Journal of the College of Education for Humanities
University of Thi-Qar \ ISSN:2707-5672
مجلة كلية التربيـة للعلـوم الانسـانيـة
جامعة ذي قار / الرقم المعياري 2707-5672
https://doi.org/10.32792/utq/jedh/v15i4

مستوى وعي الأفراد بالأمن السيبراني: دراسة تحليلية للمعرفة والممارسات في وسائل الاعلام الرقمي

م.م ضرغام كامل عبد / كلية التربية للعلوم الإنسانية جامعة ذي قار
DharkhamkamelAbd@utq.edu.iq

الملخص

هدف البحث إلى التعرف على مستوى وعي الأفراد بالأمن السيبراني عن طريق تحليل معارفهم وممارساتهم في وسائل الإعلام الرقمي، عبر الكشف عن مستوى وعيهم بمخاطر وانتهاكات الأمن السيبراني في وسائل الإعلام الرقمي، ومدى معرفتهم ووعيهم بتطبيقات الأمن السيبراني وممارساتهم للوقاية من الأضرار التي قد تلحق بهم، فضلاً عن مستوى وعيهم بمفاهيم الأمن السيبراني، وتوصل البحث إلى أن أفراد العينة المختارة والبالغ عددها (50) فرداً، كان وعيهم وممارساتهم تجاه مخاطر وانتهاكات الأمن السيبراني، وتجاه تطبيقات الأمن السيبراني بدرجة (مرتفعة)، اما وعيهم وممارساتهم تجاه مفاهيم الأمن السيبراني فكان بدرجة متوسطة. واوصى الباحث؛ بضرورة تنفيذ حملات توعوية؛ تستهدف مختلف فئات المجتمع لزيادة إدراكهم بالمخاطر السيبرانية، وتعزيز ثقافة الإبلاغ؛ عن الإساءة عبر منصات التواصل الاجتماعي، وتوفير قنوات رسمية، تضمن استجابة فعالة لحماية الأفراد من التهديدات الإلكترونية.

الكلمات المفتاحية: الأمن السيبراني, و سائل الإعلام الرقمي

Journal of the College of Education for Humanities
University of Thi-Qar \ ISSN:2707-5672

مجلة كلية التربيـة للعلـوم الانسـانيـة
جامعة ذي قار / الرقم المعياري 2707-5672

https://doi.org/10.32792/utq/jedh/v15i4

Individuals' level of Awareness of Cybersecurity: An Analytical Study of Knowledge and Practices in Digital Media

Dhurgam Kamel Abed
DharkhamkamelAbd@utq.edu.iq

Abstract

This research aimed to determine individuals' level of awareness of cybersecurity by analyzing their knowledge and practices in digital media. This study explored their level of awareness of cybersecurity risks and violations in digital media, their knowledge and awareness of cybersecurity applications and practices to prevent potential harm, and their level of awareness of cybersecurity concepts. The research found that the selected sample, numbering (50) individuals, had a high level of awareness and practices regarding cybersecurity risks and violations, as well as regarding cybersecurity applications. However, their awareness and practices regarding cybersecurity concepts were moderate. The researcher recommended the need to implement awareness campaigns targeting various segments of society to increase their awareness of cybersecurity risks, promote a culture of reporting abuse on social media platforms, and provide official channels that ensure an effective response to protect individuals from cyber threats.

Keywords: Cybersecurity, Digital Media

المقدمة

أدت الثورة الرقمية المعاصرة إلى تطورات هائلة غير مسبوقة، ومن أهم إفرازات هذه الثورة ما يُعرف بالفضاء السيبراني، الذي أصبح جزءاً من نشاطات الفرد في مجالات عديدة، وفي ظل التطور التكنولوجي المتسارع، وزيادة الاعتماد على منصات الوسائل الرقمية في مختلف جوانب الحياة، أصبحت هذه المنصات نافذة رئيسة للتواصل والتعلم، وعلى الرغم من الايجابيات التي يحملها الفضاء السيبراني، إلاَّ أنه يقبع خلفه واقع افتراضي خطير، إذ يسكن تجار المخدرات، والمجرمون، والمنظمات الإرهابية، واللصوص، والمحتالون، والمبتزون، الأمر الذي جعل هذا الفضاء مصدر تهديد للمستخدمين له، عبر ما يعرف بالهجمات السيبرانية، التي تسبب خسائر فادحة، تصل إلى حد التلاعب بالبيانات، أو تزييفها، أو محوها من الأجهزة المستخدمة للفضاء، وتزداد الخطورة عندما تتعرض خصوصيات الأفراد للاختراق، وتعرضهم للابتزاز، والقرصنة، وسرقة هوياتهم، وتسرب المعلومات إلى أشخاص غير مخولين.

وفي سياق ذلك، ظهر ما يُعرف بالأمن السبراني الذي يهدف إلى حماية البيانات التي تخص الأفراد، والمؤسسات، وحماية أجهزة الكومبيوتر، والبرمجيات، والشبكات من الوصول غير المصرح به، ما جعل الأمن السيبراني إطاراً أساسياً لحماية الأشخاص، وأحد أهم الركائز التي تحمي البيانات، والمعلومات الشخصية، والمؤسسية من الاختراقات، والهجمات الإلكترونية، واصبح الخط الدفاعي الأول في مواجهة هذه المخاطر، ومع ذلك، تشير دراسات عديدة إلى أن مستوى الوعي السبراني لا يزال محدوداً لدى الكثير من مستخدمي وسائل الاتصال الالكترونية، ما يجعلهم عرضة للاستغلال الإلكتروني.

ومن هنا تبرز أهمية هذا البحث الذي جاء بعنوان "مستوى وعي الأفراد بالأمن السيبراني: دراسة تحليلية للمعرفة والممارسات في وسائل الاعلام الرقمي"، الذي يهدف إلى تحليل مستوى وعي الأفراد بالأمن السيبراني، ومدى معرفتهم بالممارسات الآمنة في التعامل مع وسائل الإعلام الرقمي.

قسم البحث على مقدمة وثلاثة مباحث، تناولنا في المبحث الأول "الاطار المنهجي"، الذي شمل مشكلة البحث، وأهميته، وأهدافه، ونوع البحث ومنهجيته، ومجتمع البحث وعينته، والأدوات التي اعتمد عليها الباحث لجمع البيانات، أما المبحث الثاني "الاطار النظري"، فشمل تعريف المصطلحات الواردة في البحث، والنظرية المؤطرة للبحث "نظرية السلوك المخطط"، فيما خصص المبحث الثالث لعرض النتائج.

الاطار النظري

اولاً. مشكلة البحث

على الرغم من إنتشار التوعية بالأمن السيبراني عبر وسائل الإعلام، والحملات التثقيفية، فإنه لا يزال هناك نقص كبير في فهم العديد من مستخدمي وسائل التواصل الالكترونية للمخاطر الإلكترونية وكيفية مواجهتها. وتكمن مشكلة البحث في أنَّ بعض الأفراد قد يمتلكون معرفة نظرية بمبادئ الأمن السيبراني، إلاَّ أنهم لا يطبقونها عملياً، ما يجعلهم عرضة للاختراق، أو الاحتيال الإلكتروني، لذا، يسعى هذه البحث إلى الإجابة عن مجموعة تساؤلات تدور في ذهن الباحث التي تتفرع عن السؤال الرئيس التالي: **ما هو مستوى وعي الأفراد بالأمن السيبراني، وكيف تؤثر المعرفة والممارسات المرتبطة به على استخدامهم لوسائل الإعلام الرقمي؟** وتفرع منه الاسئلة الاتية:

1. ما هو مستوى وعي الأفراد بمخاطر وانتهاكات الأمن السيبراني في وسائل الإعلام الرقمي وكيفية الوقاية منها؟
2. ما مدى معرفة الأفراد بالوعي بتطبيقات الأمن السيبراني ؟
3. ما هو مستوى وعي الأفراد بمفاهيم الأمن السيبراني ؟

ثانياً. أهمية البحث

تكمن أهمية هذا البحث في أنه يُسلط الضوء على واقع الوعي السيبراني لدى الأفراد في بيئة رقمية متغيرة، ويقدم تحليلاً علمياً للممارسات الأمنية التي يتبعها المستخدمون في وسائل الإعلام الرقمي، وإسهامه في تعزيز التوعية بالأمن السيبراني، ووضع توصيات لتحسين السلوكيات الرقمية الآمنة للأفراد، فضلاً عن فائدته للجهات المعنية "الحكومات، المؤسسات التعليمية، شركات التقنية" في تصميم برامج توعوية أكثر فعالية.

ثالثاً. أهداف البحث

يهدف هذا البحث إلى:

1. الكشف عن مستوى وعي الأفراد بمخاطر وانتهاكات الأمن السيبراني في وسائل الإعلام الرقمي، وكيفية الوقاية منها.
2. معرفة مستوى وعي الأفراد بتطبيقات الأمن السيبراني.
3. الكشف عن مستوى وعي الأفراد بمفاهيم الأمن السيبراني.

رابعاً. نوع البحث ومنهجه

يقع هذا البحث ضمن البحوث الوصفية التحليلية، وهو اسلوب من أساليب التحليل المرتكز على معلومات كافية ودقيقة عن موضوع أو ظاهرة ما، خلال مدة زمنية معينة ومعلومة، للحصول على نتائج علمية تم تفسيرها بطريقة موضوعية، منسجمة مع المعطيات الفعلية للظاهرة. التي لا تقتصر على الوصف، بل تتعدى ذلك في محاولة فهم وتفسير مستوى الوعي الحالي، وتحليل الممارسات اليومية للأفراد في التعامل مع الأمن السيبراني. وأُستعمل المنهج المسحي في هذا البحث، إذ تم في اطاره استعمال اسلوب المسح الميداني على عينة من الافراد، للتعرف على كيفية اسهامهم في التوعية الصحية للحد من تعاطي المخدرات في المجتمع عبر منصات الإعلام الرقمي.

خامساً. اداة البحث

اعتمد البحث على الاستبانة لجمع بيانات ميدانية من عينة من مستخدمي الإنترنت لقياس مستوى الوعي والممارسات لديهم. وتعد الاستبانة من أدوات البحث المهمة، والشائع استعمالها في البحوث الإعلامية، والتي تُسهم في الحصول على الحقائق، والتوصل إلى الوقائع، والتعرف على الظروف، والأحوال، ودراسة المواقف والاتجاهات، اذ انها تُمكن أفراد العينة اختيار اجابة تناسبه من بين مجموعة الاسئلة التي يضعها الباحث لتحقيق هدف البحث[1].

- صدق الاستبانة: عرضت الاستبانة بعد تصميمها من قبل الباحث على مجموعة من السادة المحكمين، للتحقق من مدى مناسبتها لتحقيق أهداف البحث، ودقة صياغة فقراتها اللغوية والعلمية، وملاءمة الفقرات للمحاور التي تنتمي اليها، وأجريت التعديلات اللازمة وفقاً لملاحظاتهم.
- ثبات الاستبانة: استعملت معادلة الفا كرونباخ لقياس ثبات الاستبانة وفق الجدول الآتي:

(1) ليندة لطاد وآخرون، منهجية البحث العلمي وتقنياته في العلوم الاجتماعية، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، 2019، ص71.

جدول1: يبين قيمة الثبات لكل محور من محاور الاستبانة

المحور	العدد	معامل الفا كرونباخ
الوعي بمخاطر وانتهاكات الأمن السيبراني	6	0,95
الوعي بتطبيقات الأمن السيبراني	11	0,93
الوعي بمفاهيم بالأمن السيبراني	12	90,0

من بيانات الجدول (1) يتضح أن قيم المعامل ثابتة بدرجة عالية وهذا يدل على ثبات الاستبانة

سادساً. حدود البحث

- **الحدود الموضوعية**: مستوى وعي الأفراد بالأمن السيبراني
- **الحدود المكانية**: مركز مدينة الناصرية.
- **الحدود الزمانية**: 2025/4/1-2025/5/5

سابعا. مجتمع البحث وعينته

تمثل مجتمع البحث بكافة أفراد المجتمع في مركز مدينة الناصرية، أما عينته فتكونت من (50) فرداً من مختلف الفئات العمرية والتحصيل الدراسي.

الاطار النظري

أولاً. المفاهيم الواردة في البحث

1. الأمن السيبراني: هو الاسلوب الدفاعي عن الأنظمة الإلكترونية الموجودة في أجهزة الحاسوب، والهواتف النقالة، والشبكات والبيانات، من أيةِ هجمات، تهدف الوصول إلى معلومات حساسة أو تغييرها، أو اتلافها، أو استعمالها لابتزاز أصحابها[2].

2. وسائل الإعلام الرقمي: هي قنوات الاتصال والتعبير التي تعتمد على التكنولوجيا الرقمية، وتشترك مع الإعلام التقليدي في المفهوم والمبادئ العامة، والأهداف، وتتميز عنها بأنها تعتمد على وسيلة حديثة من وسائل الإعلام الحديثة، تتمثل في الدمج بين وسائل الاتصال التقليدي المختلفة، وجعلها في وسيلة واحدة، لإيصال المضامين المطلوبة بأشكال متمايزة ومؤثرة[3].

3. الاختراق الإلكتروني: عملية غير مصرح بها، هدفها الوصول إلى أنظمة، أو شبكات رقمية، لاستغلالها، أو سرقة البيانات، أو تعطيل العمليات، وتتم عن طريق استغلال الثغرات الأمنية في البرمجيات أو الأجهزة، ويعد الاختراق الالكتروني شكلاً من أشكال الجريمة [4].

(2) ايمان الشورة، الأمن السيبراني في البنوك الإسلامية الاردنية، رساتلة ماجستير غير منشورة، كلية الشريعة- الجامعة الاردنية، 2020، ص24.
(3) أمجد عبد القادر، ادارة المؤسسات الإعلامية وتأثيرات التقنيات، دار اليازوري العلمية للنشر والتوزيع، عمان، 2025، ص196.
(4) برامود كيه نايار، مقدمة إلى وسائل الإعلام الجديدة والثقافات الالكترونية، ترجمة: جلال الدين عز الدين علي، مؤسسة هنداوي سي أي سي، لندن، 2017، ص151.

4. التصيد الاحتيالي: نوع من الجرائم الإلكترونية، يستغل فيها المهاجمون ثقة الضحايا لخادعهم والحصول على معلومات حساسة مثل أسماء المستخدمين، كلمات المرور، أو أرقام بطاقات الائتمان. يتم ذلك عادةً عن طريق انشاء رسائل بريد الكتروني مزيفة، ومواقع تسجيل دخول تحاكي المواقع الرسمية تماماً، أو انتحال شخصية جهة موثوقة، مثل بنك أو شركة، وإرسال رسائل بريد إلكتروني أو روابط مزيفة تبدو شرعية، لكنها تهدف إلى سرقة البيانات الشخصية[5].

5. البرمجيات الخبيثة: نوع من البرمجيات المصممة لأهداف غير مشروعة، تهدف إلى الحاق الضرر بأنظمة الحاسوب أو الشبكات. تشمل هذه البرامج الفيروسات، الديدان، أحصنة طروادة، وبرامج التجسس، وتُستعمل لسرقة البيانات، وتعطيل العمليات، أو السيطرة على الأجهزة دون إذن المستخدم، وتعد هذه البرمجيات جريمة من الناحية القانونية[6].

6. انتهاكات الخصوصية: هو التدخل غير المصرح به في الحياة الشخصية للأفراد، أو الوصول إلى معلوماتهم الخاصة دون إذن منهم. ويشمل ذلك البيانات الشخصية، والتجسس، أو نشر معلومات حساسة دون موافقة، وغالباً ما يحدث ذلك عن طريق وسائل التكنولوجيا الحديثة، مثل برامج التجسس، أو تتبع النشاط عبر الإنترنت، ويؤدي إلى أضرار نفسية، واجتماعية، أو مالية للأفراد[7].

ثانياً. النظرية المؤطرة للبحث (نظرية السلوك المخطط Theory of Planned Behavior)

تُعد نظرية السلوك المخطط من أكثر النظريات استعمالاً لدراسة محددات السلوك[8]، وهي امتداد لنظرية الفعل المبرر Theory of Reasoned Action التي تطورت عن طريق اجزين Ajzen وفيشبين Fishbin، وتعتمد هذه النظرية على أن السلوك يُمكن التنبؤ به عن طريق مقصد الشخص A Person's Intention، فضلاً عن اعتمادها على فكرة إدراك التحكم السلوكي داخل المعادلة، وقياس مدى اعتقاد الفرد بضرورة التحكم في سلوك معين[9].

وتتكون النظرية من ثلاثة عناصر، وينشأ من كل عنصر بدوره عدد من المعتقدات والتقييمات، وهي[10]:

1. الاتجاهات Attitudes**:** وهي المشاعر السلبية، أو الايجابية التي تتولد نتيجة الانخراط في سلوك محدد. وعليه فإنه يجب أن تتوافق مقاييس النية، والتحكم السلوكي المُدرَك مع السلوك المراد التنبؤ به، وبعبارة أخرى، أنه يجب تقييم النوايا وإدراكات التحكم في ضوء السلوك المعني، ويجب أن يكون السياق المحدد هو نفسه السياق الذي سيحدث فيه السلوك. على سبيل المثال، إذا كان السلوك المراد التنبؤ به عبر الفضاء السيبراني هو التبرع بالمال للصليب الأحمر،

---

(5) خالد عبد الحق ودعاء عبد العال، الجرائم الالكترونية والتحقيقات الجنائية، دار اليازوري العلمية للنشر والتوزيع، عمان، 2025، ص46.

(6) فراس جمال شاكر محمود، الحروب المعلوماتية: في المجال الأمني والعسكري (امريكا والصين)، العربي للنشر والتوزيع، القاهرة، 2022، ص283.

(7) محمود مدين، فن التحقيق والاثبات في الجرائم الالكترونية، الدار المصرية للنشر والتوزيع، القاهرة، 2020، ص323.

(8) Mengxin Chen and others, Using the Extended Theory of Planned Behavior to Predict Privacy-Protection Behavioral Intentions in the Big Data Era: The Role of Privacy Concern, Journal of SHS Web of Conferences, No. 155, 2023, P. 1.

(9) ماريان ديانتن وايليان د. زيلي، تطبيق نظرية الاتصال في الحياة المهنية، ترجمة: عبد الحكيم الخزامي، دار الفجر للنشر والتوزيع، عمان، 2015، ص311.

(10)هناء احمد محمد شويخ، علم النفس الصحي، مكتبة الانجلو المصرية، القاهرة، 2012، ص67؛
Icek Ajzen, The Theory of Planned Behavior, Organizational Behavior and Human Decision Processes Journal, No.2, Vol. 50, December, 1991, P. 185.

فيجب علينا تقييم نوايا التبرع بالمال للصليب الأحمر، وليس نوايا التبرع بالمال بشكل عام، ولا نوايا مساعدة الصليب الأحمر، فضلاً عن التحكم المُدرَك في التبرع بالمال للصليب الأحمر.

2. المعايير الذاتية Subjective Norms**:** وهي معتقدات الفرد حول ما اذا كان المحيطون به يدعمونه، أو لا يدعمونه في الانخراط بسلوك محدد، وما إذا كانت لديهم دوافع لمتابعة هذه المعتقدات المهمة بالنسبة للآخرين، سواء كانوا أفراد اسرة أم أصدقاء.

3. التحكم السلوكي الذاتي Perceived Behavioral Control**:** ويهتم بقياس مدى اعتقاد الفرد بأنه قادر على أداء سلوك محدد بنجاح، وهو نتاج المزج بين خبرة الفرد السابقة عن السلوك نفسه، وقدرته على الانخراط في السلوك.

تفترض النظرية أن سلوكيات الأفراد تتأثر بمواقفهم، ومعاييرهم الذاتية، والتحكم السلوكي المتصور لدى الشخص، وأثبت عدد كبير من الأبحاث أن هذه العوامل تؤدي دوراً مهماً في النوايا السلوكية لحماية الخصوصية. فضلاً عن، قيام بعض الدراسات بتوسيع نطاق هذه النظرية عن طريق عَدْ القلق بشأن الخصوصية كسابقة. ولاحظ بعض الباحثين أن المخاوف المتعلقة بالخصوصية يمكن أن تؤثر أيضاً على تصورات الأفراد لممارسة سلوكيات حماية الخصوصية، بل وتتنبأ بشكل مباشر بالنوايا السلوكية لحماية الخصوصية. على سبيل المثال، وجد هو Ho أنَّ مخاوف مستخدمي شبكات الانترنيت بشأن الخصوصية مهمة للتأثير على نوايا سلوكهم تجاه حماية خصوصيتهم المستقبلية على الشبكة[11].

ووفقاً لنظرية السلوك المخطط، فإن أداء السلوك هو دالة مشتركة بين النوايا، والتحكم السلوكي المُدرَك، علاوة على ذلك، وجد هيرمان Heirman أن المخاوف المتعلقة بالخصوصية هي مؤشرات مهمة للمواقف تجاه سلوكيات حماية الخصوصية، والتي يمكن أن تتأثر بشكل كبير بالنوايا السلوكية لحماية الخصوصية[12].

ثالثاً. ماهية الأمن السيبراني وأهدافه

رَبَطت وسائل الاتصال بجميع أنواعها من الكومبيوترات وأجهزة الاتصال الناس في جميع أنحاء العالم عبر الإنترنت، ما يتيح تبادل المعلومات، والحصول على المعلومة بأسرع وقت ممكن، ما يعني التعرض للعديد من المخاطر عبر الشبكة الناقلة للمعلومة، نتيجة وجود ثغرات في الحواسيب وتطبيقاتها، وزيادة الهجمات والاختراقات من قبل أشخاص غير مصرح لهم بالدخول على المعلومات، أو الاطلاع عليها، ومن ثم، أصبحت هناك حاجة إلى جدار أمني لمواجهة هذه التهديدات والحد منها[13].

وهكذا ظهر مفهوم الأمن السيبراني وأصبح إطاراً لا غنى عنه، لحماية جميع الاتصالات وتبادل المعلومات، ولضمان تأمين شبكات الكمبيوتر، وأنظمة الحوسبة، والوقاية من الجرائم الإلكترونية التي تستعمل التكنولوجيا الحديثة، مثل

(11)Shirley S. Ho and Others, Understanding Factors Associated with Singaporean Adolescents' Intention to Adopt Privacy Protection Behavior Using an Extended Theory of Planned Behavior, Journal of Psychosocial Research on Cyberspace, No. 9, Vol. 20, Sep. 2017, P.14.

(12)Heirman, Wannes, and Others, Predicting Adolescents' Disclosure of Personal Information in Exchange for Commercial Incentives: An Application of an Extended Theory of Planned Behavior, journal of Psychosocial Research on Cyberspace, No. 2, Vol, 16, 2013, P. 15.

(13) هبة سليمان محمد القاضي، مستوى الوعي بالأمن السيبراني لدى معلمي الدراسات الاجتماعيةفي مديرية تربية قصبة المفرق، رسالة ماجستير غير منشورة، جامعى آل البيت، عمان، 2024، ص9.

اختراق قواعد البيانات وإدارة البرامج، وبرمجة الكمبيوتر، ومن الضروري فهم الأفراد، آليات الاختراق التي يستخدمها المتطفلون[14].

تعددت تعاريف الأمن السيبراني وفقاً لوجهات نظر الباحثين والزوايا التي وضعوا التعريف على أساسها، فعرف بأنه "الاجراءات التقنية الهادفة إلى حماية البيانات، والهوية الشخصية، والمعدات التقنية من أي شكل من أشكال الوصول غير المصرح به"[15]، وعُرف بأنه "تقديم الحماية للمستخدم وأصوله من أي مخاطر قد يتعرض لها عبر الانترنيت[16]، كما عرف الأمن السيبراني بأنه "مجموعة المهام المتعلقة بالأمن السيبراني بتجميع، وسائل وسياسات، ومبادئ توجيهية، وإجراءات، فضلاً عن المقاربات اللازمة لإدارة المخاطر، وتطوير التدريبات، والممارسات الجيدة، وتقديم تقنيات فعالة لحماية البيئة السبرانية[17].

ويهدف الأمن السيبراني إلى[18]:

1. سد كافة الثغرات الموجودة في أنظمة أمن المعلومات.
2. توفير بيئة آمنة ومناسبة وموثوقة، للتعاملات في مجتمع المعلومات.
3. مقاومة البرامج الخبيثة، ومنعها من احداث أضرار كبيرة بالمستخدمين للفضاء السيبراني.
4. تعزيز حماية أنظمة العمليات التشغيلية في كافة المستويات، وحماية مكونات هذه الانظمة المتمثلة بالأجهزة والبرامج، وما تقدمه من خدمات.
5. التصدي للهجمات التي تستهدف مستخدمي الفضاء السيبراني، سواء أفراد ام مؤسسات.
6. الحد من عمليات التجسس والتخريب الالكتروني على كافة المستويات.
7. اكتشاف نقاط الضعف في أنظمة الحاسوب، والأجهزة المحمولة لمعالجتها.

رابعاً. تهديدات الأمن السيبراني

تأتي تهديدات الأمن السيبراني في ثلاثة أشكال؛ الجرائم الإلكترونية، والهجمات الإلكترونية، والإرهاب السيبراني:

1. الجرائم الإلكترونية: هي الجرائم المرتكبة عبر الإنترنت، وغيرها من الوسائل الرقمية، وتعد هذه الجرائم أكثر أنواع تهديدات الأمن السيبراني، وترتكب هذه الجرائم ضد أفراد أو مجموعات من الأفراد، بدافع إجرامي للإضرار عمداً بسمعة الضحية أو التسبب في ضرر جسدي أو عقلي للضحية مباشرة، باستعمال شبكات الاتصال الحديثة، مثل الانترنيت، وغرف الدردشة، والرسائل البريدية، والاعلانات، والهواتف النقالة، وغيرها[19].

(14)Seki, T. and Others, The Effect of Emotional Intelligence on Cyber Security: The Mediator Role of Mindfulness, Bartin University Journal Faculty of Education, No.12, 2023, P. 191.

(15)Pusey, P., & Sadera, W. A., Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference, Journal of Digital Learning in Teacher Education, No. 2, Vol. 28, 2018, P. 82-88.

(16) حسام محمد سليمان، اثر تطبيق معايير الأمن السيبراني على أداء شركات الاتصال الاردنية، رسالة ماجستير غير منشورة، كلية الدراسات العليا-جامعة البلقاء التطبيقية، عمان، 2023، ص21.

(17) سهل محمد سودي البواعنة، أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الاردن، اطروحة دكتوراه غير منشورة، كلية الدراسات العليا- جامعة العلوم الإسلامية العالمية، عمان، 2023، ص51؛ Icek Ajzen, Op. Cit., P. 187.

(18) عاديدة عبد الكريم العيدان وبدور مسعد المسعد، درجة الوعي بالامن السيبراني ودور تكنولوجيا التعليم في تنميتهلدى طلبة كلية التربية الاساسية بدولة الكويت، مجلة كلية التربية-جامعة الاسكندرية، العدد4، ج2، مج34، 2024، ص414.

(19) فراس عقيل الدويري، البيانات الضخمة ودورها في الحد من الجرائم الالكترونية في ظل استراتيجية الأمن السيبراني، دار الخليج للنشر والتوزيع، عمان، 2024، ص103.

2. الهجمات الإلكترونية: تعد الهجمات الالكترونية فعلاً يقوض من قدرات وظائف الشبكة المعلوماتية عن طريق استغلال إحدى نقاط الضعف ما يمنح المهاجم القدرة على التلاعب بالنظام. وتهدف إلى تعطيل، أو إتلاف أو إدارة بيئة أو بنية تحتية للكمبيوتر بشكل ضار، أو تدمير سلامة البيانات، أو سرقة المعلومات الحساسة[20].

3. الإرهاب الإلكتروني: يشير إلى تعطيل البنية التحتية الوطنية الحيوية، بما في ذلك النقل، والطاقة والعمليات الحكومية، من خلال استخدام أدوات شبكات الحاسوب لإكراه أو ترهيب الحكومة أو السكان المدنيين[21].

وتنجم هذه التهديدات عن البرامج الضارة، والتصيد الاحتيالي، والهندسة الاجتماعية، وهجمات الوسيط، وهجمات حجب الخدمة الموزعة، فضلاً عن يشمل تهديد الأمن السيبراني الجهود الخبيثة لإتلاف، أو تدمير أنظمة أو شبكات الحاسوب. ومن ثم، يمكن أن تؤثر هجمات وتهديدات الأمن السيبراني على قطاعات مختلفة، مثل الرعاية الصحية، والتصنيع، والخدمات المالية، والهيئات الحكومية، والتعليم. ويجب أن يأخذ الأمن السيبراني في الاعتبار العوامل التكنولوجية، والتنظيمية، والقانونية، والأخلاقية، والاجتماعية[22].

خامساً. الوعي بالأمن السيبراني

لحماية البيانات الخاصة بالأفراد، والتعرف على السلوكيات الصحيحة للاستعمال الآمن للفضاء السيبراني، وللحد من المخاطر والتهديدات السيبرانية، وما يترتب عليها من آثار، تبرز أهمية توافر الوعي التام بكل جوانب الأمن السيبراني، لضمان ممارسة رقمية سليمة، فالأمن السيبراني عبارة عن مزيج من المعرفة والسلوكيات اللازمة لحماية المعلومات أو الاصول السيبرانية الشخصية، وعلى المستخدم الاحساس والدراية بالأعمال والممارسات غير القانونية، وغير المشروعة، التي تهدف إلى اختراق بيانات الغير، أو التعطيل، أو التعديل، أو الاستغلال غير المصرح به، كما أنه على الأفراد معرفة طرق الوقاية منها[23].

وينطوي الوعي السيبراني على مكونين رئيسين، الأول، الجانب المعرفي المتمثل بالفهم الشامل بالمشكلات والتحديات المتعلقة بالأمن السيبراني وتداعياتها، وكيفية التعامل معها، اما الجانب الثاني فيتمثل بالجانب السلوكي، الذي يشير إلى الإجراءات المتخذة فعلياً، والسلوك الذي يُظهره الأفراد لحماية أجهزتهم، وبرامجهم من التهديدات السيبرانية، بالاستناد إلى فهمهم ومعرفتهم[24].

وقد وثّقت الدراسات والبحوث في مجال ممارسات مستخدمي الفضاء السيبراني العلاقة بين المخاوف على الخصوصية، وسلوكيات حماية الخصوصية، المتمثلة بالإجراءات المختلفة المتخذة لحماية معلوماتهم في وسائل الاتصال التي يستعملونها من الاختراق، والوصول إلى أشخاص غير مخولين بذلك، عن طريق عدم مشاركتها بشكل كبير، واقتصار مشاركتها مع الجهات الموثوق بها من قبلهم، أو تجنب تقديم معلومات صادقة أو دقيقة، ورفض تقديم معلومات حقيقية عن الفرد على الإنترنت[25].

(20) فارس محمد العمارات، الأمن السيبراني: المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، عمان، 2022، ص21.
(21) عادل عبد الصادق، الارهاب الالكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية، القاهرة، 2009، ص124.
(22)Afrah Almansoori and Others, Exploring the Frontiers of Cybersecurity Behavior: ASystem-atic Review of Studies and Theories, Applied Science Journal, No. 9, Vol 13, 2023, P. 2.
(23) عاديدة عبد الكريم العيدان وبدور مسعد المسعد، المصدر السابق، ص416.
(24)Khan, N. F. et all., Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. Security Journal, No. 36, Vol. 2, 2022, P.25.
(25)Mengxin Chen and others, Op. Cit., P. 2.

الجانب العملي

أولاً. بيانات عينة البحث

جدول2: يبين النوع الاجتماعي لأفراد العينة

الجنس	التكرار	النسبة المؤية
ذكر	26	%52
انثى	24	%48
المجموع	50	%100

أظهرت معطيات الجدول احتلال الذكور الترتيب الأول بواقع (26) تكراراً، من مجموع التكرارات البالغة (50) تكراراً، وبنسبة بلغت (52%)، فيما احتلت الاناث الترتيب الثاني بواقع (24) تكراراً وبنسبة مقدارها (48%).

ثانياً. نتائج المحور الأول: التعرف على الوعي بمخاطر وانتهاكات الأمن السيبراني لعينة البحث، بحسب المتوسطات الحسابية، والانحرافات المعيارية، والرتب.

جدول3: يبين المتوسطات الحسابية والانحرافات المعيارية المتعلقة بالوعي بمخاطر وانتهاكات الأمن السيبراني مرتبة تنازلياً

ت	العبارة	الترتيب	الوسط الحسابي	الانحراف المعياري	الدرجة
6	استخدم المحتويات المرخصة	1	4,35	1,11	مرتفعة
7	أتجنب المعلومات التي تمس أمن الدولة	2	3,77	1,39	مرتفعة
3	اتجنب املاء النماذج غير الموثوقة ببياناتي الشخصية	3	3,35	1,29	مرتفعة
1	التزم بالتعليمات واللوائح المتبعة في الدولة عند استخدامي للأنترنيت	4	3,24	1,45	متوسطة
4	أحرص على عدم تداول ارقام حساباتي المصرفية عبر الانترنيت	5	3,23	1,39	متوسطة
2	التزم بسياسة المواقع التي استخدمها	6	3,22	1,47	متوسطة
5	اتجنب تنزيل برامج من شبكة الانترنيت	7	3,07	1,32	متوسطة
	المتوسط العام للوعي بمخاطر وانتهاكات الأمن السيبراني	-	**3,55**		**مرتفعة**

يتضح من بيانات الجدول (2) أن المتوسطات الحسابية الخاصة بامتلاك أفراد العينة الوعي بمخاطر وانتهاكات الأمن السيبراني تراوحت بين (4,35-3,07)، وأن مجتمع الدراسة يمتلكون درجة (مرتفعة) في هذا المحور، وكان المتوسط العام (3,55)، وهو يقع ضمن الفئة الاولى من فئات المقياس الثلاثي، وهذا يعكس ارتفاع مستوى ادراك أفراد العينة لأهمية الوعي بمخاطر وانتهاكات الأمن السيبراني، ومدى خطورته على بياناتهم الشخصية في حالة التهاون فيه، وحملت (3) فقرات مستوى (مرتفع) جاءت بالترتيب الأول العبارة التي تنص على (استخدم المحتويات المرخصة)، بمتوسط بلغ (4,35)، وهذا يعكس امتلاك أفراد العينة وعياً بأهمية استخدام المحتويات المرخصة المتوفرة على شبكة

الانترنيت، وتجنب المحتويات غير المرخصة، ويدل على إدراكهم لقيمة الحقوق الفكرية، واحترامهم لمصادر المعلومات الموثوقة، ويعكس وعيهم بالمخاطر القانونية، والأمنية المرتبطة باستعمال المحتويات غير المرخصة، مثل التعرض للبرمجيات الضارة أو انتهاك حقوق الملكية الفكرية، كما هذا يشير أيضاً إلى أهمية تعزيز هذا السلوك الإيجابي من خلال حملات توعوية مستمرة، لضمان استمرارية الالتزام بالممارسات الرقمية الآمنة والمسؤولة. اما الترتيب الثاني في مستوى (مرتفع) فاحتلته عبارة (أتجنب المعلومات التي تمس أمن الدولة)، بمتوسط حسابي مقداره (3,77)، ما يشير إلى إدراك أفراد العينة لأهمية تجنب المعلومات التي قد تؤثر على أمن الدولة، ووعيهم بالمخاطر المحتملة المرتبطة بنشر أو التعامل مع مثل هذه المعلومات. كما يعكس هذا المستوى المرتفع من الإدراك حرصهم على الالتزام بالضوابط القانونية، والأمنية التي تهدف إلى حماية استقرار الدولة، وسلامة المجتمع، ويمكن تعزيز هذا الوعي من خلال برامج التثقيف الأمني وتوضيح تأثير المعلومات الحساسة على الأمن الوطني. وجاءت عبارة (اتجنب املاء النماذج غير الموثوقة ببياناتي الشخصية) بالترتيب الثالث في مستوى (مرتفع) بمتوسط مقداره (3,35)، ما يدل على مستوى الوعي المرتفع لأفراد العينة بأهمية حماية بياناتهم الشخصية، وتجنب مشاركة المعلومات الحساسة عبر النماذج غير الموثوقة. ويشير إلى حرصهم على تفادي التعرض للمخاطر الأمنية مثل الاحتيال الإلكتروني وسرقة الهوية. ويمكن تعزيز هذا الوعي من خلال حملات التوعية الرقمية، وتوفير إرشادات واضحة حول كيفية التحقق من موثوقية النماذج الإلكترونية قبل إدخال البيانات الشخصية فيها.

وتبين أن هناك اربعة عبارات بدرجة (متوسط)، اولها عبارة (التزم بالتعليمات واللوائح المتبعة في الدولة عند استخدامي للأنترنيت)، بمتوسط حسابي قدره (3,24) وهو إشارة إلى امتلاك أفراد العينة فهماً جزئياً أو غير مكتمل حول الالتزام بالتعليمات واللوائح المتبعة في الدولة عند استعمالهم الانترنيت، وأنهم لا يملكون دراية بجميع التفاصيل والإجراءات المطلوبة، وهذا يشير إلى أهمية تعزيز التوعية بالقوانين الرقمية والتشريعات المتعلقة بأمن المعلومات والاستخدام المسؤول للإنترنت، لضمان الامتثال الكامل للأنظمة الوطنية وحماية المستخدمين من المخاطر القانونية والأمنية. وجاءت العبارة (أحرص على عدم تداول ارقام حساباتي المصرفية عبر الانترنيت) بالترتيب الثاني بمتوسط حسابي مقداره (3.24)، ما يشير إلى أن أفراد العينة لديهم مستوى إدراك متوسط لأهمية تجنب مشاركة أرقام حساباتهم المصرفية عبر الإنترنت، وامتلاكهم وعي جزئي بالمخاطر المرتبطة بكشف المعلومات المالية، مثل الاحتيال الإلكتروني وسرقة الهوية، لكنه قد لا يكون كافياً لضمان الحماية المثلى للبيانات المصرفية، ولتعزيز هذا الإدراك، يمكن تكثيف حملات التوعية حول أساليب الاحتيال المالي، وأفضل الممارسات للحفاظ على أمن المعلومات الشخصية أثناء التعاملات الإلكترونية. اما العبارة (التزم بسياسة المواقع التي استخدمها) فاحتلت الترتيب الثالث من بين العبارات في درجة (متوسط) بمتوسط حسابي مقداره (3,22)، وهذا يشير إلى أن أفراد العينة لديهم مستوى إدراك متوسط لأهمية الالتزام بسياسات المواقع التي يستخدمونها، ما يدل على فهم جزئي لقواعد الاستخدام والضوابط التي تفرضها تلك المواقع، ما يعكس حاجة إلى تعزيز الوعي بالمخاطر المرتبطة بعدم الامتثال لسياسات المواقع، مثل انتهاك الخصوصية أو التعرض لعقوبات رقمية. ويمكن تعزيز هذا الإدراك من خلال حملات التوعية الرقمية التي تشرح أهمية قراءة سياسات الاستخدام، وفهم كيفية حماية الحقوق والبيانات أثناء تصفح الإنترنت. وجاءت عبارة (اتجنب تنزيل برامج من شبكة الانترنيت) بالترتيب الرابع بمتوسط حسابي مقداره (3,07)، وهذا يشير إلى الادراك المتوسط لدى أفراد العينة حول أهمية تجنب تنزيل البرامج من الإنترنت، ويدل على وعي جزئي بالمخاطر المحتملة، مثل الفيروسات والبرمجيات الضارة التي قد تهدد أمن البيانات والأجهزة. ومع ذلك، قد يشير هذا المتوسط الحسابي إلى الحاجة لمزيد من التوعية حول أساليب التحقق من موثوقية البرامج قبل تنزيلها، وأهمية استخدام المصادر الرسمية والتحديثات الأمنية لضمان حماية الأجهزة والمعلومات الشخصية.

ثالثاً. نتائج المحور الثاني: التعرف على الوعي بتطبيقات الأمن السيبراني لعينة البحث، بحسب المتوسطات الحسابية، والانحرافات المعيارية، والرتب.

جدول4: يبين المتوسطات الحسابية والانحرافات المعيارية المتعلقة بالوعي بتطبيقات الأمن السيبراني مرتبة تنازلياً

ت	العبارة	الترتيب	الوسط الحسابي	الانحراف المعياري	الدرجة
5	احدث نظام التشغيل دائماً	1	4,64	0,63	مرتفعة
10	استعمل جدار حماية على جهاز الحاسوب الخاص بي	2	4,38	0,9	مرتفعة
2	اتنجنب فتح الروابط المجهولة المصدر	3	3,78	1,43	مرتفعة
4	استبدل كلمات المرور بشكل دوري ومنتظم	4	3,78	1,28	مرتفعة
1	اتجنب ارسال معلوماتي الشخصية عبر البريد الالكتروني أو الرسائل النصية	5	3,68	1,39	مرتفعة
8	احرص على استعمال كلمات مرور لكل تطبيق على حدة	6	3,64	1,38	مرتفعة
6	اقدم البلاغات عن الاساءات التي اتعرض لها في مواقع التواصل الاجتماعي	7	3,52	1,72	مرتفعة
3	احرص على تحميل برامج آمنة لمكافحة الفايروسات	8	3	1,28	متوسطة
9	احتفظ بنسخ احتياطية للملفات المهمة على قرص خارجي	9	2,5	1,07	منخفضة
7	اعطل خاصية الوصول إلى موقعي في التطبيقات المحملة على جهازي	10	2,46	1,37	منخفضة
-	**المتوسط العام للوعي بتطبيقات الأمن السيبراني**	**-**	**3,53**		**مرتفعة**

يتضح من بيانات الجدول (4) أن المتوسطات الحسابية الخاصة بامتلاك أفراد العينة الوعي بتطبيقات الأمن السيبراني تراوحت بين (2,46-4,64)، وأن مجتمع الدراسة يمتلكون درجة (مرتفعة) في هذا المحور، وكان المتوسط العام (3,53)، وهو يقع ضمن الفئة الاولى من فئات المقياس الثلاثي، وهذا يعكس ضعف ادراك افراد العينة لأهمية الوعي بتطبيقات الأمن السيبراني، ومدى خطورة اهمال هذا الجانب على بياناتهم الشخصية، وحملت (7) فقرات مستوى (مرتفع) جاءت بالترتيب الأول العبارة التي تنص على (احدث نظام التشغيل دائماً)، بمتوسط بلغ (4,64)، وهذا يعكس إدراكاً عالياً لدى أفراد العينة بأهمية تحديث نظام التشغيل باستمرار، ويشير إلى وعيهم بالدور الحيوي للتحديثات في تعزيز الأمان الرقمي، وإصلاح الثغرات الأمنية، وتحسين أداء الأجهزة. كما يعكس فهمهم الجيد للمخاطر التي قد تنتج عن استخدام إصدارات غير محدثة، مثل التعرض للهجمات السيبرانية، والبرمجيات الضارة. ويمكن دعم هذا الاتجاه الإيجابي من خلال نشر المزيد من التوعية حول أهمية التحديثات التلقائية، والتأكد من حصول أجهزتهم على أحدث الإصلاحات الأمنية، لضمان حماية البيانات، والمعلومات الشخصية، اما الترتيب الثاني في مستوى (مرتفع) فاحتلته عبارة (استعمل جدار حماية على جهاز الحاسوب الخاص بي)، بمتوسط حسابي مقداره (4,38)، ما يشير إلى إدراك أفراد العينة لأهمية استعمال جدار الحماية لحماية أجهزتهم من التهديدات السيبرانية، ويعكس مستوى عالٍ من الوعي بالمخاطر الأمنية المرتبطة بالاتصال بالإنترنت، ويشير هذا الإدراك المرتفع إلى فهمهم لدور جدار الحماية في منع الوصول غير المصرح به إلى أجهزتهم وحماية بياناتهم الشخصية من الاختراقات والبرمجيات الضارة، ويمكن أن يتم تعزيز هذا السلوك عن طريق توفير المزيد من المعلومات حول إعدادات جدار الحماية، وكيفية تخصيصه لضمان أقصى درجات الأمان.

وجاءت عبارة (اتنجنب فتح الروابط المجهولة المصدر) بالترتيب الثالث في مستوى (مرتفع) بمتوسط مقداره (3,78)، ما يدل على ادراك أفراد العينة المخاطر المحتملة المرتبطة بفتح الروابط غير الموثوقة، ويعكس إدراكاً جيداً لأهمية تجنب مصادر غير معروفة قد تحتوي على برمجيات ضارة أو محاولات تصيد احتيالي، إن هذا المستوى المرتفع من الإدراك يشير إلى حرص الأفراد على حماية بياناتهم الشخصية وأجهزتهم من الاختراقات الأمنية، ويمكن تعزيز هذا الوعي من خلال توفير مزيد من الإرشادات حول كيفية التحقق من الروابط قبل فتحها، واستعمال أدوات الأمان؛ مثل برامج الحماية، وجدران الحماية للكشف عن أي تهديدات محتملة. وجاءت عبارة (استبدل كلمات المرور بشكل دوري ومنتظم) بالترتيب الرابع في المستوى نفسه بمتوسط مقداره (3,68)، ما يشير إلى فهم أفراد العينة لأهمية تغيير كلمات المرور بشكل منتظم، ويعكس مستوى وعي مرتفع بالممارسات الأمنية التي تسهم في حماية الحسابات من الاختراقات، وفهم جيد للحاجة إلى تحديث كلمات المرور لتقليل مخاطر التعرض لهجمات سيبرانية مختلفة، ولتعزيز هذا السلوك، يمكن توعية الأفراد بأهمية استخدام كلمات مرور قوية وفريدة لكل حساب، مع الاستفادة من أدوات إدارة كلمات المرور لضمان الحماية الفعالة.

وجاءت عبارة (اتجنب ارسال معلوماتي الشخصية عبر البريد الالكتروني أو الرسائل النصية) بالترتيب الخامس في مستوى (مرتفع) بمتوسط مقداره (3,68)، ما يدل وعي أفراد العينة بأهمية حماية بياناتهم الشخصية، وتجنب إرسالها عبر البريد الإلكتروني أو الرسائل النصية، ويعكس إدراكاً جيداً للمخاطر المحتملة، وحرص أفراد العينة على اتخاذ تدابير احترازية لحماية معلوماتهم من الوصول غير المصرح به، ولتعزيز هذا السلوك، يمكن تقديم المزيد من التوعية حول البدائل الآمنة لتبادل المعلومات، مثل استخدام القنوات المشفرة والتأكد من هوية المستلمين قبل مشاركة أي بيانات حساسة. وجاءت عبارة (احرص على استعمال كلمات مرور لكل تطبيق على حدة) بالترتيب السادس في المستوى نفسه بمتوسط مقداره (3,64)، ما يشير إلى فهم أفراد العينة أهمية استخدام كلمات مرور مختلفة لكل تطبيق، ومن ثم يعكس إدراكاً جيداً للحماية من الاختراقات الإلكترونية وسرقة الحسابات، وهذا المستوى المرتفع من الإدراك يشير إلى وعي أفراد العينة بالمخاطر المحتملة عند استعمال كلمة مرور واحدة لتطبيقات عديدة، وامكانية تعرضهم لهجمات سيبرانية إذا تم اختراق إحدى الحسابات، ولتعزيز هذا السلوك، يمكن توعية الأفراد بأهمية استخدام مدير كلمات المرور لإنشاء كلمات قوية، وتفعيل المصادقة الثنائية لزيادة مستوى الأمان. اما عبارة (اقدم البلاغات عن الاساءات التي اتعرض لها في مواقع التواصل الاجتماعي) جاءت بالترتيب السابع في المستوى نفسه بمتوسط مقداره (3,52)، ما يشير إلى وجود مستوى إدراك مرتفع لدى أفراد العينة بأهمية الإبلاغ عن الإساءة التي يتعرضون لها في مواقع التواصل الاجتماعي، ويعكس وعيهم بحقوقهم الرقمية، وسبل الحماية المتوفرة لهم. ويدل أيضاً على فهمهم لدور الإبلاغ في الحد من السلوكيات غير الأخلاقية عبر الإنترنت، وتعزيز بيئة رقمية أكثر أماناً. ولغرض تعزيز هذا السلوك، يمكن تكثيف التوعية حول كيفية تقديم البلاغات بفعالية، وأهمية اللجوء إلى الجهات المختصة للحصول على الدعم والحماية عند التعرض للمضايقات الإلكترونية.

وتبين من معطيات الجدول (4) أن هناك عبارة واحدة بدرجة (متوسط)، ونصها (احرص على تحميل برامج آمنة لمكافحة الفايروسات)، بمتوسط حسابي قدره (3) وهو إشارة إلى أن أفراد العينة لديهم مستوى إدراك متوسط لأهمية تحميل برامج مكافحة الفيروسات، ما يعكس وعياً جزئياً بالمخاطر المرتبطة بالبرمجيات الضارة، ويشير كذلك إلى الحاجة لتعزيز التوعية حول دور هذه البرامج في حماية الأجهزة والبيانات الشخصية، عن طريق حملات تثقيفية توضح كيفية اختيار برامج موثوقة لمكافحة الفيروسات، وأهمية تحديثها بانتظام لضمان فاعليتها في مواجهة التهديدات الإلكترونية.

وتبين من معطيات الجدول (4) أن هناك عبارتين بدرجة (منخفض)، الاولى عبارة (احتفظ بنسخ احتياطية للملفات المهمة على قرص خارجي)، بمتوسط حسابي قدره (2,5) وهو إشارة إلى أن مستوى إدراك أفراد العينة لأهمية الاحتفاظ بنسخ احتياطية للملفات المهمة على قرص خارجي يعد منخفضاً نسبياً، ويعكس ضعف الوعي بالمخاطر المحتملة لفقدان البيانات نتيجة للأعطال التقنية، أو الهجمات الإلكترونية. ويشير ذلك أيضاً إلى ضرورة تكثيف التوعية حول أهمية

النسخ الاحتياطي كوسيلة للحفاظ على الملفات المهمة وضمان استرجاعها في حال حدوث خلل أو فقدان للمعلومات، ويمكن تعزيز هذا الإدراك عن طريق تقديم إرشادات حول أفضل الممارسات لحفظ البيانات، مثل استخدام وسائط التخزين الآمنة، وإجراء النسخ الاحتياطي بشكل منتظم. وجاءت العبارة (اعطل خاصية الوصول إلى موقعي في التطبيقات المحملة على جهازي) بالترتيب الثاني بمتوسط حسابي مقداره (2,46)، وهذا يشير إلى أن مستوى إدراك أفراد العينة لأهمية تعطيل خاصية الوصول إلى الموقع في التطبيقات يعد منخفضاً نسبياً، ويشير إلى عدم الوعي الكافي بالمخاطر المرتبطة بمشاركة الموقع الجغرافي مع التطبيقات، مثل انتهاك الخصوصية، أو التعرض لتتبع غير مرغوب فيه، ويشر كذلك إلى الحاجة إلى تكثيف التوعية حول كيفية ضبط إعدادات الخصوصية في الأجهزة الذكية، وتشجيع المستخدمين على التحكم في الصلاحيات التي تمنحها للتطبيقات لضمان حماية بياناتهم الشخصية بشكل أفضل.

رابعاً. نتائج المحور الثالث: التعرف على الوعي بمفاهيم الامن السيبراني لعينة البحث، بحسب المتوسطات الحسابية، والانحرافات المعيارية، والرتب.

جدول5: يبين المتوسطات الحسابية والانحرافات المعيارية المتعلقة بالوعي بمفاهيم الأمن السيبراني مرتبة تنازلياً

ت	العبارة	الترتيب	الوسط الحسابي	الانحراف المعياري	الدرجة
4	أدرك أهمية اعدادات الخصوصية للخدمة الالكترونية	1	4,24	1,06	مرتفعة
9	ادرك مفهوم التصيد الاحتيالي	2	3,49	1,50	متوسطة
2	ادرك مخاطر فتح روابط ومرفقات البريد الالكتروني	3	3,44	1,28	متوسطة
3	اعرف أن الأمن السيبراني يحمي نظم المعلومات من الاختراقات	4	3,32	1,66	متوسطة
5	اعي مخاطر فيروسات الهواتف النقالة	5	2,79	1,33	متوسطة
6	اعي كيفية التحقق من اعدادات الخصوصية للتطبيقات الالكترونية	6	2,59	1,20	منخفضة
1	ادرك اهمية الأمن السيبراني في الحفاظ على معلوماتي الشخصية	7	2,52	1,33	منخفضة
7	لدي اطلاع كافي عن الجرائم الالكترونية	8	2,43	1,22	منخفضة
-	**المتوسط العام للوعي بمفاهيم الأمن السيبراني**	**-**	**3,10**		**متوسطة**

يتضح من بيانات الجدول (5) أن المتوسطات الحسابية الخاصة بامتلاك أفراد العينة الوعي بمفاهيم الأمن السيبراني تراوحت بين (2,43-4,24)، وأن مجتمع الدراسة يمتلكون درجة (متوسط) في هذا المحور، وكان المتوسط العام (3,10)، وهو يقع ضمن الفئة الثانية من فئات المقياس الثلاثي، وهذا يعكس ضعف ادراك افراد العينة لأهمية الوعي بالأمن السيبراني، ومدى خطورة التهاون فيه على بياناتهم الشخصية، وجاءت الفقرة رقم (4) بالترتيب الأول التي تنص (أدرك أهمية اعدادات الخصوصية للخدمة الالكترونية)، بمتوسط بلغ (4,24) وهي العبارة الوحيدة التي جاءت بمستوى مرتفع من بين مجموع عبارات المحور البالغة (8) عبارات، وهذا يعكس امتلاك أفراد العينة وعياً بأهمية حماية خصوصيتهم عن طريق الاعدادات التي توفرها لهم التطبيقات.

وتبين أن هناك اربعة عبارات بدرجة (متوسط)، اولها عبارة (أدرك مفهوم التصيد الاحتيالي)، بمتوسط حسابي قدره (3,49) وهو إشارة إلى امتلاك أفراد العينة معرفة جزئية أو غير مكتملة حول مفهوم التصيد الاحتيالي، ولا

يكونون قادرين على التعرف على جميع أساليبه أو كيفية التصدي له بفعالية، وربما لديهم فهم عام بالمخاطر، لكنهم يحتاجون إلى تعزيز وعيهم وتطوير مهاراتهم في كشف الاحتيال الإلكتروني واتخاذ الإجراءات الوقائية المناسبة. وجاءت العبارة (ادرك مخاطر فتح روابط ومرفقات البريد الالكتروني) بالترتيب الثاني بمتوسط حسابي مقداره (3,44)، وهذا يشير إلى قلة وعي أفراد العينة بخطورة فتح روابط ومرفقات البريد الالكتروني، وعدم ادراكهم للتهديدات السيبرانية المحتملة، وهم إلى المزيد من التوعية والتدريب لضمان قدرتهم على التمييز بفعالية بين الروابط الآمنة والخطيرة واتخاذ الإجراءات الوقائية المناسبة. اما العبارة (اعرف أن الأمن السيبراني يحمي نظم المعلومات من الاختراقات) فاحتلت الترتيب الثالث من بين العبارات في درجة (متوسط) بمتوسط حسابي مقداره (3,32)، وهذا يشير إلى محدودية معرفتهم بالتحديات الأمنية وأساليب الحماية المتقدمة لضمان تطبيق أفضل للممارسات السيبرانية الوقائية. وجاءت عبارة (اعي مخاطر فيروسات الهواتف النقالة) بالترتيب الرابع بمتوسط حسابي مقداره (2,79)، وهذا يشير إلى الادراك غير الكافي لأفراد العينة بمخاطر فيروسات الهواتف النقالة، وحاجتهم إلى تعزيز وعيهم بهذا الاتجاه.

وتبين من معطيات الجدول نفسه أن هناك ثلاثة عبارات بدرجة (منخفض)، اولها عبارة (اعي كيفية التحقق من اعدادات الخصوصية للتطبيقات الالكترونية)، بمتوسط حسابي قدره (2,59) وهو إشارة إلى ضعف مستوى إدراك أفراد العينة لكيفية التحقق من إعدادات الخصوصية للتطبيقات الإلكترونية، ويدل على نقص الوعي بأهمية حماية البيانات الشخصية، والتحكم في إعدادات الأمان. وقد يشير ذلك أيضاً إلى الحاجة لتعزيز التثقيف الرقمي وتوفير إرشادات واضحة حول كيفية ضبط إعدادات الخصوصية لضمان حماية المعلومات الشخصية من الوصول غير المصرح به. وجاءت العبارة (ادرك اهمية الأمن السيبراني في الحفاظ على معلوماتي الشخصية) بالترتيب الثاني بمتوسط حسابي مقداره (2,52)، وهذا يشير إلى تدني مستوى إدراك أفراد العينة لأهمية الأمن السيبراني في حماية معلوماتهم الشخصية، ما يدل على قلة الوعي بالمخاطر التي تهدد البيانات الشخصية، والسبل الفعالة لحمايتها. ويشير إلى الحاجة لتكثيف جهود التوعية والتدريب حول أهمية تبني ممارسات الأمن السيبراني، مثل استخدام كلمات مرور قوية، تجنب مشاركة المعلومات الحساسة عبر الإنترنت، وتحديث أنظمة الحماية بشكل منتظم. اما العبارة (لدي اطلاع كافي عن الجرائم الالكترونية) فاحتلت الترتيب الثالث من بين العبارات في درجة (متوسط) بمتوسط حسابي مقداره (2,43)، وهذا يشير وجود قاعدة معرفية منخفضة وغير كافية لدى أفراد العينة بهذا الاتجاه، وأنهم لا يعرفون مفاهيم أساسية كافية للتعامل مع التهديدات الحديثة بكفاءة.

الخاتمة

اولاً. نتائج البحث

أ. النتائج المتعلقة بقياس مستوى وعي الأفراد بمخاطر وانتهاكات الأمن السيبراني في وسائل الإعلام الرقمي:

كشف التحليل أن وعي وممارسات أفراد العينة تجاه مخاطر وانتهاكات الأمن السيبراني كان بدرجة (مرتفعة)، وكالاتي:

1. كان مستوى ادراكهم وممارساتهم بدرجة (مرتفعة) تجاه استخدم المحتويات المرخصة، وتجنب المعلومات التي تمس أمن الدولة، وتجنب املاء النماذج غير الموثوقة ببياناتي الشخصية
2. كان مستوى وعيهم وممارساتهم بدرجة (متوسطة) تجاه الالتزام بالتعليمات واللوائح المتبعة في الدولة عند استخدامهم للأنترنيت، والحرص على عدم تداول ارقام حساباتهم المصرفية عبر الانترنيت، والالتزام بسياسة المواقع التي يستخدمونها.

ب. النتائج المتعلقة بقياس مستوى وعي الأفراد بتطبيقات الأمن السيبراني في وسائل الإعلام الرقمي:

كشف التحليل أن وعي وممارسات أفراد العينة تجاه تطبيقات الأمن السيبراني كان بدرجة (مرتفعة) وكالاتي:

1. كان مستوى ادراكهم وممارساتهم بدرجة (مرتفعة) تجاه تحديث نظام التشغيل دائماً، ودور جدار الحماية في الحماية من الاختراقات، وتجنبهم فتح الروابط المجهولة. واستبدال كلمات المرور بشكل دوري ومنتظم، وتجنب ارسالهم معلومات شخصية عبر البريد الالكتروني أو الرسائل النصية، وحرصهم على استعمال كلمات مرور لكل تطبيق على حدة، والابلاغ عن الاساءات التي يتعرضون لها في مواقع التواصل الاجتماعي.
2. كان مستوى وعيهم وممارساتهم بدرجة (متوسطة) تجاه تحميل برامج آمنة لمكافحة الفيروسات، وحاجتهم إلى التوعية في هذا المجال.
3. كان مستوى وعيهم وممارساتهم بدرجة (منخفضة) تجاه الاحتفاظ بنسخ احتياطية للملفات المهمة على قرص خارجي، وتعطيل خاصية الوصول إلى مواقعهم في التطبيقات المحملة على أجهزتهم.

ج. النتائج المتعلقة بقياس مستوى وعي الأفراد بمفاهيم الأمن السيبراني في وسائل الإعلام الرقمي:

كشف التحليل أن وعي وممارسات أفراد العينة تجاه مفاهيم الأمن السيبراني كان بدرجة (متوسطة)، وكالاتي:
1. كان مستوى ادراكهم وممارساتهم بدرجة (مرتفعة) تجاه أدرك أهمية اعدادات الخصوصية للخدمة الالكترونية.

2. كان مستوى وعيهم وممارساتهم بدرجة (متوسطة) تجاه ادراك مفهوم التصيد الاحتيالي، ومخاطر فتح روابط ومرفقات البريد الالكتروني، ومعرفتهم بأن الأمن السيبراني يحمي نظم المعلومات من الاختراقات، ووعيهم بمخاطر فيروسات الهواتف النقالة.

3. كان مستوى وعيهم وممارساتهم بدرجة (منخفضة) تجاه كيفية التحقق من اعدادات الخصوصية للتطبيقات الالكترونية، واهمية الأمن السيبراني في الحفاظ على معلوماتي الشخصية، والاطلاع الكافي عن الجرائم الالكترونية.

ثانياً. التوصيات

1. ضرورة تنفيذ حملات توعوية؛ تستهدف مختلف فئات المجتمع لزيادة إدراكهم بالمخاطر السيبرانية.
2. تعزيز ثقافة الإبلاغ؛ عن الإساءة عبر منصات التواصل الاجتماعي، وتوفير قنوات رسمية، تضمن استجابة فعالة لحماية الأفراد من التهديدات الإلكترونية.
3. التعاون بين الجهات المعنية؛ لتقديم محتوى توعوي شامل يسهم في زيادة الوعي بتطبيقات الأمن السيبراني، وضمان حماية البيانات الشخصية للمستخدمين.

المصادر والمراجع

اولاً. الكتب

1. أمجد عبد القادر، ادارة المؤسسات الإعلامية وتأثيرات التقنيات، دار اليازوري العلمية للنشر والتوزيع، عمان، 2025.
2. برامود كيه نايار، مقدمة إلى وسائل الإعلام الجديدة والثقافات الالكترونية، ترجمة: جلال الدين عز الدين علي، مؤسسة هنداوي سي أي سي، لندن، 2017.

3. خالد عبد الحق ودعاء عبد العال، الجرائم الالكترونية والتحقيقات الجنائية، دار اليازوري العلمية للنشر والتوزيع، عمان، 2025.
4. عادل عبد الصادق، الارهاب الالكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية، القاهرة، 2009.
5. فارس محمد العمارات، الأمن السيبراني: المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، عمان، 2022.
6. فراس جمال شاكر محمود، الحروب المعلوماتية: في المجال الأمني والعسكري (امريكا والصين)، العربي للنشر والتوزيع، القاهرة، 2022.
7. فراس عقيل الدويري، البيانات الضخمة ودورها في الحد من الجرائم الالكترونية في ظل استراتيجية الأمن السيبراني، دار الخليج للنشر والتوزيع، عمان، 2024.
8. ليندة لطاد وآخرون، منهجية البحث العلمي وتقنياته في العلوم الاجتماعية، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، 2019.
9. ماريان ديانتن وايليان د. زيلي، تطبيق نظرية الاتصال في الحياة المهنية، ترجمة: عبد الحكيم الخزامي، دار الفجر للنشر والتوزيع، عمان، 2015.
10. محمود مدين، فن التحقيق والاثبات في الجرائم الالكترونية، الدار المصرية للنشر والتوزيع، القاهرة، 2020.
11. هناء احمد محمد شويخ، علم النفس الصحي، مكتبة الانجلو المصرية، القاهرة، 2012.

ثانياً. الرسائل والاطاريح

1. ايمان الشورة، الأمن السيبراني في البنوك الإسلامية الاردنية، رسالة ماجستير غير منشورة، كلية الشريعة-الجامعة الاردنية، 2020.
2. حسام محمد سليمان، اثر تطبيق معايير الأمن السيبراني على أداء شركات الاتصال الاردنية، رسالة ماجستير غير منشورة، كلية الدراسات العليا-جامعة البلقاء التطبيقية، عمان، 2023.
3. سهل محمد سودي البواعنة، أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الاردن، اطروحة دكتوراه غير منشورة، كلية الدراسات العليا- جامعة العلوم الإسلامية العالمية، عمان، 2023.
4. هبة سليمان محمد القاضي، مستوى الوعي بالأمن السيبراني لدى معلمي الدراسات الاجتماعية في مديرية تربية قصبة المفرق، رسالة ماجستير غير منشورة، جامعي آل البيت، عمان، 2024.

ثالثاً. المجلات والبحوث

1. عادية عبد الكريم العيدان وبدور مسعد المسعد، درجة الوعي بالأمن السيبراني ودور تكنولوجيا التعليم في تنميته لدى طلبة كلية التربية الاساسية بدولة الكويت، مجلة كلية التربية-جامعة الاسكندرية، العدد4، ج2، مج34، 2024.
2. Afrah Almansoori and Others, Exploring the Frontiers of Cybersecurity Behavior: ASystematic Review of Studies and Theories, Applied Science Journal, No. 9, Vol 13, 2023.
3. Heirman, Wannes, and Others, Predicting Adolescents' Disclosure of Personal Information in Exchange for Commercial Incentives: An Application of an Extended Theory of Planned Behavior, journal of Psychosocial Research on Cyberspace, No. 2, Vol, 16, 2013.
4. Icek Ajzen, The Theory of Planned Behavior, Organizational Behavior and Human Decision Processes Journal, No.2, Vol. 50, December, 1991, P. 185.
5. Khan, N. F. et all., Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. Security Journal, No. 36, Vol. 2, 2022.

6. Mengxin Chen and others, Using the Extended Theory of Planned Behavior to Predict Privacy-Protection Behavioral Intentions in the Big Data Era: The Role of Privacy Concern, Journal of SHS Web of Conferences, No. 155, 2023.
7. Pusey, P., & Sadera, W. A., Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference, Journal of Digital Learning in Teacher Education, No. 2, Vol. 28, 2018.
8. Seki, T. and Others, The Effect of Emotional Intelligence on Cyber Security: The Mediator Role of Mindfulness, Bartin University Journal Faculty of Education, No.12, 2023.
9. Shirley S. Ho and Others, Understanding Factors Associated with Singaporean Adolescents'. Intention to Adopt Privacy Protection Behavior Using an Extended Theory of Planned Behavior, Journal of Psychosocial Research on Cyberspace, No. 9, Vol. 20, Sep. 2017.