وعي الجمهور العراقي بالتهديدات السيبرانية عبر مواقع التواصل الاجتماعي للحماية من المخاطر الإرهابية

Iraqi public awareness of cyber threats Via social media for protection against terrorist risks

م.م. قيصر جبار كاطع

Qayssar Jabbar Gatea

قسم الإعلام/ كلية الآداب / الجامعة المستنصرية

Mustansiriyah University/College of Literature/ Department of Media

kisaer@uomustansiriyah.edu.iq

المستخلص:

يظهر الأمن السيبراني في ظل تصاعد الهجمات الإرهابية المستهدفة للمؤسسات والأفراد كدرع ضروري لحماية النسيج الاجتماعي، إذ يعتمد الإرهاب على تكنولوجيا متقدمة للترويج للعنف وتنفيذ هجمات إلكترونية فضلا عن ذلك يتسبب الاختراق الإرهابي في نشر الفوضى والخوف، لذا من المؤكد أن تعزيز قدرات الأمن السيبراني للتصدي لتلك التحديات ولضمان استقرار البنية الاجتماعية والاقتصاد أمراً ضروريا، وانطلاقا من ذلك فان هذا البحث يهدف إلى معرفة مستوى وعي المجتمع العراقي بشأن تهديدات الأمان السيبراني عبر مواقع أو شبكات التواصل الاجتماعي للحماية من المخاطر الإرهابية المتصلة بها، عن طريق تطبيق دراسة مسحية استخدم فيها استمارة استبيان وزعت على (٤٠٠) مبحوثاً مِن مدينةِ بغداد المركز بجانبيها (الكرخ، والرصافة) وممّن بلغت أعمارهم (١٨ عاماً فأكثر) مِن الإناث والذكور بطريقة العينة العشوائية العنقودية.

أظهرت النتائج وجود وعي جزئي لدى ٤٥.٨٪ من العينة حيال التهديدات السيبرانية مع كون نشر المعلومات المضللة أبرز تهديد بنسبة ٣٤.٨٪، وتبين أن وسائل الإعلام هي المصدر الرئيس لتعلم تقنيات الأمان السيبراني بنسبة ٣٦.٢٪، أيضًا أن فاعلية التوعية السيبرانية كانت "فعّالة إلى حد ما" بنسبة ٣٧٪.

الكلمات المفتاحية: الوعي، الأمن السيبراني، المخاطر الإرهابية، مواقع التواصل الاجتماعي، الجمهور العراقي.

Abstract:

Cybersecurity in the context of the escalating terrorist attacks targeting institutions and individuals, emerges as a crucial shield for protecting the social fabric. Terrorism increasingly relies on advanced technologies to promote violence and carry out cyberattacks. Additionally, terrorist breaches lead to the spread of chaos and fear. Therefore, it is essential to enhance cybersecurity capabilities to address these challenges and ensure the stability of the social and economic structures. Based on this, the aim of this research is to assess the level of awareness of the Iraqi society regarding cybersecurity threats through social media platforms or networks to safeguard against associated terrorist risks. A survey study was conducted using a questionnaire distributed to 400 participants from Baghdad, both from the Karkh and Rusafa sides, aged 18 and above, including both males and females, through a cluster random sampling method.

The results revealed partial awareness among 45.8% of the sample regarding cyber threats, with the dissemination of misleading information being the most prominent threat at 34.8%. It was also found that the media is the primary source for learning cybersecurity techniques, accounting for 36.2%. Furthermore, the results indicated that the effectiveness of cybersecurity awareness was "moderately effective," with a response rate of 37%.

Keywords: Awareness, Cybersecurity, Terrorism Risks, social media, Iraqi Public.

المقدمة: يشهد العالم في الآونة الأخيرة تصاعداً في التوترات الأمنية التي تستهدف المنشآت والأفراد، وأصبح الأمن السيبراني أحد أهم الأدوات التي يمكن عن طريقها حماية النسيج الاجتماعي من هذه الهجمات، وتعتمد الهجمات الإرهابية على وسائل التقانة الحديثة مواقع التواصل الاجتماعي لتعزيز الدعاية المؤيدة وتحريض العنف وتنفيذ عمليات تخريب إلكتروني مثل الاعتداءات الإلكترونية على البنية التحتية الحيوية أو سرقة البيانات الحساسة، ويمكن أن يؤدي الاختراق الإرهابي إلى عواقب وخيمة على النسيج الاجتماعي مثل نشر الفوضى والاضطرابات وإثارة الخوف والقلق بين الناس والإضرار بالاقتصاد الوطني.

المبحث الأول: منهجية البحث

أولا: مشكلة البحث: تعد التطورات الهائلة في مجال تقانة المعلومات أداة حيوية للمجتمعات الحديثة، إلا أنها تثير تحديات أمنية خطيرة، خاصة في ظل تزايد التهديدات السيبرانية والمخاطر الإرهابية المتنوعة. ويشهد العراق، كدولة تعاني من تحديات أمنية متعددة، تزايدًا في التهديدات السيبرانية المرتبطة بالإرهاب. لذا، يتمحور التساؤل الرئيس للبحث بـ: ما دور الأمن السيبراني في حماية المجتمعات من التهديدات الإرهابية. وتنبعث من التساؤل الرئيس مجموعة من التساؤلات الفرعية يمكن تحديدها على النحو التالي:

١. ما مستويات الوعي حاليا بين المجتمع العراقي بشأن التهديدات السيبرانية والمخاطر الإرهابية المتصلة بها؟
٢. ما العوامل المؤثرة في تشكيل الوعي العام بتقنيات الأمن السيبراني؟
٣. ما الصعوبات التي تواجه الجهود الآنية لرفع الوعي السيبراني في العراق؟
٤. كيف يمكن تحفيز المجتمع العراقي لتعزيز التقنيات السيبرانية للحماية الفعّالة من التهديدات الإرهابية؟

ثانيا: أهمية البحث: يعد البحث حول وعي الجمهور العراقي بتقنيات الأمان السيبراني أمرًا حيويًا إذ يسهم في تحسين حماية الأمان الوطني وضمان الاستقرار، ويؤدي البحث دورًا هامًا في تحقيق توازن بين حقوق الأفراد والتحضير لتحديات التهديدات السيبرانية مستقبلا. فضلا عن ذلك تعزز التوعية العامة من قبل الجمهور التعاون الدولي في مكافحة الجريمة السيبرانية ومواجهة التهديدات الإرهابية مسهمًا في تعزيز الأمان الشامل والاستجابة الفعالة للتحديات المعاصرة.

ثالثا: أهداف البحث: تتمحور لتحقيق ما يلي:

١. قياس مستوى الوعي الحالي بين الجمهور العراقي بشأن التهديدات السيبرانية والمخاطر الإرهابية المتصلة بها.

٢. تحديد العوامل المؤثرة في تشكيل الوعي العام بتقنيات الأمن السيبراني.

٣. تحديد التحديات والمشكلات التي تعرقل جهود رفع الوعي السيبراني في العراق.

٤. اقتراح مجموعة من الإجراءات لتحفيز المجتمع العراقي لتعزيز تقنيات الأمن السيبراني للحماية الفعّالة من التهديدات الإرهابية.

رابعا: نوع البحث ومنهجه: يُعد هذا البحث أحد البحوث الوصفية الذي يهدف إلى وصف ظاهرة أو موقف، وهنا يركز على ظاهرة وعي الجمهور العراقي بتقنيات الأمن السيبراني للحماية من المخاطر الإرهابية. أما المنهج الذي اعتمده الباحث فهو المنهج المسحي بالعينة الذي يهدف إلى جمع المعلومات من عينة محددة من الأفراد، ويتم تنظيم ومعالجة هذه البيانات بشكل إحصائي للتوصل إلى أجوبة عن التساؤلات التي ينشدها الباحث.

خامسا: أدوات البحث:

الاستبانة: أعدَّ الباحث استبانة بوصفها أداة رئيسة لجمع البيانات، لاستطلاع وعي سكان بغداد بتقنيات الأمن السيبراني وسبل الوقاية من المخاطر الإرهابية. واشتملت على أسئلة مغلقة، استُخلصت من تساؤلات البحث ووزعت على عينة قوامها (٤٠٠) فرد من جانبي الكرخ والرصافة بما يعكس التوزيع السكاني.

سادسا: مجتمع البحث وعينته: تحدد مجتمع البحث بجمهور مدينة بغداد المركز، مع تضمين جانبيها الكرخ والرصافة؛ وذلك لشمول كافة فئات السكان ويشمل البحث كل الفئات العمرية من النساء والرجال الذين تجاوزوا سن الـ١٨ عامًا، ويتمثل المجتمع الدراسي في مدينة بغداد بشمولية جميع أقضيتها وتحديدًا قضاء الرصافة وقضاء الأعظمية وقضاء الكرخ وقضاء الصدر الأولى والثانية وقضاء الكاظمية، وتم اعتماد منهجية اختيار العينة العشوائية المتعددة المراحل إذ استخدمت القرعة لاختيار مناطق وأحياء في مدينة بغداد، وتم اختيار ناحيتين عشوائيًا من كل قضاء ومن ثم تم اختيار حيين سكنيين بطريقة احتمالية من كل حي، وجدول (١) يبين العينة الميدانية لفهم تفاصيل أكثر لهيكل العينة.

جدول (١) يبين توزيع عينة البحث وفقا للمتغيرات

المتغير	الفئات	ت	%
الجنس	ذَكر	٢٨٢	٧٠.٥٪
	أنثى	١١٨	٢٩.٥٪

العمر	١٨– ٣٠ سنة	١٤٢	٣٥.٥٪
	٣١–٤٠ سنة	١١٦	٢٩٪
	٤١– ٥٠ سنة	٧٠	١٧.٥٪
	٥١– ٦٠ سنة	٤٨	١٢٪
	٦١ فما فوق	٢٤	٦٪
المستوى التعليمي	ابتدائية فما دون	١٢	٣٪
	ثانوية "متوسطة/إعدادية"	٥٢	١٣٪
	دبلوم	٧٢	١٨٪
	بكالوريوس	١٩٨	٤٩.٥٪
	شهادة عليا	٦٦	١٦.٥٪
المجموع		٤٠٠	١٠٠٪

سابعا: الصدق والثبات: بعد إعداد استمارة الاستبانة لفحص مدى وعي الجمهور العراقي بتقنيات الأمان السيبراني للدفاع عن نفسهم من المخاطر الإرهابية، قام الباحث بتقديم الاستمارة لمجموعة من الخبراء(*) للحصول على مراجعتهم وتوجيهاتهم بعدها قام الباحث بتعديلات استنادًا إلى التوجيهات المقترحة من قبل الخبراء، وأخذ بعين الاعتبار آراءهم وبلغت نسبة اتفاق الخبراء حول فئات الاستبانة ٨٨٪ مما يشير إلى صدق الاستبيان الظاهري. أما بالنسبة لثبات النتائج تم إجراء اختبار إعادة الاختبار على عينة تمثل ١٠٪ من إجمالي عينة البحث خلال مدة ١٥ يومًا وبلغ متوسط ثبات الإجابات (٠.٨٩) مما يُظهر ثبات الاستبيان بشكل جيد.

ثامنا: مجالات البحث: حدد الباحث المجال الزماني للبحث من (١ آب ٢٠٢٤ إلى ٣١ كانون الأول ٢٠٢٤)، وهي المدة التي تم خلالها تصميم استمارة الاستبانة وتوزيعها على العينة في مدينة بغداد المركز، وتم تحديد المجال المكاني في مدينة بغداد مع التركيز على مناطق الكرخ والرصافة. ويمثل المجال البشري جمهور سكان بغداد وفقًا لإحصائيات الجهاز المركزي للإحصاء لعام ٢٠١٩.

(*) الخبراء حسب ألقابهم العلمية وتخصصهم.

١. أ.م.د. مدين عمران التميمي، جامعة الإسراء، كلية الآداب.

٢. م.د. محمد شاكر محمود، الجامعة المستنصرية، كلية الآداب، قسم الإعلام.

٣. م.د. محمد فالح التميمي، جامعة الإمام جعفر الصادق (ع)، كلية الآداب، قسم الإعلام.

المبحث الثاني: وعي الجمهور بالتهديدات السيبرانية في مواقع التواصل الاجتماعي

أولا: مفهوم الوعي، وأنواعه: يشير الوعي إلى درجة إدراك الأفراد للمعلومات والتفاهم الشامل للأمور المحيطة بهم. يتضمن الوعي فهمًا عميقًا للظروف والتحديات والمفاهيم التي تؤثر على الفرد والمجتمع، أي أنه حالة شاملة تعبر عن إدراك الفرد للمحيط الذي يحيا فيه ويمتاز بفهم عميق للمعلومات والظروف التي تؤثر عليه وعلى المجتمع الذي ينتمي إليه، إذ يظهر الوعي قدرة الفرد على استيعاب وتحليل البيانات المحيطة به بأسلوب مستفيض (Krishnamurthy, 2005, p. 190). ويشمل الوعي في جوانبه الأساسية فهمًا للتاريخ والثقافة والقيم التي يتشاركها مع الجمهور ويمتد ليشمل الأبعاد الاقتصادية والاجتماعية والبيئية ويتيح للفرد فهم التحديات والفرص التي تعترضه (Bennet & Schafer, 2022, p. 442). ويمكن أن يكون الوعي ديناميًا إذ يتطور ويتغير مع تطور الزمان والمكان ويتأثر بعوامل متعددة مثل التعليم ووسائل الإعلام والتجارب الشخصية، لذا يُعَدُّ أساسًا أساسيًا لتفعيل الفرد في مجتمعه وهو أداة حيوية لتحقيق تحول الإيجابي وتعزيز التفاعل البناء بين الأفراد والمجتمعات (Dienstmann, 2021, p. 171).

ويتيح العصر الرقمي في ضوء التقانة المتقدمة وسائل الإعلام وتقنيات التقانة المعلوماتية توسيع نطاق الوعي بشكل لم يكن ممكنًا في السابق إذ تؤدي التقانة دورًا حيويًا في نقل المعلومات بشكل فوري وفعّال إلى جمهور واسع مثلاً مواقع التواصل الاجتماعي توفر وسيلة فعّالة لتبادل الأفكار والتجارب مما يسهم في بناء وعي قوي بين المجتمعات (Ktoridou, Doukanari, & Eteokleous, 2020, p. 111). ويمكن أن تؤدي التقانة أيضًا دورًا في توفير مصادر تعلم إلكترونية تسهم في توجيه الأفراد نحو فهم أعمق للقضايا الثقافية والاجتماعية والأمنية. مثلا مواقع التعلم عبر الإنترنت توفر وصولاً سهلاً ومرنًا إلى المعلومات التي تعزز التفاعل وتوسيع آفاق الفهم (Ktoridou, Doukanari, & Eteokleous, 2020, p. 112).

ويمكن باستخدام التقنيات الحديثة مثل التعلم الآلي والواقع الافتراضي تحقيق تجارب تفاعلية ترفع من فاعلية توصيل البيانات وتعزز الفهم، بذلك يظهر أن التقانة تؤدي دورًا حيويًا في تعزيز وتوسيع مفهوم الوعي لدى الأفراد والمجتمعات في عصرنا الحديث (مواسي، ٢٠١٦).

ويشهد الوعي في عصر الابتكار التقاني تطورًا ملحوظًا؛ نتيجة لتأثير التقانة ووسائل الإعلام الرقمية ويظهر هذا التطور التحولات السريعة في كيفية تبادل المعلومات وكيفية وصول الأفراد إلى مصادر المعرفة، إذ يتجلى تأثير التقانة في سبل تفاعلية ومبتكرة لنقل وتبادل المعرفة وللوعي أنواع، منها:

١. الوعي الاجتماعي: يشير إلى إدراك الفرد لديناميات المجتمع وتفاعلاته الاجتماعية، ويتكون هذا النوع من الوعي فهمًا عميقًا للقيم والتقاليد والتوجهات الثقافية التي تؤثر على التفاعلات بين الأفراد في المجتمع، ويسمح الوعي الاجتماعي للأفراد بفهم القضايا الاجتماعية، مثل العدالة، وحقوق الإنسان، والتنوع الثقافي، ويمكن أن يؤثر على توجهات الفرد نحو الانخراط في مبادرات المجتمع المحلي أو المشاركة في حل المشاكل الاجتماعية، إذ إن الوعي الاجتماعي يعزز التواصل والتفاعل الفعّال بين الأفراد، ما يعزز بناء مجتمعات مبنية على التعاون والتفاهم (مسعود، ٢٠١١، صفحة ١٠٤).

٢. الوعي التقاني: يمثل جوانب تفاعل الأفراد مع التقنيات والتطورات الرقمية، ويتيح هذا النوع من الوعي للأفراد فهماً أعمق لكيفية استخدام التقانة في حياتهم اليومية وكيف تؤثر على تفاعلاتهم المهنية والشخصية، ويشمل الوعي التقاني الفهم الشامل للأجهزة الإلكترونية، والتطبيقات، وشبكات الاتصالات، إذ يُمكن للأفراد الذين يمتلكون وعيًا تقانيًا قويًا أن يكونوا أكثر فعالية في التفاعل مع التحديثات التقانية واستيعاب التطورات الرقمية بشكل أسرع، ليسهم ذلك في تعزيز مهارات استخدام الأدوات الرقمية، مما يسهم في تحسين أداء الأفراد في مختلف مجالات حياتهم (احمد، ٢٠١٥، صفحة ٧٣).

٣. الوعي الأمني: هو جانب آخر يعبر عن تفاعل الأفراد مع تهديدات الأمان الرقمي، ويتضمن هذا النوع من الوعي فهمًا للمخاطر السيبرانية والصعوبات التي قد تواجه البيانات الشخصية والمعلومات الحساسة على الإنترنت، ويشمل التدابير الوقائية والاحترازات التي يمكن للأفراد اتخاذها لحماية أنفسهم ومعلوماتهم من التهديدات السيبرانية، مثل الاحتيال الإلكتروني، والبرامج الضارة، والاختراقات الأمنية، ومخاطر الإرهاب (Tashi & Ghernaouti-Helie, 2011, p. 149).

٤. الوعي السيبراني: يشير إلى درجة إدراك الأفراد لتهديدات الأمان الرقمي وكيفية التصدي لها، يتضمن فهمًا للهجمات السيبرانية وتقنيات الحماية منها، ويعزز الوعي السيبراني قدرة التعرف على الاختراقات الإلكترونية وحماية البيانات الحساسة، ويتيح هذا الوعي للفرد تبني ممارسات أمان رقمي والمشاركة في جهود تحسين الأمان السيبراني على المستوى الشخصي والجماعي (Ziemba & Wątróbski, 2024, p. 293).

٥. الوعي الإرهابي: يمثل استيعاب الأفراد للتهديدات الإرهابية وكيفية التعامل معها، ويعزز الوعي الإرهابي فهمًا عميقًا للتحديات الأمنية ويسهم في تشكيل استعداد الأفراد لمواجهة تلك التحديات، فضلًا عن ذلك يتيح هذا

الوعي للفرد التفاعل بفعالية مع التهديدات الإرهابية والمساهمة في جهود الحماية والتصدي للتحديات الأمنية على مستوى المجتمع (Argomaniz & Lynch, 2015).

٦. الوعي التقني: يُعبر عن فهم الأفراد للتقنيات المستخدمة في مجال الأمان السيبراني وكيفية تسخيرها للحماية من التهديدات السيبرانية، ويتضمن هذا الوعي فهمًا عميقاً للأدوات والتقنيات المستخدمة لتأمين الشبكات والمعلومات، ويسهم الوعي التقني في تمكين الأفراد من تبني أفضل الخطوات في مجال السلامة الرقمية. ليتيح هذا الفهم للأفراد الاستجابة بفعالية للتحديات التقنية والمساهمة في تعزيز الحماية السيبرانية للفرد والمجتمع عمومًا (Ziemba & Wątróbski, 2024, p. 293).

ثانيا: الأمن السيبراني والمخاطر الإرهابية: الأمن السيبراني هو "مجموعة من الممارسات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات السيبرانية"، ويتضمن ذلك حماية أجهزة الحاسوب والشبكات والتطبيقات والبيانات من الوصول غير المسموح به والاستخدام غير المرخص والنشر غير المرغوب فيه فضلا عن تعزيز الوعي بأمور الأمان، ويشمل أيضًا الحماية من سرقة البيانات والبرمجيات الخبيثة وغيرها من التهديدات التي قد تؤثر على أمان المعلومات والأنظمة الرقمية (Sukhostat & Popov, 2022, p. 28). ويشمل مجال الأمن السيبراني أيضًا تعزيز الوعي والتدريب للمستخدمين لتحقيق بيئة رقمية آمنة فضلاً عن تطوير سياسات وإجراءات فعّالة للتصدي للتحديات المستمرة في عالم الإنترنت ويتطلب الأمن السيبراني التحقق المستمر واستخدام تقنيات الكشف عن الاختراق للتعرف على التهديدات المستحدثة (العمارات و الحمامصة، ٢٠٢٢، صفحة ١٨١). ليؤدي إلى الهجمات الإلكترونية التي تؤدي الى تهديدًا متعدد الأوجه إذ يمكن استخدامها لأغراض متنوعة مثل الحصول على بيانات حساسة ككلمات المرور وأسماء المستخدمين وبيانات بطاقات الائتمان، ويمكن أن تُستخدم لتعطيل الأنظمة والشبكات مما يتسبب بتعطيل الخدمات أو الأعمال وحتى تسبب الضرر المادي عبر إتلاف المعدات أو البنية التحتية (الدويري ، ٢٠٢٣، صفحة ١٣٧).

ويؤدي الأمن السيبراني دورًا مهمًا في حماية المجتمع فأمان الأنظمة والشبكات والبيانات تحقق الحماية من مجموعة واسع من المخاطر مثل فقدان البيانات، إذ يمكن أن يؤدي خسائر مالية كبيرة أو حتى إلى تعطيل الأعمال وكذلك التعطيل الذي يؤدي إلى تعطيل الأنظمة والشبكات مما يتسبب بتعطيل الخدمات أو الأعمال أو حتى التسبب في خسائر بشرية، فضلا عن الضرر المادي الذي يؤدي إلى إتلاف المعدات أو البنى التحتية، مما يتسبب بخسائر مادية وكذلك التأثير على الأمن القومي إذ يمكن أن تستخدم الجماعات الإرهابية الهجمات الإلكترونية لشن هجمات إرهابية (Watters , 2023, p. 164)

ويُشير مصطلح "المخاطر الإرهابية السيبرانية" إلى استخدام التقنيات السيبرانية في اتجاه الأهداف الإرهابية إذ تأخذ هذه الهجمات أشكالًا متعددة منها الهجمات على البنية التحتية الحيوية مثل شبكات المياه والكهرباء والمواصلات مما يتسبب بتعطيل الخدمات الأساسية وتكبيد خسائر مادية وبشرية جسيمة، وتستخدم هجمات نشر المعلومات الإشاعات والمضللة عبر الإنترنت لزعزعة الاستقرار الاجتماعي أو السياسي وتشمل أيضًا هجمات سرقة البيانات إذ يتم استهداف بيانات حساسة مثل بيانات الموظفين أو العملاء أو البيانات الحكومية ويمكن استخدام هذه البيانات لتهديد الأفراد أو المؤسسات أو حتى لممارسة الضغط على الحكومات، وتبرز تلك الهجمات خطورة تزايد الارتباط بين التقانة والتهديدات الإرهابية مما يستدعي الضرورة لتعزيز التدابير الأمنية وتعاون دولي فعّال للتصدي لتلك التحديات المتزايدة (Johnson, 2005, p. 222).

وتتباين أساليب الهجمات الإرهابية السيبرانية وتتوقف على أهداف الإرهابيين إذ تشمل الهجمات الإلكترونية استهداف الأنظمة والشبكات الإلكترونية بهدف تعطيلها أو سرقة بياناتها وكذلك تتضمن هجمات البرمجيات الخبيثة مثل الفيروسات أو الديدان لإصابة الأنظمة والشبكات الإلكترونية سواء لأغراض سرقة البيانات أو تعطيل الأنظمة، فضلاً عن استخدام تقنيات القرصنة لاختراق الأنظمة والشبكات الإلكترونية (مركز الحضارة، ٢٠٢٢، صفحة ٤٦٣).

ثالثا: عوامل تشكيل وعي الجمهور بتقنيات الأمن السيبراني: يُعد وعي الجمهور بتقنيات الأمن السيبراني أمرًا بالغ الأهمية لتعزيز الأمن السيبراني فكلما كان الجمهور أكثر وعياً بالمخاطر السيبرانية زادت احتمالية اتخاذهم خطوات للحماية من هذه المخاطر وهناك الكثير من الأمور التي تسهم في تشكيل وعي الجمهور بتقنيات الأمن السيبراني، ويمكن تقسيمها إلى عوامل داخلية وخارجية (Nehme, 2023, p. 19). فالعوامل الداخلية تشمل العوامل التي تتسبب في تشكيل وعي الجمهور بتقنيات الأمن السيبراني: مثل المستوى التعليمي الذي يُعد أحد أهم الأمور التي تؤثر على وعي الجمهور بتقنيات الأمن السيبراني فكلما كان الجمهور أكثر تعليماً زادت احتمالية فهمهم للمخاطر السيبرانية وكيفية حماية أنفسهم منها، والثقافة إذ تؤدي الثقافة دورًا في تشكيل وعي الجمهور بتقنيات الأمن السيبراني ففي بعض الثقافات يُنظر إلى الأمن السيبراني على أنه أمر مهم بينما في ثقافات أخرى يُنظر إليه على أنه أمر ثانوي (عنتر، ٢٠٢٣). أما العوامل الخارجية فتتمثل بالعوامل التي تتسبب في تشكيل وعي الجمهور بتقنيات الأمن السيبراني ومنها الحملات التوعوية: إذ تؤدي دورًا هاماً في نشر الوعي العام بتقنيات الأمن السيبراني وهذه الحملات يمكن أن تستهدف الجمهور العام أو شرائح معينة من الجمهور مثل الشباب أو مستخدمي الإنترنت، ووسائل الإعلام التي تؤدي دورًا مهمًا في نشر الوعي العام بتقنيات الأمن السيبراني فتقارير وسائل الإعلام عن الهجمات السيبرانية تساعد في توعية الجمهور بالتهديد السيبراني، والحادثة السيبرانية تسهم في

زيادة الوعي العام بتقنيات الأمن السيبراني فعندما يتعرض الجمهور لخسارة مالية أو شخصية بسبب حادثة سيبرانية يكون أكثر عرضة للاهتمام بالموضوع والتعلم عنه (Alqahtani, 2022, pp. 4–6).

رابعاً: مواقع التواصل الاجتماعي: يُعد مفهوم مواقع التواصل الاجتماعي تطورًا تقانيًا مهمًا غيّر الطريقة التي يتفاعل بها الأفراد والجماعات مع بعضهم البعض على شبكة الإنترنت، وعن طريق المواقع يمكن للمستخدمين تحقيق اهتماماتهم وأنشطتهم والتواصل مع الآخرين من جميع أنحاء العالم (شمخي، ٢٠٢٣، صفحة ٧٠٠).

وتُعرَّف المواقع الاجتماعية بأنها "مواقع ويب تقدم مجموعة متنوعة من الخدمات بما في ذلك الدردشة الفورية والبريد الإلكتروني والرسائل الخاصة والفيديو والتدوين ومشاركة الملفات وغيرها"، وأنها تشمل المواقع التي تجمع أصدقاء المدرسة أو العمل فضلاً عن شبكات المدونات الصغيرة ومن أشهر الشبكات الاجتماعية اليوم فيسبوك وأكس ويوتيوب وإنستغرام إلخ... (خليل، ٢٠١٢، صفحة ١٣١).

وتعد مواقع التواصل الاجتماعي من أكثر المواقع شيوعًا وشعبية على الإنترنت وذلك لأنها توفر خاصية التواصل بين الأفراد والجماعات التي تستخدمها، وتشير بعض الإحصائيات إلى أن من بين أكثر ٥٠ موقعًا زيارة في العالم نجد ١٠ مواقع للشبكات الاجتماعية (منصوري، ٢٠١٤، صفحة ٦٢).

وتُعرَّف "مواقع التواصل الاجتماعي بأنها مواقع إلكترونية تقدم مجموعة متنوعة من الخدمات، مثل الدردشة الفورية والرسائل الخاصة والبريد الإلكتروني والفيديو والمدونات المكتوبة والصوتية ومشاركة الملفات". (الفيصل، ٢٠١٤، صفحة ٦٥) و (قنبر و محمد، ٢٠٢٣، صفحة ٢٩٣)، وتتباين استخدامات مواقع التواصل الاجتماعي حول العالم إذ يستخدم معظم المستخدمين هذه المواقع لتبادل البيانات مع الأصدقاء والاستمتاع بأغراض مفيدة ومع ذلك تظهر أغراضٌ ودوافع أخرى لاستخدام هذه المواقع لأغراض دعائية أو إرهابية تهدد أمن المجتمع (رابح، ٢٠٠٧، صفحة ٢٣).

خامساً: أساليب استخدام الإرهابيين للتقنيات السيبرانية في تحقيق أهدافهم الإرهابية: يُعرَّف الإرهاب السيبراني بأنه "استخدام الأسلحة الإلكترونية لتخويف أو إرهاب أو إلحاق الأذى بالأفراد أو المجتمعات أو الحكومات"، إذ يهدف الإرهاب السيبراني إلى تحقيق أهداف أيديولوجية أو سياسية معينة مثل تغيير سياسات الحكومة أو نشر الفوضى أو نشر الرعب ويعتمد على التقانة لتحقيق أهدافه، ويسعى الإرهابيون السيبرانيون إلى البقاء مجهولين لصعوبة تعقبهم ويتميز بتكلفة منخفضة مقارنةً بأشكال الإرهاب الأخرى، إذ يمكن للإرهابيين السيبرانيين الوصول إلى التقانة من أي مكان في العالم (جبور، ٢٠١٨، صفحة ٨٥). وهناك الكثير من الأساليب المستخدمة في الإرهاب السيبراني منها البريد الإلكتروني الذي يعد الوسيلة الأولى من الوسائل التي يستخدمها الإرهابيين إذ يستغلون هذه

لخدمة للتواصل فيما بينهم بسرعة ودون رقابة وكذلك إنشاء مواقع الإنترنت فضلاً عن تدمير واختراق المواقع المعارضة لهم من أي مكان في العالم (التميمي، ٢٠٢٤، صفحة ٩٢٣).

وأصبح استخدام الإرهاب السيبراني ظاهرة متزايدة التهديد إذ يمكن للإرهابيين استخدام التقنيات السيبرانية لتحقيق أهدافهم الإرهابية بطرق مختلفة، منها:

١. نشر البيانات المضللة والدعاية: يمكن للإرهابيين استخدام الجوانب السيبرانية لنشر المعلومات أو البيانات المضللة والدعاية من أجل زعزعة استقرار المجتمعات ونشر الخوف، مثلاً استخدم (داعش) وسائل التواصل الاجتماعي لنشر دعايته والتجنيد (الشمري و العبيدي، ٢٠١٩، صفحة ٧٧).
٢. شن الهجمات الإلكترونية: تؤدي هذه الهجمات إلى انقطاع الخدمات الأساسية وخلق الذعر عن طريق أراقة مثل هذه الهجمات على الهياكل التنظيمية الحيوية كشبكات المياه والنقل (البهي، ٢٠١٩، صفحة ١٥).
٣. اختراق الأنظمة والشبكات: يعنى ذلك بحصول الإرهابيين على معلومات حساسة عن طريق اختراق الأنظمة والشبكات للوصول إلى معلومات سرية لنشر برامج ضارة (Sukhostat & Popov, 2022, p. 16).
٤. التحكم في أجهزة الكمبيوتر والأجهزة المتصلة بالإنترنت: يمكن للإرهابيين استخدام التكنولوجيا السيبرانية للتحكم في أجهزة الكمبيوتر والأجهزة المتصلة بالإنترنت مثل السيارات والطائرات بدون طيار، ويمكن أن يستخدموا هذه القدرة لشن هجمات أو إلحاق الأذى بالناس (Alqahtani, 2022, p. 10).
٥. الهجمات النفسية والإعلامية: يُستخدم الإرهابيون تقنيات سيبرانية متطورة لتحقيق أهدافهم إذ يعتمدون على الهجمات الإلكترونية واستخدام وسائل التواصل للترويج لأفكارهم وتأثير الرأي العام ويظهر ذلك تطور التهديدات الأمنية إذ يتخذ الإرهاب شكلًا رقميًا يتضمن الهجمات النفسية والإعلامية التي تستهدف التأثير النفسي لإشاعة الرعب والهلع مما يبرز أهمية تعزيز الأمن السيبراني ومكافحة التطرف الرقمي بشكل فعّال لضمان الأمان الوطني (Krishnamurthy, 2005, p. 75).

ولمواجهة التحديات المتزايدة للإرهاب السيبراني يتعين على الجهات الحكومية والمنظمات غير الحكومية والشركات التعاون وتكامل جهودها، إذ يشدد الحل على ضرورة تطوير سياسات وقوانين فعّالة للأمان السيبراني مع تحديد المسؤوليات وفرض عقوبات للمخالفين، ويجب زيادة الاستثمار في البحث لتطوير تقنيات مبتكرة وفعّالة لمواجهة التهديدات السيبرانية فضلًا عن ذلك يتعين نشر الوعي العام بالمخاطر السيبرانية عن طريق حملات إعلامية توعية شاملة وتقديم تدريبات لرفع مستوى الوعي والمهارات (حكيم، ٢٠١٨، صفحة ١٠٦).

سادساً: مخاطر الإرهاب السيبرانية على العراق: يعد الإرهاب السيبراني من الصعوبات الأمنية الحديثة التي تهدد العديد من القطاعات في المجتمع إذ يستخدم الهجمات السيبرانية لتحقيق أهداف سياسية واقتصادية وعسكرية واجتماعية، وتعد هذه الهجمات تهديداً شاملاً يتطلب فهماً علمياً دقيقاً للمجتمعات والدول التي قد تتأثر بها.

المبحث الثالث: وعي الجمهور العراقي بتقنيات الأمن السيبراني للحماية من المخاطر الإرهابية

يعرض هذا المبحث نتائج البحث الَّتي تم التوصل إليها بعدما وزع الباحث أداة الاستبانة عَلى عينّة مِن جمهور مدينة بغداد المركز مِن (١٨ عاماً فأكثر) ومِن الذكور والإناث، ويُظهر هذا الجزء ردود فعل الجمهور العراقي مع التركيز على فهمهم ووعيهم تجاه الأمن السيبراني وكيف يمكن أن تحميهم من المخاطر الإرهابية[*].

١. جدول (٢) يبين ادراك عينة البحث للتهديدات الإلكترونية والمخاطر المتعلقة بها عبر مواقع التواصل

ت	مستوى الإدراك	ت	%
١.	بعض الفهم	١٨٣	٤٥.٨٪
٢.	أنا ملم بالموضوع	٩٦	٢٤٪
٣.	قليل	٦٣	١٥.٧٪
٤.	أنا غير ملم	٥٨	١٤.٥٪
المجموع		٤٠٠	١٠٠٪

يتضح مِن الجدولِ (٢) أنَّ (٤٥.٨٪) من العينة قد ادركوا (بعض الفهم) للتهديدات الإلكترونية والمخاطر المرتبطة بها وهو جاء بالمرتبة الأولى في حين أن (أنا ملم بالموضوع) جاء بالدرجة الثانية وبنسبة (٢٤٪) وفي المرتبة الثالثة جاءت فئة (قليل) وبنسبة (١٥.٧٪)، أما الذين كانوا غير ملمين عبر أجابتهم (أنا غير ملم) جاءوا بنسبة (١٤.٥٪) فقط وهم في المرتبة الأخيرة، تعكس هذه النتائج أهمية تعزيز برامج التوعية الإلكترونية لسد الفجوة المعرفية ورفع مستوى الإدراك العام بالمخاطر الإلكترونية.

[*]) يمكن الإشارة إلى أن الجداول التي يكون مجموعها أكثر من (٤٠٠) هي من الأسئلة التي سمح للعينة باختيار أكثر من بديل

٢- جدول (٣) يبين أنواع التهديدات السيبرانية التي تعرفها عينة البحث

ت	التهديدات	ت	%
.١	نشر المعلومات المضللة	٢٦٠	٣٤.٨٪
.٢	سرقة البيانات	٢٥١	٣٣.٦٪
.٣	الهجمات على البنية التحتية الحيوية	١١٩	١٥.٩٪
.٤	الهجمات على الأفراد	١١٧	١٥.٦٪
	المجموع	٧٤٧	١٠٠٪

يظهر من جدول (٣) أن (نشر المعلومات المضللة) كانت الأكثر شيوعًا بين أنواع التهديدات السيبرانية المعروفة لدى عينة البحث بنسبة (٣٤.٨٪)، وجاءت فئة (سرقة البيانات) في المرتبة الثانية بنسبة (٣٣.٦٪)، أما الهجمات على البنية التحتية الحيوية فكانت في المرتبة الثالثة بنسبة (١٥.٩٪)، بينما جاءت الهجمات على الأفراد في المرتبة الأخيرة بنسبة (١٥.٦٪)، وتبين هذه النتائج الحاجة لتوسيع الوعي بمختلف أنواع التهديدات السيبرانية، خاصة الأقل إدراكًا منها.

٣- يوضح جدول (٤) المخاطر الإرهابية المتأتية من التهديدات السيبرانية وفقًا لرأي المبحوثين

ت	المخاطر الإرهابية	ت	%
.١	إثارة الاضطرابات الاجتماعية أو السياسية	٢٧١	٣٢.٢٪
.٢	إلحاق الضرر بالممتلكات أو الأرواح	٢٦٤	٣١.٣٪
.٣	الضغط على الحكومة	١٩٤	٢٣٪
.٤	تعطيل الخدمات الأساسية	١١٢	١٣.٣٪
	المجموع	٨٤١	١٠٠٪

يوضح جدول (٤) أن هناك (٢٧١) من المشاركين اختاروا (إثارة الاضطرابات الاجتماعية أو السياسية) كأكثر المخاطر الإرهابية الناتجة عن التهديدات السيبرانية، إذ حصلت هذه الفئة على المرتبة الأولى بنسبة (٣٢.٢٪)

وفي المرتبة الثانية جاءت (الحاق الضرر بالممتلكات أو الأرواح) بنسبة (٣١.٣٪)، بينما جاءت فئة (الضغط على الحكومة) في المرتبة الثالثة بنسبة (٢٣٪). أما في المرتبة الأخيرة فقد اختار المشاركون (تعطيل الخدمات الأساسية) كمخاطر إرهابية ناتجة عن التهديدات السيبرانية، بنسبة (١٣.٣٪)، ويمكن أن نعزو تصدّر "إثارة الاضطرابات" لأن هذا النوع من المخاطر يُعد الأسرع تأثيرًا والأوضح حضورًا في الواقع الرقمي، بينما تراجعت "تعطيل الخدمات" لارتباطها بهجمات متخصصة نادرة الحدوث في البيئة المحلية

٤- جدول (٥) يوضح مصادر المعلومات التي يعرفها المبحوثين عن تقنيات الأمن السيبراني

ت	مصادر المعلومات	ت	%
.١	وسائل الإعلام	٣٠٤	٣٦.٢٪
.٢	منشورات الأصدقاء	٢٢١	٢٦.٣٪
.٣	الجهات الحكومية	١٩٨	٢٣.٥٪
.٤	المؤسسات التعليمية	١١٧	١٣.٩٪
	المجموع	٨٤٠	١٠٠٪

يظهر من جدول (٥) أن (وسائل الإعلام) تعتبر من أهم مصادر المعلومات التي يعرفها المبحوثين عن تقنيات الأمن السيبراني، إذ حصلت على المرتبة الأولى بنسبة (٣٦.٢٪) وفي المرتبة الثانية جاءت (منشورات الأصدقاء) بنسبة (٢٦.٣٪)، بينما جاءت (الجهات الحكومية) في المرتبة الثالثة بنسبة (٢٣.٥٪). وفي المرتبة الأخيرة جاءت (المؤسسات التعليمية) بنسبة (١٣.٩٪) من أفراد العينة، ويمكن أن نعزو تصدّر وسائل الإعلام كونها المصدر الأسرع والأوسع انتشارًا للمعلومات التقنية، في حين تراجعت المؤسسات التعليمية بسبب ضعف برامج التوعية السيبرانية فيها مقارنة بالإعلام ومنصات التواصل

٥- يبين جدول (٦) مدى معرفة المبحوثين بتقنيات الأمن السيبراني عبر استخدام المواقع

ت	معرفة التقنيات	ت	%
.١	متوسطة	٢٧٨	٦٩.٥٪
.٢	عالية	٦٢	١٥.٥٪

٣.	منخفضة	٦٠	١٥٪
المجموع		٤٠٠	١٠٠٪

يبين جدول (٦) أن نسبة المعرفة بتقنيات الأمن السيبراني بين أفراد العينة تتراوح بين المتوسطة والعالية والمنخفضة. إذ أظهرت النتائج أن (٦٩.٥٪) من العينة يمتلكون معرفة متوسطة، في حين يمتلك (١٥.٥٪) معرفة عالية وكذلك (١٥٪) يمتلكون معرفة منخفضة بتقنيات الأمن السيبراني، وتظهر النتائج أن معظم أفراد العينة يمتلكون معرفة متوسطة بتقنيات الأمن السيبراني، مما يعكس الوعي العام بالمفهوم دون التعمق الكافي، بينما تشير النسب الأقل للمعرفة العالية والمنخفضة إلى تفاوت كبير في فهم الأفراد لهذه التقنيات.

٦- جدول(٧) يبيّن تقنيات الأمان المستخدمة للحماية من المخاطر السيبرانية عبر مواقع التواصل

ت	التقنيات المستخدمة	ت	%
١.	عدم فتح المرفقات من مصادر غير معروفة	١٣٢	٢٨.٨٪
٢.	استخدام برامج الحماية	١١٥	٢٥٪
٣.	تحديث التطبيقات باستمرار	١٠٩	٢٣.٧٪
٤.	كلمات مرور قوية	١٠٣	٢٢.٤٪
المجموع		٤٥٩	١٠٠٪

يتضح مِن الجدولِ (٧) أنَّ (عدم فتح المرفقات من مصادر غير معروفة) جاءت في المرتبة الأولى بين التقنيات الأمنية التي يستخدمها المبحوثين لحماية أنفسهم من التهديدات السيبرانية وبنسبة (٢٨.٨٪)، وجاءت فئة (استخدام برامج الحماية) في المرتبة الثانية وبنسبة (٢٥٪)، وحصلت على المرتبة الثالثة فئة (تحديث التطبيقات باستمرار) وبنسبة (٢٣.٧٪)، في حين جاءت فئة (كلمات مرور قوية) بالمرتبة الأخيرة وبنسبة (٢٢.٤٪) من عينة البحث، وتُظهر النتائج أن المبحوثين يعتمدون بشكل رئيس على تجنب المرفقات من مصادر غير معروفة كأول وسيلة دفاعية ضد التهديدات السيبرانية ما يعكس الوعي بالتهديدات الشائعة مثل الرسائل الاحتيالية في حين يأتي استخدام برامج الحماية وتحديث التطبيقات كخيارات موازية تدل على اهتمام بالوقاية التقنية أما كلمات المرور القوية فجاءت في المرتبة الأخيرة، ما قد يشير إلى قلة التركيز على هذه التقنية مقارنة بالبقية.

٧- جدول (٨) تحديات رفع الوعي السيبراني عبر مواقع التواصل الاجتماعي حسب رأي المبحوثين

ت	التحديات	ت	%
١.	قوانين ضعيفة	١٨٢	٣٩.٦٪
٢.	ضعف الوعي العام بأهمية الأمن السيبراني	١٦٥	٣٥.٩٪
٣.	نقص الموارد المالية والبشرية	١٤٣	٣١٪
٤.	عدم وجود برامج تعليمية كافية حول الأمن السيبراني	١١٩	٢٥.٩٪
٥.	صعوبة الوصول إلى المعلومات	١٠٧	٢٣.٣٪
	المجموع	٧١٦	١٠٠٪

يتبين مِن الجدولِ (٨) أنَّ من اهم الصعوبات التي تواجه جهود رفع الوعي السيبراني في العراق هي الـ(قوانين ضعيفة) والتي أجيب بها بنسبة (٣٩.٦٪) إذ حصلت هذه الفئة على المرتبة الأولى، أما في المرتبة الثانية حصلت فئة (ضعف الوعي العام بأهمية الأمن السيبراني) على نسبة (٣٥.٩٪)، أما المرتبة الثالثة فقد جاءت فئة (نقص الموارد المالية والبشرية) وبنسبة (٣١٪)، وفي المرتبة الرابعة جاءت فئة (عدم وجود برامج تعليمية كافية حول الأمن السيبراني) وبنسبة (٢٥.٩٪)، أما (صعوبة الوصول إلى المعلومات) فقد جاءت بالمرتبة الأخيرة وبنسبة (٢٣.٣٪) من عينة البحث. مما يعني أن القوانين الضعيفة تُعد أبرز الصعوبات التي تواجه رفع الوعي السيبراني في العراق إذ إن غياب تشريعات فعّالة يعيق تطوير آليات حماية الأفراد والمؤسسات من التهديدات السيبرانية.

٨- جدول (٩) يبين مصادر رفع الوعي بمخاطر استخدام الإنترنت التي يقترحها المبحوثين

ت	مصادر الوعي	ت	%
١.	تشديد التشريعات والعقوبات	٣١٧	٢٩.٣٪
٢.	حملات توعية إعلامية	٢١٧	٢٠٪
٣.	برامج تعليمية في المدارس	٢١٢	١٩.٥٪
٤.	الدعم تقني وتحسين الأمان	١٢٢	١١.٢٪

.٥	ورش عمل وندوات توعية	١٠٨	٩.٩٪
.٦	تعاون مع القطاع الخاص	١٠٦	٩.٨٪
	المجموع	١٠٨٢	١٠٠٪

من الجدول (٩) يتبين أن استخدام (تشديد التشريعات والعقوبات) يتصدر قائمة مصادر رفع الوعي حول مخاطر استخدام الإنترنت، إذ حصل على نسبة (٢٩.٣٪) وجاء في المرتبة الأولى، وفي المرتبة الثانية جاءت (حملات توعية الإعلامية) بنسبة (٢٠٪)، وفي المرتبة الثالثة جاءت (برامج تعليمية في المدارس) بنسبة (١٩.٥٪)، أما في المرتبة الرابعة فقد جاء (الدعم التقني وتحسين الأمان) بنسبة (١١.٢٪)، بينما جاءت (ورش عمل وندوات توعية) في المرتبة الخامسة بنسبة (٩.٩٪)، وجاء (التعاون مع القطاع الخاص) في المرتبة الأخيرة بنسبة (٩.٨٪)، وتتصدر "تشديد التشريعات والعقوبات" كأهم مصدر لرفع الوعي حول مخاطر الإنترنت، ما يعكس أهمية التدابير القانونية في الحد من المخاطر السيبرانية، بينما تراجعت مصادر مثل ورش العمل والتعاون مع القطاع الخاص لأدنى مستوى مما يشير إلى أن الجهود القانونية والإعلامية تعتبر أكثر تأثيرًا في تعزيز الوعي لدى الأفراد، وتظهر النتائج أن "تشديد التشريعات والعقوبات" يُعتبر المصدر الأكثر فعالية لرفع الوعي حول مخاطر الإنترنت، مما يعكس دور القوانين في تقليص المخاطر السيبرانية. في المقابل، تراجعت أهمية ورش العمل والتعاون مع القطاع الخاص، ما يشير إلى أن التدابير القانونية والإعلامية تحظى بأولوية أكبر في تعزيز الوعي لدى الأفراد.

٩- جدول (١٠) يظهر تصرف المبحوثين للوقاية من تهديد سيبراني على حساباتهم في وسائل التواصل الاجتماعي

ت	سلوك الوقاية	ت	%
.١	تنبيه الأصدقاء والمتابعين	٢٦١	١٧.٩٪
.٢	تفعيل التحقق الثنائي للدخول	٢٠٩	١٤.٣٪
.٣	أغلاق الحساب	١٩١	١٣.١٪
.٤	مراجعة الأنشطة في الحساب	١٩٠	١٣٪
.٥	استشارة خبير أمان سيبراني	١٦٢	١١.١٪

٦.	استخدام برامج مكافحة الفيروسات	١٢٢	٨.٣٪
٧.	تحديث برامج الحماية والتطبيقات	١١٥	٧.٩٪
٨.	إبلاغ مزود الخدمة	١٠٣	٧٪
٩.	احتفاظ بنسخة احتياطية للبيانات	١٠١	٦.٩٪
	المجموع	١٤٥١	١٠٠٪

يتوضح مِن الجدولِ (١٠) أنَّ (تنبيه الأصدقاء والمتابعين) جاء أولا من إذ تصرف المبحوثين للوقاية من تهديد سيبراني لاحد حساباتهم عبر الإنترنت وذلك بنسبة (١٧.٩٪) من بين عينة البحث، أما (تفعيل التحقق الثنائي للدخول) فقد جاء ثانيا وبنسبة (١٤.٣٪)، وثالثا جاء (إغلاق الحساب) بنسبة (١٣.١٪) وهو قريب جدا من المرتبة الرابعة التي جاءت فيها فئة (مراجعة الأنشطة في الحساب) بنسبة (١٣٪) أما خامسا فجاء بديل (استشارة خبير أمان سيبراني) بنسبة مئوية قدرها (١١.١٪)، يليه بديل (استخدام برامج مكافحة الفيروسات) بنسبة مئوية بلغت (٨.٣٪)، أما بديل (تحديث برامج الحماية والتطبيقات) جاء سابعا بنسبة مئوية (٧.٩٪)، ومن ثم بديل (إبلاغ مزود الخدمة) الذي جاء ثامنا بنسبة مئوية قدرها (٧٪)، أما في المرتبة الأخيرة جاء بديل (احتفاظ بنسخة احتياطية للبيانات) بنسبة مئوية بلغت (٦.٩٪).

١٠- جدول (١١) يبين مدى مشاركة المبحوثين لمعلومات التوعية بالأمن السيبراني مع الأصدقاء في المواقع

ت	مدى المشاركة	ت	%
١.	أشارك إذا طُلِبَ مني	١٤٨	٣٧٪
٢.	أشارك بشكل منتظم	١١٨	٢٩.٥٪
٣.	أشارك بناءً على الحاجة	١٠٢	٢٥.٥٪
٤.	لا أشارك	٣٢	٨٪
	المجموع	٤٠٠	١٠٠٪

من الجدول (١١) يبدو أن عينة البحث تشارك المعلومات التوعوية بشأن الأمن السيبراني مع الأهل أو الأصدقاء في حال طُلِبَ منهم ذلك فبديل "أشارك اذا طلب مني" حصل على المرتبة الأولى بنسبة (٣٧٪)، فيما

جاءت "أشارك بشكل منتظم" في المرتبة الثانية بنسبة (٢٩.٥٪)، أما في المرتبة الثالثة فقد جاء "أشارك بناءً على الحاجة" بنسبة (٢٥.٥٪)، بينما جاء بديل "لا أشارك" في المرتبة الأخيرة بنسبة (٨٪).

١١- جدول(١٢) يظهر سلوك المبحوثين تجاه تهديد سيبراني تعرض له شخص ما على وسائل التواصل الاجتماعي

ت	التصرف عند التهديد	ت	%
١.	أدلي بشهادتي على الحادثة	١٩٩	٢٠.٩٪
٢.	أبلغ الجهات الأمنية إذا كان التهديد خطيرًا	١٩٣	٢٠.٢٪
٣.	أنصحه بتغيير كلمات المرور وتعزيز الأمان	١٦١	١٦.٩٪
٤.	أقدم المساعدة بشكل فوري	١٥٠	١٥.٧٪
٥.	أشاركه تجارب شخصية مماثلة	١٠٢	١٠.٨٪
٦.	أشاركه معلومات عن الأمن السيبراني	٩٧	١٠.١٪
٧.	لا أتدخل	٥١	٥.٣٪
	المجموع	٩٥٣	١٠٠٪

من الجدول (١٢) يظهر أن المشاركين يتبعون سلوكًا معينًا عند رؤية شخص يتعرض لتهديد سيبراني إذ يُفضل الإبلاغ عن الحادثة بنسبة (٢٠.٩٪) مما جعله يحتل المرتبة الأولى، وفي المرتبة الثانية يأتي "الإبلاغ عن الحادثة للجهات الأمنية إذا كان التهديد خطيرًا" بنسبة (٢٠.٢٪)، بينما جاء "تقديم النصائح للشخص المتعرض عن تغيير كلمات المرور وتعزيز الأمان" في المرتبة الثالثة بنسبة (١٦.٩٪)، أما "تقديم المساعدة الفورية" فقد جاء في المرتبة الرابعة بنسبة (١٥.٧٪)، وفي المرتبة الخامسة جاءت "مشاركة تجارب شخصية مماثلة" بنسبة (١٠.٨٪)، وفي المرتبة السادسة جاء "مشاركة معلومات حول الأمن السيبراني" بنسبة (١٠.١٪). وأخيراً جاء "عدم التدخل" بنسبة (٥.٣٪).

١٢- يُظهر جدول (١٣) تقييم المشاركين لفاعلية حملات التوعية السيبرانية في تعزيز السلوك الآمن على الإنترنت

ت	مستوى الفاعلية	ت	%
١.	فعّالة إلى حد ما ورفعت وعيي	١٤٨	٣٧٪

.٢	ضعيفة التأثير ولم تغير سلوكي	١٠٨	٪٢٧
.٣	فعّالة جداً وساهمت في تغيير سلوكي	٨٦	٪٢١.٥
.٤	لم أتعرض لأي توعية سيبرانية	٥٨	٪١٥.٥
المجموع		٤٠٠	٪١٠٠

يُظهر جدول (١٣) أن فاعلية التوعية السيبرانية تتفاوت بين المشاركين إذ أفاد (٣٧٪) من المبحوثين بأن التوعية كانت "فعّالة إلى حد ما" وساهمت في رفع وعيهم، فيما أكد (٢١.٥٪) أنها كانت "فعّالة جداً" وأدت إلى تغيير سلوكهم الرقمي ما يدل على وجود تأثير إيجابي نسبي للتوعية، بينما أفاد (٢٧٪) من المبحوثين بأنها ضعيفة التأثير ولم تؤثر على سلوكهم، وصرّح (١٤.٥٪) أنهم لم يتعرضوا لأي حملات توعوية مما يكشف عن فجوة في وصول هذه الحملات إلى جميع شرائح المستخدمين.

❖ نتائج البحث:

١- أنَّ (٤٥.٨٪) من المبحوثين لديهم "بعض الفهم" إزاء موضوع الأمن السيبراني ما يشير إلى إدراك متوسط للتهديدات الإلكترونية والمخاطر المرتبطة بها.

٢- أنَّ "نشر المعلومات المضللة" جاء في المرتبة الأولى بنسبة (٣٤.٨٪) ضمن أنواع التهديدات السيبرانية التي تعرفها عينة البحث

٣- تُعد "إثارة الاضطرابات الاجتماعية أو السياسية" أبرز المخاطر الإرهابية الناجمة عن التهديدات السيبرانية بنسبة (٣٢.٢٪).

٤- أنَّ "وسائل الإعلام" شكّلت المصدر الأول للمعلومات المتعلقة بتقنيات الأمن السيبراني لدى المبحوثين بنسبة (٣٦.٢٪).

٥- أظهرت النتائج أنَّ معرفة عينة البحث بتقنيات الأمن السيبراني عبر المواقع تُعد "متوسطة" وبنسبة بلغت (٦٩.٥٪).

٦- أنَّ "عدم فتح المرفقات من مصادر غير معروفة" جاء بالمرتبة الأولى من بين تقنيات الأمان المستخدمة من قبل المبحوثين للحماية من المخاطر السيبرانية بنسبة (٢٨.٨٪).

٧- أنَّ "ضعف القوانين" جاء كأهم التحديات التي تعيق رفع الوعي السيبراني عبر مواقع التواصل الاجتماعي وبنسبة (٣٩.٦٪).

٨- أنَّ "تشديد التشريعات والعقوبات" يُعد المصدر الأهم لرفع الوعي بمخاطر استخدام الإنترنت حسب رأي المبحوثين بنسبة (٢٩.٣٪).

٩- أنَّ "تنبيه الأصدقاء والمتابعين" جاء في مقدمة تصرفات المبحوثين للوقاية من تهديد سيبراني على حساباتهم بنسبة (١٧.٩٪).

١٠- أظهرت النتائج أنَّ أغلب المبحوثين يلجؤون إلى "الإدلاء بشهاداتهم على الحادثة" عند تعرض شخص ما لتهديد سيبراني وبنسبة (٢٠.٩٪).

١١- أنَّ مشاركة المبحوثين لمعلومات التوعية بالأمن السيبراني تكون غالبًا "إذا طُلب منهم" بنسبة (٣٧٪).

١٢- أنَّ فاعلية التوعية السيبرانية لدى المبحوثين كانت فعّالة إلى حد ما ورفعت وعيهم وبنسبة (٣٧٪).

❖ التوصيات:

١. تنفيذ حملات توعية إعلامية مستمرة لتعريف الجمهور بمخاطر التهديدات السيبرانية وأساليب الوقاية منها.
٢. إدراج برامج تعليمية في المدارس والجامعات لتعزيز الوعي بالأمن السيبراني وتطوير مهاراتهم.
٣. تعزيز التعاون بين الجهات الحكومية والخاصة لتبادل الخبرات في مواجهة الهجمات السيبرانية.
٤. تحديث التشريعات الخاصة بالجرائم السيبرانية وتشديد العقوبات بما يواكب تطورات التهديدات الرقمية.
٥. تشجيع الأفراد على استخدام أدوات الأمان الرقمي مثل كلمات المرور القوية، وتفعيل التحقق الثنائي.

المراجع

Alqahtani, M. A. (2022, March). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences, Vol 12*, pp. 2-21.

Argomaniz, J., & Lynch, O. (2015). *International Perspectives on Terrorist Victimisation An Interdisciplinary Approach.* London: Palgrave Macmillan.

Bennet, A., & Schafer, S. B. (2022). *Handbook of Research on Global Media's Preternatural Influence on Global Technological Singularity, Culture, and Government.* USA: IGI.

Dienstmann, G. (2021). *Mindful Self-Discipline.* United States: LiveAndDare Publications.

Johnson, T. (2005). *Forensic Computer Crime Investigation.* USA: Taylor & Francis.

Krishnamurthy, S. (2005). *Contemporary Research in E-marketing.* London: Idea Group Pu.

Ktoridou, D., Doukanari, E., & Eteokleous, N. (2020). *Fostering Meaningful Learning Experiences Through Student Engagement.* USA: IGI Global.

Nehme, C. (2023). *Tech Horizons (Navigating the Latest Frontiers in Innovation).* Charles Nehme.

Sukhostat, L., & Popov, O. (2022). *Cybersecurity for Critical Infrastructure Protection Via Reflection of Industrial Control Systems.* London: IOS Press.

Tashi, I., & Ghernaouti-Helie, S. (2011). *Information Security Evaluation A Holistic Approach from a Business Perspective.* USA: CRC Press.

Watters , P. (2023). *Cybercrime and Cybersecurity.* USA: CRC Press.

Ziemba, E., & Wątróbski, J. (2024). *Adoption of Emerging Information and Communication Technology for Sustainability.* USA: CRC Press.

Zwilling, M., Klien, G., Lesjak, D., & Basım, N. H. (2022, January). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems, Vol 1*, pp. 1-17.

احمد طاهر مسعود. (٢٠١١). *المدخل إلى علم الإجتماع العام*. الأردن: دار جليس الزمان للنشر و التوزيع.

أحمد عنتر. (٤ ديسمبر, ٢٠٢٣). *تقنيات الأمن السيبراني والتحديات المستقبلية*. تاريخ الاسترداد ٢٦ ديسمبر, ٢٠٢٣، من موقع الجزيرة: https://n9.cl/j9a20

أريج مواسي. (٢ اكتوبر, ٢٠١٦). *تقنيات الواقع المعزز والواقع الافتراضي*. تاريخ الاسترداد ١٢ ديسمبر, ٢٠٢٣، من معهد الجزيرة للإعلام: https://institute.aljazeera.net/ar/ajr/article/231

الصادق رابح. (٢٠٠٧). الإنترنت كفضاء لتشكُلْ الذات. *المجلة المصرية لبحوث الرأي العام، المجلد الثامن*(العدد الثاني).

جمال محمد احمد. (٢٠١٥). *الإعلام السياسي*. الاردن: دار غيداء للنشر والتوزيع.

حمزة السيد حمزة خليل. (٢٠١٢). استخدام الشباب مواقع الشبكات الاجتماعية لإطلاق ثورة ٢٥ يناير ٢٠١١ المصرية والإشباعات المتحققة منها / (رسالة ماجستير غير منشورة). كلية التربية النوعية: جامعة طنطا.

رغدة البهي. (تشرين الاول, ٢٠١٩). الوكالة السيبرانية عوامل النشأة وأنماط الفواعل اتجاهات نظرية. *مجلة السياسة الدولية*.

عبد الأمير الفيصل. (٢٠١٤). *دراسات في الإعلام الإلكتروني*. مصر: دار الكتاب الجامعي.

غريب حكيم. (كانون الاول, ٢٠١٨). الارهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب مواجهتها،. *المجلة الجزائرية للدراسات السياسية*، عدد ٢ .

فارس العمارات، و ابراهيم محمد الحمامصة. (٢٠٢٢). *الامن السيبراني (المفهوم وتحديات العصر)*. الأردن: دار الخليج للنشر والتوزيع.

فراس عقيل الدويري . (٢٠٢٣). *البيانات الضخمة ودورها في الحد من الجرائم الإلكترونية في ظل إستراتيجية الأمن السيبراني*. الأردن: دار الخليج للنشر والتوزيع.

للدراسات والبحوث مركز الحضارة. (٢٠٢٢). *السيبرانية.. واقع وتحولات*. القاهرة: مركز الحضارة للدراسات والبحوث.

مدين عمران محمود التميمي. (٢٠٢٤). العوامل المؤثرة في عمل المراسل الحربي بالقنوات الفضائية العراقية. *مجلة آداب المستنصرية، ٤٨(١٠٥ جزء١)*، الصفحات ٩٢٠-٩٥٣.

منى الاشقر جبور. (٢٠١٨). *السيبرانية هاجس العصر*. القاهرة: المركز العربي للبحوث القانونية.

منى تركي شمخي. (٢٠٢٣). أخلاقيات التواصل في العصر الرقمي وانعكاسها على تواصل الجمهور. *مجلة آداب المستنصرية، ٤٧(١٠٤)*، الصفحات ٦٨٩-٧١٦.

نايف احمد الشمري، و عمر عباس العبيدي. (تشرين الثاني, ٢٠١٩). دور مجلس حقوق الانسان في مكافحة التطرف الديني. *مجلة قضايا التطرف والجماعات المسلحة*.

نديم منصوري. (٢٠١٤). *سيسيولوجيا الإنترنت*. بيروت: منتدى المعارف.

هدى عباس قنبر، و أحلام جبار قاسم محمد. (٢٠٢٣). أهمية استخدام موقع التواصل الاجتماعي (LinkedIn) بين الباحثين والمتخصصين في مجال المعلومات وتقنيات المعرفة. *مجلة آداب المستنصرية، ٤٧(١٠٣)*، الصفحات ٢٨٧-٣١٠.