبيان إلكتروني تم توزيعها على عينة عمدية قوامها (440 مُفردة) من مُستخدمي مواقع التَّواصل الاجتماعي من مختلف الأعمار والمُستويات (التعليمية ، الاقتصادية ، الاجتماعية)، وقد تم اختيار هذه العينة بشكل عمدي فهي عينة عمدية أي أنها تعتمد على قيام الباحثة باختيار مفردات العينة بناءً على خبرتها الشخصية وتقييمها الشخصي للخصائص التي يجب توافرها في عينة الدِرَاسَةِ (44)، وهناك مجموعة من المُبررات التي تم علي أساسها اختيار عينة الدِرَاسَةِ الميدانية، وهي كالتَّالي:

- **أولاً:** يستخدمون مواقع التَّواصل الاجتماعي.
- **ثانيًا:** أنهم على علم بالأمن السيبراني ومدركين لأهميَّته.
- **ثالثًا:** تنوع العوامل الديموغرافية لهذه العينة مما سيوضِّح للباحثة إن كانت هذه العوامل تؤثر علي إدراك المبحوثين لأهميَّة الأمن السيبراني ودوره في الحفاظ على أمن المعلومات الخاصة بهم.

وقد وزعت عينة الدِرَاسَةِ من حيث الخصائص الديموغرافية للمبحوثين علي النحو المُبيَّن بالجدول التَّالي:

جدول رقم (1)

خصائص عينة الدِرَاسَةِ (ن=440)

خصائص عينة الدِرَاسَةِ		ك	%
النوع	ذكر	217	%49,3
	انثى	223	%50,7
السن	من 18 إلى 25 سنة	284	%64,5
	من 26 إلى 35 سنة	78	%17,7
	من 36 إلى 45 سنة	43	%9,7
	من 46 إلى 55 سنة	25	%5,8
	56 سنة فأكثر	10	%2,3
المؤهل التعليمي	مؤهل مُتوسط	79	%18
	مؤهل جامعي	306	%69,5
	دراسات عليا	55	%12,5
المُستوى الاقتصادي الاجتماعي	مُنخفض	160	%36,4
	مُتوسط	208	%47,2
	مُرتفع	72	%16,4

تُوضح بيانات هذا الجدول الخصائص الديموغرافية للمبحوثين (عينة الدِرَاسَةِ)، حيث جاءت علي النحو التَّالي:

- **من حيث النوع**: بلغت نسبة الإناث ضمن عينة الدِرَاسَةِ (50,7%)، بينما بلغت نسبة الذكور (49,3%).
- **من حيث السن**: كانت غالبية المبحوثين بنسبة (64,5%) تقع في الفئة العمرية من 18 إلي 25 عامًا، بينما بلغت نسبة المبحوثين في الفئة العمرية من 26 إلي 35 عامًا (17,7%)، علي حين بلغت نسبة المبحوثين من 36 إلي 45 عامًا (9,7%)، أما عن نسبة المبحوثين في الفئة العمرية من 46 إلي 55 عامًا فقد كانت (5,8%)، وأخيرًا نجد أن نسبة المبحوثين في الفئة العمرية من 56 عامًا فأكثر (2,3%) من إجمالي عينة الدِرَاسَةِ.
- **من حيث نوع التعليم**: كانت غالبية المبحوثين بنسبة (69,5%) من الحاصلين علي مؤهل جامعي فقط، بينما بلغت نسبة المبحوثين ذوي المُؤهل المُتوسط (18%)، علي حين كانت نسبة المبحوثين الحاصلين علي دراسات عليا (12,5%) من إجمالي عينة الدِرَاسَةِ.
- **من حيث المُستوى الاقتصادي الاجتماعي**: كانت غالبية المبحوثين بنسبة (47,2%) ذات المُستوى الاقتصادي والاجتماعي المُتوسط، بينما بلغت نسبة المبحوثين ذات المُستوى الاقتصادي والاجتماعي المُنخفض (36,4%)، علي حين بلغت نسبة المبحوثين ذات المُستوى الاقتصادي والاجتماعي المُرتفع (16,4%) من إجمالي العينة.

تَسَاؤُلَاتُ الدِرَاسَةِ:

1) ما مُعدلات استخدام مواقع التَّواصل الاجتماعي، وما دوافع استخدامه؟
2) ما مدى إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني؟
3) ما مدى إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني؟
4) ما مدى إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر وانتهاكات الأمن السيبراني؟
5) ما العوامل الديموغرافية لمُستخدمي مواقع التَّواصل الاجتماعي الذين يدركون أهميَّة الأمن السيبراني؟

فروض الدِرَاسَةِ:

- **الفرض الأول:** توجد علاقة ارتباطية دالة إحصائيًا بين مُعدلات استخدام مواقع التَّواصل الاجتماعي والمتغيرات التَّالية: (دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك

مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

- **الفرض الثاني**: توجد علاقة ارتباطية دالة إحصائيًا بين دوافع استخدام مواقع التَّواصل الاجتماعي وإدراك مُستخدمي هذه المواقع للأمن السيبراني وطرق المحافظة على نظامه ومخاطره وانتهاكاته.
- **الفرض الثالث**: توجد علاقة ارتباطية دالة إحصائيًا بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني وإدراكهم لطرق المحافظة على نظامه ومخاطره وانتهاكاته.
- **الفرض الرابع**: توجد علاقة ارتباطية دالة إحصائيًا بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني وإدراكهم لمخاطره وانتهاكاته.
- **الفرض الخامس**: توجد علاقة ارتباطية دالة إحصائيًا بين كل من إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني وإدراكهم لانتهاكات الأمن السيبراني.
- **الفرض السادس:** توجد فروق ذات دلالة إحصائية بين المبحوثين (عينة الدِرَاسَةِ) بحسب النوع في المتغيرات التَّالية: (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).
- **الفرض السابع:** توجد فروق ذات دلالة إحصائية بين المبحوثين (عينة الدِرَاسَةِ) بحسب السن في المتغيرات التَّالية: (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).
- **الفرض الثامن:** توجد فروق ذات دلالة إحصائية بين المبحوثين (عينة الدِرَاسَةِ) بحسب المؤهل التعليمي في المتغيرات التَّالية: (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع

التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

- **الفرض التاسع:** توجد فروق ذات دلالة إحصائية بين المبحوثين (عينة الدِرَاسَةِ) بحسب المُستوى الاقتصادي الاجتماعي في المتغيرات التَّالية: (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

متغيرات ومقاييس الدِرَاسَةِ وأساليب القياس المُستخدمة وإجراءات صدق وثبات المقاييس:

1) **المُستوى الاقتصادي** (المُتوسط الحسابي=9,643، الانحراف المعياري=2,930، ثبات ألفا كرونباخ=0,735)، يتكون من **نوع السكن** (فيلا "5 درجات"، وشقة فى حى راقٍ "4 درجات"، وشقة فى حى مُتوسط "3 درجات"، وشقة فى حى شعبى "درجتين"، وحجرة واحدة أو حجرات مشتركة مع أخرين "درجة واحدة")، **ونوع ملكية السكن** (تمليك "3 درجات"، وإيجار قديم "درجتين"، وإيجار جديد "درجة واحدة")، **ومُتوسط الدخل للأسرة** (من 500 لأقل من 1000 جنيه "درجة واحدة"، من 1000 لأقل من 3000 جنيه "درجتين"، ومن 3000 لأقل من 5000 جنيه "3 درجات"، ومن 5000 جنيه فأكثر "4 درجات")، **وعضوية نادى رياضي** (نعم "درجتين"، ولا "درجة واحدة")، **ومُستوى النادى** (نادى ممتاز "3 درجات"، نادى مُتوسط "درجتين"، ونادى متواضع "درجة واحدة"). وتراوح إجمالي درجات المقياس ككل بين 4 و17، وعلى هذا الأساس تم تصنيف المبحوثين إلى ثلاث فئات على النحو التَّالي: (مُنخفض "4-8"/ مُتوسط "9-12"/ مُرتفع "13-17").

2) **مُعدلات استخدام مواقع التَّواصل الاجتماعي** (المُتوسط الحسابي=9,731، الانحراف المعياري=1,847، ثبات ألفا كرونباخ=0,839) يتكون من **مدى استخدام مواقع التَّواصل الاجتماعي** (دائمًا "3 درجات"، وأحيانًا "درجتين"، ونادرًا "درجة واحدة")، **وبداية استخدام مواقع التَّواصل الاجتماعي** (أكثر من أربعة سنوات "4 درجات"، ومن ثلاث سنوات إلى أربعة "3 درجات"، ومن سنة إلى سنتين "درجتين"، وأقل من سنة "درجة واحدة")، **ومُعدلات استخدام مواقع التَّواصل الاجتماعي في الأسبوع** (يوميًا "4 درجات"، ومن أربعة إلي ستة مرات في الأسبوع

"3 درجات"، ومن مرتين إلي ثلاث مرات في الأسبوع "درجتين"، ومرة واحدة في الأسبوع "درجة واحدة"). وتراوح إجمالي درجات المقياس ككل بين 3 و11، وعلى هذا الأساس تم تصنيف المبحوثين إلى ثلاث فئات على النحو التَّالي: (مُنخفض "3-5"/ مُتوسط "6-8"/ مُرتفع "9-11").

وقد تم التحقق من صدق مقياس "مُعدلات استخدام مواقع التَّواصل الاجتماعي" بحساب الاتساق الداخلي للمقياس Internal Consistency؛ حيث تم عمل مصفوفة الارتباطات Correctation Matrix بين العبارات المكونة للمقياس لاختبار دلالة هذا الارتباط، ويوضِّح الجدول التَّالي قيم معاملات الارتباط بين عبارات المقياس:

جدول رقم (2)

مصفوفة الارتباطات بين البنود المكونة لمقياس مُعدلات استخدام مواقع التَّواصل الاجتماعي

البنود		مدى الاستخدام	بداية الاستخدام	معدل الاستخدام الأسبوعي
بداية الاستخدام	معامل بيرسون	,512**		
	مُستوى المعنوية	,000		
معدل الاستخدام الأسبوعي	معامل بيرسون	,597**	,561**	
	مُستوى المعنوية	,000	,000	
مجمل معدل الاستخدام	**معامل بيرسون**	**,795**	**,840**	**,876**
	مُستوى المعنوية	**,000**	**,000**	**,000**

** دال عند مُستوى معنوية 0,01

يتضح من بيانات هذا الجدول معنوية العلاقة الارتباطية بين عبارات مقياس "مُعدلات استخدام مواقع التَّواصل الاجتماعي"، حيث كانت جميع قيم معاملات الارتباطات بين العبارات دالة إحصائيًا عند مُستوى معنوية أقل من 0,01.

3) دوافع استخدام مواقع التَّواصل الاجتماعي (المُتوسط الحسابي=36,74، الانحراف المعياري=6,231، ثبات ألفا كرونباخ=0,748) يتكون من 10 عبارات يحدد المبحوث موقفه منها على مقياس خماسي (موافق بشدة "خمس درجات"، وموافق "4 درجات"، ومحايد "3 درجات"، ومعارض "درجتين"، ومعارض بشدة "درجة

واحدة"). والعبارات هي: (التسلية والترفيه/ بحكم العادة استخدام مواقع التَّواصل الاجتماعي جزء من حياتي اليومية/ يُساعدني على شغل وقت فراغي/ للهروب من ضغوط الحياة ومسئولياتها/ استخدام مواقع التَّواصل الاجتماعي يريح أعصابي ويشعرني بالاسترخاء/ تُساعدني في حل بعض المشكلات التي تواجهني/ التعرف على عادات وتقاليد المجتمعات الأخرى/ التَّواصل مع الأصدقاء والأقارب والمعارف/ باستخدام مواقع التَّواصل الاجتماعي لا أشعر بالوحدة/ مُتابعة الأخبار والأحداث الجارية)، وتراوح إجمالي درجات المقياس ككل بين 10 و50، وعلى هذا الأساس تم تصنيف المبحوثين إلى ثلاث فئات على النحو التَّالي: (مُنخفض "10-23"/ مُتوسط "24-36"/ مُرتفع "37-50").

وقد تم التحقق من صدق مقياس "دوافع استخدام مواقع التَّواصل الاجتماعي" بحساب الاتساق الداخلي للمقياس Internal Consistency؛ حيث تم عمل مصفوفة الارتباطات Correctation Matrix بين العبارات العشرة المكونة للمقياس لاختبار دلالة هذا الارتباط، وقد اتضح من نتائج هذه المصفوفة أنه يوجد بالفعل معنوية العلاقة الارتباطية بين العبارات العشر لمقياس "دوافع استخدام مواقع التَّواصل الاجتماعي"، حيث كانت جميع قيم مُعاملات الارتباط بين العبارات دالة إحصائيًا عند مُستوى معنوية أقل من 0,01.

4) إدراك الأمن السيبراني (المُتوسط الحسابي=34,47، الانحراف المعياري=6,581، ثبات ألفا كرونباخ=0,749)، يتكون من 15 عبارة يحدد المبحوث مدى انطباقها عليه على مقياس ثلاثي (تنطبق علي تمامًا "3 درجات"، وتنطبيق علي إلى حد ما "درجتين"، ولا تنطبق علي "درجة واحدة"). والعبارات هي: (اختار كلمة مرور قوية تحتوى على مجموعة من الأحرف والأرقام والرموز/ أتجنب فتح أي رابط أو رسالة إلكترونية من شخص غير معروف/ أحرص على استخدام متصفح أمن للإنترنت/ أحذر كثيرًا عند الاتصال بالشبكات العامة/ أتوخى الحذر عند مُشاركة الآخرين معلومات حساسة باستخدام إعدادات الخصوصية للخدمات الإلكترونية/ أحرص على تحميل التحديثات والبرامج الأمنة/ ألغي أي اشتراك لي في الإعلانات المُستهدفة لحماية بياناتي الشخصية والمالية/ استخدم أدوات الإبلاغ عن الاساءات التي يتعرض لها المستخدمون/ استخدم تقنية التحقق الثنائي (كلمة المرور - البصمة)/ أفحص الروابط التي يبدو لي أنها ضارة/ أحرص على تعطيل خدمات الوصول لموقعي في التطبيقات المحملة على جهازي/ أغير إعدادات جهازي بشكل مُستمر حفاظًا على اختراق شبكة الوايفاي/ أهتم بتغيير كلمات المرور الخاصة بدخول مواقع التَّواصل الاجتماعي الخاصة بي كل فترة/ أتجنب الكشف عن أي بيانات شخصية أو عائلية أثناء تصفحي لمواقع التَّواصل الاجتماعي/ أحرص على الإبلاغ عن المواقع المشكوك فيها للجهات المُختصة)، وتراوح إجمالي درجات المقياس ككل بين 15

و45، وعلى هذا الأساس تم تصنيف المبحوثين إلى ثلاث فئات على النحو التَّالي: (مُنخفض "15-24"/ مُتوسط "25-35"/ مُرتفع "36-45").
وقد تم التحقق من صدق مقياس "إدراك الأمن السيبراني" بحساب الاتساق الداخلي للمقياس Internal Consistency؛ حيث تم عمل مصفوفة الارتباطات Correctation Matrix بين العبارات الخمسة عشر المكونة للمقياس لاختبار دلالة هذا الارتباط، وقد اتضح من نتائج هذه المصفوفة أنه يوجد بالفعل معنوية العلاقة الارتباطية بين العبارات الخمسة عشر لمقياس "إدراك الأمن السيبراني"، حيث كانت جميع قيم مُعاملات الارتباط بين العبارات دالة إحصائيًا عند مُستوى معنوية أقل من 0,01.

5) إدراك طرق المحافظة على نظام الأمن السيبراني (المُتوسط الحسابي=29,81، الانحراف المعياري=5,670، ثبات ألفا كرونباخ=0,735) يتكون من 14 عبارة يُحدد المبحوث مدى انطباقها عليه على مقياس ثلاثي (تنطبق علي تمامًا "3 درجات"، وتنطبيق علي إلى حد ما "درجتين"، ولا تنطبق علي "درجة واحدة"). والعبارات هي: (استخدم برنامج للحماية من الفيروسات بشكل مُستمر/ أتفحص جهاز الحاسب الآلي المكتبي - المحمول بصورة منتظمة/ أقوم بتحديث برنامج الحماية من الفيروسات بصورة مُستمرة/ أقوم بتحديث نظام التشغيل بصورة دورية/ أقوم بعمل نسخة احتياطية للملفات المهمة/ لا أفتح رسالة إلكترونية غير معروفة لدي/ أقوم بالرد عندما تصلني رسالة بريد إلكتروني عن الفوز بجائزة نقدية أو عينة أو شراكة في صفقة تجارية/ لا أتسوق أو أشتري سلعة مُعلن عنها في مواقع التَّواصل الاجتماعي أو من خلال الإعلانات/ أعلم بالخصائص اللازمة لإنشاء كلمة مرور جيدة عند الدخول لمواقع التَّواصل الاجتماعي أو المواقع على الويب/ استخدم نفس كلمة المرور لجميع مواقع التَّواصل الاجتماعي والبريد الإلكتروني/ استخدم نفس كلمة المرور للمواقع التي أحتاجها لإجراء عمليات مالية مثل مواقع البنوك ومواقع التسوق الإلكتروني/ لدي معرفة بخطورة إرسال كلمة المرور عبر البريد الإلكتروني/ أقوم بتغيير كلمة المرور بانتظام/ أقوم بقراءة اتفاقيات المُستخدم لبرنامج مجاني قبل الضغط "أوافق")، وتراوح إجمالي درجات المقياس ككل بين 14 و42، وعلى هذا الأساس تم تصنيف المبحوثين إلى ثلاث فئات على النحو التَّالي: (مُنخفض "14-23"/ مُتوسط "24-32"/ مُرتفع "33-42").
وقد تم التحقق من صدق مقياس "إدراك طرق المحافظة على نظام الأمن السيبراني" بحساب الاتساق الداخلي للمقياس Internal Consistency؛ حيث تم عمل مصفوفة الارتباطات Correctation Matrix بين العبارات الأربعة عشر المكونة للمقياس لاختبار دلالة هذا الارتباط، وقد اتضح من نتائج هذه المصفوفة أنه يوجد بالفعل معنوية العلاقة الارتباطية بين العبارات الأربعة عشر لمقياس "إدراك طرق المحافظة على

نظام الأمن السيبراني"، حيث كانت جميع قيم مُعاملات الارتباط بين العبارات دالة إحصائيًا عند مُستوى معنوية أقل من 0,01.

6) إدراك مخاطر الأمن السيبراني (المُتوسط الحسابي=14,96، الانحراف المعياري=2,666، ثبات ألفا كرونباخ=0,772) يتكون من 6 عبارات يُحدد المبحوث مدى انطباقها عليه على مقياس ثلاثي (تنطبق علي تمامًا "3 درجات"، وتنطبيق علي إلى حد ما "درجتين"، ولا تنطبق علي "درجة واحدة"). والعبارات هي: (أحرص على تجنب المعلومات المُخالفة للعقيدة والدين/ أحترم أنظمة الدولة في التعامل مع الشبكة العنكبوتية/ احترم سياسات مواقع التَّواصل الاجتماعي والمواقع الإلكترونية التي أستخدمها/ أنشر الوعي الرقمي عند التعرض للمواقف السلبية في شبكة الإنترنت بصورة عامة ومواقع التَّواصل الاجتماعي بصورة خاصة/ أتجنب تجاوز القوانين التي تفرضها الدولة في استخدام شبكة الإنترنت ومواقع التَّواصل الاجتماعي/ استخدم المحتوى المرخص من قبل الناشر أو المؤلف) وتراوح إجمالي درجات المقياس ككل بين 6 و18، وعلى هذا الأساس تم تصنيف المبحوثين إلى ثلاث فئات على النحو التَّالي: (مُنخفض "6-9"/ مُتوسط "10-14"/ مُرتفع "15-18").

وقد تم التحقق من صدق مقياس "إدراك مخاطر الأمن السيبراني" بحساب الاتساق الداخلي للمقياس Internal Consistency؛ حيث تم عمل مصفوفة الارتباطات Correctation Matrix بين العبارات الستة المُكونة للمقياس لاختبار دلالة هذا الارتباط، ويوضّح الجدول التَّالي قيم معاملات الارتباط بين عبارات المقياس:

جدول رقم (3)

مصفوفة الارتباطات بين البنود المكونة لمقياس إدراك مخاطر الأمن السيبراني

البنود		عبارة 1	عبارة 2	عبارة 3	عبارة 4	عبارة 5	عبارة 6
عبارة 2	معامل بيرسون	,409**					
	مُستوى المعنوية	,000					
عبارة 3	معامل بيرسون	,410**	,517**				
	مُستوى المعنوية	,000	,000				
عبارة 4	معامل بيرسون	,244**	,258**	,287**			
	مُستوى المعنوية	,000	,000	,000			
عبارة 5	معامل بيرسون	,398**	,491**	,477**	,244**		
	مُستوى المعنوية	,000	,000	,000	,000		
عبارة 6	معامل بيرسون	,316**	,390**	,445**	,402**	,361**	
	مُستوى المعنوية	,000	,000	,000	,000	,000	
مجمل العبارات	**معامل بيرسون**	**,645****	**,728****	**,739****	**,616****	**,707****	**,720****
	مُستوى المعنوية	**,000**	**,000**	**,000**	**,000**	**,000**	**,000**

**** دال عند مُستوى معنوية 0,01**

يتضح من بيانات هذا الجدول معنوية العلاقة الارتباطية بين عبارات مقياس "إدراك مخاطر الأمن السيبراني"، حيث كانت جميع قيم معاملات الارتباطات بين العبارات دالة إحصائيًا عند مُستوى معنوية أقل من 0,01.

7) **إدراك انتهاكات الأمن السيبراني** (المُتوسط الحسابي=11,05، الانحراف المعياري=2,729، ثبات ألفا كرونباخ=0,785) يتكون من 5 عبارات يُحدد المبحوث مدى انطباقها عليه على مقياس ثلاثي (تنطبق علي تمامًا "3 درجات"، وتنطبيق علي إلى حد ما "درجتين"، ولا تنطبق علي "درجة واحدة"). والعبارات هي: (أضع نظام يمنع الوصول إلى مواقع إلكترونية يُمكن أن تضر بجهاز الحاسب الألي المكتبي- المحمول/ أحدث برنامج الحماية الموجود على جهاز الحاسب الألي المكتبي – المحمول بشكل دوري/ أضع إجراءات وسياسات لحفظ الأمن السيبراني الخاص بمعلوماتي على جهاز الحاسب الألي المكتبي – المحمول/ استخدم التشفير لملفاتي المهمة التي أقوم بإرسالها من خلال شبكة الإنترنت أو مواقع التَّواصل الاجتماعي/ أراعي النزاهة في هويتي الرقمية حين استخدم مواقع التَّواصل الاجتماعي)، وتراوح إجمالي درجات المقياس ككل بين 5 و15، وعلى هذا الأساس تم تصنيف المبحوثين إلى ثلاث فئات على النحو التَّالي: (مُنخفض "5-8"/ مُتوسط "9-11"/ مُرتفع "12-15").

وقد تم التحقق من صدق مقياس "إدراك انتهاكات الأمن السيبراني" بحساب الاتساق الداخلي للمقياس Internal Consistency؛ حيث تم عمل مصفوفة الارتباطات Correctation Matrix بين العبارات الخمس المُكونة للمقياس لاختبار دلالة هذا الارتباط، ويوضّح الجدول التَّالي قيم معاملات الارتباط بين عبارات المقياس:

جدول رقم (4)

مصفوفة الارتباطات بين البنود المكونة لمقياس إدراك انتهاكات الأمن السيبراني

البنود		عبارة 1	عبارة 2	عبارة 3	عبارة 4	عبارة 5
عبارة 2	معامل بيرسون	,467**				
	مُستوى المعنوية	,000				
عبارة 3	معامل بيرسون	,567**	,471**			
	مُستوى المعنوية	,000	,000			
عبارة 4	معامل بيرسون	,403**	,396**	,463**		
	مُستوى المعنوية	,000	,000	,000		
عبارة 5	معامل بيرسون	,275**	,385**	,344**	,265**	
	مُستوى المعنوية	,000	,000	,000	,000	
مجمل العبارات	**معامل بيرسون**	**,751****	**,749****	**,787****	**,718****	**,609****
	مُستوى المعنوية	**,000**	**,000**	**,000**	**,000**	**,000**

** دال عند مُستوى معنوية 0,01

يتضح من بيانات هذا الجدول معنوية العلاقة الارتباطية بين عبارات مقياس "إدراك انتهاكات الأمن السيبراني"، حيث كانت جميع قيم معاملات الارتباطات بين العبارات دالة إحصائيًا عند مُستوى معنوية أقل من 0,01.

نَتَائِجُ الدِرَاسَةِ:

أولًا: النتائج التفصيلية للدِرَاسَةِ الميدانية:

جدول رقم (5)

معدل استخدام مواقع التَّواصل الاجتماعي

معدل استخدام مواقع التَّواصل الاجتماعي	ك	%
مُنخفض	23	%5,2
مُتوسط	60	%13,6
مُرتفع	357	%81,2
الإجمالي	**440**	**%100**

تُبين لنا بيانات هذا الجدول أن غالبية المبحوثين بنسبة (81,2%) كانوا من مُرتفعي الاستخدام لمواقع التَّواصل الاجتماعي، وقد ظهر ذلك من خلال استجابات المبحوثين حيث أوضح (67,7%) منهم أنهم يستخدمون هذه المواقع بصفة دائمة وأفادا (73,9%) منهم أنهم يستخدمون هذه المواقع بشكل يومي، كما أشار (69,1%) منهم أنهم يستخدمون هذه المواقع منذ أكثر من أربعة سنوات، يليهم في الترتيب المبحوثون مُتوسطو الاستخدام إذ بلغت نسبتهم (13,6%) من إجمالي (عينة الدِرَاسَةِ)، علي حين بلغت نسبة مُنخفضي الاستخدام لمواقع التَّواصل الاجتماعي (5,2%) من إجمالي المبحوثين حيث نجد أن (4,1%) من المبحوثين أفادوا أنهم نادرًا ما يستخدمون هذه المواقع وكذلك أشارت نسبة (4,5%) من المبحوثين أنهم يستخدمون هذه المواقع مرة واحدة في الأسبوع، كما بينت نسبة (3,9%) أنهم يستخدمون هذه المواقع منذ أقل من سنة.

جدول رقم (6)

دوافع استخدام مواقع التَّواصل الاجتماعي

دوافع استخدام مواقع التَّواصل الاجتماعي	ك	%
مُنخفضة	7	%1,6
مُتوسطة	213	%48,4
مُرتفعة	220	%50
الإجمالي	**440**	**%100**

يُفيد هذا الجدول بأن نصف المبحوثين (عينة الدِرَاسَةِ) كانوا لديهم دوافع مُرتفعة لاستخدام مواقع التَّواصل الاجتماعي، أما النصف الأخر فقد كانت نسبة (48,4%)

منهم من لديهم دوافع مُتوسطة لاستخدام مواقع التَّواصل الاجتماعي، أما عن المبحوثين الذين لديهم دوافع مُنخفضة فقد كانوا 7 أفراد فقط أي بنسبة (1,6%)، وقد تبين ذلك من خلال استجابات المبحوثين على مقياس الدوافع حيث كانت تمثلت أعلى استجابة في أنهم يستخدمون مواقع التَّواصل الاجتماعي لمُتابعة الأخبار والأحداث الجارية حيث كانت وزنها النسبي (83,8%)، وتلتها أنهم يستخدمون مواقع التَّواصل الاجتماعي لتواصل مع الأصدقاء والأقارب والمعارف فقد بلغ وزنها النسبي (83,5%)، أما عن الدوافع التي حصلت على أقل استجابه فقد كانت أنهم يستخدمون مواقع التَّواصل الاجتماعي لـــ (الهروب من ضغوط الحياة ومسئولياتها/ حتى لا يشعرون بالوحدة/ يريحوا أعصابهم ويشعرون بالاسترخاء) حيث حصلوا على أوزان نسبية (67,3%/ 66,1%/ 60%) على التوالي.

جدول رقم (7)

إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني

إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني	ك	%
مُنخفض	31	%7
مُتوسط	210	%47,8
مُرتفع	199	%45,2
الإجمالي	**440**	**%100**

يتضح من بيانات هذا الجدول أن أغلبية المبحوثين (عينة الدِرَاسَةِ) يتراوح إدراكهم للأمن السيبراني بين الدرجة المُتوسطة والمُرتفعه حيث كانت نسبتهم (47,8%/ 45,2%) على التوالي، أما عن بقية المبحوثين والذي بلغت نسبتهم (7%) كانوا يدركون الأمن السيبراني بدرجة مُنخفضة، وقد تبينت الباحثة ذلك من خلال استجابات المبحوثين على مقياس إدراك الأمن السيبراني حيث أن العبارات التي قد حصلت على أعلى استجابة تمثلت في (أحرص على استخدام متصفح أمن للإنترنت/ أتوخى الحذر عند مُشاركة الآخرين معلومات حساسة باستخدام إعدادات الخصوصية للخدمات الإلكترونية/ أتجنب فتح أي رابط أو رسالة إلكترونية من شخص غير معروف) حيث حصلوا على أوزان نسبية (83,3%/ 82,7%/ 81,4%) على التوالي، أما عن العبارات التي حصلت على أقل استجابة فقد اشتملت على (أغير إعدادات جهازي بشكل مُستمر حفاظًا على اختراق شبكة الوايفاي/ أفحص الروابط التي يبدو لي أنها ضارة/ أهتم بتغيير كلمات المرور الخاصة بدخول مواقع التَّواصل الاجتماعي الخاصة بي كل فترة) حيث تمثلت أوزانهم النسبية في (70,8%/ 68%/ 66,2%) على التوالي، ومن هنا يتضح لنا أن مُستخدمي مواقع التَّواصل الاجتماعي (عينة الدِرَاسَةِ) على دراية إلى حد ما بالأمن السيبراني وكيفية الحفاظ على المعلومات الخاصة بهم على مواقع التَّواصل الاجتماعي.

جدول رقم (8)

إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني

إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني	ك	%
مُنخفض	49	%11,1
مُتوسط	243	%55,3
مُرتفع	148	%33,6
الإجمالي	**440**	**%100**

تُشير بيانات هذا الجدول أن أغلبية المبحوثين (عينة الدِرَاسَةِ) يدركون بدرجة مُتوسطة طرق المُحافظة على نظام الأمن السيبراني حيث كانت نسبتهم (55,3%)، في حين بلغت نسبة المبحوثين الذين يدركون بدرجة مُرتفعة طرق المُحافظة على نظام الأمن السيبراني (33,6%)، أما عن بقية المبحوثين والذين تمثلت نسبتهم (11,1%) فهم يدركون بدرجة مُنخفضة طرق المُحافظة على نظام الأمن السيبراني، وقد توضح ذلك من خلال استجابات المبحوثين على مقياس إدراك طرق المُحافظة على نظام الأمن السيبراني فقد كانت العبارات التي حصلت على أعلى وزن نسبي (أقوم بعمل نسخة احتياطية للملفات المهمة/ أعلم بالخصائص اللازمة لإنشاء كلمة مرور جيدة عند الدخول لمواقع التَّواصل الاجتماعي أو المواقع على الويب/ لا أفتح رسالة إلكترونية غير معروفة لدى) وقد كان الوزن (78%/ 77,5%/ 76,4%) على التوالي، أما عن العبارات التي حصلت على أقل وزن نسبي (أقوم بتغيير كلمة المرور بانتظام/ استخدم نفس كلمة المرور للمواقع التي أحتاجها لإجراء عمليات مالية مثل مواقع البنوك ومواقع التسوق الإلكتروني/ أقوم بالرد عندما تصلني رسالة بريد إلكتروني عن الفوز بجائزة نقدية أو عينة أو شراكة في صفقة تجارية) حيث كان الوزن (66,1%/ 61,4%/ 53,8%) على التوالي، وتؤكد نتائج بيانات هذا الجدول والمقياس نتائج الجدول رقم (7) الذي يوضِّح إدراك المبحوثين للأمن السيبراني حيث أنه أفاد أن أغلبية المبحوثين يدركون الأمن السيبراني بدرجة مُتوسطة ومُرتفعة وبالتَّالي فهم يدركون طرق المُحافظة على نظام هذا الأمن بدرجة مُتوسطة ومُرتفعة.

جدول رقم (9)

إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني

إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني	ك	%
مُنخفض	16	%3,6
مُتوسط	146	%33,2
مُرتفع	278	%63,2
الإجمالي	**440**	**%100**

توضح بيانات هذا الجدول أن أغلبية المبحوثين (عينة الدِرَاسَةِ) يدركون بشكل مُرتفع مخاطر الأمن السيبراني حيث كانت نسبتهم (63,2%)، أما عن المبحوثين الذين يدركون مخاطر الأمن السيبراني بشكل مُتوسط فقد بلغت نسبتهم (33,2%)، بينما كانت نسبة المبحوثين الذين يدركون مخاطر الأمن السيبراني بشكل مُنخفض (3,6%)، وقد توصلت الباحثة إلى هذه النتيجة بناء على استجابات المبحوثين على مقياس إدراك مخاطر الأمن السيبراني والذي اشتمل على العبارات التَّالية (أحرص على تجنب المعلومات المُخالفة للعقيدة والدين/ احترم سياسات مواقع التَّواصل الاجتماعي والمواقع الإلكترونية التي أستخدمها/ أحترم أنظمة الدولة في التعامل مع الشبكة العنكبوتية/ أتجنب تجاوز القوانين التي تفرضها الدولة في استخدام شبكة الإنترنت ومواقع التَّواصل الاجتماعي/ أستخدم المحتوى المرخص من قبل الناشر أو المؤلف/ أنشر الوعي الرقمي عند التعرض للمواقف السلبية في شبكة الإنترنت بصورة عامة ومواقع التَّواصل الاجتماعي بصورة خاصة) وقد حصلوا على الأوزان النسبية التَّالية (89,9%/ 86,3%/ 84,7%/ 83,7%/ 80,5%/ 73,8%) على التوالي، ونتائج هذا الجدول تتفق إلى حد ما مع نتائج كلًا من الجدول رقم (7) الذي يوضِّح إدراك المبحوثين للأمن السيبراني والجدول رقم (8) الذي يوضِّح إدراك المبحوثين لطرق المُحافظة على نظام هذا الأمن والذين أفادوا بأن أغلبية المبحوثين يتراوحون بين أنهم يدركون الأمن السيبراني وطرق المُحافظة على نظامه بدرجة مُتوسطة ومُرتفعة، ومما سبق يتبين لنا أن مُستخدمي مواقع التَّواصل الاجتماعي (عينة الدِرَاسَةِ) على علم جيد إلى حد ما بكيفية الحفاظ على معلوماتهم الخاصة على هذه المواقع.

جدول رقم (10)

إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني

إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني	ك	%
مُنخفض	83	%18,9
مُتوسط	152	%34,5
مُرتفع	205	%46,6
الإجمالي	**440**	**%100**

تُبين بيانات هذا الجدول أن أغلبية المبحوثين (عينة الدِرَاسَةِ) يدركون بشكل مُرتفع إنتهاكات الأمن السيبراني حيث كانت نسبتهم (46,6%)، أما عن المبحوثين الذين يدركون إنتهاكات الأمن السيبراني بشكل مُتوسط فقد بلغت نسبتهم (34,5%)، بينما كانت نسبة المبحوثين الذين يدركون إنتهاكات الأمن السيبراني بشكل مُنخفض (18,9%)، وقد استنتجت الباحثة هذه النتيجة بناء على استجابات المبحوثين على مقياس إدراك إنتهاكات الأمن السيبراني والذي اشتمل على العبارات التَّالية (أراعي

النزاهة في هويتي الرقمية حين استخدم مواقع التَّواصل الاجتماعي/ أضع نظام يمنع الوصول إلى مواقع إلكترونية يُمكن أن تضر بجهاز الحاسب الألي المكتبي- المحمول/ أضع إجراءات وسياسات لحفظ الأمن السيبراني الخاص بمعلوماتي على جهاز الحاسب الألي المكتبي - المحمول/ أحدث برنامج الحماية الموجود على جهاز الحاسب الألي المكتبي – المحمول بشكل دوري/ استخدم التشفير لملفاتي المهمة التي أقوم بإرسالها من خلال شبكة الإنترنت أو مواقع التَّواصل الاجتماعي) وقد حصلوا على الأوزان النسبية التَّالية (79,5%/ 76,4%/ 73,3%/ 73%/ 66,5%) على التوالي، ونتائج هذا الجدول تتفق إلى حد ما مع نتائج كلًا من الجدول رقم (7) الذي يوضِّح إدراك المبحوثين للأمن السيبراني والجدول رقم (8) الذي يوضِّح إدراك المبحوثين لطرق المُحافظة على نظام هذا الأمن والذين أفادوا بأن أغلبية المبحوثين يتراوحون بين أنهم يدركون الأمن السيبراني وطرق المُحافظة على نظامه بدرجة مُتوسطة ومُرتفعة، في حين أنها اتفقت تمامًا مع الجدول رقم (9) الذي أفاد بأن أغلبية المبحوثين يتراوح إدراكهم لمخاطر الأمن السيبراني بين الإدراك بشكل مُرتفع وبشكل مُتوسط، ومما سبق يتضح لنا أن مُستخدمي مواقع التَّواصل الاجتماعي (عينة الدِرَاسَةِ) على علم جيد إلى حد ما بكيفية الحفاظ على معلوماتهم الخاصة على هذه المواقع.

ثانيًا: نتائج اختبار صحة فروض الدِرَاسَةِ الميدانية:

أ) الفرض الأول: توجد علاقة ارتباطية دالة إحصائيًا بين مُعدلات استخدام مواقع التَّواصل الاجتماعي والمتغيرات التَّالية: (دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

جدول رقم (11)

معنوية العلاقة الارتباطية دالة إحصائيًا بين مُعدلات استخدام مواقع التَّواصل الاجتماعي والمتغيرات الخمسة

المتغيرات	معامل بيرسون	مُستوى المعنوية
دوافع استخدام مواقع التَّواصل الاجتماعي	0,325**	0,000
إدراك الأمن السيبراني	0,304**	0,000
إدراك طرق المُحافظة على نظام الأمن السيبراني	0,207**	0,000
إدراك مخاطر الأمن السيبراني	0,283**	0,000
إدراك انتهاكات الأمن السيبراني	0,164**	0,001

**** دال عند مُستوى معنوية 0,01**

لاختبار معنوية العلاقة بين مُعدلات استخدام مواقع التَّواصل الاجتماعي والمتغيرات التَّالية: (دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)، وبالنظر إلي أن كلا المُتغير المُستقل والمُتغيرات التابعة جري قياسه علي المُستوى الفتري Interval، فقد تم استخدام مُعامل ارتباط بيرسون لتحقيق هذا الغرض.

يتضح لنا من بيانات هذا الجدول أن هناك علاقة طردية بين كلًا من المُتغير المُستقل المُتمثل في مُعدلات استخدام مواقع التَّواصل الاجتماعي والمُتغيرات التابعة المُتمثلة في (دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)، ومن حيث شدة العلاقة يُمكن تصنيفها بالضعيفة. كما توضح لنا أن مُعامل ارتباط بيرسون لهذه المُتغيرات قيمة دالة إحصائيًا عند مُستوى معنوية أقل من 0,01.

وبذلك يكون **اختبار الفرض الأول** القائل "بوجود علاقة ارتباطية دالة إحصائيًا بين مُعدلات استخدام مواقع التَّواصل الاجتماعي والمتغيرات التَّالية: (دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)" **قد انتهي إلي ثبوت صحته بشكل كلي**. وانطلاقًا من هذه النتيجة يُمكن القول بأن مُستخدمي مواقع التَّواصل الاجتماعي يُدركون الأمن السيبراني وطرق المحافظة عليه ومخاطره وانتهاكاته.

ب) الفرض الثاني: توجد علاقة ارتباطية دالة إحصائيًا بين دوافع استخدام مواقع التَّواصل الاجتماعي وإدراك مُستخدمي هذه المواقع للأمن السيبراني وطرق المحافظة على نظامه ومخاطره وانتهاكاته.

جدول رقم (12)

معنوية العلاقة الارتباطية دالة إحصائيًا بين دوافع استخدام مواقع التَّواصل الاجتماعي والمتغيرات الأربعة

المتغيرات	معامل بيرسون	مُستوى المعنوية
إدراك الأمن السيبراني	0,278**	0,000
إدراك طرق المُحافظة على نظام الأمن السيبراني	0,276**	0,000
إدراك مخاطر الأمن السيبراني	0,198**	0,000
إدراك انتهاكات الأمن السيبراني	0,235**	0,000

**** دال عند مُستوى معنوية 0,01**

لاختبار معنوية العلاقة بين دوافع استخدام مواقع التَّواصل الاجتماعي والمتغيرات التَّالية: (إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)، وبالنظر إلي أن كلا المُتغير المُستقل والمُتغيرات التابعة جري قياسه علي المُستوى الفتري Interval، فقد تم استخدام مُعامل ارتباط بيرسون لتحقيق هذا الغرض.

تُشير بيانات هذا الجدول إلى أن هناك علاقة طردية بين كلًا من المُتغير المُستقل المُتمثل في دوافع استخدام مواقع التَّواصل الاجتماعي والمُتغيرات التابعة المُتمثلة في (إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)، ومن حيث شدة العلاقة يُمكن تصنيفها بالضعيفة. كما توضح لنا أن مُعامل ارتباط بيرسون لهذه المُتغيرات قيمة دالة إحصائيًا عند مُستوى معنوية أقل من 0,01.

وبذلك يكون **اختبار الفرض الثاني** القائل "بمعنوية العلاقة بين دوافع استخدام مواقع التَّواصل الاجتماعي وإدراك مُستخدمي هذه المواقع للأمن السيبراني وطرق المحافظة على نظامه ومخاطره وانتهاكاته" **قد انتهي إلي ثبوت صحته بشكل كلي**.

ج) الفرض الثالث: توجد علاقة ارتباطية دالة إحصائيًا بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني وإدراكهم لطرق المحافظة على نظامه ومخاطره وانتهاكاته.

جدول رقم (13)

معنوية العلاقة الارتباطية دالة إحصائيًا بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني والمتغيرات الثلاثة

المتغيرات	معامل بيرسون	مُستوى المعنوية
إدراك طرق المُحافظة على نظام الأمن السيبراني	0,733**	0,000
إدراك مخاطر الأمن السيبراني	0,616**	0,000
إدراك انتهاكات الأمن السيبراني	0,684**	0,000

**** دال عند مُستوى معنوية 0,01**

لاختبار معنوية العلاقة بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني والمتغيرات التَّالية: (إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)، وبالنظر إلي أن كلا المُتغير المُستقل والمُتغيرات التابعة جري قياسه علي المُستوى الفتري Interval، فقد تم استخدام مُعامل ارتباط بيرسون لتحقيق هذا الغرض.

وتوضح لنا بيانات هذا الجدول أن هناك علاقة طردية بين كلًا من المُتغير المُستقل المُتمثل في إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني والمُتغيرات التابعة المُتمثلة في (إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)، ومن حيث شدة العلاقة يُمكن تصنيفها كالتَّالي (مُرتفعة في العلاقة الموجودة بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني وإدراكهم لطرق المُحافظة على نظام الأمن السيبراني/ ومُتوسطة في العلاقة بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني وإدراكهم لمخاطره وانتهاكاته). كما توضح لنا أن مُعامل ارتباط بيرسون لهذه المُتغيرات قيمة دالة إحصائيًا عند مُستوى معنوية أقل من 0,01.

وبذلك يكون **اختبار الفرض الثالث** القائل "بوجود علاقة ارتباطية دالة إحصائيًا بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني وإدراكهم لطرق المحافظة على نظامه ومخاطره وانتهاكاته" **قد انتهي إلي ثبوت صحته بشكل كلي**.

د) الفرض الرابع: توجد علاقة ارتباطية دالة إحصائيًا بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني وإدراكهم لمخاطره وانتهاكاته.

جدول رقم (14)

معنوية العلاقة الارتباطية دالة إحصائيًا بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني والمتغيرين

المتغيرات	معامل بيرسون	مُستوى المعنوية
إدراك مخاطر الأمن السيبراني	0,545**	0,000
إدراك انتهاكات الأمن السيبراني	0,698**	0,000

**** دال عند مُستوى معنوية 0,01**

لاختبار معنوية العلاقة بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني والمتغيرات التَّالية: (إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)، وبالنظر إلي أن كلا المُتغير المُستقل والمُتغيرات التابعة جري قياسه علي المُستوى الفتري Interval، فقد تم استخدام مُعامل ارتباط بيرسون لتحقيق هذا الغرض.

تُبين لنا بيانات هذا الجدول أن هناك علاقة طردية بين كلًا من المُتغير المُستقل المُتمثل في إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني والمُتغيرات التابعة المُتمثلة في (إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)، ومن حيث شدة العلاقة يُمكن تصنيفها بالمُتوسطة. كما توضح لنا أن مُعامل ارتباط بيرسون لهذه المُتغيرات قيمة دالة إحصائيًا عند مُستوى معنوية أقل من 0,01.

وبذلك يكون **اختبار الفرض الرابع** القائل "بمعنوية العلاقة بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني وإدراكهم لمخاطره وانتهاكاته" **قد انتهي إلي ثبوت صحته بشكل كلي**.

ه) الفرض الخامس: توجد علاقة ارتباطية دالة إحصائيًا بين كل من إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني وإدراكهم لانتهاكات الأمن السيبراني.

جدول رقم (15)

معنوية العلاقة الارتباطية دالة إحصائيًا بين كل من إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني وإدراك انتهاكات الأمن السيبراني

معامل بيرسون	مُستوى المعنوية
**0,582	0,000

**** دال عند مُستوى معنوية 0,01**

تُفيد بيانات هذا الجدول بوجود علاقة ارتباطية دالة إحصائيًا بين إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني وإداركهم لانتهاكات الأمن السيبراني، حيث بلغت قيمة معامل ارتباط بيرسون 0,582، وهى قيمة دالة إحصائيًا عند مُستوى معنوية أقل من 0,01.

ومن حيث الاتجاه فهى علاقة طردية، ما يعنى أنه كلما زادت إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني زادت معها بالتبعية إداركهم لانتهاكات الأمن السيبراني؛ فالأكثر إدراكًا لمخاطر الأمن السيبراني يكون أكثر إدراكًا لانتهاكات الأمن السيبراني، والعكس بالعكس. أما من حيث شدة العلاقة، فيُمكن وصفها بأنها بالمُتوسطة.

وعليه يُمكن القول أن **اختبار صحة الفرض الخامس** من فروض الدِرَاسَةِ القائل "بوجود علاقة ارتباطية دالة إحصائيًا بين كل من إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني وإدراكهم لانتهاكات الأمن السيبراني" **قد انتهى إلى ثبوت صحة هذا الفرض**.

و) الفرض السادس: توجد فروق ذات دلالة إحصائية بين المبحوثين (عينة الدِرَاسَةِ) بحسب النوع في المتغيرات التَّالية: (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

جدول رقم (16)

معنوية الفروق بين المبحوثين بحسب النوع في متغيرات الدِرَاسَةِ

المتغيرات		العدد	المُتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجة الحرية	مُستوى المعنوية
مُعدلات استخدام مواقع التَّواصل الاجتماعي	ذكر	217	9,84	1,838	1,198	438	0,232
	أنثى	223	9,63	1,855			
دوافع استخدام مواقع التَّواصل الاجتماعي	ذكر	217	36,96	6,301	0,722	438	0,471
	أنثى	223	36,53	6,169			
إدراك الأمن السيبراني	ذكر	217	34,82	6,550	1,086	438	0,278
	أنثى	223	34,14	6,608			
إدراك طرق المُحافظة على نظام الأمن السيبراني	ذكر	217	30,71	5,365	3,306	438	0,001
	أنثى	223	28,94	5,834			
إدراك مخاطر الأمن السيبراني	ذكر	217	14,85	2,640	0,880-	438	0,380
	أنثى	223	15,08	2,693			
إدراك انتهاكات الأمن السيبراني	ذكر	217	11,18	2,870	0,949	438	0,343
	أنثى	223	10,94	2,586			

توضح بيانات هذا الجدول نتيجة اختبار معنوية الفروق بين المبحوثين (عينة الدِرَاسَةِ) بحسب النوع فى المتغيرات التَّالية: (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

فبالنسبة لمتغير مُعدلات استخدام مواقع التَّواصل الاجتماعي، أظهر اختبار معنوية الفروق بين المبحوثين بحسب النوع عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة T (1,198) وهى قيمة غير دالة إحصائيًا عند درجة حرية (438) ومُستوى معنوية أقل من 0,05.

أما فيما يتعلق بمتغير دوافع استخدام مواقع التَّواصل الاجتماعي، أظهر اختبار معنوية الفروق بين المبحوثين بحسب النوع عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة T (0,722) وهى قيمة غير دالة إحصائيًا عند درجة حرية (438) ومُستوى معنوية أقل من 0,05.

أما متغير إدراك الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين بحسب النوع عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة T (1,086) وهى

قيمة غير دالة إحصائيًا عند درجة حرية (438) ومُستوى معنوية أقل من 0,05.

بينما مُتغير إدراك طرق المُحافظة على نظام الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين بحسب النوع وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة T (3,306) وهى قيمة دالة إحصائيًا عند درجة حرية (438) ومُستوى معنوية أقل من 0,05 .

وبالنسبة لمتغير إدراك مخاطر الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين بحسب النوع عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة T (-0,880) وهى قيمة غير دالة إحصائيًا عند درجة حرية (438) ومُستوى معنوية أقل من 0,05.

وأخيرًا بالنسبة لمُتغير إدراك انتهاكات الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين بحسب النوع عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة T (0,949) وهى قيمة غير دالة إحصائيًا عند درجة حرية (438) ومُستوى معنوية أقل من 0,05.

وعليه يمكن القول أن اختبار صحة الفرض القائل بوجود فروق ذات دلالة إحصائية بين المبحوثين عينة الدِرَاسَةِ بحسب النوع فى متغيرات (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)، **قد انتهى إلى ثبوت عدم صحة هذا الفرض بشكل جزئيًا**.

ز) الفرض السابع: توجد فروق ذات دلالة إحصائية بين المبحوثين (عينة الدِرَاسَةِ) بحسب السن في المتغيرات التَّالية: (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

تبين للباحثة من نتيجة اختبار معنوية الفروق بين المبحوثين (عينة الدِرَاسَةِ) طبقًا للسن فى متغيرات (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/

إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

فبالنسبة لمتغير مُعدلات استخدام مواقع التَّواصل الاجتماعي، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للسن وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (12,413) وهى قيمة دالة إحصائيًا عند درجتى حرية (4 ، 435) ومُستوى معنوية أقل من 0,05، فالأصغر سنًا (من 18 إلي 25 عامًا) (م=10,11) يستخدمون مواقع التَّواصل الاجتماعي أكثر مقارنة بالأكبر سنًا (55 سنة فأكثر) (م=8,50).

أما فيما يتعلق بمتغير دوافع استخدام مواقع التَّواصل الاجتماعي، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للسن عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (0,918) وهى قيمة غير دالة إحصائيًا عند درجتى حرية (4 ، 435) ومُستوى معنوية أقل من 0,05.

أما متغير إدراك الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للسن عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (1,930) وهى قيمة غير دالة إحصائيًا عند درجتى حرية (4 ، 435) ومُستوى معنوية أقل من 0,05.

أما متغير إدراك طرق المُحافظة على نظام الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للسن عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (0,861) وهى قيمة غير دالة إحصائيًا عند درجتى حرية (4 ، 435) ومُستوى معنوية أقل من 0,05.

وبالنسبة لمتغير إدراك مخاطر الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للسن وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (5,373) وهى قيمة دالة إحصائيًا عند درجتى حرية (4 ، 435) ومُستوى معنوية أقل من 0,05.

وأخيرًا بالنسبة لمُتغير إدراك انتهاكات الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للسن عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (0,391) وهى قيمة غير دالة إحصائيًا عند درجتى حرية (4 ، 435) ومُستوى معنوية أقل من 0,05.

وعليه يمكن القول أن اختبار صحة الفرض القائل بوجود فروق ذات دلالة إحصائية بين المبحوثين عينة الدِرَاسَةِ طبقًا للسن فى (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي

لانتهاكات الأمن السيبراني)، قد انتهى إلى عدم ثبوت صحة هذا الفرض بشكل جزئى.

لاختبار مصدر الفروق بين المبحوثين (عينة الدِرَاسَةِ) بحسب السن في متغيري مُعدلات استخدام مواقع التَّواصل الاجتماعي وإدراك مخاطر الأمن السيبراني، قامت الباحثة بإجراء اختبار بعدي PostHoc بطريقة LSD، والذي أسفر عن النتائج التَّالية:

- أنه فيما يخص متغير مُعدلات استخدام مواقع التَّواصل الاجتماعي فإنه توجد فروق ذات دلالة إحصائية بين كل من مجموعة المبحوثين التي تتراوح أعمارهم (من 18 إلي 25 عامًا) وبين مجموعة المبحوثين التي تتراوح أعمارهم (من 26 إلى 35 سنة) حيث كانت مُستوى معنويتها (0,009)، كما توجد فروق ذات دلالة إحصائية بين مجموعة المبحوثين التي تتراوح أعمارهم (من 18 إلي 25 عامًا) وبين أصحاب المجموعة التي تتراوح أعمارهم (من 36 إلى 45 سنة) حيث بلغ مُستوى معنويتها (0,000)، كذلك يوجد فروق ذات دلالة إحصائية بين مجموعة المبحوثين التي تتراوح أعمارهم (من 18 إلي 25 عامًا) وبين أصحاب المجموعة التي تتراوح أعمارهم (من 46 إلى 55 سنة) حيث بلغت مُستوى معنويتها (0,000)، وأيضًا توجد فروق ذات دلالة إحصائية بين مجموعة المبحوثين التي تتراوح أعمارهم (من 18 إلي 25 عامًا) وبين أصحاب المجموعة التي تتراوح أعمارهم (55 سنة فأكثر) حيث كانت مُستوى معنويتها (0,005)، أما فيما يتعلق بمجموعة المبحوثين التي تتراوح أعمارهم (من 26 إلى 35 سنة) فيتضح أنه توجد فروق ذات دلالة إحصائية بينها وبين أصحاب المجموعة التي تتراوح أعمارهم (من 36 إلى 45 سنة) حيث بلغ مُستوى معنويتها (0,003)، كذلك نفس الأمر بالنسبة للعلاقة بين أصحاب مجموعتى التي تتراوح أعمارهم (من 26 إلى 35 سنة) والتي تتراوح أعمارهم (من 46 إلى 55 سنة) حيث ثبت وجود فروق ذات دلالة إحصائية بينهم حيث بلغ مُستوى معنويتها (0,029)، بينما يختلف الأمر بالنسبة لأصحاب مجموعتى التي تتراوح أعمارهم (من 26 إلى 35 سنة) والتي تتراوح أعمارهم (55 سنة فأكثر) حيث ثبت عدم وجود فروق ذات دلالة إحصائية بينهم حيث بلغ مُستوى معنويتها (0,083)، والأمر ذاته بالنسبة لأصحاب المجموعة التي تتراوح أعمارهم (من 36 إلى 45 سنة) والتي تتراوح أعمارهم (من 46 إلى 55 سنة) حيث لا توجد فروق ذات دلالة إحصائية بينهما حيث سجل مُستوى معنويتها (0,772)، وكذلك الأمر بالنسبة لأصحاب المجموعة التي تتراوح أعمارهم (من 36 إلى 45 سنة) والتي تتراوح أعمارهم (55 سنة فأكثر) حيث لا توجد فروق ذات دلالة إحصائية بينهما حيث بلغت مُستوى معنويتها (0,985)، وأخيرًا الأمر ذاته بالنسبة لمجموعة المبحوثين التي تتراوح أعمارهم (من 46 إلى 55 سنة) فيتضح أنه لا توجد فروق ذات دلالة إحصائية بينها وبين أصحاب المجموعة التي تتراوح أعمارهم (55 سنة فأكثر) حيث بلغ مُستوى معنويتها (0,832).

- أما فيما يتعلق بمتغير إدراك مخاطر الأمن السيبراني فقد أشارت نتائج الاختبار إلى أنه توجد فروق ذات دلالة إحصائية بين كل من مجموعة المبحوثين التي تتراوح أعمارهم (من 18 إلي 25 عامًا) وبين مجموعة المبحوثين التي تتراوح أعمارهم (من 26 إلى 35 سنة) حيث كانت مُستوى معنويتها (0,008)، كما توجد فروق ذات دلالة إحصائية بين مجموعة المبحوثين التي تتراوح أعمارهم (من 18 إلي 25 عامًا) وبين أصحاب المجموعة التي تتراوح أعمارهم (من 36 إلى 45 سنة) حيث بلغ مُستوى معنويتها (0,000)، ولكن لا توجد فروق ذات دلالة إحصائية بين مجموعة المبحوثين التي تتراوح أعمارهم (من 18 إلي 25 عامًا) وبين أصحاب المجموعة التي تتراوح أعمارهم (من 46 إلى 55 سنة) حيث بلغت مُستوى معنويتها (0,220)، وكذلك لا توجد فروق ذات دلالة إحصائية بين مجموعة المبحوثين التي تتراوح أعمارهم (من 18 إلي 25 عامًا) وبين أصحاب المجموعة التي تتراوح أعمارهم (55 سنة فأكثر) حيث كانت مُستوى معنويتها (0,412)، أما فيما يتعلق بمجموعة المبحوثين التي تتراوح أعمارهم (من 26 إلى 35 سنة) فيتضح أنه لا توجد فروق ذات دلالة إحصائية بينها وبين أصحاب المجموعة التي تتراوح أعمارهم (من 36 إلى 45 سنة) حيث بلغ مُستوى معنويتها (0,110)، كذلك نفس الأمر بالنسبة للعلاقة بين أصحاب مجموعتى التي تتراوح أعمارهم (من 26 إلى 35 سنة) والتي تتراوح أعمارهم (من 46 إلى 55 سنة) حيث ثبت عدم وجود فروق ذات دلالة إحصائية بينهم حيث بلغ مُستوى معنويتها (0,718)، والأمر ذاته بالنسبة لأصحاب مجموعتى التي تتراوح أعمارهم (من 26 إلى 35 سنة) والتي تتراوح أعمارهم (55 سنة فأكثر) حيث ثبت عدم وجود فروق ذات دلالة إحصائية بينهم حيث بلغ مُستوى معنويتها (0,073)، وكذلك أصحاب المجموعة التي تتراوح أعمارهم (من 36 إلى 45 سنة) والتي تتراوح أعمارهم (من 46 إلى 55 سنة) فلا توجد فروق ذات دلالة إحصائية بينهما حيث سجل مُستوى معنويتها (0,124)، في حين اختلف الأمر بالنسبة لأصحاب المجموعة التي تتراوح أعمارهم (من 36 إلى 45 سنة) والتي تتراوح أعمارهم (55 سنة فأكثر) حيث توجد فروق ذات دلالة إحصائية بينهما حيث بلغت مُستوى معنويتها (0,010)، وأخيرًا نجد أن بالنسبة لمجموعة المبحوثين التي تتراوح أعمارهم (من 46 إلى 55 سنة) عدم وجود فروق ذات دلالة إحصائية بينها وبين أصحاب المجموعة التي تتراوح أعمارهم (55 سنة فأكثر) حيث بلغ مُستوى معنويتها (0,165).

ح) الفرض الثامن: توجد فروق ذات دلالة إحصائية بين المبحوثين (عينة الدِرَاسَةِ) بحسب المؤهل التعليمي في المتغيرات التَّالية: (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل

الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

قد اتضح للباحثة من نتيجة اختبار معنوية الفروق بين المبحوثين (عينة الدِرَاسَةِ) طبقًا للمؤهل التعليمي فى متغيرات (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

فبالنسبة لمتغير مُعدلات استخدام مواقع التَّواصل الاجتماعي، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمؤهل التعليمي وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (30,226) وهى قيمة دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية أقل من 0,05، فالمبحوثين الحاصلين على دراسات عليا (م= 10,24) يستخدمون مواقع التَّواصل الاجتماعي أكثر مقارنة بالحاصلين على مؤهل مُتوسط (م=8,37).

أما فيما يتعلق بمتغير دوافع استخدام مواقع التَّواصل الاجتماعي، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمؤهل التعليمي عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (1,983) وهى قيمة غير دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية أقل من 0,05.

أما متغير إدراك الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمؤهل التعليمي وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (6,681) وهى قيمة دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية أقل من 0,05، فالمبحوثين الحاصلين على دراسات عليا (م= 35,49) يدركون الأمن السيبراني بشكل أكبر مُقارنة بالحاصلين على مؤهل مُتوسط (م=32,09).

أما متغير إدراك طرق المُحافظة على نظام الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمؤهل التعليمي عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (1,874) وهى قيمة غير دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية أقل من 0,05.

وبالنسبة لمتغير إدراك مخاطر الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمؤهل التعليمي وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (8,038) وهى قيمة دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية

أقل من 0,05، فالمبحوثين الحاصلين على دراسات عليا (م= 15,33) يدركون مخاطر الأمن السيبراني بشكل أكبر مُقارنة بالحاصلين على مؤهل مُتوسط (م=13,90).

وأخيرًا بالنسبة لمُتغير إدراك انتهاكات الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمؤهل التعليمي عدم وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (0,952) وهى قيمة غير دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية أقل من 0,05.

وعليه يمكن القول أن اختبار صحة الفرض القائل بوجود فروق ذات دلالة إحصائية بين المبحوثين (عينة الدِرَاسَةِ) طبقًا للمؤهل التعليمي فى (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)، **قد انتهى إلى ثبوت صحة هذا الفرض بشكل جزئى**.

لاختبار مصدر الفروق بين المبحوثين (عينة الدِرَاسَةِ) بحسب المؤهل التعليمي في متغيرات مُعدلات استخدام مواقع التَّواصل الاجتماعي وإدراك الأمن السيبراني وإدراك مخاطر الأمن السيبراني، قامت الباحثة بإجراء اختبار بعدي PostHoc بطريقة LSD، والذي أسفر عن النتائج التَّالية:

- أنه فيما يخص متغير مُعدلات استخدام مواقع التَّواصل الاجتماعي فنجد أن هناك فروق ذات دلالة إحصائية بين كل من المبحوثين أصحاب المؤهلات المُتوسطة والمبحوثين أصحاب المؤهلات الجامعية حيث كانت مُستوى معنويتها (0,000)، كما توجد فروق ذات دلالة إحصائية بين المبحوثين أصحاب المؤهلات المُتوسطة وبين المبحوثين الحاصلين على الدِّرَاسَاتُ العليا حيث بلغ مُستوى معنويتها (0,000)، أما عن المبحوثين أصحاب المؤهلات الجامعية فقد اتضح أنه لا توجد فروق ذات دلالة إحصائية بينها وبين المبحوثين الحاصلين على الدِّرَاسَاتُ العليا حيث سجل مُستوى معنويتها (0,340).
- أما عن متغير إدراك الأمن السيبراني فنجد أن هناك فروق ذات دلالة إحصائية بين كل من المبحوثين أصحاب المؤهلات المُتوسطة والمبحوثين أصحاب المؤهلات الجامعية حيث كانت مُستوى معنويتها (0,001)، كما توجد فروق ذات دلالة إحصائية بين المبحوثين أصحاب المؤهلات المُتوسطة وبين المبحوثين الحاصلين على الدِّرَاسَاتُ العليا حيث بلغ مُستوى معنويتها (0,003)، أما عن المبحوثين أصحاب

المؤهلات الجامعية فقد اتضح أنه لا توجد فروق ذات دلالة إحصائية بينها وبين المبحوثين الحاصلين على الدِّرَاسَاتُ العليا حيث سجل مُستوى معنويتها (0,541).

- بالنسبة لمتغير إدراك مخاطر الأمن السيبراني فنجد أن هناك فروق ذات دلالة إحصائية بين كل من المبحوثين أصحاب المؤهلات المُتوسطة والمبحوثين أصحاب المؤهلات الجامعية حيث كانت مُستوى معنويتها (0,000)، كما توجد فروق ذات دلالة إحصائية بين المبحوثين أصحاب المؤهلات المُتوسطة وبين المبحوثين الحاصلين على الدِّرَاسَاتُ العليا حيث بلغ مُستوى معنويتها (0,002)، أما عن المبحوثين أصحاب المؤهلات الجامعية فقد اتضح أنه لا توجد فروق ذات دلالة إحصائية بينها وبين المبحوثين الحاصلين على الدِّرَاسَاتُ العليا حيث سجل مُستوى معنويتها (0,695).

ط) الفرض التاسع: توجد فروق ذات دلالة إحصائية بين المبحوثين (عينة الدِرَاسَةِ) بحسب المُستوى الاقتصادي الاجتماعي في المتغيرات التَّالية: (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

قد تبين للباحثة من نتيجة اختبار معنوية الفروق بين المبحوثين (عينة الدِرَاسَةِ) طبقًا للمُستوى الاقتصادي الاجتماعي فى متغيرات (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني).

فبالنسبة لمتغير مُعدلات استخدام مواقع التَّواصل الاجتماعي، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمُستوى الاقتصادي الاجتماعي وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (22,825) وهى قيمة دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية أقل من 0,05، فالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع (م= 10,38) يستخدمون مواقع التَّواصل الاجتماعي أكثر مُقارنة بالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض (م=8,99).

أما فيما يتعلق بمتغير دوافع استخدام مواقع التَّواصل الاجتماعي، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمُستوى الاقتصادي الاجتماعي وجود فروق ذات

دلالة إحصائية، حيث بلغت قيمة F (4,821) وهى قيمة دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية أقل من 0,05، فالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع (م= 38,40) لديهم دوافع أكثر لاستخدام مواقع التَّواصل الاجتماعي مُقارنة بالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض (م=35,74).

أما متغير إدراك الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمُستوى الاقتصادي الاجتماعي وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (6,145) وهى قيمة دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية أقل من 0,05، فالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع (م= 35,81) يدركون الأمن السيبراني بشكل أكبر مُقارنة بالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض (م=33,08).

أما متغير إدراك طرق المُحافظة على نظام الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمُستوى الاقتصادي الاجتماعي وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (5,826) وهى قيمة دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية أقل من 0,05، فالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع (م= 31,56) يدركون طرق المُحافظة على نظام الأمن السيبراني بشكل أكبر مُقارنة بالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض (م=28,86).

وبالنسبة لمتغير إدراك مخاطر الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمُستوى الاقتصادي الاجتماعي وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (7,542) وهى قيمة دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية أقل من 0,05، فالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع (م= 15,50) يدركون مخاطر الأمن السيبراني بشكل أكبر مُقارنة بالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض (م=14,33).

وأخيرًا بالنسبة لمُتغير إدراك انتهاكات الأمن السيبراني، أظهر اختبار معنوية الفروق بين المبحوثين طبقًا للمُستوى الاقتصادي الاجتماعي وجود فروق ذات دلالة إحصائية، حيث بلغت قيمة F (8,091) وهى قيمة دالة إحصائيًا عند درجتى حرية (2 ، 437) ومُستوى معنوية أقل من 0,05، فالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع (م= 11,74) يدركون إنتهاكات الأمن السيبراني بشكل أكبر مُقارنة بالمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض (م=10,58).

وعليه يمكن القول أن اختبار صحة الفرض القائل بوجود فروق ذات دلالة إحصائية بين المبحوثين (عينة الدِرَاسَةِ) طبقًا للمُستوى الاقتصادي الاجتماعي فى (مُعدلات استخدام مواقع التَّواصل الاجتماعي/ دوافع استخدام مواقع التَّواصل

الاجتماعي/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي للأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لطرق المُحافظة على نظام الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لمخاطر الأمن السيبراني/ إدراك مُستخدمي مواقع التَّواصل الاجتماعي لانتهاكات الأمن السيبراني)، **قد انتهى إلى ثبوت صحة هذا الفرض بشكل كلي**.

لاختبار مصدر الفروق بين المبحوثين (عينة الدِرَاسَةِ) بحسب المُستوى الاقتصادي الاجتماعي في متغيرات الدِرَاسَةِ، قامت الباحثة بإجراء اختبار بعدي PostHoc بطريقة LSD، والذي أسفر عن النتائج التَّالية:

- أنه فيما يخص متغير مُعدلات استخدام مواقع التَّواصل الاجتماعي فنجد أن هناك فروق ذات دلالة إحصائية بين كل من المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض والمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُتوسط حيث كانت مُستوى معنويتها (0,000)، كما توجد فروق ذات دلالة إحصائية بين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث بلغ مُستوى معنويتها (0,000)، أما عن المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُتوسط فقد اتضح أنه لا توجد فروق ذات دلالة إحصائية بينها وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث سجل مُستوى معنويتها (0,217).
- بالنسبة لمتغير دوافع استخدام مواقع التَّواصل الاجتماعي فنجد أنه لا توجد فروق ذات دلالة إحصائية بين كل من المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض والمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُتوسط حيث كانت مُستوى معنويتها (0,065)، ولكن توجد فروق ذات دلالة إحصائية بين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث بلغ مُستوى معنويتها (0,003)، أما عن المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُتوسط فقد اتضح أنه لا توجد فروق ذات دلالة إحصائية بينها وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث سجل مُستوى معنويتها (0,084).
- أما عن متغير إدراك الأمن السيبراني فنجد أن هناك فروق ذات دلالة إحصائية بين كل من المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض والمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُتوسط حيث كانت مُستوى معنويتها (0,003)، كما توجد فروق ذات دلالة إحصائية بين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث بلغ مُستوى معنويتها (0,003)، أما عن المبحوثين ذو المُستوى الاقتصادي

الاجتماعي المُتوسط فقد اتضح أنه لا توجد فروق ذات دلالة إحصائية بينها وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث سجل مُستوى معنويتها (0,422).

- فيما يخص متغير إدراك طرق المُحافظة على نظام الأمن السيبراني فنجد أنه لا توجد فروق ذات دلالة إحصائية بين كل من المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض والمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُتوسط حيث كانت مُستوى معنويتها (0,068)، ولكن توجد فروق ذات دلالة إحصائية بين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث بلغ مُستوى معنويتها (0,001)، وكذلك الأمر نفسه بالنسبة المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُتوسط فقد اتضح أنه توجد فروق ذات دلالة إحصائية بينها وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث سجل مُستوى معنويتها (0,036).
- بالنسبة لمتغير إدراك مخاطر الأمن السيبراني فنجد أن هناك فروق ذات دلالة إحصائية بين كل من المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض والمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُتوسط حيث كانت مُستوى معنويتها (0,001)، كما توجد فروق ذات دلالة إحصائية بين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث بلغ مُستوى معنويتها (0,002)، أما عن المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُتوسط فقد اتضح أنه لا توجد فروق ذات دلالة إحصائية بينها وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث سجل مُستوى معنويتها (0,521).
- أما عن متغير إدراك انتهاكات الأمن السيبراني فنجد أن هناك فروق ذات دلالة إحصائية بين كل من المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض والمبحوثين ذو المُستوى الاقتصادي الاجتماعي المُتوسط حيث كانت مُستوى معنويتها (0,029)، كما توجد فروق ذات دلالة إحصائية بين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُنخفض وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث بلغ مُستوى معنويتها (0,003)، أما عن المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُتوسط فقد اتضح أنه لا توجد فروق ذات دلالة إحصائية بينها وبين المبحوثين ذو المُستوى الاقتصادي الاجتماعي المُرتفع حيث سجل مُستوى معنويتها (0,146).

توصيات الدِرَاسَةِ:

- عقد دورات تدريبية وورش عمل تابعة للجامعات المصرية في مجال الأمن السيبراني وإجراءات الحماية ضد مخاطره وانتهاكاته بإشراف مدربين مختصين في مجال الأمن السيبراني.
- التنسيق بين وزارة التربية التعليم وزارة التربية والتعليم العالي والجهات المُشرفة على الأمن السيبراني؛ لاتخاذ الإجراءات اللازمة لتعريف الطلاب داخل المدارس والجامعات بالأمن السيبراني وإجراءات الحماية ضد مخاطره وانتهاكاته، وذلك لأن أكثر مُستخدمي مواقع التَّواصل الاجتماعي في عصرنا الحالي هم طلاب المدارس والجامعات وذلك لاتجاه التعليم من التعليم المُباشر إلى التعليم الأون لاين.
- استقطاب كفاءات بشرية في مجال الأمن السيبراني، وإدراج مقررات دراسية خاصة بمفاهيم الأمن السيبراني ضمن برنامج تعليم الحاسب الآلي في المدارس والجامعات.
- الاهتمام بالدِّرَاسَاتُ الخاصة بالأمن السيبراني، فلا يزال الأمن السيبراني في مصر تُربة خصبة قابلة للمزيد من الدِرَاسَةِ والبحث، حيث أن هناك جوانب في هذا المجال لم يتم البحث فيها والدِرَاسَةِ بعد كـــ (علاقة الأمن السيبراني بالأمن القومي/ كيفية استخدام الجهات الحكومية لنظام الأمن السيبراني لحماية معلوماتهم/ الفروق بين استخدام الجهات الحكومية والخاصة لأنظمة الأمن السيبراني لحماية المعلومات الخاصة بهم/ الجرائم الإلكترونية وأسباب انتشارها .... وغيرها من الجوانب)، ولذلك يجب القيام بالمزيد من الدِّرَاسَاتُ والأبحاث لتطوير هذا المجال وتحقيق الغرض المرجو منه.

مراجع الدِرَاسَةِ:

أولًا: المراجع العربية:

1) الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني، 2018، مُتاح على:- https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf., accessed on 17/12/2020.
2) تغريد معين حسن المشهدي، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، **مجلة البحوث الجغرافية**، العدد 30 (العراق: جامعة الكوفة، كلية التربية للبنات، 2019).
3) جبريل بن حسن العريشي، سلمى بنت عبد الرحمن الدوسري، أثر استخدام وسائل التَّواصل الاجتماعي على القيم والأمن الفكري لديهم: دِرَاسَةٍ ميدانية وصفية مطبقة على طلاب وطالبات الجامعات السعودية، **مجلة دراسات في الخدمة الاجتماعية والعلوم الإنسانية**، المجلد17، العدد 38 (مصر: مجلة دراسات في الخدمة الاجتماعية والعلوم الإنسانية، 2015).
4) حسن محمد على حسن، مخاطر استخدام الفضاء السبراني في الحياة الاجتماعية والثقافية والأسرية دون حماية وآثارها، **المؤتمر السابع لأمن وسلامة الفضاء السيبراني (الإنترنت) في الدول العربية** (لبنان: بيروت، 2018).
5) حمد بن حمود بن حميد السواط، وآخرون، العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الأبتدائية والمُتوسطة بمدينة الطائف، **مجلة البحث العلمي في التربية**، المجلد4، العدد21 (القاهرة: جامعة عين شمس، كلية البنات للأداب والعلوم والتربية، 2020).
6) شيماء ذو الفقار زعيب، **مناهج البحث والاستخدامات الإحصائية في الدِرَاسَاتُ الإعلامية**، ط2 (القاهرة: الدار المصرية اللبنانية، 2015).
7) صالح بن علي بن عبد الرحمن الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، مُتاح على:

https://edu.moe.gov.sa/jeddah/DocumentCentre/Docs/%D9%85%D8%20Security.pdf., accessed on 17/12/2020.

8) عبد الرحيم محمد، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، 2015، مُتاح على:

http://dr-ama.com/wpcontent/uploads/2019/12/%D8%A7%.pdf, accessed on 17/12/2020.

9) عبد الفتاح الطاهري، الجريمة المعلوماتية بين ثبات النص وتطور الجريمة، مجلة القانون والأعمال، مُتاح على:

https://www.droitetentreprise.com/?p=12729, accessed on 17/12/2020.

10) علم الدين بانقا، **مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دِرَاسَةِ حالة دول مجلس التعاون الخليجي**، العدد63 (الكويت: المعهد العربي للتخطيط، سلسلة دراسات تنموية، 2019).
11) عماد عبده محمد علوان، أشكال التنمر في ضوء بعض المتغيرات الديموغرافية بين الطلاب المراهقين بمدينة أبها، **مجلة كلية التربية**، العدد168، المجلد35، الجزء الأول (القاهرة: جامعة الأزهر، كلية التربية، 2016).

12) فاطمة يوسف المنتشري، دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، **المجلة العربية للعلوم التربوية والنفسية**، المجلد4، العدد17 (المؤسسة العربية للتربية والعلوم والآداب: المجلة العربية للعلوم التربوية والنفسية، 2020).
13) فاطمة يوسف المنتشري، رندة حريري، درجة وعي معلمات المرحلة المُتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، **المجلة العربية للتربية النوعية**، المجلد4، العدد13 (القاهرة: المؤسسة العربية للتربية والعلوم والآداب، 2020).
14) لحمر عباس ابن تاج، يحياوي سليمان، أخلاقيات الأعمال الإلكترونية وتحديات الأمن المعلوماتي في ظل الاقتصاد الرقمي، **المجلة المصرية للدراسات القانونية والاقتصادية**، العدد10 (مصر: المجلة المصرية للدراسات القانونية والاقتصادية، 2018).
15) ماجدة غريب، حسن الأمير، مدى الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي، **المجلة العربية الدولية للمعلوماتية**، المجلد 5، العدد 9 (المملكة العربية السعودية: جامعة نايف للعلوم الأمنية، كلية أمن الحاسب والمعلومات، 2017) ص17 – 32.
16) محمد بن حمد البادي، الابتزاز الإلكتروني، جريدة الرؤية العمانية، 2017، مُتاح على:

https://alroya.om/post/197625/%D8%A7%, accessed on 17/12/2020.

17) محمد بن ناصر محمد الهزاني، المسؤولية الجنائية عن انتهاك قواعد الفضاء السيبراني: دِرَاسَةٍ تأصيلية مُقارنة بالقانون الإماراتي، **رسالة ماجستير غير منشورة** (المملكة العربية السعودية: جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الشريعة والقانون، 2018).
18) محمد قاسم أسعد الردفاني، تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية، **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 30، العدد 61 (المملكة العربية السعودية: جامعة نايف العربية للعلوم الامنية، 2014).
19) مصباح أحمد حامد الصحفي، سناء صالح عسكول، مُستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة، **مجلة البحث العلمي في التربية**، المجلد10، العدد20 (القاهرة: جامعة عين شمس، كلية البنات للآداب والعلوم والتربية، 2019).
20) مصطفى الطيب، الفرق بين أمن المعلومات والأمن السيبراني، مُتاح على:

https://www.oolom.com/6124/%D8%A7%, accessed on 17/12/2020.

21) منى الأشقر جبور، **السيبرانية ـ هاجس العصر** (بيروت: جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، 2016).
22) نورة بنت ناصر القحطاني، مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دِرَاسَةٍ ميدانية، **شؤون اجتماعية**، المجلد36، العدد144 (الأمارات العربية المُتحدة: جمعية الاجتماعيين في الشارقة، 2019).
23) نورة عمر الصانع، وآخرون، وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم، **مجلة كلية التربية**، المجلد36، العدد6 (أسيوط: جامعة أسيوط، كلية التربية، 2020).
24) هاني خميس أحمد عبده، الدين والثورات السياسية: الحالة المصرية نموذجًا، **سلسلة رؤى إستراتيجية**، العدد3 (الإمارات: مركز الإمارات للدِّرَاسَاتُ والبحوث الاستراتيجية، 2013).
25) وفاء بنت حسن عبد الوهاب صائغ، وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية، **المجلة العربية للعلوم الاجتماعية**، المجلد3، العدد14

(مدينة الملك عبد العزيز للعلوم والتقنية: المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية، 2018).

ثانيًا: المراجع الأجنبية:

1) Alan McKee, **The Public Sphere: An Introduction** (United Kingdom: Cambridge University Press, 2004).
2) Arjen Spiering, Improving cyber security safety awareness education at Dutch elementary schools, **MA** (leiden: leidein university, 2013).
3) Charles E. Wilson, Cybersecurity Education: The Emergence of an Accredited Academic Discipline?, **Journal of The Colloquium for Information Systems Security Education**, Vol. 2, No. 1, 2014.
4) Davina Pruitt-Mentle, The C3 framework: Cyberethics, cybersafety, and cybersecurity implications for the educational setting, 2000, Available At:

http://knowwheretheygo.org/static/content/MATRIX.pdf, accessed on 17/12/2020.

5) Eliza Tanner, Chilean Conversation: internet Forum Participants Debate Augusto Pinochet's Detention, **Jornal of communication**, Vol. 51, Issue 2, 2001.
6) Elmarie Kritzinger, Cultivating a cyber-safety culture among school learners in South Africa, **Africa Education Review**, Vol. 14, Issue 1, 2017.
7) Lauren K. Mark, Thanh Truc T. Nguyen, An Invitation to Internet Safety and Ethics: School and Family Collaboration, **Journal of Invitational Theory and Practice**, Vol. 23, 2017.
8) Mike Westing, Expanding the public Sphere: The impact of facebook on political communication, **Journal of The UK's European University**, Vol. 28, Issue 5, 2007.
9) Noluxolo Kortjan, Rossouw von Solms, Cyber Security Education in Developing Countries: A South African Perspective, **4th International ICST Conference, AFRICOMM 2012,** Yaounde, Cameroon, 2012.
10) Rituparna Das, Mayank Patel, Cyber Security for Social Networking Sites: Issues, Challenges and Solutions**, International Journal for Research in Applied Science & Engineering Technology**, Vol.5, Issue 4, 2017.
11) Robyn Eckersley, A Green Public Sphere in the WTO?: The Amicus Curiae Interventions in the Transatlantic Biotech Dispute, **European Journal of International Relations**, Vol. 13, No. 3, 2007.
12) Rossouw Von Solms, Suné Von Solms, Cyber Safety Education in Developing Countries, Available At:

http://researchspace.csir.co.za/dspace/bitstream/handle/10204/8226/Von%20Solms_2015.pdf;sequence=1, accessed on 16/12/2020.
13) Steven Michael Schneider, Expanding the public sphere through computer-mediated communication: political discussion about abortion in a Usenet newsgroup, **PHD** (Canada: Massachusetts Institute of Technology, Department of Political Science, 1997).

هوامش الدراسة

1) منى الأشقر جبور، **السيبرانية ـ هاجس العصر** (بيروت: جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، 2016) ص149.
2) Rossouw Von Solms, Suné Von Solms, Cyber Safety Education in Developing Countries, Available At: http://researchspace.csir.co.za/dspace/bitstream/handle/10204/8226/Von%20Solms_2015.pdf;sequence=1, accessed on 16/12/2020.
3) Charles E. Wilson, Cybersecurity Education: The Emergence of an Accredited Academic Discipline?, **Journal of The Colloquium for Information Systems Security Education**, Vol. 2, No. 1, 2014, pp. 1 – 13.
4) Noluxolo Kortjan, Rossouw von Solms, Cyber Security Education in Developing Countries: A South African Perspective, **4th International ICST Conference, AFRICOMM 2012,** Yaounde, Cameroon, 2012, pp. 289 – 297.
5) فاطمة يوسف المنتشري، رندة حريري، درجة وعي معلمات المرحلة المُتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، **المجلة العربية للتربية النوعية**، المجلد4، العدد13 (القاهرة: المؤسسة العربية للتربية والعلوم والآداب، 2020) ص95 – 140.
6) حمد بن حمود بن حميد السواط، وآخرون، العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الأبتدائية والمُتوسطة بمدينة الطائف، **مجلة البحث العلمي في التربية**، المجلد4، العدد21 (القاهرة: جامعة عين شمس، كلية البنات للأداب والعلوم والتربية، 2020) ص278 – 306.
7) نورة عمر الصانع، وآخرون، وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم، **مجلة كلية التربية**، المجلد36، العدد6 (أسيوط: جامعة أسيوط، كلية التربية، 2020) ص41 – 90.
8) وفاء بنت حسن عبد الوهاب صائغ، وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية، **المجلة العربية للعلوم الاجتماعية**، المجلد3، العدد14 (مدينة الملك عبد العزيز للعلوم والتقنية: المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية، 2018) ص18 – 70.
9) مصباح أحمد حامد الصحفي، سناء صالح عسكول، مُستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة، **مجلة البحث العلمي في التربية**، المجلد10، العدد20 (القاهرة: جامعة عين شمس، كلية البنات للآداب والعلوم والتربية، 2019) ص493 – 534.
10) Elmarie Kritzinger, Cultivating a cyber-safety culture among school learners in South Africa, **Africa Education Review**, Vol. 14, Issue 1, 2017, pp. 22 – 41.
11) نورة بنت ناصر القحطاني، مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دِرَاسَةٍ ميدانية، **شؤون اجتماعية**، المجلد36، العدد144 (الأمارات العربية المُتحدة: جمعية الاجتماعيين في الشارقة، 2019) ص 85 – 120.
12) فاطمة يوسف المنتشري، دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية

للبنات بمدينة جدة من وجهة نظر المعلمات، **المجلة العربية للعلوم التربوية والنفسية**، المجلد4، العدد17 (المؤسسة العربية للتربية والعلوم والآداب: المجلة العربية للعلوم التربوية والنفسية، 2020) ص457 – 484.

13) Lauren K. Mark, Thanh Truc T. Nguyen, An Invitation to Internet Safety and Ethics: School and Family Collaboration, **Journal of Invitational Theory and Practice**, Vol. 23, 2017, pp. 62 – 75.

14) Arjen Spiering, Improving cyber security safety awareness education at Dutch elementary schools, **MA** (leiden: leidein university, 2013).

15) ماجدة غريب، حسن الأمير، مدى الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي، **المجلة العربية الدولية للمعلوماتية**، المجلد 5، العدد 9 (المملكة العربية السعودية: جامعة نايف للعلوم الأمنية، كلية أمن الحاسب والمعلومات، 2017) ص17 – 32.

16) Rituparna Das, Mayank Patel, Cyber Security for Social Networking Sites: Issues, Challenges and Solutions**, International Journal for Research in Applied Science & Engineering Technology**, Vol.5, Issue 4, 2017, pp. 833 – 838.

17) Steven Michael Schneider, Expanding the public sphere through computer-mediated communication: political discussion about abortion in a Usenet newsgroup, **PHD** (Canada: Massachusetts Institute of Technology, Department of Political Science, 1997) p. 17.

18) Alan McKee, **The Public Sphere: An Introduction** (United Kingdom: Cambridge University Press, 2004) p. 8.

19) هاني خميس أحمد عبده، الدين والثورات السياسية: الحالة المصرية نموذجًا، **سلسلة رؤى إستراتيجية**، العدد3 (الإمارات: مركز الإمارات للدِّرَاسَاتُ والبحوث الاستراتيجية، 2013) ص38.

20) Mike Westing, Expanding the public Sphere: The impact of facebook on political communication, **Journal of The UK's European University**, Vol. 28, Issue 5, 2007, pp. 835 – 860.

21) Robyn Eckersley, A Green Public Sphere in the WTO?: The Amicus Curiae Interventions in the Transatlantic Biotech Dispute, **European Journal of International Relations**, Vol. 13, No. 3, 2007, p. 332.

22) Eliza Tanner, Chilean Conversation: internet Forum Participants Debate Augusto Pinochet's Detention, **Jornal of communication**, Vol. 51, Issue 2, 2001, pp. 386 – 387.

23) Davina Pruitt-Mentle, The C3 framework: Cyberethics, cybersafety, and cybersecurity implications for the educational setting, 2000, Available At: http://knowwheretheygo.org/static/content/MATRIX.pdf, accessed on 17/12/2020.

24) حمد بن حمود بن حميد السواط، وآخرون، **مرجع سَّابق**، ص283.

25) مصطفى الطيب، الفرق بين أمن المعلومات والأمن السيبراني، مُتاح على: https://www.oolom.com/6124/%D8%A7%, accessed on 17/12/2020.
26) عبد الرحيم محمد، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، 2015، مُتاح على: http://dr-ama.com/wpcontent/uploads/2019/12/%D8%A7%.pdf, accessed on 17/12/2020.
27) تغريد معين حسن المشهدي، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، **مجلة البحوث الجغرافية**، العدد 30 (العراق: جامعة الكوفة، كلية التربية للبنات، 2019) ص240.
28) راجعت الباحثة إلى:
- صالح بن علي بن عبد الرحمن الربيعة، الأمن الرقمي وحماية المُستخدم من مخاطر الإنترنت، مُتاح على: https://edu.moe.gov.sa/jeddah/DocumentCentre/Docs/%D9%85%D8%20Security.pdf., accessed on 17/12/2020.
- وفاء بنت حسن عبد الوهاب صائغ، **مرجع سَّابق**.

29) **المرجع نفسه**.
30) مصباح أحمد حامد الصحفي، سناء صالح عسكول، **مرجع سَّابق**، ص498 – 499.
31) محمد بن حمد البادي، الابتزاز الإلكتروني، جريدة الرؤية العمانية، 2017، مُتاح على: https://alroya.om/post/197625/%D8%A7%, accessed on 17/12/2020.
32) عماد عبده محمد علوان، أشكال التنمر في ضوء بعض المتغيرات الديموغرافية بين الطلاب المراهقين بمدينة أبها، **مجلة كلية التربية**، العدد168، المجلد35، الجزء الأول (القاهرة: جامعة الأزهر، كلية التربية، 2016) ص441 – 474.
33) عبد الفتاح الطاهري، الجريمة المعلوماتية بين ثبات النص وتطور الجريمة، مجلة القانون والأعمال، مُتاح على: https://www.droitetentreprise.com/?p=12729, accessed on 17/12/2020.
34) علم الدين بانقا، **مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دِرَاسَةِ حالة دول مجلس التعاون الخليجي**، العدد63 (الكويت: المعهد العربي للتخطيط، سلسلة دراسات تنموية، 2019).
35) محمد بن ناصر محمد الهزاني، المسؤولية الجنائية عن انتهاك قواعد الفضاء السيبراني: دِرَاسَةِ تأصيلية مقارنة بالقانون الإماراتي، **رسالة ماجستير غير منشورة** (المملكة العربية السعودية: جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الشريعة والقانون، 2018).
36) محمد قاسم أسعد الردفاني، تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية، **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 30، العدد 61 (المملكة العربية السعودية: جامعة نايف العربية للعلوم الامنية، 2014) ص157 – 192.
37) لحمر عباس ابن تاج، يحياوي سليمان، أخلاقيات الأعمال الإلكترونية وتحديات الأمن المعلوماتي في ظل الاقتصاد الرقمي، **المجلة المصرية للدراسات القانونية والاقتصادية**، العدد10 (مصر: المجلة المصرية للدراسات القانونية والاقتصادية، 2018) ص299 – 329.
38) محمد بن ناصر محمد الهزاني، **مرجع سَّابق**.

39) الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني، 2018، مُتاح على: https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf, accessed on 17/12/2020.

40) حسن محمد على حسن، مخاطر استخدام الفضاء السبراني في الحياة الاجتماعية والثقافية والأسرية دون حماية وآثارها، **المؤتمر السابع لأمن وسلامة الفضاء السيبراني (الإنترنت) في الدول العربية** (لبنان: بيروت، 2018).

41) جبريل بن حسن العريشي، سلمى بنت عبد الرحمن الدوسري، أثر استخدام وسائل التَّواصل الاجتماعي على القيم والأمن الفكري لديهم: دِرَاسَةٍ ميدانية وصفية مُطبقة على طلاب وطالبات الجامعات السعودية، **مجلة دراسات في الخدمة الاجتماعية والعلوم الإنسانية**، المجلد17، العدد 38 (مصر: مجلة دراسات في الخدمة الاجتماعية والعلوم الإنسانية، 2015) ص3273 – 3346.

42) محمد قاسم أسعد الردفاني، **مرجع سَّابق**.

43) أسماء الأساتذة المُحكمين طبقًا للترتيب الأبجدي والمنصب الجامعي:

- أ.د/ الأميرة سماح فرج أستاذ وعميد كلية الإعلام جامعة سيناء فرع شرق القنطرة.
- أ.د/ بركات عبد العزيز أستاذ بقسم الإذاعة والتليفزيون بكلية الإعلام جامعة القاهرة، ووكيل الدِّرَاسَاتُ العليا سَّابقا.
- أ.د/ رمضان إبراهيم محمد أستاذ ورئيس قسم العلاقات العامة بكلية الإعلام جامعة الأزهر.
- أ.د/ عادل فهمي البيومي الاستاذ بقسم الإذاعة والتليفزيون كلية الإعلام جامعة القاهرة.
- أ.د/ عبد الرحيم دوريش استاذ ووكيل شؤون الدِّرَاسَاتُ العليا بكلية الإعلام جامعة بني سويف.
- أ.د/ علي عجوة أستاذ بقسم العلاقات العامة كلية الإعلام جامعة القاهرة.
- أ.د/ محمود حسن إسماعيل أستاذ ورئيس قسم الإعلام بمعهد الدِّرَاسَاتُ العليا للطفولة جامعة عين شمس.
- أ.د/ نسمة البطريق الاستاذ بقسم الإذاعة والتليفزيون كلية الإعلام جامعة القاهرة.
- د/ رجاء الغمراوي الأستاذ المُساعد بقسم الإذاعة والتليفزيون جامعة فاروس.
- د/ فاطمة شعبان محمد الأستاذ المُساعد بقسم الإذاعة والتليفزيون بالمعهد الدولي العالي للإعلام بالشروق.

44) شيماء ذو الفقار زعيب، **مناهج البحث والاستخدامات الإحصائية في الدِّرَاسَاتُ الإعلامية**، ط2 (القاهرة: الدار المصرية اللبنانية، 2015) ص243.