تعزيز الوعي بالخصوصية الرقمية في عصر الشبكات الاجتماعية

(دراسة ميدانية على طلاب كلية الحاسبات وتقنية المعلومات بجامعة حضرموت)

Enhancing Awareness of Digital Privacy in the Social Networks Era
An Empirical Study on Students of the Faculty of Computers and Information Technology at Hadhramout University

د. نزيهة محمد علي العيدروس
أستاذ مشارك، قسم معلم مجال رياضيات/حاسوب
كلية التربية، جامعة حضرموت

الملخص:

في ظل التطور المتسارع للتكنولوجيا واعتمادنا المتزايد على وسائل التواصل الاجتماعي، أصبحت الخصوصية الرقمية قضية ملحة تتطلب اهتمامًا خاصًا. تهدف هذه الدراسة إلى تقييم مستوى وعي طلاب كلية الحاسبات وتقنية المعلومات بجامعة حضرموت بأهمية حماية خصوصيتهم الرقمية على هذه المنصات. إذ تم استخدام المنهج الوصفي المسحي كطريقة لجمع المعلومات؛ وذلك لملاءمته لأهداف الدراسة الحالية، واستخدمت الأستبانة كأداة لجمع البيانات. وقد خلصت هذه الدراسة إلى أن مستوى الوعي بالخصوصية الرقمية لدى غالبية الطلاب منخفض نسبيًا. كما أظهرت نتائج الاستبانة أن الطلاب يمارسون سلوكيات غير آمنة على شبكات التواصل الاجتماعي، مثل مشاركة معلومات شخصية حساسة، وقبول طلبات صداقة من غرباء. زيادة على ذلك، هناك فجوة معرفية كبيرة في مجال الأدوات التقنية لحماية الخصوصية. تشكل نتائج هذه الدراسة نقطة انطلاق مهمة لتطوير برامج توعية شاملة تستهدف طلاب الجامعات، وتسهم في بناء مجتمع رقمي أكثر أمانًا ووعيًا.

الكلمات المفتاحية:
- الخصوصية الرقمية
- شبكات التواصل الاجتماعي
- كلية الحاسبات وتقنية المعلومات
- حماية البيانات

ABSTRACT:

With the rapid advancement of technology and our increasing reliance on social media, digital privacy has become a pressing issue demanding special attention. This study aimed to assess the level of awareness among students at the Faculty of Computers and Information Technology at Hadhramout University regarding the importance of protecting their digital privacy on these platforms. A descriptive survey approach was employed to collect data, aligning with the study's objectives. A questionnaire was used as a data collection tool. The findings revealed that the level of awareness of digital privacy among most students is relatively low. The survey results also indicated that students engage in risky behaviors on social media, such as sharing sensitive personal information and accepting friend requests from strangers. Moreover, there is a significant knowledge gap regarding technical tools for privacy protection. The results of this study serve as a crucial starting point for developing comprehensive awareness programs targeting university students and contributing to the building of a safer and more informed digital society

Key Words
- **Digital Privacy**
- **Social Networks**
- **Faculty of Computers and Information Technology**
- **Data Security**

مقدّمة:

مع التطور التكنولوجي الهائل في الآونة الأخيرة، وانتشار استخدام الإنترنت، ظهرت عدد من المواقع الإلكترونية والمدونات الشخصية وشبكات المحادثة، التي سهلت طرق التواصل بين مختلف شرائح المجتمع، كما ظهر مايعرف بشبكات التواصل الاجتماعي، مثل الفيس بوك، الواتس اب، السناب شات وغيرها من هذه الشبكات، التي أتاحت طرقًا عدة لمشاركة المعلومات وتبادلها بين المستخدمين، مما أدى إلى انتشارها الواسع على شبكة الإنترنت، وزاد الإقبال عليها من قبل متصفحي الإنترنت من أنحاء العالم كافة. وبالرغم من الانتقادات الشديدة التي تتعرض لها هذه الشبكات من تأثيرها السلبي والمباشر في المجتمع الأسري، والإسهام في انفراط عقده وانهياره، بالإضافة إلى ضياع خصوصية المستخدم على تلك الشبكات، فإن هناك من يرى أنَّ فيها وسيلة مهمة للتواصل بين المجتمعات، وتقريب المفاهيم والرؤى مع الآخرين، والاطلاع والتعرف على ثقافات الشعوب المختلفة، إضافة لدورها الفاعل والمتميز كوسيلة اتصال ناجعة في الهبات والانتفاضات الجماهيرية.

ولعل أبرز المشكلات التي صاحبت ظهور مواقع التواصل الاجتماعي، "الخصوصية" وكيفية حماية المستخدم لبياناته من الوصول غير المصرح به.

تهدف هذه الدراسة إلى تقييم مستوى الوعي بالخصوصية الرقمية على شبكات التواصل الاجتماعي لدى طلاب جامعة حضرموت، إذ تم اعتماد طلاب كلية الحاسبات وتقنية المعلومات كنموذج لدراسة الحالة.

مشكلة الدراسة:

يواجه الطلاب عددًا من التحديات في الحفاظ على الخصوصية والأمان عبر الإنترنت خصوصًا في أثناء استخدام منصات التواصل الاجتماعي، تشمل هذه التحديات عدم الوعي بمخاطر الخصوصية، ومشاركة المعلومات الحساسة، وإمكانية تسرب المعلومات الشخصية. بالإضافة إلى ذلك، فإن الانتشار السريع للمعلومات على وسائل التواصل الاجتماعي يجعل من الجذاب للمهاجمين استغلال المحتوى المشترك، وخاصة الصور الشخصية ومقاطع الفيديو والتسجيلات الصوتية، مما يشكل تهديدًا كبيرًا لخصوصية المستخدمين. للتخفيف من هذه التهديدات، ضرورة دراية الطلاب بالمخاطر المرتبطة بالاستخدام المجاني لوسائل التواصل الاجتماعي، وأن يتخذوا تدابير لحماية خصوصيتهم وأمنهم عبر الإنترنت.

تتمثل مشكلة هذه الدراسة في الأسئلة الآتية:

1- ما مدى الوعي بالخصوصية الرقمية لدى الطلاب.

2- ما هي سلوكيات الطلاب عند استخدام شبكات التواصل الاجتماعي .

3- ما مدى معرفة الطلاب بطرق حماية خصوصيتهم على شبكات التواصل الاجتماعي.

4- ما دور الجامعة والكلية في تنمية الوعي بالخصوصية الرقمية لدى الطلاب.

أهمية الدراسة:

تكمن أهمية هذه الدراسة في تقييم مستوى الوعي بالخصوصية الرقمية على شبكات التواصل الاجتماعي لدى طلاب كلية الحاسبات وتقنية المعلومات بجامعة حضرموت. إذ ستبحث الدراسة في معرفتهم وفهمهم لقضايا الخصوصية الرقمية على منصات التواصل الاجتماعي. وستستكشف الدراسة أيضًا سلوك الطلاب وممارساتهم المتعلقة بإعدادات الخصوصية على وسائل التواصل الاجتماعي، بالإضافة إلى مواقفهم تجاه حماية معلوماتهم الشخصية عبر الإنترنت، والخطوات التي يتخذونها لضمان خصوصيتهم. زيادة على ذلك، ستحلل الدراسة أي تحديات أو مخاوف قد تكون لدى الطلاب فيما يتعلق بمعلوماتهم الرقمية. إضافة الى محاولة تحديد المجالات المحتملة لتعزيز الوعي بالخصوصية الرقمية من قبل الجامعة والكلية كمؤسسات تعليمية .

نظرًا للاستخدام المتزايد من قبل الطلاب على هذه الشبكات، ولأهمية تعزيز الوعي بالخصوصية الرقمية لدى المجتمع، إضافة الى شحة مثل هذه الدراسات في مجتمعنا، فإن الباحثة تأمل أن تفتح هذه الدراسة باباً واسعاً امام الدارسين والباحثين وصناع القرار للخوض في غمار شبكات التواصل الاجتماعي وعلاقتها بالخصوصية، واستخلاص نتائج جديدة قادرة على الإسهام في تعزيز الوعي بالخصوصية الرقمية لدى المجتمع.

أهداف الدراسة:

يمكن تلخيص أهداف الدراسة في النقاط الآتية :

1- تقييم مستوى الوعي بالخصوصية الرقمية لدى طلاب كلية الحاسبات وتقنية المعلومات بجامعة حضرموت.

2- تحليل سلوكيات استخدام شبكات التواصل الاجتماعي لدى طلاب كلية الحاسبات وتقنية المعلومات بجامعة حضرموت.

3- تقييم مدى معرفة الطلاب بطرق حماية خصوصيتهم على شبكات التواصل الاجتماعي.

4- تقييم دور الجامعة والكلية في تنمية الوعي بالخصوصية الرقمية لدى الطلاب.

5- تقديم توصيات لتعزيز الوعي بالخصوصية الرقمية لدى الطلاب .

حدود الدراسة:

الحدود الزمانية: طبقت الدراسة في نهاية الفصل الدراسي الثاني للعام الجامعي 2023- 2024 م.

الحدود المكانية: تنحصر الحدود المكانية للدراسة داخل كلية الحاسبات وتقنية المعلومات – جامعة حضرموت المكلا، اليمن.

الحدود البشرية: تم إجراء الدراسة على عينة عشوائية من طلاب كلية الحاسبات وتقنية المعلومات بجامعة حضرموت يتراوح عددهم 157 طالباً وطالبة.

الإطار النظري والدراسات السابقة:

الخصوصية:

من وجهة نظر روجر كلارك (كلارك، 2008)، الاستشاري والخبير في خصوصية البيانات والأعمال الإلكترونية، فقد عرف الخصوصية بأنها "قدرة الأشخاص على المحافظة على مساحتهم الشخصية في مأمن من التدخل من قِبل منشآت أو أشخاص آخرين"، وقام بتحديد مستويات من الخصوصية وهي (نوي، 2023) :

1- خصوصية الشخص (Privacy of The Person):

والمعنية بسلامة الفرد في جسده، مثل قضايا التطعيم أو نقل الدم دون الحصول على موافقة الشخص المعني، أو الإجبار على تقديم عينات من سوائل الجسد أو أنسجته.

2- خصوصية السلوك الشخصي (Privacy of Personal Behavior)

ويتصل ذلك بكل الجوانب السلوكية، وبشكل خاص الأمور الحساسة، مثل الأنشطة السياسية والممارسات الدينية، سواءً في الحياء الخاصة أو الأماكن العامة، وقد يشار إليه "بوسائل الخصوصية".

3- خصوصية الاتصالات الشخصية (Privacy of Personal Communications)

وهي مطالبة الأشخاص بالقدرة على الاتصال فيما بينهم دون المراقبة الروتينية من قِبل أشخاص آخرين أو منظمات.

4- خصوصية البيانات الشخصية (Privacy of Personal Data)

وهي مطالبة الأشخاص بأن لا تكون البيانات الخاصة عنهم متوافرة تلقائياً لغيرهم من الأفراد أو المنظمات، حتى في حالة أن تكون البيانات مملوكة من طرف آخر، فلهم القدرة على ممارسة قدر كبير

من السيطرة أو التحكم بتلك البيانات وطريقة استخدامها. وهذا ما يعرف "بخصوصية المعلومات أو خصوصية البيانات". وعرّفها روجر "بأنها رغبة الشخص بالتحكم، أو على الأقل التأثير بشكل كبير في كيفية التعامل مع بياناته الشخصية".

تعد الخصوصية من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي بصفته الإنسانية كأصل عام، فهي تعد أساس بنيان كل مجتمع سليم. لذا تحرص المجتمعات خاصة الديمقراطية منها على كفالة هذا الحق، وتعده حقاً مستقلاً قائماً بذاته، ولاتكتفي بسن القوانين لحمايته، بل تسعى إلى ترسيخه في الأذهان، وذلك بغرس القيم النبيلة التي تؤدي دوراً كبيراً وفعالاً في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم.

الخصوصية الرقمية:

مع الثورة الرقمية الهائلة التي شهدها العالم في العقود الأخيرة في مجال التكنولوجيا والشبكات ظهر مصطلح "الخصوصية الرقمية"؛ وذلك نظراً للاعتماد المتزايد على التقنيات الرقمية في جميع جوانب الحياة، فقد أصبح الحفاظ على خصوصية المعلومات الشخصية تحديًا جديدًا ومعقدًا.

الخصوصية الرقمية تعد من أهم حقوق الإنسان في العصر الحالي، وتشمل كل ما يتعلق بالأفراد والمؤسسات في العالم الرقمي (حمود، 2021)، ويمكن تعريفها بأنها "الحق في التحكم في جمع واستخدام وكشف المعلومات الشخصية في البيئة الرقمية. يشمل ذلك الحق في حماية الهوية الرقمية، والبيانات الشخصية، والاتصالات الخاصة من الوصول غير المصرح به أو الاستخدام غير المشروع".

تتمثل أهمية الخصوصية الرقمية في نواحٍ عدة، منها:

- **الحفاظ على الهوية:** إذ تحمي الخصوصية الرقمية الهوية الرقمية للأفراد من الانتحال والاحتيال.
- **تعزيز الثقة:** تسهم في بناء الثقة بين الأفراد والمؤسسات الرقمية.
- **الحفاظ على الحرية:** تتيح للفرد حرية التعبير والتفكير دون خوف من المراقبة.
- **الحفاظ على الأمن:** تساعد الخصوصية الرقمية في حماية الأجهزة والشبكات من الهجمات الإلكترونية.

مع الاستخدام الهائل للانترنت ظهرت عدد من الجهات التي تسهم في خرق الخصوصية، مثل:

1- **مزودي خدمات الإنترنت (ISPs):**

إذ يتم الاحتفاظ بسجلات مفصلة عن المواقع التي يزورها المستخدم ، الملفات التي يقوم برفعها أو تنزيلها، زمن الدخول للشبكة ومكانه، وغيرها من هذه البيانات التي قد يتم بيعها لشركات التسويق أو جهات أخرى لأغراض استهداف الإعلانات.

2- **مواقع الويب والتطبيقات:**

إذ تجمع غالب المواقع والتطبيقات التي يتم استخدامها معلومات شخصية عن المستخدمين مثل العمر، الجنس، الموقع الجغرافي، اهتماماتهم، وغيرها من هذه المعلومات التي قد تهدف إلى تحسين تجربة المستخدم وتخصيص إعلانات معينه له. أيضًا قد تشارك هذه البيانات مع أطراف أخرى، مثل شركات التسويق، أو شركات تحليل البيانات.

3- **شبكات التواصل الاجتماعي:**

تقوم هذه الشبكات بمراقبة نشاط المستخدمين، وتجميع بيانات هائلة عنهم، مثل علاقاتهم، اهتماماتهم، سلوكهم على الإنترنت. ويتم استخدام هذه البيانات لعرض إعلانات مخصصة للمستخدمين.

4- **محركات البحث:**

هي أيضاً تقوم بتسجيل كل مايبحث عنه المستخدم على الإنترنت، وبالتالي يتم تكوين صورة واضحة عن اهتماماته، وقد تستخدم هذه البيانات لتخصيص نتائج البحث التي تراها.

5- **شركات الإعلانات:**

تقوم هذه الشركات بتجميع البيانات من بعض المصادر، مثل مواقع الويب، أو التطبيقات؛ لتكوين ملفات تعريف مفصَّلة عن المستخدمين. وبالتالي تستخدم هذه الملفات لتقديم إعلانات مخصصة للمستخدمين في جميع أنحاء الويب.

6- **الحكومات:**

قد تقوم الحكومات بمراقبة الاتصالات الإلكترونية لأسباب أمنية أو سياسية. كما تستطيع أيضاً طلب هذه البيانات من شركات التكنولوجيا للتحقيق في الجرائم أو لأسباب أمنية أخرى.

7- **البرامج الضارة:**

إذ تستطيع هذه البرامج سرقة المعلومات المهمة والحساسة، مثل كلمات المرور، وأرقام بطاقات الائتمان.

شبكات التواصل الاجتماعي:

أصبحت شبكات التواصل الاجتماعي (Social Media Networks) جزءًا لا يتجزأ من حياتنا الرقمية؛ إذ تشكل الطريقة التي نتواصل بها ونتشارك المعلومات، كما أثرت في طريقة التفاعل والعلاقات بين مستخدمي الإنترنت.

تعرّف شبكات التواصل الاجتماعي بأنها منصات رقمية تتيح للأفراد التواصل والتفاعل بعضهم مع بعض عبر الإنترنت. إذ تتيح هذه الشبكات للمستخدمين بمشاركة المعلومات والصور ومقاطع الفيديو والأفكار مع أصدقائهم وعائلاتهم وزملائهم، وبناء مجتمعات افتراضية عن اهتماماتهم المشتركة.

ظهرت الأفكار الأولى لشبكات التواصل الاجتماعي في التسعينيات، مع مواقع مثل SixDegrees وFriendster. غير أن شهرتها ظهرت مع ظهور مواقع مثل MySpace وFacebook، إذ قدمت واجهات مستخدم سهلة الاستخدام، وميزات تفاعلية جذابة، وتطورت هذه الشبكات بشكل كبير جداً؛ إذ ظهر عدد من المنصات المتخصصة في مجالات معينة.

أنواع شبكات التواصل الاجتماعي:

تصنف شبكات التواصل الاجتماعي إلى الفئات الآتية :

1- **شبكات اجتماعية عامة:** مثل Facebook وTwitter، حيث يمكن لأي شخص الانضمام إليها والتفاعل مع بقية المستخدمين.

2- **شبكات اجتماعية مهنية:** مثل LinkedIn، مصممة للتواصل وبناء علاقات مهنية بين المحترفين.

3- **شبكات اجتماعية لمشاركة الصور والفيديوهات:** مثل Instagram وYouTube، تركز على المحتوى المرئي.

4- **شبكات اجتماعية للمجموعات الصغيرة:** مثل WhatsApp وTelegram، تتيح التواصل ضمن مجموعات محددة.

فوائد شبكات التواصل الاجتماعي:

لشبكات التواصل الاجتماعي جملة من المزايا والفوائد، منها:

1- أنها تسهل التواصل مع الأصدقاء والعائلة، وتتيح للمستخدم بناء علاقات جديدة.

2- أنها تتيح للمستخدم مشاركة الأخبار والأحداث والآراء مع الآخرين.

3- أنه يمكن للأفراد والشركات استخدامها للتسويق لمنتجاتهم وخدماتهم.

4- أنها توفر عددًا من المنصات محتوى تعليمي مجاني.

5- أنها تساعد في نشر الوعي بالقضايا الاجتماعية والسياسية.

عيوب شبكات التواصل الاجتماعي:

رغم المميزات المتعددة لشبكات التواصل الاجتماعي لكن لها عيوب وسلبيات كثيرة أيضاً، مثل :

1- أنها قد تؤدي إلى إدمان الإنترنت وإضاعة الوقت.

2- أنها قد تعرض المستخدمين لانتهاكات الخصوصية، وتسريب البيانات الشخصية.

3- أنها تسهل انتشار الأخبار الكاذبة والشائعات.

4- أنها تؤثر سلبياً في الصحة النفسية، حيث قد يؤدي إلى الشعور بالوحدة والاكتئاب والمقارنة الاجتماعية.

5- أنها تلهي المستخدم، وبالتالي التأثير في تركيزه وإنتاجيته.

الخصوصية على مواقع الشبكات الاجتماعية:

تشمل الخصوصية على مواقع الشبكات الاجتماعية حقوق المستخدمين في التحكم في معلوماتهم الشخصية، بما في ذلك متى وكيف وإلى أي مدى تتم مشاركتها مع الآخرين. يتضمن هذا الحق الوصول إلى معلوماتهم وتصحيحها وحذفها إذا لزم الأمر. تسهل طبيعة هذه المنصات التفاعل بين الأصدقاء والمعارف، مما قد يعقد إدارة الخصوصية. إذ تشمل العناصر الرئيسة للخصوصية حماية البيانات الشخصية المتعلقة بالحياة الأسرية والصحة والوضع المالي والمعتقدات الشخصية، من جملة أمور أخرى. وبالتالي، فإن الخصوصية لا تتعلق فقط بأمن البيانات، ولكن أيضًا باستقلالية الأفراد في إدارة معلوماتهم الشخصية في سياق اجتماعي. (القحطاني، 2015)

الدراسات السابقة:

ناقش عدد من الدراسات السابقة موضوع الخصوصية الرقمية وارتباطها بشبكات التواصل الاجتماعي، من أمثلة هذه الدراسات:

- (قدوري، 2024):

هدفت هذه الدراسة إلى استكشاف مستوى إدراك الخصوصية وأهميتها لمستخدمي مواقع شبكات التواصل الاجتماعي في الوطن العربي، وقد أظهرت النتائج، أن مفهوم الخصوصية للمستخدم العربي لموقع الفيسبوك من المفاهيم المعقدة التي يصعب على المستخدم التعبير عنها. كما أن المستخدم العربي رغم إدراكه المنخفض للخصوصية، لكن لديه مستوى اهتمام متوسط بأهميتها. كما بينت الدراسة عدم ثقة المستخدمين في الخصوصية عبر المنصات الاجتماعية، واعتبرت المعايير ضرورية للتحكم في الخصوصية، إضافة إلى أهمية التواصل وحتميته مقابل الخصوصية.

- (الكربي، 2023):

ناقشت هذه الدراسة دور شبكات التواصل الاجتماعي في تحقيق الأمن الرقمي للطالب الإماراتي في دولة الإمارات العربية المتحدة، إذ أكدت الدراسة على ضرورة الاستخدام الفعال للشبكات الاجتماعية لدعم احتياجات الطلاب الأكاديمية ومعالجة التحديات التي تواجههم أثناء التعلم عن بُعد. أيضاً قامت الباحثة بتقديم مبادرة أسمتها "مسابقة الأمن الرقمي في شبكات التواصل الاجتماعي لطلاب الثانوية العامة"؛ لتفعيل استخدام شبكات التواصل الاجتماعي في خدمة الأمن الرقمي للطلاب.

- (Andi وآخرون، 2023):

هدفت هذه الدراسة إلى تحديد وعي مستخدمي وسائل التواصل الاجتماعي بأمن المعلومات والخصوصية، إذ ناقشت التغير الذي حصل في الاتصالات بسبب التقدم في التكنولوجيا، خصوصاً من خلال شبكات التواصل الاجتماعي التي سهلت الوصول الى المعلومات ومشاركتها من قبل عدد من المستخدمين.

كما سلطت الدراسة الضوء على أن عددًا من مستخدمي الإنترنت لايدركون كيف يمكن الكشف عن بياناتهم الشخصية عبر الإنترنت. و قدمت عددًا من التوصيات للحد من هذه المخاطر.

- (Triveni، 2023):

هدفت هذه الدراسة إلى تقييم وعي المستخدمين بتدابير الأمن والخصوصية وفهمهم للمخاطر والثغرات المحتملة على مواقع التواصل الاجتماعي. إذ تم تحليل النتائج لتحديد الاتجاهات والفجوات المعرفية وتصورات المستخدمين مما وفر رؤى واضحة للوضع الحالي لوعي المستخدم. وكانت نتائج هذه الدراسة مفيدة في صياغة الخطط والتوصيات لتحسين تدابير الأمن وتعزيز السلوك المسؤول عبر الإنترنت بين مسؤولي الشبكات الاجتماعية وصناع السياسات والمستخدمين.

- (Albulayhi & Khediri ، 2022):

هدف هذا البحث إلى التحقيق في تحديات الخصوصية والأمان التي يواجهها المستخدمون على منصات التواصل الاجتماعي، واقترح حلولًا محتملة لتعزيز حماية البيانات. وكشفت الدراسة أن المستخدمين غالبًا ما يفتقرون إلى الوعي فيما يتعلق بأهمية حماية معلوماتهم الشخصية، والتي تشمل البيانات الحساسة، مثل التفاصيل المصرفية والاتصالات الخاصة. وقد توصلت الدراسة إلى تحديد الانقسام بين المستخدمين: فبعضهم على استعداد لمشاركة المعلومات الشخصية دون تردد، في حين يكون البعض الآخر أكثر حذرًا، مما يسلط الضوء على الحاجة إلى آليات أمنية قوية لبناء الثقة. بالإضافة إلى ذلك، اكد البحث أن تدابير الخصوصية الحالية على وسائل التواصل الاجتماعي غير كافية، مما يستلزم إصلاحات لتحسين خصوصية المستخدم وأمانه.

- (Padmavathi & Mohanlal، 2021):

هدف هذا البحث إلى تحليل وعي طلاب الجامعات فيما يتعلق بقضايا الأمن والخصوصية المرتبطة باستخدام وسائل التواصل الاجتماعي. وقد أبرز أن عددًا من المستخدمين، وخاصة الطلاب، غالبًا ما يجهلون مخاطر الخصوصية التي تنطوي عليها مشاركة المعلومات الحساسة على هذه المنصات. وقد أشارت النتائج إلى أنه في حين تعمل وسائل التواصل الاجتماعي كأداة اتصال قيمة، يجب على المستخدمين اتخاذ تدابير استباقية لحماية معلوماتهم الشخصية من التهديدات المحتملة. كما أكدت الدراسة على ضرورة أن يفهم الطلاب نقاط ضعفهم، وتنفيذ استراتيجيات لحماية خصوصيتهم.

- (Ali وآخرون، 2019):

هدف هذا البحث إلى استكشاف مخاوف الخصوصية في الشبكات الاجتماعية عبر الإنترنت (OSNs) من منظور المستخدمين، مع تسليط الضوء على الطبيعة المتعددة الأوجه لقضايا الخصوصية والتهديدات المختلفة التي يواجهها المستخدمون. وقد تضمنت النتائج تطوير تصنيف يصنف التهديدات لخصوصية المستخدم، والذي يشمل نقاط الضعف في البنية التحتية والمخاطر الخاصة بالتطبيق والتهديدات المتعلقة بالمستخدم. وفرت الدراسة أيضًا إرشادات الخصوصية للمستخدمين، وحثت على ممارسات المشاركة المسؤولة والوعي بالمخاطر المحتملة المرتبطة باستخدام وسائل التواصل الاجتماعي.

- (Glenn وآخرون، 2019):

هدفت هذه الدراسة إلى دراسة تطور الوعي بالأمان والخصوصية في مجال تقنية المعلومات والإنترنت، وسلطت الضوء على النقص في الوعي الأمني بين المبتكرين. فقد نمت التكنولوجيا وتطبيقاتها في ظل الحد الأدنى من التنظيمات، دون قيود. وعندما ظهر الوعي الأمني التقني بين المهندسين والأشخاص من ذوي المعرفة، ظل المستخدمون العاديون غير مدركين للمخاطر الأمنية التي قد تحدث عند استخدامهم للتطبيقات غير الآمنة. وفي غياب الوعي الاجتماعي الكافي بالآثار المترتبة على الأدوات والأنظمة القائمة على الإنترنت، أصبح المجتمع الشبكي يحتوي على كميات ضخمة من المعلومات، معظمها من غير القدر الكافي من الحماية للأمن والخصوصية. وشددت الدراسة على أهمية وضع الضوابط والتوازنات الاجتماعية لتحسين الوضع الحالي للأمن والخصوصية.

- (صفوري، 2019):

بحثت هذه الدراسة الدوافع وراء انتهاكات الخصوصية بين الشباب الأردني باستخدام منصات التواصل الاجتماعي، مثل Facebook و WhatsApp. وكشفت النتائج الرئيسة أن عددًا من المشاركين يشعرون بأن خصوصيتهم معرضة للخطر، ويرجع ذلك أساسًا إلى النوايا الخبيثة، والافتقار إلى القيم الأخلاقية، والأغراض الترفيهية. كانت الطريقة الأكثر شيوعًا لانتهاك الخصوصية التي تم تحديدها هي إساءة استخدام الصور الشخصية. وقد أكدت الدراسة على الحاجة إلى قوانين أكثر صرامة ضد المخالفين، ودعت إلى تعزيز التعليم الإعلامي لتعزيز الاستخدام المسؤول للإنترنت.

- (المعداوي، 2018):

بحث هذا البحث في حماية خصوصية المستخدم على مواقع الشبكات الاجتماعية، مع التركيز على النصوص القانونية العربية والأوروبية والأحكام القضائية، وخاصة في القضاء الفرنسي. وأكد على أهمية حماية البيانات الشخصية، والتي تشمل معرفات مختلفة، مثل الأسماء، وعناوين البريد الإلكتروني، ومعلومات التسجيل الأخرى. خلصت الدراسة إلى أن البيانات الشخصية مهمة للخصوصية الفردية، وسلطت الضوء على مظاهر انتهاكات الخصوصية في العالم الرقمي. بالإضافة إلى ذلك، أشار هذا البحث إلى التوجيهات الأوروبية ذات الصلة، المتعلقة بحماية البيانات والخصوصية في الاتصالات الإلكترونية .

- (الفيصل وسيد،2017):

هدف هذا البحث إلى دراسة تأثير وسائل التواصل الاجتماعي، وخاصة Facebook، في خصوصية المستخدم، والتحديات الأخلاقية التي تنشأ من مشاركة المعلومات الشخصية. كما سعى إلى تقييم وعي المستخدمين بقضايا الخصوصية وأنواع الانتهاكات التي تحدث داخل هذه المنصات.

وقد كشفت النتائج عن نقص كبير في الوعي بين المستخدمين فيما يتعلق بمخاطر الخصوصية، مع التأكيد على ضرورة تحسين التعليم بشأن حماية البيانات. زيادة على ذلك، سلطت الدراسة الضوء على المعضلات الأخلاقية التي يواجهها كل من المستخدمين والشركات في تحقيق التوازن بين حرية التعبير وحماية البيانات الشخصية.

- (فضيلة، 2017):

تناول البحث ظاهرة عرض الذات على منصات التواصل الاجتماعي بشكل عميق، مُسلطًا الضوء على المخاطر التي تحيط بهذه الظاهرة، مثل انتهاك الخصوصية، والتحرش الإلكتروني، والتلاعب بالمعلومات. كما بحث في تحديات الحفاظ على الخصوصية في بيئة رقمية تزداد شفافية يوماً بعد يوم. وأشار البحث إلى أن المستخدمين يشاركون كميات هائلة من المعلومات الشخصية دون إدراك كامل للمخاطر المترتبة على ذلك. وركز البحث على آليات إدارة الخصوصية التي يتبعها المستخدمون، مع التركيز على تطبيع ظاهرة عرض الذات والمراقبة الذاتية. وخلص البحث إلى أن عرض الذات على منصات التواصل الاجتماعي ظاهرة معقدة، تتطلب من المستخدمين توخي الحذر، واتخاذ إجراءات لحماية خصوصيتهم، وأن هناك حاجة ماسة إلى مزيد من الأبحاث في هذا المجال.

- (أبو حمادة وآخرون، 2014):

هدفت هذه الدراسة إلى قياس الاهتمام بالخصوصية على الشبكات الاجتماعية لدى مستخدميها في قطاع غزة من المرحلة الإعدادية والثانوية، ومعرفة أهم العناصر التي تسهم في عملية انتهاك الخصوصية، وكذلك نقاط الضعف بالاهتمام بالخصوصية. وقد شملت الدراسة خمسة أبعاد لدراسة الخصوصية وهي (التقنية، القانونية، الشرعية، النفسية والاجتماعية) وتناولت أثر هذه الأبعاد في حماية الخصوصية على الشبكات الاجتماعية.

وقد توصلت الدراسة إلى مجموعة من النتائج، منها: أن هناك أثرًا واضحًا في انخفاض الاهتمام بالخصوصية على الشبكات الاجتماعية للفئات المبحوثة قبل عملية التوعية، ولقد طرأ على هذه الفئات تحسن واضح في

الاهتمام بالخصوصية على الشبكات الاجتماعية أثر عملية التوعية، كذلك توصلت الدراسة الى أن عملية التوعية عملية مستمرة، ولذلك لابد أن يكون للحكومة من خلال وزارات التربية والتعليم والثقافة والأوقاف دور في الإرشاد والتوعية وسن القوانين الضرورية لحماية المستخدمين في حال ما تم انتهاك الخصوصية على تلك الشبكات.

منهجية الدراسة وإجراءاتها:

منهجية الدراسة: تم استخدام المنهج الوصفي المسحي كطريقة لجمع المعلومات؛ وذلك لملاءمته لأهداف الدراسة الحالية، واستخدمت الأستبانة كأداة لجمع البيانات.

مجتمع الدراسة: هو عبارة عن جميع مفردات المجتمع الذي طبقت عليه الدراسة، وفي هذا البحث تكون مجتمع الدراسة من جميع الطلاب المقيدين في كلية الحاسبات وتقنية المعلومات، جامعة حضرموت- اليمن، للعام الجامعي 2023-2024 م.

عينة الدراسة: تكونت عينة الدراسة من 157 طالباً وطالبة.

أداة الدراسة:

تم استخدام الاستبانة كأداة لجمع البيانات بشكل منظم ودقيق، وتكونت الأداة من خمسة أقسام رئيسة، هي:

القسم الأول : يشمل المعلومات الشخصية للمشاركين، مثل: الجنس، التخصص، والمستوى الدراسي.

القسم الثاني : هو عبارة عن محور الوعي بالخصوصية الرقمية، واشتمل على عدد من التساؤلات، هي:

- هل تعرف: ما الخصوصية الرقمية؟
- ما مفهومك للخصوصية الرقمية؟
- هل تقرأ سياسات الخصوصية للمواقع والتطبيقات قبل استخدامها؟
- هل تعرف كيفية تغيير إعدادات الخصوصية لحساباتك على شبكات التواصل الاجتماعي؟
- ما أهم المخاطر التي تهدد الخصوصية الرقمية على شبكات التواصل الاجتماعي من وجهة نظرك؟

القسم الثالث: وهو عبارة عن محور سلوكيات استخدام شبكات التواصل الاجتماعي، واشتمل على عدد من التساؤلات هي:

- ما شبكات التواصل الاجتماعي التي تستخدمها بشكل يومي؟

- كم من الوقت تقضيه يوميًّا على شبكات التواصل الاجتماعي؟
- ما هي أهم الأنشطة التي تمارسها على شبكات التواصل الاجتماعي بشكل دائم؟
- ما هي المعلومات الشخصية التي يمكن أن تشاركها على شبكات التواصل الاجتماعي؟

القسم الرابع: محور حماية الخصوصية على شبكات التواصل الاجتماعي، واشتمل على عدد من التساؤلات، هي:

- ما مدى وعيك بمخاطر مشاركة المعلومات الشخصية على شبكات التواصل الاجتماعي؟
- ما الإجراءات التي تتخذها لحماية خصوصيتك على شبكات التواصل الاجتماعي؟
- هل تستخدم كلمات مرور قوية ومختلفة لحساباتك على شبكات التواصل الاجتماعي؟
- هل تُغير إعدادات الخصوصية الخاصة بك على شبكات التواصل الاجتماعي بانتظام؟
- كم مرةً تقوم بتغيير كلمات المرور لحساباتك على شبكات التواصل الاجتماعي؟
- هل تستخدم تقنيات التحقق الثنائي لحساباتك؟
- هل سبق لك أن حضرت أي دورة تدريبية أو ورشة عمل عن الخصوصية الرقمية؟
- هل تشارك بمعلوماتك الشخصية، مثل: رقم الهاتف، أو العنوان، على شبكات التواصل الاجتماعي؟
- هل تعرضت لأي موقف يتعلق بانتهاك الخصوصية على شبكات التواصل الاجتماعي؟
  - في حالة الإجابة بنعم عن السؤال السابق، هل اتخذت أي إجراءات لحماية الخصوصية بعد ذلك؟
- ما التحديات التي تواجهها في فهم ممارسات الخصوصية الرقمية، أو تطبيقها؟

القسم الخامس: هو عبارة عن دور الجامعة والكلية في تنمية الوعي بالخصوصية الرقمية لدى الطلاب، واشتمل على عدد من التساؤلات:

- هل تعقد الجامعة أو الكلية ندوات توعوية أو ورش عمل؛ عن الخصوصية الرقمية؟
- هل تحوي المناهج الدراسية في الكلية مقررات تهتم بالخصوصية الرقمية؟
- هل تنفذ الجامعة أو الكلية حملات توعوية عن الخصوصية الرقمية؟

- ما الوسائل التي ترغب في أن توفرها الجامعة أو الكلية؛ لرفع مستوى وعي الطلاب بالخصوصية الرقمية؟

صدق أداة الدراسة وثباتها:

للتحقق من صدق أداة الدراسة تم عرضها على مجموعة من المحكمين من ذوي الاختصاص والخبرة من أعضاء هيئة التدريس في عدد من الجامعات المحلية والعربية، إذ أبدوا بعض الملاحظات القيمة، وفي ضوء توجيهاتهم تم تعديل بعض الفقرات وإضافة البعض الآخر وحذفه، وبالتالي تحقق الصدق الظاهري للبيانات.

وللتحقق من ثبات أداة الدراسة، تم توزيع الاستبانة على عينة تجريبية من الطلاب بلغت (20) طالبًا وطالبة، للتحقق من مدى وضوح الأسئلة للمبحوثين تم أخذ ملاحظاتهم بعين الاعتبار قبل توزيع الاستبانة بصورتها النهائية.

نتائج الدراسة وتفسيرها

من خلال تحليل البيانات في الاستبانة الالكترونية، نجد ما يأتي:

أولاً: تحليل بيانات المعلومات الشخصية:

بلغ عدد الذكور المشاركين في الاستبانة 106 ذكور بنسبة 67.5% ، في حين بلغ عدد الإناث 51 أنثى، أي 32.5%، توزعوا وفق التخصصات والمستويات الموضحة في جدول رقم 1 و 2 كالآتي :

جدول رقم (1) توزيع العينة على أقسام الكلية.

القسم	التكرار	النسبة المئوية
تقنية المعلومات	89	%56.7
علوم الحاسوب	68	%43.3
المجموع	**157**	**%100**

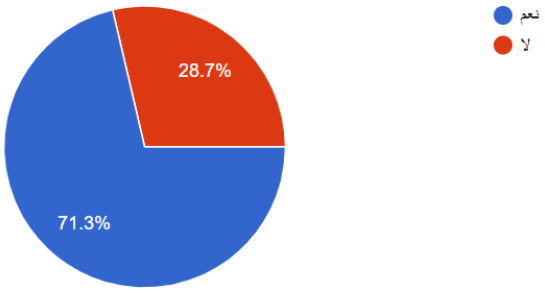
جدول رقم (2) توزيع العينة على المستويات الدراسية بالكلية.

المستوى	التكرار	النسبة المئوية
الأول	48	%30.6
الثاني	22	%14
الثالث	37	%23.6
الرابع	50	%31.8
المجموع	**157**	**%100**

ثانياً: تحليل بيانات محور الوعي بالخصوصية الرقمية:

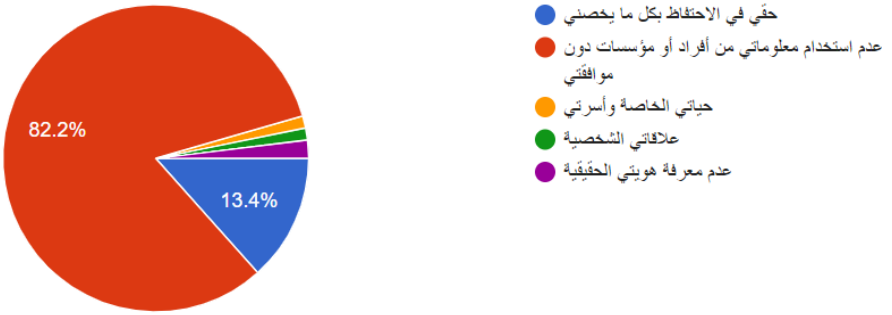
تشير البيانات أن غالبية المشاركين في الاستبيان 71.3% لديهم معرفة بماهية الخصوصية الرقمية، في حين أن 28.7% من المشاركين لايعرفون ماهي الخصوصية الرقمية (شكل 1).

الشكل رقم (1) هل تعرف: ما الخصوصية الرقمية؟



وبسؤال المشاركين عن مفهومهم للخصوصية الرقمية (شكل 2) تم ملاحظة أن النسبة الأعلى من المشاركين 82.2%، يرى أن مفهوم الخصوصية الرقمية يتمثل في عدم استخدام معلوماتهم الشخصية من أفراد أو مؤسسات دون موافقتهم، وهذا يدل على وعي متزايد بأهمية الموافقة على استخدام بياناتهم الشخصية، في حين يعد 13.4 % من المشاركين أن الخصوصية الرقمية تتمثل في حقهم بالاحتفاظ بكل مايخصهم، وهذا يدل على فهم أوسع للخصوصية كحق أساسي للفرد، في حين توزعت آراء بقية المشاركين 4.4% في أن الخصوصية الرقمية تمثل حياتهم الخاصة وأسرهم، أو علاقاتهم الشخصية، أو عدم معرفة هويتهم الحقيقية على مواقع التواصل الاجتماعي.

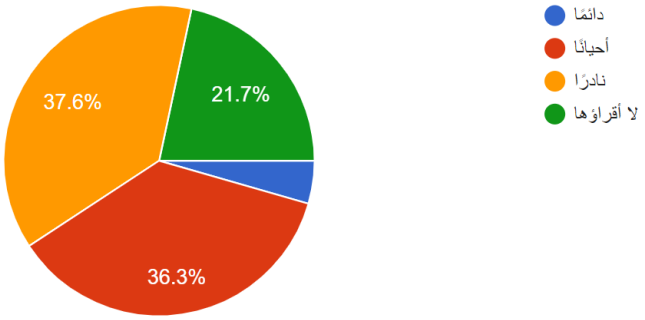
الشكل رقم (2) مفهوم الخصوصية الرقمية.



كما يتضح لنا من خلال تحليل بيانات هذا المحور (شكل رقم 3) أن نسبة قليلة جداً من المشاركين 4.4% تهتم بقراءة سياسات الخصوصية للمواقع والتطبيقات بشكل كامل قبل استخدامها، في حين أن

نسبة كبيرة تقدر بحوالي 73.9% يقرأون هذه السياسات أحياناً أو نادراً، في حين أن نسبة لابأس بها من المشاركين 21.7% لا يقرأون سياسات الخصوصية إطلاقاً.

الشكل رقم (3) نتائج قراءة سياسات الخصوصية للمواقع والتطبيقات.



تشير النسب المذكورة في شكل رقم (3) إلى أن غالبية الطلاب المشاركين لا يقرأون سياسات الخصوصية للمواقع والتطبيقات قبل استخدامها، وهذا له مدلولات عدة، منها:

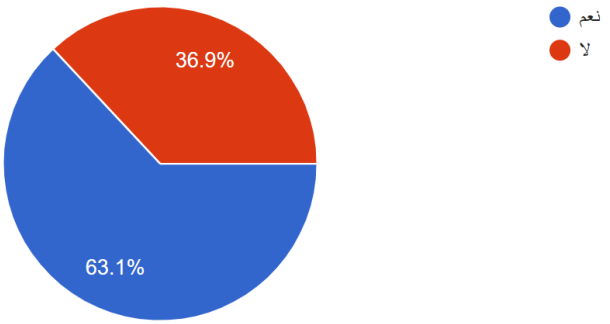
- قلة وعي الطلاب بأهمية سياسات الخصوصية، وكيفية تأثيرها في خصوصيتهم وأمن بياناتهم الشخصية.
- الثقة المفرطة في هذه المواقع والشركات التي تقدم هذه الخدمات، مما يدفعهم إلى تجاهل قراءة سياسات الخصوصية.
- تعقيد اللغة المستخدمة في كتابة هذه السياسات قد يكون سبباً في عدم قراءاتها نظراً لصعوبة فهمها من قبل الطلاب.
- أيضاً قد يكون ضيق الوقت وعدم الرغبة في قراءة وثائق طويلة ومعقدة قبل استخدام الخدمة.

وهذه النتائج قد يكون لها آثار في حماية خصوصية الفرد، إذ قد تتعرض خصوصيته لخطر الانتهاك، وقد تستغل بعض الشركات هذا الجهل لجمع البيانات الشخصية للمستخدمين بطرق مخادعة.

كما أوضحت النتائج أن حوالي 63.1% من المشاركين لديهم معرفة كافية عن كيفية تغيير إعدادات الخصوصية لحساباتهم الشخصية على شبكات التواصل الاجتماعي، وهي نسبة مرتفعة تدل على أن عددًا من الأشخاص أصبحوا يدركون المخاطر المحتملة المرتبطة بمشاركة المعلومات الشخصية عبر الإنترنت، وأنهم يتخذون خطوات لحماية أنفسهم. ومع ذلك، فإن نسبة الـ 36.9% من المشاركين الذين ليس لديهم معرفة

كافية بإعدادات الخصوصية تشير إلى وجود فجوة معرفية لديهم، وحاجتهم إلى مزيد من التوعية بأهمية الخصوصية الرقمية وكيفية حماية أنفسهم (شكل 4).

الشكل رقم (4) معرفة المستخدمين بإعدادات الخصوصية.



جدول رقم (3) يوضح أهم المخاطر التي تهدد الخصوصية الرقمية على شبكات التواصل الاجتماعي من وجهة نظر المشاركين.

جدول رقم (3) أهم المخاطر التي تهدد الخصوصية الرقمية على شبكات التواصل الاجتماعي.

أهم المخاطر التي تهدد الخصوصية الرقمية على شبكات التواصل الاجتماعي	التكرار	النسبة المئوية
سرقة البيانات الشخصية	72	%45.8
الابتزاز الإلكتروني	41	%26.1
انتحال الشخصية	26	%16.6
التتبع والمراقبة	18	%11.5

تشير النتائج في الجدول السابق إلى أن 45.8% من الطلاب يرون أن سرقة البيانات الشخصية هي أكبر تهديد يواجه خصوصيتهم الرقمية، مما يدل على ادراكهم قيمة بياناتهم الشخصية، وكيف يمكن أن يتم استغلالها بشكل غير مشروع اذا وقعت في الأيدي الخاطئة، وأن نسبة 26.1% من المشاركين ترى أن اكبر خطر يواجههم هو الابتزاز الإلكتروني، في حين أن 16.6% من المشاركين يرون أن أكبر خطر يهددهم هو انتحال الشخصية مما يدل على إدراك الطلاب أهمية الحفاظ على هويتهم الرقمية، والخطر الذي قد يسببه انتحال أحدهم لهويتهم، مثل استخدامها لارتكاب جرائم أو نشر معلومات كاذبة باسمهم. في حين نجد أن

11.5 % من الطلاب قلقون من أن يتم تتبع تحركاتهم عبر الإنترنت وجمع بيانات عنهم دون علمهم أو موافقتهم.

ثالثاً: تحليل بيانات محور سلوكيات استخدام الطلاب لشبكات التواصل الاجتماعي:

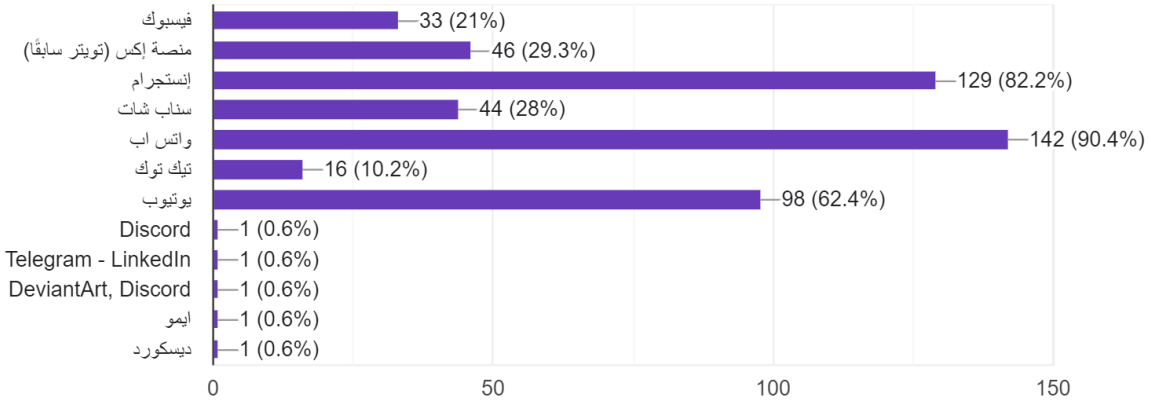
يوضح الرسم البياني في شكل رقم (5) توزيع تفضيلات الطلاب المشاركين في الاستبيان لعدد من شبكات التواصل الاجتماعي المختلفة، إذ يمكن ملاحظة هيمنة منصات محددة بشكل أكبر من غيرها، فنجد أن تطبيق الانستجرام حصل على أعلى نسبة من الأصوات مما يشير إلى شعبيته الواسعة بين المستخدمين، والتي قد يعود سببها إلى تركيزه على المحتوى المرئي والتفاعلات الاجتماعية التي يقدمها التطبيق. يليه في المرتبة الثانية تطبيق الواتس آب مما يعكس أهميته كأداة أساسية للتواصل اليومي والمجموعات.

هناك تراجع ملحوظ في شعبية تطبيق الفيسبوك مقارنة بالماضي لكنه لايزال يحتل مكانة مهمة .

كما نلاحظ ان تطبيق التيك توك حظي بشعبية متزايدة مما يعكس جاذبيته لدى فئات عمرية معينة، خاصةً الشباب.

نظراً لطبيعة المتغير المدروس (استخدام شبكات التواصل الاجتماعي)، والذي يتسم بتعددية الأبعاد، فقد سمحنا للمبحوثين باختيار أكثر من إجابة واحدة. هذا النهج، على الرغم من أنه أدى إلى تجاوز حجم العينة في الإجابات، لكنه زاد من دقة النتائج، وسمح لنا بفهم أكثر عمقاً لهذا المحور المهم.

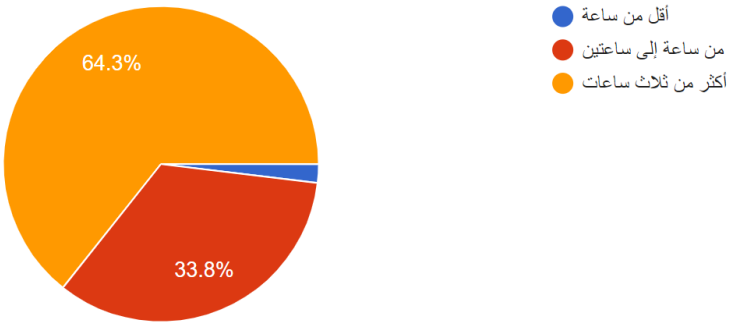
الشكل رقم (5) شبكات التواصل الاجتماعي التي يستخدمها الطلاب بشكل يومي



من خلال شكل رقم (6) نلاحظ الوقت الذي يقضيه المشاركون يوميًّا على شبكات التواصل الاجتماعي، إذ تشير النسبة العالية للطلاب الذين يقضون أكثر من 3 ساعات على شبكات التواصل الاجتماعي (64.3%)، إلى أن الاستخدام الكثيف لهذه المنصات هو السائد بين هذه الفئة العمرية من المستخدمين،

في حين أوضح التحليل أن نسبة 33.8% يقضون مابين ساعة إلى ساعتين ، وعددًا ضئيلًا جدًا منهم (1.9%) يقضون أقل من ساعة يوميًا على هذه المنصات.

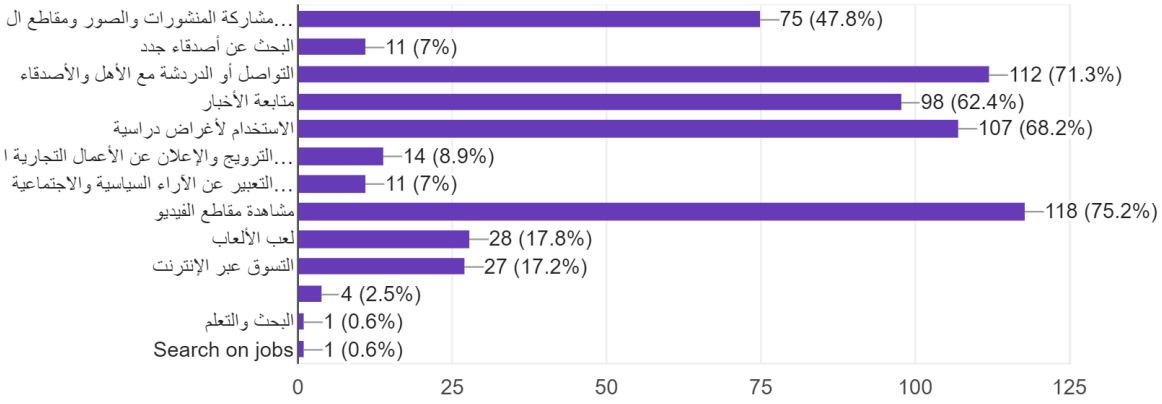
الشكل رقم (6) الوقت الذي يقضيه المشاركون في العينة على شبكات التواصل الاجتماعي.



تشير البيانات الموضحة في الشكل السابق إلى أن هناك اعتماداً كبيراً على شبكات التواصل الاجتماعي بين فئة الطلاب، إذ يقضي غالبية الطلاب وقتاً طويلاً على هذه المنصات، وأنها أصبحت جزءاً لا يتجزأ من روتين الطلاب اليومي. وهذا الإقبال على هذه المنصات يعد ظاهرة تستدعي الاهتمام، يجب التعامل معها بوعي وحذر، والعمل على تحقيق التوازن بين الاستفادة من هذه المنصات، وتجنب الآثار السلبية الناجمة عن الإفراط في استخدامها.

وبسؤال المبحوثين عن أهم الأنشطة التي يمارسونها على شبكات التواصل الاجتماعي بشكل دائم ، نجد أن الترفيه عبر مشاهدة مقاطع الفيديو، والتواصل الاجتماعي مع الأهل والأصدقاء ، إضافة إلى الاستخدام لأغراض دراسية تشكل النسبة الأكبر من الأنشطة. تليها متابعة الأخبار ومشاركة المنشورات والصور ومقاطع الفيديو (شكل رقم 7).

الشكل رقم (7) أهم الأنشطة التي يمارسها الطلاب على شبكات التواصل الاجتماعي.

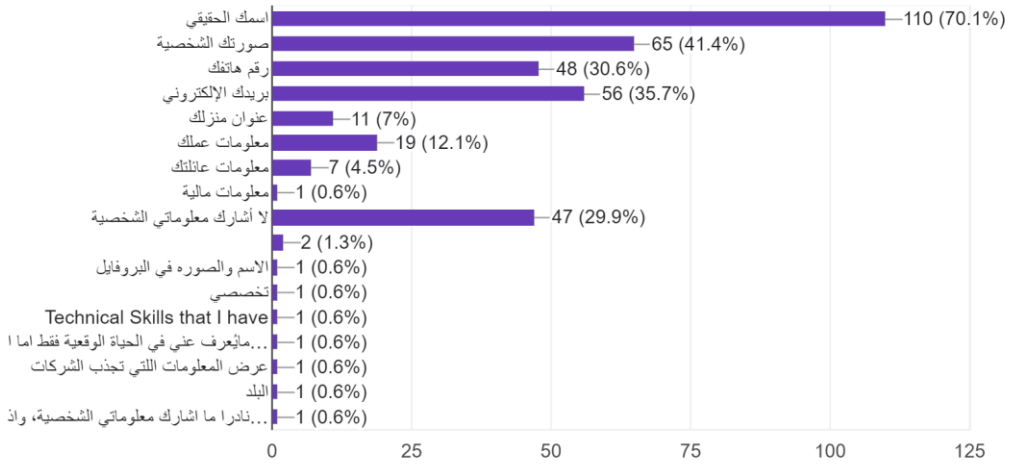


رغم أن الأنشطة مثل لعب الألعاب والتسوق عبر الإنترنت كانت نسبتها أقل مقارنة بالأنشطة السابقة لكنها تشير إلى تزايد استخدام منصات التواصل الاجتماعي للاسترخاء والترفيه وللتسوق عبر الإنترنت.

وتفاوتت بقية الاستخدامات بين البحث عن أصدقاء جدد، والترويج والإعلان عن الأعمال التجارية الخاصة، والتعبير عن الآراء السياسية والاجتماعية بحرية، ومتابعة الأخبار.

شكل رقم (8) يوضح أهم المعلومات الشخصية التي يمكن أن يشاركها الطلاب على شبكات التواصل الاجتماعي، حيث نلاحظ أن المشاركين يميلون لمشاركة الهوية والانتماء، مثل الاسم الحقيقي، والصورة الشخصية، والبريد الالكتروني، ورقم الهاتف، بنسبة عالية، مما يشير إلى أن المستخدمين لا يدركون مخاطر مشاركة المعلومات الحساسة، مما قد يعرضهم إلى انتهاك الخصوصية والتعرض للاختراق.

الشكل رقم (8) المعلومات الشخصية التي يمكن أن يشاركها الطلاب على شبكات التواصل الاجتماعي



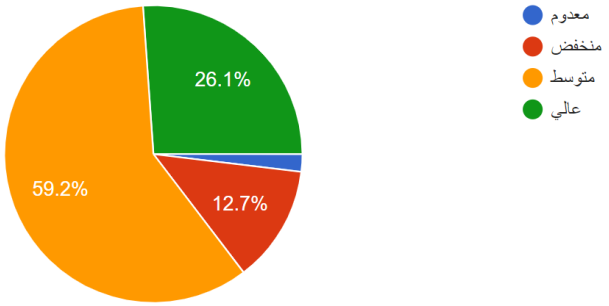
نلاحظ أن هناك تجاوزًا في حجم العينة في الأشكال رقم 7 و 8 وذلك نظراً لطبيعة هذين المحورين إذ تم السماح للمبحوثين باختيار أكثر من إجابة واحدة.

رابعاً: تحليل بيانات محور حماية الخصوصية على شبكات التواصل الاجتماعي:

يظهر الشكل رقم (9) تقسيمًا واضحًا لمستويات وعي المشاركين بمخاطر مشاركة المعلومات الشخصية على شبكات التواصل الاجتماعي، حيث تشير النسبة الكبيرة (59.2%) إلى أن غالبية المشاركين لديهم فهم متوسط لمخاطر مشاركة المعلومات الشخصية. وعلى الرغم من أهمية الموضوع، غير أن النسبة المئوية لمن يمتلكون وعيًا عاليًا بالمخاطر (26.1%) ليست مرتفعة بشكل ملحوظ مما يشير إلى ضرورة تكثيف جهود التوعية بمخاطر الأمن السيبراني وحماية البيانات الشخصية.كما تشير النسبة المئوية الصغيرة (12.7%) إلى وجود فئة من المشاركين لا تدرك تمامًا المخاطر المترتبة على مشاركة معلوماتهم الشخصية على الإنترنت. أما

2% من المشاركين وهي نسبة ضئيلة جداً فلا يوجد لديهم الوعي الكافي بمخاطر مشاركة معلوماتهم االشخصية على شبكات التواصل الاجتماعي.

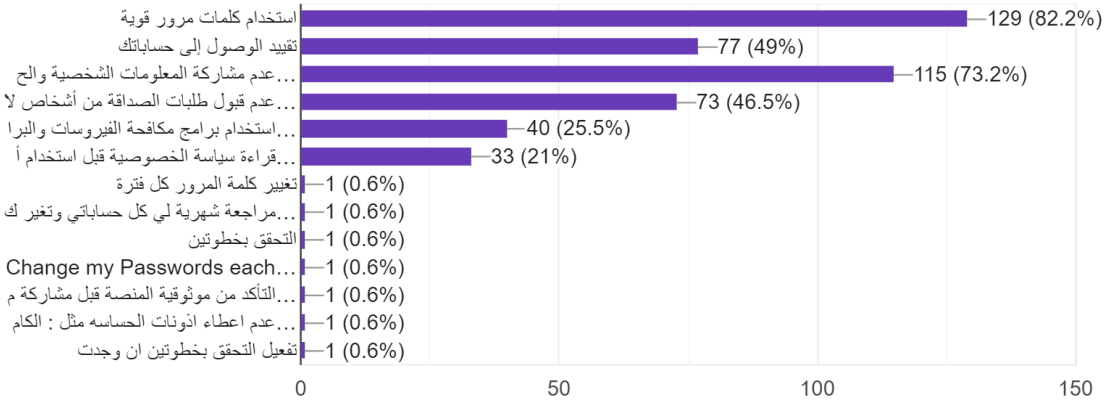
الشكل رقم (9) مدى وعي المشاركين بمخاطر مشاركة المعلومات الشخصية على شبكات التواصل الاجتماعي.



يوضح الشكل رقم (10) مجموعة من الإجراءات التي يتخذها الطلاب لحماية خصوصيتهم على منصات التواصل الاجتماعي، حيث نلاحظ أن أعلى نسبة تشمل استخدام كلمات مرور قوية، يليها عدم مشاركة المعلومات الشخصية والحساسة، ثم تقييد الوصول إلى الحسابات، وعدم قبول طلبات الصداقة من اشخاص لا نعرفهم مما يدل على وعي الطلاب بأهمية حماية خصوصيتهم. ورغم أهمية استخدام برامج مكافحة الفيروسات والبرامج الضارة إضافة إلى قراءة سياسة الخصوصية قبل استخدام أي شبكة تواصل اجتماعي لكن النتائج أظهرت انخفاضًا في اختيار هذين الخيارين مما يجعل أجهزة الطلاب عرضة للهجمات الإلكترونية.

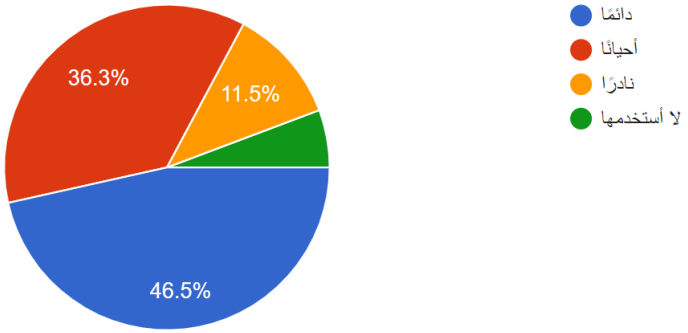
أيضاً تم هنا السماح للمبحوثين باختيار أكثر من إجابة واحدة وذلك نظراً لطبيعة هذا المحور مما أدى إلى تجاوز حجم العينة في الإجابات.

الشكل رقم (10) الإجراءات التي يتخذها الطلاب لحماية خصوصيتهم على شبكات التواصل الاجتماعي



يوضح الرسم البياني في الشكل رقم (11) أن الغالبية العظمى من المشاركين تستخدم كلمات مرور قوية ومختلفة لحساباتهم على مواقع التواصل الاجتماعي (46.5 %). كما تشير النسبة المتوسطة (36.3%) إلى أن عددًا من المشاركين يستخدمون كلمات مرور غير قوية أو متشابهة لحساباتهم المختلفة، مما يسهل اختراقها، كما توجد قلة من المشاركين (11.5%) نادرًا ما يطبقون هذه الممارسة الأمنية المهمة، إضافة إلى أن 5.7 % من المشاركين أظهروا عدم استخدامهم لكلمات المرور القوية والمختلفة لحماية حساباتهم على مواقع التواصل الاجتماعي، مما يشير إلى قلة الوعي بأهمية هذه الخطوة، أو تفضيلهم لاختيار الراحة على الأمن، مما يؤدي إلى استخدام كلمات مرور سهلة التذكر ولكنها غير آمنة.

الشكل رقم (11) استخدام كلمات مرور قوية ومختلفة للحسابات على شبكات التواصل الاجتماعي.

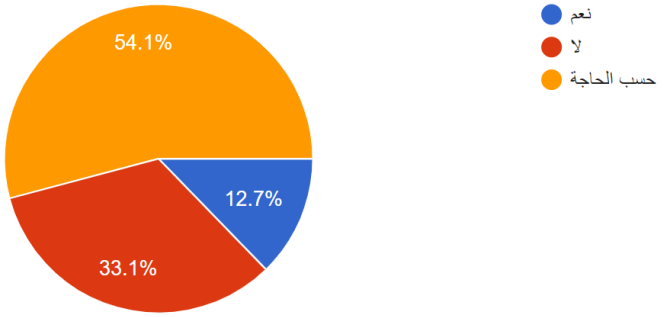


وبسؤال المشاركين في الاستبيان عما إذا كانوا يغيرون إعدادات الخصوصية الخاصة بهم على شبكات التواصل الاجتماعي بانتظام، نجد أن غالبية المشاركين 54.1% يقومون بتغيير إعدادات الخصوصية حسب الحاجة، وهذا يعني أنهم يقومون بذلك عند حدوث تغييرات معينة أو عند الشعور بضرورة ذلك، في حين أن نسبة 33.1% أجابوا بلا، وهذا يدل على أن هناك شريحة كبيرة من المستخدمين لا تقوم بتغيير إعدادات الخصوصية الخاصة بهم، مما يعرضهم لمخاطر انتهاك الخصوصية. في حين أن 12.7% من المشاركين وهي نسبة قليلة يقومون بتحديث إعدادات الخصوصية الخاصة بهم بانتظام، مما يشير إلى مستوى عالٍ من الوعي بأهمية الخصوصية لدى هذه الشريحة شكل رقم (12).

يرجع هذا التفاوت في الإجابات إلى التفاوت في مستوى الوعي بأهمية الخصوصية بين المستخدمين، إذ قد يكون البعض غير مدرك للمخاطر المرتبطة بمشاركة المعلومات الشخصية. أيضا قد تكون إعدادات الخصوصية في بعض المنصات معقدة وصعبة الفهم، مما يجعل المستخدمين يترددون في تغييرها. إضافة إلى أن بعض المستخدمين قد يفضل الراحة على الأمن، مما يدفعهم إلى ترك إعدادات الخصوصية على وضعها

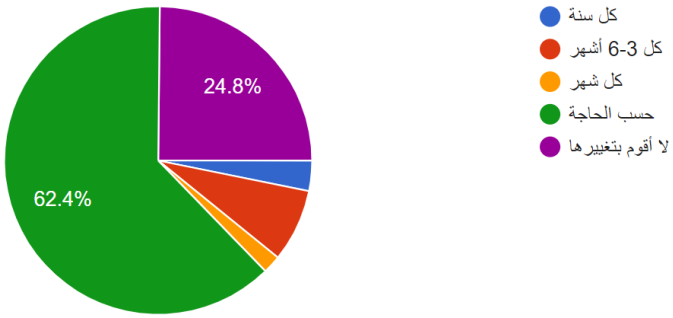
الافتراضي. والبعض الآخر قد لا يشعر بالحاجة إلى تغيير إعدادات الخصوصية ما لم يواجه أي مشكلة تتعلق بالخصوصية.

الشكل رقم (12) تغيير إعدادات الخصوصية الخاصة بالطلاب على شبكات التواصل الاجتماعي بانتظام.



يوضح شكل (13) أن غالبية المشاركين 62.4% يقومون بتغيير كلمات مرور حساباتهم على شبكات التواصل الاجتماعي "حسب الحاجة"، وهذا يعني أنهم يقومون بذلك عند حدوث تغييرات معينة أو عند الشعور بضرورة ذلك، مما يدل على أن هناك وعيًا لدى معظم المشاركين بأهمية تغيير كلمات المرور، ولكنهم لا يقومون بذلك بشكل روتيني، في حين أن نسبة متوسطة منهم 24.8% لا تقوم بتغيير كلمات مرورها، مما يعرض حساباتهم لمخاطر الاختراق. والنسبة الأصغر من المشاركين 12.8 % تقوم بتغيير كلمات مرورها بشكل دوري، ولكن بنسب متفاوتة (كل سنة، كل 3–6 أشهر، كل شهر).

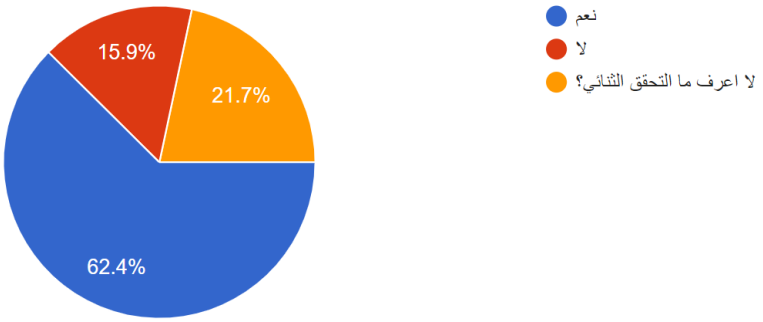
الشكل رقم (13) كم مرةً يقوم المستخدمين بتغيير كلمات المرور لحساباتهم على شبكات التواصل الاجتماعي؟



يوضح شكل رقم (14) أن نسبة عالية من المشاركين 62.4% يستخدمون تقنية التحقق الثنائي لحماية حساباتهم على شبكات التواصل الاجتماعي، مما يدل على وجود وعي بأهمية استخدام هذه التقنية لدى عدد كبير من المشاركين، كما أن نسبة متوسطة من المستخدمين 21.7% لايعرفون ماهو التحقق الثنائي مما يدل على وجود فجوة في الوعي بأهمية استخدام هذه التقنية وكيفية تفعيلها لديهم، والنسبة الأقل من

المشاركين 15.9% أشاروا إلى عدم استخدامهم لهذه التقنية رغم معرفتهم بها، وقد يرجع هذا إلى قلة الوعي لدى المشاركين لأهمية التحقق الثنائي، وكيف يمكن أن يحمي حساباتهم، إضافة إلى أن بعض المشاركين قد يجدون أن عملية تفعيل التحقق الثنائي معقدة أو مملة. أو أنهم قد يشعرون بعدم الراحة تجاه استخدام تقنيات إضافية لتأمين حساباتهم، أو اعتقادهم أن حساباتهم ليست مهمة بما يكفي لتبرير استخدام طبقة أمان إضافية.

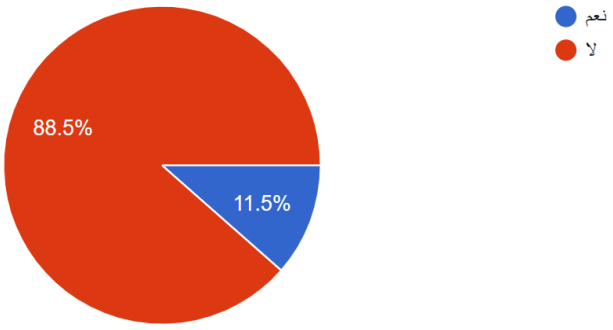
الشكل رقم (14) هل يستخدم المشاركون تقنيات التحقق الثنائي لحساباتك؟



يوضح شكل رقم (15) أن قلة قليلة من المشاركين 11.5% لديهم خبرة سابقة في مجال الخصوصية الرقمية من خلال حضورهم دورات تدريبية وورش عمل في حين نجد أن الغالبية العظمى من المشاركين 88.5% لم يحضروا أي دورة تدريبية أو ورشة عمل عن الخصوصية الرقمية، مما يشير إلى وجود فجوة كبيرة في المعرفة عن الخصوصية الرقمية لدى الكثير من المستخدمين، قد تعود أسبابها إلى:

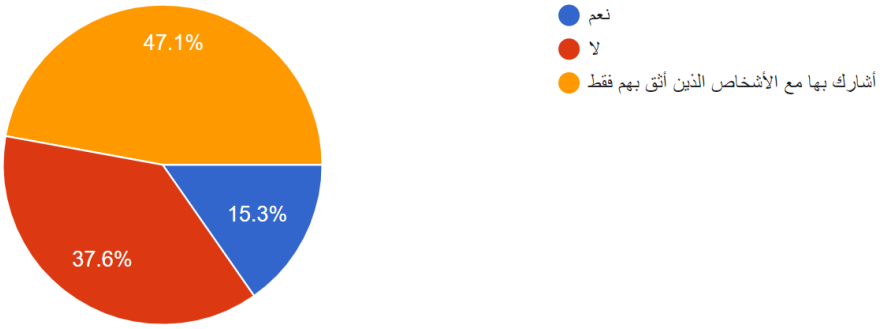
- عدم ادارك المشاركين لأهمية الخصوصية الرقمية، وكيف يمكنها أن تؤثر في حياتهم اليومية.
- أو إلى عدم توافر الدورات التدريبية المتخصصة في مجال الخصوصية الرقمية بسهولة أو بتكلفة معقولة.
- أو أن المشاركين لديهم أولويات أخرى للتركيز عليها بدلاً من الاهتمام بالخصوصية.

الشكل رقم (15) هل سبق أن حضر المشاركون أي دورة تدريبية أو ورشة عمل عن الخصوصية الرقمية؟



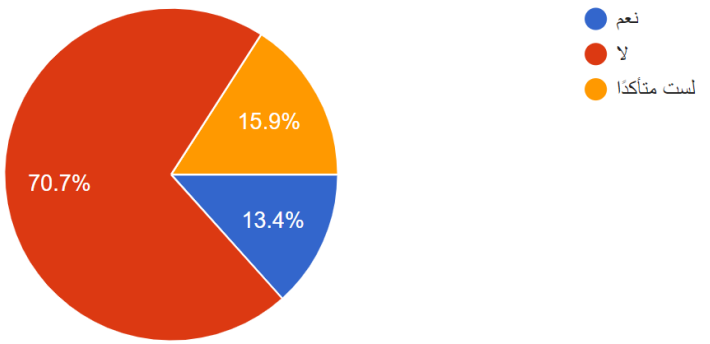
يوضح شكل رقم (16) أن غالبية الطلاب (47.1%) يشاركون بمعلوماتهم الشخصية على شبكات التواصل الاجتماعي، ولكن ليس مع أي شخص بل مع الأشخاص الذين يثقون بهم فقط مما يدل على إدراكهم لأهمية حماية خصوصيتهم. في حين أن هناك نسبة متوسطة (37.6%) تحرص على حماية خصوصيتها بشكل كامل ولا تشارك معلوماتها الشخصية على الإطلاق، في حين أن النسبة الأقل من الطلاب (15.3%) تشارك معلوماتها الشخصية بشكل عام مع أي شخص مما يدل عى عدم اهتمامهم بخصوصيتهم ورغبتهم في مشاركة كل شيء عن حياتهم على الإنترنت.

الشكل رقم (16) هل يشارك الطلاب بمعلوماتهم الشخصية، مثل: رقم الهاتف، أو العنوان، على شبكات التواصل الاجتماعي؟



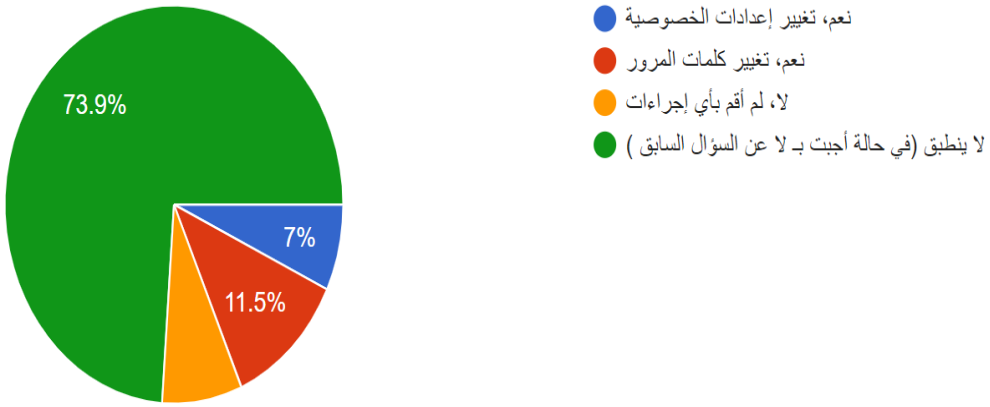
في شكل (17) نلاحظ أن الغالبية العظمى من المشاركين (70.7%) لم يتعرضوا لموقف يتعلق بانتهاك الخصوصية على شبكات التواصل الاجتماعي ربما لأنهم أكثر حذرًا، أو محظوظون في تجنب هذه المشكلة. في حين أن نسبة متوسطة منهم 15.9% قد لا يكونون على دراية كاملة بما يشكل انتهاكًا للخصوصية أو قد لا يتذكرون مواقف سابقة، ونسبة أقل من المشاركين (13.4%) تعرضوا لمثل هذه الانتهاكات على شبكات التواصل الاجتماعي، وذلك قد يكون إما لقلة الوعي لديهم بالمخاطر المرتبطة بمشاركة المعلومات الشخصية على الإنترنت، وإمَّا لسهولة الوصول إلى معلوماتهم على شبكات التواصل الاجتماعي، مما يجعلهم هدفًا جذابًا للمخترقين والمتسللين، أو قد يكون لأن إجراءات الأمن والحماية في بعض المنصات غير كافية لحماية بيانات المستخدمين.

الشكل رقم (17) تعرض المشاركين لانتهاكات الخصوصية على شبكات التواصل الاجتماعي.



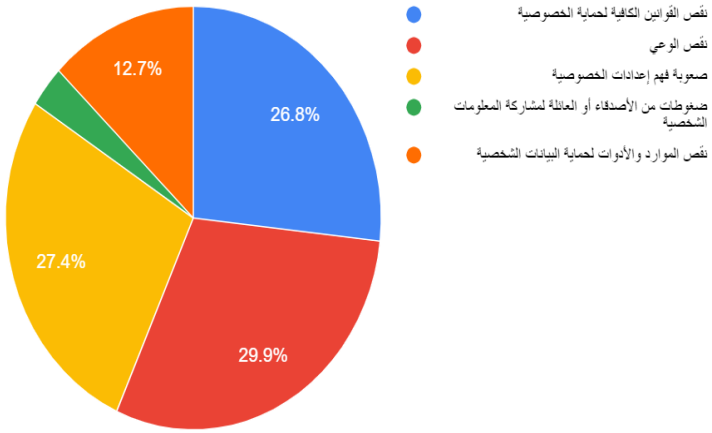
بتحليل نتائج الاستبيان عن إجراءات حماية الخصوصية التي يتخذها المشاركون بعد تعرضهم للانتهاك نجد أن النسبة الأعلى من المشاركين الذين واجهوا مشكلة انتهاك الخصوصية 11.5% أدركوا أهمية حماية بياناتهم واتخذوا خطوات عملية لحماية أنفسهم عبر تغيير كلمات المرور، و 7 % منهم قاموا بتغيير إعدادات الخصوصية، في حين أن 7.6% من المشاركين لم يقوموا بأي إجراءات لحماية أنفسهم بعد التعرض للانتهاك، مما يجعلهم عرضة لخطر تكرار هذه المشكلة (شكل رقم 18).

الشكل رقم (18) إجراءات الحماية بعد التعرض لانتهاك الخصوصية.



يوضح الشكل رقم (19) تحليل نتائج الاستبيان عن التحديات التي تواجه المشاركين في فهم ممارسات الخصوصية الرقمية وتطبيقها، حيث نجد أن أعلى نسبة من المشاركين 29.9% تشير إلى أن لديهم نقصًا في الوعي العام بأهمية الخصوصية الرقمية وكيفية حماية البيانات الشخصية. في حين نجد أن 27.4% من المشاركين يجدون صعوبة في فهم إعدادات الخصوصية، وقد يرجع سبب ذلك إلى أن تغير سياسات الخصوصية في المنصات والتطبيقات بشكل متكرر يجعل من الصعب على المستخدمين متابعتها وفهمها. في حين أن 26.8 % من المشاركين يرون أن نقص القوانين الكافية لحماية الخصوصية من أهم التحديات التي قد تواجههم . في حين أن 12.7 % من المشاركين يجدون أن نقص الموارد والأدوات لحماية البيانات الشخصية من أهم التحديات التي قد تواجههم لحماية خصوصيتهم. في حين أن نسبة ضئيلة جدًا من المشاركين 3.2% يرون أن ضغوطات من الأصدقاء أو العائلة لمشاركة المعلومات الشخصية من أهم التحديات التي تواجههم في فهم ممارسات الخصوصية الرقمية.

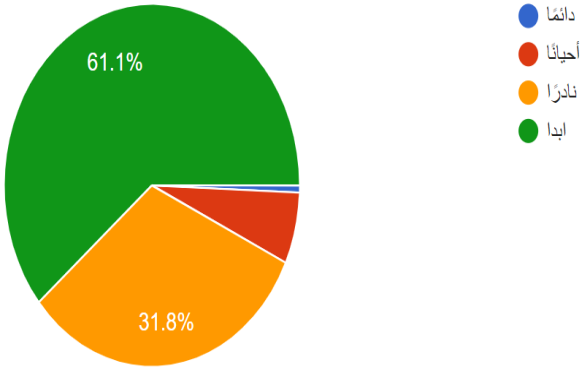
الشكل رقم (19) التحديات التي يواجهها المشاركون في فهم ممارسات الخصوصية الرقمية، أو تطبيقها.



خامساً: تحليل بيانات محور دور الجامعة والكلية في تنمية الوعي بالخصوصية الرقمية لدى الطلاب:

بتحليل نتائج الاستبيان عن عقد الجامعة أو الكلية لندوات وورش عمل عن الخصوصية الرقمية، نلاحظ أن النسبة الأعلى من المشاركين 61.1% لايعلمون بوجود مثل هذه الندوات أو ورش العمل عن الخصوصية الرقمية، في حين تشير بقية النسب (31.8% ، 6.4%) إلى أن هناك نسبة قليلة من الطلاب يحضرون هذه البرامج، ولكن بشكل غير منتظم أو نادر. ونسبة ضئيلة جدًا منهم 0.7% هم من يحضرون مثل هذه الأنشطة بشكل دائم (شكل رقم 20).

الشكل رقم (20) هل تعقد الجامعة أو الكلية ندوات توعوية أو ورش عمل؛ عن الخصوصية الرقمية؟

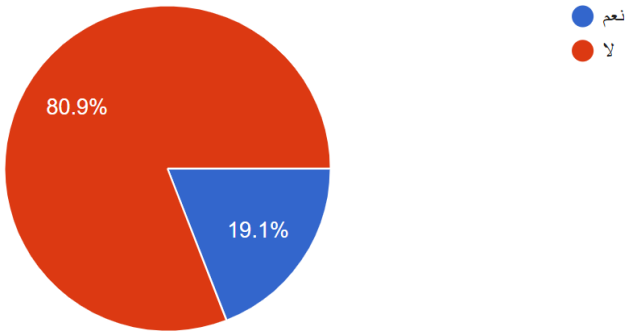


قد يرجع سبب عدم معرفة الطلاب بمثل هذه الأنشطة لعدم اهتمام الجامعة أو الكلية بتنفيذها، وتوعية الطلاب بأهمية حماية بياناتهم، والمخاطر المرتبطة بانتهاك الخصوصية الرقمية؛ إذ أصبح من الضروري توفير التوعية اللازمة عن كيفية استخدام التكنولوجيا بأمان، وحماية الخصوصية في ظل التطور السريع للتكنولوجيا، وزيادة الاعتماد عليها في الحياة اليومية، أو لقلة الدعاية لهذه الأنشطة إذ قد لا يتم الترويج لها بالشكل الكافي

للطلاب. إضافة إلى أن الجامعة أو الكلية قد يعانون من النقص في الموارد اللازمة لتنظيم هذه البرامج، مثل الميزانية والقوى العاملة.

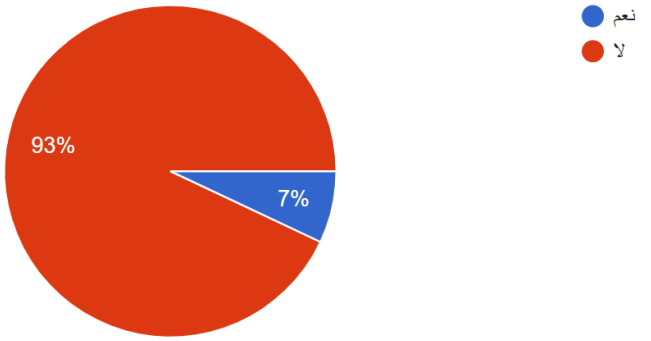
كما نلاحظ أن هناك فجوة كبيرة في تغطية موضوع الخصوصية الرقمية في المناهج الدراسية بالكلية (شكل رقم 21)، حيث إن 80.9% من المشاركين يؤكدون على غياب هذا الموضوع المهم من مناهجهم الدراسية في الكلية، مما يدل على وجود نقص كبير في الاهتمام بتعليم الطلاب كيفية حماية خصوصيتهم الرقمية. على عكس 19.1% من المشاركين الذين يرون أن المناهج الدراسية الحالية تحوي مقررات تهتم بالخصوصية الرقمية. قد يرجع هذا التباين في الآراء إلى أن المناهج الدراسية الحالية لم يتم تحديثها لتشمل المواضيع الحديثة، مثل الخصوصية الرقمية، مما يجعلها غير قادرة على مواكبة التطورات السريعة في عالم التكنولوجيا. إضافة إلى أنه قد لا يكون هناك وعي كافٍ لدى واضعي المناهج الدراسية بأهمية الخصوصية الرقمية وتأثيرها في حياة الطلاب. كما قد تواجه الكلية نقصًا في الموارد اللازمة لتطوير مناهج جديدة، وتدريب أعضاء هيئة التدريس على تدريس هذه المواضيع.

الشكل رقم (21) هل تحوي المناهج الدراسية في الكلية مقررات تهتم بالخصوصية الرقمية؟



كما يوضح شكل رقم (22) ان 93% من المشاركين يرون أن الجامعة أو الكلية لاتنفذان أي حملات توعوية عن الخصوصية الرقمية، وقد يرجع ذلك إلى الأسباب نفسها المذكورة في محور عقد الجامعة أو الكلية لندوات أو ورش عمل عن الخصوصية الرقمية .

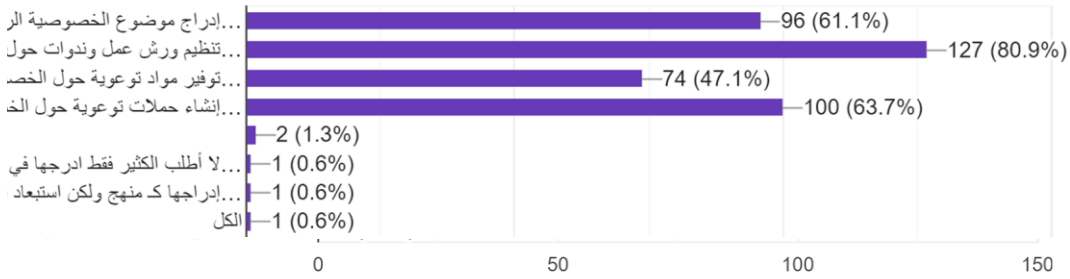
الشكل رقم (22) هل تنفذ الجامعة أو الكلية حملات توعوية عن الخصوصية الرقمية؟



وبسؤال الطلاب عن الوسائل التي يرغبون في أن توفرها الجامعة أو الكلية؛ لرفع مستوى وعيهم بالخصوصية الرقمية، وجدنا أن النسب الأعلى للطلاب الذين يرغبون في تنظيم ورش عمل وندوات عن الخصوصية الرقمية، وإدراج موضوع الخصوصية الرقمية في المناهج الدراسية، إضافة إلى توفير مواد توعوية عن الخصوصية الرقمية على موقع الجامعة أو الكلية، كما أراد البعض الآخر إنشاء حملات توعوية عن الخصوصية الرقمية على منصات التواصل الاجتماعي (شكل رقم 23).

مع ملاحظة أنه تم هنا السماح للمبحوثين باختيار أكثر من إجابة واحدة؛ وذلك نظراً لطبيعة هذا المحور، مما أدى إلى تجاوز حجم العينة في الإجابات.

الشكل رقم (23) الوسائل التي يرغب الطلاب في أن توفرها الجامعة أو الكلية؛ لرفع مستوى وعيهم بالخصوصية الرقمية.



النتائج:

استهدفت الدراسة طلاب كلية الحاسبات وتقنية المعلومات في جامعة حضرموت– اليمن، وذلك لقياس مستوى الوعي لديهم بموضوع الخصوصية الرقمية على شبكات التواصل الاجتماعي، ومن خلال تحليل نتائج أسئلة الاستبانة ومناقشتها، نستطيع تلخيص النتائج الرئيسة في مايأتي:

- كشفت الدراسة عن مستوى وعي منخفض نسبيًا بالخصوصية الرقمية لدى غالبية الطلاب.
- كشف التحليل عن سلوكيات محفوفة بالمخاطر وغير آمنة لدى الطلاب عند استخدام شبكات التواصل الاجتماعي، مثل مشاركة معلومات شخصية حساسة، أو قبول طلبات صداقة من أشخاص غرباء.
- أظهرت الدراسة وجود فجوة معرفية كبيرة في معرفة الطلاب بالطرق التقنية لحماية خصوصيتهم على الإنترنت، مثل إعدادات الخصوصية في مختلف شبكات التواصل الاجتماعي.

- أظهرت الدراسة أن دور الجامعة / الكلية في توعية الطلاب بالخصوصية الرقمية محدود، وأن المناهج الدراسية الحالية لا تغطي هذا الموضوع بشكل كافٍ.

التوصيات:

إن معالجة مشكلة نقص الوعي بالخصوصية الرقمية تتطلب جهودًا متضافرة من قبل المؤسسات التعليمية والطلاب وصناع السياسات ككل. من خلال تحليل النتائج السابقة نقترح مجموعة من التوصيات لبناء مجتمع رقمي أكثر أمانًا ووعيًا كما يأتي:

- **على مستوى الطلاب:**
  - يجب على الطلاب المشاركة في برامج التوعية التي تنظمها الجامعة أو الكلية أو أي جهة تعليمية موثوقة.
  - يجب على الطلاب البحث والتعلم بشكل ذاتي عن موضوع الخصوصية الرقمية، وتطوير مهاراتهم في هذا المجال.
  - يجب على الطلاب تطبيق المعرفة التي اكتسبوها عن الخصوصية الرقمية في حياتهم اليومية.
  - تشجيع الطلاب على تبادل المعلومات والمعارف عن الخصوصية الرقمية مع أقرانهم وعائلاتهم.
  - تحذير الطلاب من مخاطر مشاركة المعلومات الشخصية على الإنترنت، وتشجيعهم على استخدام إعدادات الخصوصية القوية.
- **على مستوى الجامعة أو الكلية:**
  - إدراج وحدة تعليمية شاملة عن الخصوصية الرقمية في المناهج الدراسية ذات الصلة لجميع التخصصات، مع التركيز على الجوانب النظرية والعملية.
  - يجب تحديث المناهج بشكل دوري لضمان مواكبتها للتطورات التكنولوجية.
  - يجب تدريب أعضاء هيئة التدريس على كيفية تدريس مادة الخصوصية الرقمية، وتزويدهم بالمصادر والمواد التعليمية اللازمة.
  - يجب تنظيم برامج توعية منتظمة للطلاب عن أهمية الخصوصية الرقمية في حياتهم على الإنترنت، وكيفية حماية بياناتهم الشخصية.

- يجب التعاون مع الخبراء في مجال الأمن السيبراني والخصوصية الرقمية لتطوير برامج تدريبية متخصصة.
- إنشاء منصة إلكترونية شاملة تقدم معلومات وموارد تعليمية عن الخصوصية الرقمية للطلاب.
- يجب توفير الموارد اللازمة لتنفيذ هذه التوصيات، بما في ذلك الميزانية والقوى العاملة.

- **على مستوى صناع السياسات:**

- يجب رفع الوعي العام بأهمية الخصوصية الرقمية من خلال الحملات الإعلامية وبرامج التوعية المجتمعية.
- يجب سن قوانين صارمة لحماية البيانات الشخصية، وتجريم انتهاكات الخصوصية.
- دعم البحث العلمي في مجال الخصوصية الرقمية؛ لتطوير حلول مبتكرة لحماية البيانات.
- تعزيز التعاون بين القطاع العام والخاص؛ لتطوير برامج توعية مشتركة، وحلول تقنية لحماية الخصوصية.

المراجع:

المراجع العربية:

- أبو حمادة، محمد. الشامي، اياد حسني. عابد، رمزي محمد. برهوم، توفيق. (2014)، تحسين حماية الخصوصية لمستخدمي الشبكات الاجتماعية في قطاع غزة من خلال التوعية الأمنية والتقنية، مجلة جامعة الأزهر-غزة (العلوم الطبيعية)، 16، 69 - 98.
- الفيصل، عبدالامير و سيد، اسراء. (2017). انتهاك الخصوصية في مواقع التواصل الاجتماعي (بحث مستل). مجلة الباحث الإعلامي، 36، 213-240.
- القحطاني، محمد .(2015)، حماية الخصوصية الشخصية لمستخدمي مواقع التواصل الاجتماعي (دراسة تأصيلية مقارنة)، قسم الشريعة والقانون، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض.
- الكربي، نورة ناصر. (2023). دور شبكات التواصل الاجتماعي في تحقيق الأمن الرقمي للطالب الإماراتي. مجلة واسط للعلوم الانسانية، 19(55)، 11-42.
- المعداوى، محمد احمد. (2018). حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي: دراسة مقارنة. مجلة كلية الشريعة والقانون بطنطا ،جامعة الازهر، 2018(33)، 1926 – 2057.
- تومي، فضيلة. (2017). إيديولوجيا الشبكات الاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق. مجلة العلوم الإنسانية والاجتماعية، 30، 41-50.
- حمود، واثق عبد الكريم. (2022). الخصوصية الرقمية في نطاق القانون الدولي . مجلة الباحث للعلوم القانونية، 2 (1).
- صفوري، أمجد. (2019). الشباب الاردني وانتهاك خصوصية الآخرين باستخدام شبكات التواصل الاجتماعي والتطبيقات الرقمية. مجلة أنساق، 3(2)، دار نشر جامعة قطر، 89-107.
- قدوري، ريم فتيحة. (2024). إدراك الخصوصية وأهميتها لمستخدمي مواقع شبكات التواصل الاجتماعي دراسة استطلاعية لمستخدمي موقع Facebook في الوطن العربي. الأكاديمية للدراسات الاجتماعية والإنسانية، 16(01)، 249-260.
- نوي، أحمد. (2023). الخصوصية المعلوماتية في ظل التطور التكنولوجي وآليات حمايتها.

المراجع الاجنبية

- Albulayhi، M. S.، & Khediri، S. E. (2022). A Comprehensive Study on Privacy and Security on Social Media. International Journal of Interactive Mobile Technologies (iJIM)، 16(01)، pp. 4–21. https://doi.org/10.3991/ijim.v16i01.27761
- Ali، & Malik، Ahmad & Ahmed، Mansoor & Raza، Basit & Ilyas، Muhammad. (2019). Privacy Concerns in Online Social Networks: A Users' Perspective. International Journal of Advanced Computer Science and Applications. 10(7). 601- 613.

- Andi، Alkila. ، Aurelia ، Firjatullah. ، Ridho ، Bramula. ، Anderes ، Gui. ، Drajad ، Wiryawan. ، Lianna ، Sugandi. (2023). The Security Awareness of Social Media Users. 1-5. doi: 10.1109/icraie59459.2023.10468199.
- Clarke، R. (2008). Personalia Page. Retrieved from http://www.rogerclarke.com/Person.html
- Glenn ، Mansfield ، Keeni. ، Hiroshi ، Tsunoda. (2019). Security and Privacy Awareness: for Software Creators and Users. 1-4. doi: 10.1109/ICAWST.2019.8923148.
- Padmavathi، Dr & Mohanlal، Sirvi. (2021). A Study on Extent of Awareness Among College Students in Security and Privacy Issues in Social Media. International Journal of Scientific Research in Computer Science، Engineering and Information Technology. 676-682. 10.32628/CSEIT2173147.
- Triveni، Krishnappa. (2023). User Awareness Of Security And Privacy In Social Networking Sites. International journal of engineering applied science and technology، doi: 10.33564/ijeast.2023.v08i05.006.