الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد حمة لخضر الوادي
كلية العلوم الاجتماعية والإنسانية
قسم علوم الإعلام والاتصال

مذكرة بعنوان:

الوعي بالأمن السيبيراني والمعلومات الرقمية لدى طلبة الإعلام والاتصال بجامعة الوادي

دراسة ميدانية لعينة من طلبة قسم الإعلام والاتصال بجامعة الشهيد حمة لخضر

تخصص: سمعي بصري

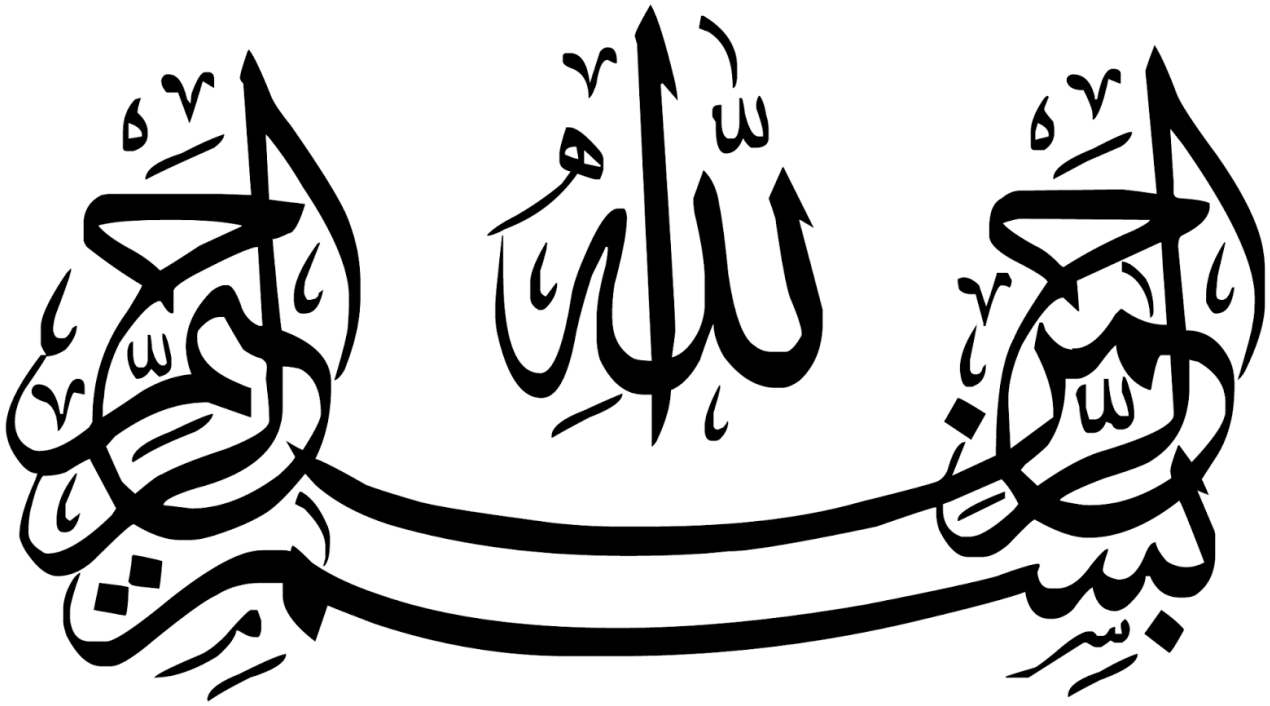
إعداد الطلبة:
سلامة يوسف الصديق

إشراف الأستاذ
محمودي محمد البشير

لجنة المناقشة:

الاسم واللقب	الصفة	الرتبة العلمية
	أستاذ تعليم عالي	رئيسا
محمودي محمد البشير	أستاذ محاضر أ	مشرفا ومقررا
		مناقشا

السنة الجامعية: 2025 / 2026


بسم الله الرحمن الرحيم

الإهـــداء

إلى من كان لهم الفضل بعد الله في كل خطوة خطوتها... إلى من ساندوني بصمت، وشجعوني بكلمة، ودفعوني للاستمرار حين تعبت... إلى عائلتي الحبيبة، إلى والديّ العزيزين، مصدر قوتي وأمان حياتي، إلى إخوتي الذين كانوا لي دومًا سندًا ورفقةً لا تعوّض... أهديكم ثمرة هذا الجهد المتواضع، عرفانًا وامتنانًا لكل لحظة صبر، ودعاء، ومحبة قدمتموها لي.

يوسف الصديق

شكر وعرفان

بكل فخر وامتنان، نتقدم بخالص عبارات الشكر والتقدير إلى كل من كان له دور في مسيرتنا الأكاديمية، ولكل من أسهم بكلمة أو توجيه أو دعم في رحلتنا العلمية. نتوجه بأسمى معاني العرفان إلى أساتذتنا الكرام، الذين كان لهم الفضل بعد الله في بناء معارفنا وصقل مهاراتنا، ونخص بالشكر والعرفان الأستاذ المشرف محمودي محمد البشير ، الذي لم يبخل علينا بخبرته، وكان دومًا موجّهًا وداعمًا لنا خلال كل مراحل إعداد هذه المذكرة. لقد كان بحق منارة علم ورفيق درب، نستنير بإرشاداته ونسترشد بخبرته. كما نرفع شكرنا العميق إلى إدارة كلية العلوم الإنسانية والاجتماعية، من عميدها إلى كل العاملين فيها، على ما قدموه لنا من دعم وتسهيلات وبيئة تعليمية محفزة، جعلت من سنواتنا الدراسية تجربة مميزة وغنية. ولا يفوتنا أن نعبر عن امتناننا لإدارة جامعة الشهيد حمة لخضر – الوادي، التي لم تدّخر جهدًا في توفير الوسائل الضرورية لتذليل العقبات أمامنا وتحقيق بيئة جامعية تسعى دوماً نحو التقدم والتميز.

إن ما وصلنا إليه اليوم هو ثمرة تكاتفكم وجهودكم المباركة، ونأمل أن نكون على قدر الثقة والمسؤولية، حاملين ما اكتسبناه من علم نحو خدمة مجتمعنا ومساهمة فعّالة في تنميته.

ملخص الدراسة:

هدفت هذه الدراسة إلى التعرف على مستوى الوعي بالأمن السيبراني والمعلومات الرقمية لدى طلبة الإعلام والاتصال بجامعة الشهيد حمه لخضر بالوادي، مع التركيز على فهم مدى إدراكهم للمخاطر المرتبطة باستخدام التكنولوجيا الحديثة ووسائل الاتصال الرقمية، ووعيهم بكيفية حماية بياناتهم الشخصية والمهنية في الفضاء السيبراني. اعتمدت الدراسة على المنهج الوصفي التحليلي، بوصفه الأنسب لطبيعة الموضوع، وتم تصميم استمارة استبيان كأداة لجمع البيانات، وُزعت على عينة مسحية من طلبة قسم علوم الإعلام والاتصال، حيث تم اعتماد أسلوب المعاينة غير الاحتمالية القصدية في اختيار الأفراد المبحوثين.

وتكوّن مجتمع الدراسة من جميع طلبة القسم، بينما بلغت عينة الدراسة (٥٠) مفردة، تم تحليل إجاباتهم لاستخلاص النتائج والتوصيات التي ستسهم في رفع مستوى الوعي السيبراني لدى الطلبة، وتعزيز ممارسات الاستخدام الآمن للمعلومات والبيانات الرقمية.

وقد توصلت الدراسة إلى النتائج التالية:

-خلصت الدراسة إلى أن غالبية الطلبة يتمتعون بمعرفة متوسطة حول مفهوم الأمن السيبيراني.

-بينت الدراسة أن أكثر من نصف المبحوثين درجة وعيهم ضعيفة بمخاطر الأمن السيبيراني وسرقة البيانات.

-يرى أغلب أفراد عينة الدراسة أنهم لا يعرفون القوانين المحلية أو الدولية المرتبطة بالأمن السيبيراني.

-٧٨ بالمئة من المبحوثين لم يسبق لهم حضور أية ورشات تدريبية أو عمل تتعلق بالأمن السيبيراني.

-استخدام برامج الحماية مثل مضادات الفيروسات غير كافي لمواجهة المخاطر السيبيرانية بحسب أغلب أفراد العينة.

-يعتقد أكثر من نصف المبحوثين أنهم لا يولون أية ثقة بالمواقع الإلكترونية التي تطلب منهم إدخال بيانات شخصية.

-٥٨ بالمئة من افراد العينة يرون أن وسائل الإعلام ووسائل التواصل الاجتماعي هي الأداة الأكثر فعالية في نشر الوعي بالأمن السيبيراني.

-٨٠ بالمئة من الطلبة لا يستخدمون برامج حماية مرخصة لحماية بياناتهم.

-٧٠ بالمئة من الطلبة تعرضوا للفيروسات أثناء استخدامهم لتطبيقات مجهولة المصدر.

الكلمات المفتاحية: الوعي، الأمن السيبيراني، المعلومات الرقمية، طلبة الاعلام والاتصال.

Study Summary: This study aimed to assess the level of awareness regarding cybersecurity and digital information among media and communication students at El Oued University (Université El Chahid Hamma Lakhdar). It focused on understanding their perception of the risks associated with modern technology and digital communication tools, as well as their awareness of how to protect their personal and professional data in cyberspace.

The study adopted a descriptive-analytical approach, deemed most suitable for the subject matter. A questionnaire was designed as the primary data collection tool and distributed to a purposive non-probability sample of students from the Department of Media and Communication Sciences.

The study population comprised all students in the department, while the sample consisted of 50 respondents. Their responses were analyzed to derive findings and recommendations aimed at enhancing students' cybersecurity awareness and promoting safe practices in handling digital information.

The study reached the following results:

-The majority of students demonstrated moderate knowledge of the concept of cybersecurity.

- Over half of the respondents exhibited low awareness of cybersecurity risks and data theft.

- Most participants reported no familiarity with local or international laws related to cybersecurity.

- 78% of respondents had never attended any training workshops or activities on cybersecurity.

- According to most participants, using protective software (e.g., antivirus programs) alone is insufficient to counter cyber threats.

-More than half of the respondents stated they do not trust websites requesting personal data.

-58% believed that media and social media platforms are the most effective tools for raising cybersecurity awareness.

Keywords: Awareness, Cybersecurity, Digital Information, Media and Communication Students

فهرس المحتويات

فهرس الجداول

فهرس الأشكال

14	شكل بياني يمثل توزيع أفراد العينة حسب حضورك لدورات أو ورش عمل تتعلق بالامن السيبيرني	
15	شكل بياني يمثل توزيع أفراد العينة حسب الجهة المسؤولة عن حماية الافراد من الهجمات السيبيرانية	
١٦	شكل بياني يمثل توزيع أفراد العينة حسب التوعية القانونية اللازمة لحماية الأفراد من الهجمات السيبيرانية	
١٧	شكل بياني يمثل توزيع أفراد العينة حسب اهم وسيلة لحماية الأفراد من الهجمات السيبيرانية	
١٨	شكل بياني يمثل توزيع أفراد العينة حسب استخدام برامج الحماية	
١٩	شكل بياني يمثل توزيع أفراد العينة حسب كيفية حماية البيانات الشخصية	
٢٠	شكل بياني يمثل توزيع أفراد العينة حسب مدى ثقتك في المواقع الالكترونية	
٢١	شكل بياني يمثل توزيع أفراد العينة حسب دور الحكومات في حماية المستخدمين من الهجمات الالكترونية	
22	شكل بياني يمثل توزيع افراد العينة حسب موثوقية الروابط الالكترونية	
٢٣	شكل بياني يمثل توزيع افراد العينة حسب الوسيلة الأكثر فعالية في نشر الوعي	

مـقـدمـة عـــــامة

أدت الثورة الرقمية المعاصرة إلى تطورات هائلة غير مسبوقة، شملت جميع مجالات النشاط الإنساني العلمية والتربوية والسياسية والاقتصادية. ومن أهم إفرازات هذه الثورة ما يعرف بالفضاء السيبراني، الذي ساهم في تكوين العلاقات الاجتماعية في حدود المجتمع الافتراضي الذي تغلب على الحدود والحواجز والاختلافات الثقافية والعرقية والدينية بين الجماعات. وعلى المستوى التعليمي أصبح الفضاء السيبراني وسيلة تعليمية يمكن للطلبة اللجوء إليها لمساعدتهم في أداء واجباتهم.

وعلى الرغم من الإيجابيات التي يحملها الفضاء السيبراني إلا أنه يقبع خلفه واقع افتراضي مخيف؛ إذ يسكن المجرمون وتجار المخدرات ومنظمات الإرهاب واللصوص، والمتنمرون الأمر الذي شكل مصدر تهديد المستخدمي الشبكة العنكبوتية، عبر ما يعرف بالهجمات السيبرانية أو الجرائم السيبرانية التي يمكن من خلالها إيقاع خسائر فادحة، قد يصل إلى التلاعب بالبيانات أو تزييفها، أو محوها من أجهزة الحواسيب.

وتزداد خطورته في أنه يعرض خصوصية الأفراد للاختراق وشخصيتهم للابتزاز، وارتكاب بعض السلوكيات والانحرافات بالإضافة إلى بعض التهديدات والقرصنة، والمواد الإباحية، وسرقة الهوية، ناهيك عن الآثار السلبية مثل الاكتئاب والقلق والكثير من الأضرار الصحية والجسمية والاجتماعية.

في سياق ذلك؛ ظهر ما يعرف بالأمن السيبراني الذي يهدف إلى حماية البيانات التي تخص الأفراد والمؤسسات في العالم وحماية أجهزة الكمبيوتر والشبكات والبرمجيات من الوصول غير المصرح به أو الهجمات التي تهددها .

وأصبح حديث العالم بأسره، وأصبح جزءا أساسيا من أي سياسات أمنية واقتصادية أو سياسية أخرى، حيث يلامس اهتمام كل من له علاقة بالعالم الرقمي، سواء كان من الأفراد أو المنظمات أو الحكومات، لذلك بات من الأهمية بمكان تحقيق الأمن السيبراني من خلال استخدام الآليات والوسائل الممكنة التي تساعد على تحقيقه .

وظهرت الحاجة إلى رفع مستوى الوعي بالأمن السيبراني لتثقيف الطلبة، لتحسين إجراءات الأمان التفاعلية والاستباقية للحد من اختراق البيانات الشخصية، أو مشاركها دون حماية كافية حيث يواجه الطلبة انتهاكات كبيرة في الخصوصية.

وأصبح من الضروري تطوير الوعي الأمني السيبراني لدى الطلبة، وإدراج موضوع الأمن السيبراني في المناهج المدرسية، وتوجيه الطلبة لاستخدام الكمبيوتر والإنترنت بطريقة آمنة، واتخاذ التدابير الأمنية اللازمة بما يتوافق مع المتغيرات التقنية المتسارعة في ضوء حاجات المتعلمين وخبراتهم، وذلك للتقليل من خطورة الهجمات السيبرانية في المؤسسات التعليمية، حيث إن الوعي بالأمن السيبراني يعمل على حماية البيئة الرقمية وجعلها آمنة قادرة على التصدي لجميع هجمات وجرائم الفضاء السيبراني بمختلف أشكالها.

وسوف نتناول في هذه الدراسة:"الوعي بالأمن السيبيراني والمعلومات الرقمية لدى طلبة الإعلام والاتصال بجامعة الوادي"

وقد قسمنا دراستنا هذه إلى فصلين كل فصل يحتوي على مجموعة من العناصر وهي بالترتيب كما يأتي:

قمنا في البداية بالتطرق إلى مقدمة عامة ثم طرح إشكالية الدراسة مع تساؤلاتها، وتطرقنا أيضا إلى الأسباب التي جعلتنا نختار الموضوع، بالإضافة إلى أهمية الدراسة وأهدافها وقمنا بتحديد المفاهيم ومصطلحات الدراسة.

في الفصل الأول المعنون بالأدبيات النظرية والتطبيقية قمنا بتقسيمه إلى ثلاثة مباحث حيث تطرقنا في المبحث الأول إلى ماهية الأمن السيبيراني من مفاهيم وخصائص وأنواع وغيرها .. كما كان المبحث الثاني معنون بماهية المعلومات الرقمية ، ليأتي المبحث الأخير الذي عرجنا فيه إلى الدراسات السابقة.

في الفصل الثاني المعنون بالإطار الميداني شمل هذا الفصل الإجراءات المنهجية كنوع الدراسة والأدوات المستعملة في جمع البيانات، وصولا إلى إجراءات الصدق والثبات، كما تم عرض وتحليل ومناقشة نتائج الدراسة ، وصولا إلى الاستنتاجات العامة.

١-إشكالية الدراسة :

في عصر الفضاء الإلكتروني وشبكات التواصل الاجتماعي والتطبيقات الحاسوبية سريعة التطور، أحتلت المعلومات موقعا مميزا من اهتمام العالم الرقمي على الأصعدة المختلفة الاجتماعية والسياسية والاقتصادية والتربوية والعلمية وغيرها، ولم يعد من الممكن السماح بالمخاطرة بدقة هذه المعلومات أو صحتها أو سهولة تدفقها، أو السماح بمعرفتها أو الاستيلاء عليها من غير الأطراف المعنية، وبات من الضروري اتخاذ كافة الوسائل التي تُؤمن فيها معلومات وبيانات الأفراد ويتم فيها حماية الأنظمة الحاسوبية من أي اختراقات تحول دون تأدية عملها بالطريقة المطلوبة، ولذا لم يعد الأمن مرتبط فقط بالمعنى التقليدي المعروف بل أصبح للأمن السيبراني أهمية كبيرة لأي شخص في المجتمع ما دام يتعامل مع الشبكة الإلكترونية وتطبيقاتها.

كما أدت التطورات الهائلة والمتلاحقة في التكنولوجيا الاتصال والمعلومات إلى إمكانية تحويل المعطيات فروع المعرفة المختلفة إلى معلومات رقمية يسهل الحصول عليها وتخزينها، واسترجاعها ونقلها من جهاز لأخر بغير عناء، واستخدمها بتكاليف قليلة وفي وقت قصيرة للغاية، كما أنها توفر العديد من الخدمات لمستخدميها منها البريد الإلكتروني للاتصال والتواصل والاستفادة من الرسائل العلمية والكتب والمعلومات، ونقل التكنولوجيا للمجتمعات النامية التي في طريق التقدم، والاستفادة من المنجزات العلمية وغير ذلك من المجالات التي يستفيد منها الإنسان في مجالات حياته. وبالرغم من التطور الهائل لتكنولوجيا أصبح من السهل التلاعب بها بشكل اكبر مما كانت عليه لكن كل فرد منا محاط بالتكنولوجيا ويستخدمها بالفعل مع قدرة جزء كبير من المستخدمين أيضا على التعديل في تلك التكنولوجيا بخدمة أغراضهم وحماية خصوصياتهم بشكل أفضل ، ولقد أصبح الأمن السيبراني حديث العالم بأسره، بل وأصبح جزاء أساسيا من أساسيات أمنية واقتصادية، حيث أصبح صناع القرار في مختلف الدول

ومن هنا ظهرت أهمية الأمن السيبراني في توفير أمن المعلومات وبدأت الدول تهتم بتطوير الأمن السيبراني بهدف التخفيف من مخاطر إختراق المعلومات والهجمات الالكترونية ، وتعمل الكثير من المنظمات الدولية لمواكبة الاهتمام بشأن أمن الفضاء السيبيري والشباب والطلبة الجامعيين على وجه الخصوص يشكلون ثروة الأمم ويشكل وعيهم نقطة أساسية في تجنب المخاطر.

ومن هنا تبرز أهمية مشكلة البحث، والتي جاءت لمعرفة مستوى وعي الطلبة بمفهوم الأمن السيبراني وإجراءاته لحماية أنفسهم، ومن ثم القيام بدورهم الفعال في تقليل الجرائم الإلكترونية إلى أقصى حد ممكن في المجتمع. وبذلك فقد تحددت مشكلة الدراسة في التساؤل الرئيس كالتالي : **هل لطلبة قسم الإعلام والاتصال بجامعة الوادي وعي بموضوع الأمن السيبيراني والمعلومات الرقمية ؟**

وتتفرع من هذه الإشكالية التساؤلات الفرعية الأتية :

أ ماهي درجة وعي الطلبة بمفهوم الأمن السيبيراني ؟

ب ما مدى اطلاع الطالب الجامعي على القوانين والنظم التي تواجه مخاطر الامن السيبيراني ؟

ت ماهي طرق وأساليب مواجهة الأمن السيبيراني بحسب تصورات مجتمع البحث ؟

ث مدى استخدام الطالب الجامعي لتطبيقات الحماية المحترفة المرخصة لحماية البيانات ؟

٢-أسباب اختيار الموضوع :

١-٢ أسباب ذاتية:

-رغبتنا في معرفة إدراك الطلبة بالأمن السيبراني ومعرفة المشكلات التي نلاحظها معا لزملاء حول انتهاكات المعلومات الرقمية والبيانات لشخصية.

-الميل الشخصي نحو دراسة ومعرفة عمليات الاختراق لدى بعض الحسابات الشخصية في شبكات التواصل الاجتماعي.

-اهتمامنا بالمواضيع المتعلقة بالأمن السيبراني والجرائم الالكترونية.

٢-٢ أسباب موضوعية:

-التطور التكنولوجي وما نتج عنه من انتشار الجرائم الالكترونية على المستوى الداخلي والخارجي.

-مشاكل المستخدمين نظرا للاستفزاز المرتبط بخصوصيتهم عبر مواقع التواصل الاجتماعي.

-قلة الدراسات التي عالجت موضوع الوعي بالأمن السيبراني وانتهاك المعلومات الرقمية عبر شبكات التواصل الاجتماعي بجامعة الشهيد حمه لخضر بالوادي.

٣- أهداف الدراسة :

في إطار إنجازنا للبحث العلمي المتعلق بموضوع الوعي بالأمن السيبيراني والمعلومات الرقمية لدى طلبة الإعلام والاتصال بجامعة الوادي بحيث تصاغ الأهداف المتعلقة بهذا الموضوع كما يلي:

-وعي الطالب الجامعي بمفهوم الأمن السيبراني وحماية البيانات الرقمية.

-استكشاف مدى التهديدات والاختراقات التي تواجه المستخدمين في الفضاء الإلكتروني.

-تسلط الدراسة الضوء على القوانين والتشريعات المعنية بمكافحة مخاطر الأمن السيبراني.

-تهدف هذه الدراسة إلى إبراز أهمية الإجراءات الوقائية والاستراتيجيات اللازمة لضمان خصوصية المستخدمين وحمايتهم من التهديدات الرقمية.

٤- أهمية الدراسة :

-رفع درجة الوعي لدى الطلبة الجامعيين بخصوص الأمن السيبراني، وأهمية الالتزام بمفاهيم الأمن السيبراني عند التعامل مع مصادر المعلومات المختلفة.

-العمل على توجيه اهتمام الباحثين لتناول موضوع الأمن السيبراني، والذي لم يحظ بالاهتمام الكافي من قبل الباحثين، على الرغم من أهميته في عصر المعلوماتية.

-تساعد هذه الدراسة على توضيح أهمية الأمن السيبراني في عصر التحول الرقمي.

-تعزيز الوعي لدى الطلبة الجامعيين بأهمية اتباع أسس ومبادئ الأمن السيبراني في حياتهم الأكاديمية والمهنية، وتوضيح تأثير ذلك على سلامة البيانات الشخصية والمؤسساتية.

٥- تحديد ومفاهيم ومصطلحات الدراسة :

١-٥ الوعي :

لغويا: ورد في المعجم الوجيز أن الوعي يُطلق على معان عدة: الحفظ والفهم والإدراك والقبول، يقال: وعى الشيء يعيه وعيًا أي حفظه وقبله فهو واع، ووعى الأمر: أي أدركه على حقيقته، وعلى ذلك فإن الوعي يتضمن جانبين اثنين، أحدهما معرفي يتمثل في الحفظ والفهم، والثاني سلوكي يتمثل في التطبيق العملي لما تم حفظه وفهمه ويشير قاموس (أكسفورد) إلى أن الوعي هو الأساس الأكثر أهمية في مواجهة الحقيقة الخارجية.

اصطلاحا: يعرف الوعي المجتمعي بأنه "إدراك الإنسان لذاته، ولما يحيط به إدراكًا مباشرًا، وهو أساس كل معرفة، كما يشير الوعي إلى الفهم وسلامة الإدراك، أي إدراك الإنسان لنفسه وللبيئة المحيطة به، ولعل هذا يعني فهم الإنسان لذاته وللآخرين عند تفاعله معهم سعيا لإشباع حاجاته، وقضاء مصالحه وهو مدرك للعلاقات بينه وبين الآخرين والبيئة من خلال المواقف المختلفة".[١]

إجرائيا : التصور الفكري والصورة الذهنية التي يحملها طلبة الاعلام والاتصال عن الجوانب المختلفة ذات الصلة بالأمن السيبراني وطرق الوقاية من جرائم الفضاء السيبراني.

٢-٥ الأمن السيبيراني :

هو اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستخدمة تقنيا وتنظيميا وإداريا في منع الوصول غير المشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية ونظامية.[٢]

إجرائيا : الأمن السيبراني هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تهدف إلى الوصول غير المصرح به أو التدمير أو التعديل أو التعطيل.

٣-٥ المعلومات الرقمية : تشير المعلومات الرقمية إلى البيانات التي تتم معالجتها وتخزينها بواسطة الأجهزة الإلكترونية والحواسيب. يتم تمثيل هذه البيانات بنظام عددي، حيث تُحوَّل المعلومات (سواء كانت نصوصا، صورا، صوتيات، أو فيديوهات) إلى شكل رقمي يمكن معالجته إلكترونيا، مما يُسهل نقلها وتخزينها وتحليلها بوسائل تقنية متقدمة.[٣]

---

[١] سعود شباب سدر العتيبي : مدى توفر الوعي بالأمن السيبيراني لدى أفراد الأسر في المجتمع السعودي –دراسة استطلاعية– المجلة الدولية لنشر البحوث والدراسات، جامعة الملد عبد العزيز السعودية ، المجلد ٠٣، يناير ٢٠٢٢ ، ص ٠٦،٠٥.

[٢] منى عبد الله السمحان : متطلبات تحقيق الأمن السيبراني في للانظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية جامعة المنصورة ع١١١ يوليو ٢٠٢٠ ص٩.

[٣] منى عبد الله السمحان : مرجع سابق ، ص١٠.

إجرائيا: هي أي بيانات أو محتوى تخص الطالب الجامعي يتم إنشاؤه، تخزينه، أو نقلها باستخدام الأجهزة الإلكترونية والأنظمة الرقمية، مثل النصوص، الصور، الفيديوهات، أو الملفات الصوتية.

٦- المنهج المستخدم وأدواته :

١-٦ المنهج المستخدم:

هو الطريق المؤدي إلى الكشف عن الحقيقة في العلوم بواسطة طائفة من القواعد العامة التي تهيمن على سير العقل وتحديد عملياته، يصل إلى النتائج المعلومة.[١]

ولقد اقتضت دارستنا إلى استخدام المنهج المسح الوصفي بغية تحقيق أهداف الدراسة وإعطاء لمحة على موضوع دراستنا المتعلقة بشأن وعي وإدراك الطالب الجامعي بالأمن السيبراني والمعلومات الرقمية.

إذ يعرف المنهج المسح الوصفي بأنه أسلوب من أساليب التحليل المرتكز على معلومات كافية ودقيقة عن ظاهرة أو موضوع محدد عبر فترة أو فترات زمنية معلومة وذلك من اجل الحصول على نتائج علمية تم تفسيرها بطريقة موضوعية تنسجم مع المعطيات الفعلية للظاهرة.[٢]

٢-٦ أدواته :

لقد اعتمدنا في موضوع دراستنا على أداة الاستبيان، فهو من أدوات البحث المهمة والشائعة استعمالها في ميدان العلوم الإنسانية وخاصة علوم الإعلام والاتصال. وتعد استمارة البحث من أكثر أدوات جمع البيانات شيوعا في البحوث الاجتماعية، هذا ما يدفع الباحث إلى بذل الجهد من اجل صياغة استمارة البحث بصورة تؤدي إلى تحقيق أهداف الدراسة.[٣]

كما كانت الملاحظة إحدى أدوات جمع البيانات التي اعتمدنا عليها، وتعني الانتباه والنظر لشيء ما وهي أداة من أدوات البحث العلمي تجمع بواسطتها المعلومات التي تمكن الباحث من الاجابة عن أسئلة البحث واختبار فروضه. وتعرف أيضا بأنها التنبه للظواهر أو الحوادث بقصد تفسيرها واكتشاف أسبابها وعواملها والوصول إلى القوانين التي تحكمها.[٤]

واستخدمنا الملاحظة تلقائيا في الظروف الطبيعية للظاهرة كاستطلاع أولي من خلال معاينة تزايد ظاهرة نقص الوعي بالأمن السيبيراني لدى الطلبة الجامعيين.

---

[١] عبد الرحمن بدوي مناهج البحث العلمي وكالة المطبوعات، الكويت ١٩٧٧،ص١-٥

[٢] فارس رشيد البياتي، الحاوي في مناهج البحث العلمي، دار السواقي العلمية، ط ١ ، عمان ٢٠١٨، ص٩٣

[٣] حمد مرسلي، مناهج البحث العلمي في علوم الاعلام والاتصال، ديوان المطبوعات الجامعية، ط ٤ ، الجزائر ٢٠١٠ ص ٢٢٠.

[٤]عبد الله باشيوة وآخرون: البحث العلمي مفاهيم. أساليب. تطبيقات، الوراق للنشر والتوزيع، الأردن، 2009، ص378.

٧- مجتمع البحث وعينته:

يعرف مجتمع الدراسة بـ المجتمع الاحصائي الذي تجرى عليه الدراسة ويشمل كل أنواع المفردات مثل الأشخاص، السيارات، الشوارع.. الخ. وحسب قراوتز فإن مجتمع البحث هو مجموعة منتهية أو غير منتهية من العناصر المحددة مسبقا والتي ترتكز عليها الملاحظات وهو مجموعة عناصر لها خاصية، عدة خصائص مشتركة تميزها عن غيرها من العناصر الأخرى والتي يجرى عليها البحث.[١]

وعليه يكون مجتمع بحثنا لهذه الدراسة هو طلبة وطالبات قسم الاعلام والاتصال بجامعة الوادي ، وكان اختيارنا لهذا المجتمع مبنيا على مجموعة من الاعتبارات والمتمثلة في امكانية الوصول إلى المجتمع المتناول بالدراسة، ومنه القدرة على التعامل معه ميدانيا.حيث بلغ حجم العينة ٥٠ مفردة ، تم اختيارهم بأسلوب العينة القصدية وهي عينة يتم اختيارها على أساس من الخبرة السابقة فقد يلاحظ الباحث من الدراسات السابقة أن مجموعة من المفردات يتمثل فيها من الخصائص ما يجعل نتائجها قريبة من المجتمع ككل، ومن الملاحظ أن العينة القصدية هي أكثر العينات استخداما نظرا لسهولة الوصول إلى المفردات بالإضافة إلى اعتقاد الباحث بأن هذه المفردات تحديدا هي الأقدر على تزويده بالبيانات التي يحتاجها في دراسته.

---

[١] منى عبد الله السمحان : مرجع سابق ، ص١٢.

الأدبيات النظرية والتطبيقية

المبحث الأول: ماهية الأمن السيبيراني

المطلب الأول: مفهوم الأمن السيبيراني

يعد مفهوم الأمن السيبراني مفهوماً حديثاً جاء متزامناً مع الثورة الرقمية التكنولوجية العالمية التي هددت أمن الإنسان الإلكتروني الذي أصبح يعتمد اعتماداً أساسيًا على الإنترنت في جميع احتياجاته الفكرية والروحية والجسدية.

وحسب تعريف الهيئة العالمية للأمن السيبراني فإن الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك".

وتعرف صائغ الأمن السيبراني باعتباره "مجموعة الإجراءات التقنية والإدارية التي تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به للتجسس أو الاختراق لاستخدام أو الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات، كما تضمن تأمين وحماية وسرية وخصوصية البيانات الشخصية للمواطنين، كما تشمل استمرارية عمل حماية معدات الحاسب الآلي سوء ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف".

ويفيد المختصون بأن كلمة (سيبراني) هي ترجمة حرفية لكلمة (Cyber) وهي كلمة يونانية الأصل تعني التحكم أو التواصل، وتستخدم للإشارة إلى تواصل الآلات مع غيرها من الأجهزة والكائنات، وتحكمها ببعضها البعض. كما عُرف بأنه: "فن وجود واستمرارية مجتمع المعلومات من خلال ضمان وحماية المعلومات وأصولها وبنيتها التحتية في الفضاء السيبراني".

وعرف أيضا بأنه أمن الشبكات ، والأنظمة المعلوماتية، والبيانات والمعلومات، والأجهزة المتصلة بالإنترنت، وعليه فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها أو الالتزام بها، لمواجهة التهديدات ومنع التعديات، أو للحد من آثارها في أقسى وأسوأ الأحوال.[1]

---

[1] ماجد عبد الله الحبيب : درجة الوعي بالأمن السيبراني لدى طالب وطالبات الدراسات العليا بكلية التربية بجامعة الامام محمد بن سعود ، وسبل تعزيزهم من وجهة نظرهم، السعودية ، ٢٠١٨، ص ١٠-١١.

المطلب الثاني: تاريخ ظهور الأمن السيبيراني

تعود بدايات الأمن السيبراني إلى أواخر الأربعينات من القرن الماضي وبالتحديد عام ١٩٤٩ ، عندما قام العالم الأمريكي المجري جون فون نيومان بالتنبؤ بإمكانية تناسخ برمجيات الحاسوب أو إ عادة إنتاج نفسها. و بعد)١٨ (ً عاما جرت أول عملية اختراق حيث كان ً مسموحا للطلبة الوصول إلى جزء محدود من النظام، حيث قام مجموعة من طالب الثانوية باستخدام حواسيبهم بتعلم لغة الحاسوب، و استطاعوا الوصول إلى النظام بالكامل. وفي السبعينات من القرن الماضي قام بوب توماس باختراع أول فيروس وكان يسمى الزاحف أو Creeper، ثم جاء بعده المبرمج الشهير اري توم لينسون مخترع البريد الإلكتروني، ليخترع أول برنامج مضاد للفيروسات للقضاء على فيروس الزاحف ً ض (Creeper ،(و في أواخر السبعينات ا، من القرن الماضي أي قام كيفين متينيك أحد مخترقي الأنظمة في العالم وهو في سن)١٦ (ً عاما باختراق حاسوب شركة برمجيات.

و في النهاية ألقي القبض عليه وسجنه كمنفذ أول الهجمات الإلكترونية، أما في عام ١٩٨٦ قام الهاكر الألماني ماركوس هس باختراق حواسيب عسكرية تابعة لوزارة الدفاع الأمريكية، وكان على وشك بيع البيانات والمعلومات السرية للمخابرات السوفيتية، لوال أن تم القبض عليه، أما في عام ١٩٨٨ فكان أول دودة موريس تصيب الأجهزة المتصلة بالإنترنت حول العالم، وهكذا استمر تطور الهجمات والجرائم الإلكترونية، وتطور معها الأمن السيبراني حتى وصل إلى التقدم والتطور الذي نعيشه اليوم، وجاء مصطلح الأمن السيبيراني من لفظ السيبر Cyber اللاتينية، ومعناها الفضاء المعلوماتي وهو تعبير يصف جميع الأمور المتعلقة بحماية البيانات والمعلومات والأجهزة باستخدام آليات وتجهيزات وتطبيقات وبرمجيات من خلال شبكات الحواسيب والاتصالات والإنترنت.[١]

وظهر أول فيروس رقمي في سبعينيات القرن العشرين على شبكة "أربانت"، إحدى أوائل الشبكات في العالم لنقل البيانات باستخدام تقنية تبديل الرزم، وكان على شكل رسالة نصية بسيطة لم تتسبب بأضرار تقنية لكنها دفعت إلى اتخاذ تدابير وقائية. وفي عام ١٩٨٣، طوّر معهد ماساتشوستس للتقنية نظام اتصالات يعتمد على التشفير، أصبح أساسا لتطوير تقنيات الأمن السيبراني الحديثة. وشكل ظهور الإنترنت ثورة نوعية في حياة البشرية، إذ بدأ استخدامه في المجالين الأمني والعسكري وتسابقت الدول في تطويره مع مطلع تسعينيات القرن العشرين، حتى سميت تلك الفترة بـ"الحرب السيبرانية الباردة" أو "سباق التسلح السيبراني"، وظهرت حينئذ هجمات التصيد الاحتيالية "فيشينغ" والتجسس الإلكتروني و"الهجوم الموزع لحجب الخدمة" (دي دي أو إس). وظهرت الحاجة دوليا إلى وجود قوة غير مادية إلى جانب

---

[١] عبير أحمد عبد الرحمان : درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك، مجلة الزرقاء للبحوث والدراسات الإنسانية-المجلد الثالث و العشرون -العدد الثالث- ٢٠٢٣، ص١٢.

القدرات العسكرية والاقتصادية، فبدأت الدول تولي اهتمامها بالقوة السيبرانية لتأثيرها على المستويين المحلي والدولي.

ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي، واعتبار عدد من الباحثين الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، ظهرت الحاجة لتوفير ضمانات أمنية، خاصة مع بداية ظهور التهديدات والجرائم السيبرانية مع دخول القرن الـ٢١. ودخل الأمن السيبراني ضمن حقل الدراسات الأمنية، وظهرت تقنيات متطورة مثل التشفير والأمان السحابي والكشف عن التهديدات بالذكاء الاصطناعي، ومع ذلك فإن الهجمات السيبرانية مجال معقد وسريع التطور، مما يستلزم استجابات أمنية سريعة تضاهي وتيرة نموه السريع.[1]

المطلب الثالث: خصائص الأمن السيبيراني

1- الثقة وعدم الثقة :

يمتلك جدار الحماية الخاص بنظام الأمن السيبراني بما يشبه مرشح إلكتروني لنوع وطبيعة البرامج والتقنيات المسموح بتفعيلها بحيث يسمح بمرور البرامج التي بالفعل تمتلك الثقة من المستخدم وكذلك المتجر الإلكتروني وتم التأكد من أمان استخدامها ومنع البرامج الخبيثة من التطفل أو استغلال الثغرات يمكن ترجمة فلسفة أمن المعلومات في هذه النقطة كون الأمن السيبراني يتعامل مع كافة البرامج كونها برامج غير جديرة بالثقة، حتى يتم السماح لها من قبل المستخدم والتأكد من أمانها من خلال مصداقيتها في المتاجر الإلكتروني، فيسمح بمرور ما تم التأكد من سلامته، ويمنع المصادر المجهولة من اختراق النظام

2- الحماية من التهديدات الداخلية:

واحدة من أهم خصائص الأمن السيبراني هو حماية الجهاز من التهديدات الداخلية والتي قد تتم بناء على قلة ثقافة المستخدم أو جهله بمجال أمن المعلومات وفيه قد يقوم بالسماح ببرامج مجهولة المصدر أن يتم تفعيلها أو أن يقوم باستخدام أدوات تمس أمنه الشخصي أو حساسية مشاركة ما يملكه من معلومات، أو تحتوى إحدى الأدوات التي يقوم باستخدامها بفيروس خبيث لا يجب أن يحتوي نظامه عليه، حينها يقوم الأمن السيبراني بسرعة تنبيه الفرد أو المؤسسة بالخطر التي تواجهه ويقوم بمنع حدوث هذا الإجراء في أسرع وقت .

3- الحماية من التهديدات الخارجية:

تمثل خاصية الحماية من التهديدات الخارجية أهم صفات الأمن السيبراني، حيث يتم فيها بناء جدار

---

[1] سليم عبد الرحمان : الأمن السيبراني مفهومه وتاريخه، موقع الجزيرة للدراسات،١٩ سبتمبر٢٠٢٤،متاح على الرابط : https://www.aljazeera.net/encyclopedia/2024/9/19/ ، ٢٦ فيفري ٢٠٢٥.

الحماية قادر على تصفية المخاطر الخارجية التي يسفر عنها التعامل مع العالم الرقمي، بداية من مخاطر الرسائل الإلكترونية الخطرة أو الروابط الخبيثة أو الفيروسات أو معالجة الضعف في النظام أو الثغرات التي قد يستغلها طرف ثالث في السيطرة والتحكم.

4-رؤية شاملة:

تقوم الادوات الخاصة بالأمن السيبراني على منح مستخدميها-أفراد كان أو شركات-رؤية شاملة على ما يحتويه أنظمتهم من نقاط قوة وضعف، بحيث يمكنهم معرفة الثغرات التكنولوجية والعمل على حلها بأسرع وقت، مع منحهم اقتراحات تخص الطريقة المثالية لمنع تكراره مرة أخرى.

5-مراقبة مستمرة:

يقوم الأمن السيبراني على خاصية المراقبة المستمرة، حيث لا تقوم جدار الحماية الخاص به بالعمل لمرة واحدة أو في ساعات معينة، بل النظام يعمل طوال الوقت بهدف اكتشاف أي خلل بمجرد وجوده والعمل على سرعة إصلاحه ومنعه من إحداث أي ضرر والحفاظ على أمن المعلومات والأمن الخاص بالمستخدم لأطول فترة ممكنة.

6-الامتثال للسياسات والقوانين:

الهدف من الأمن السيبراني في المقام الأول هو الحفاظ على سرية وخصوصية البيانات والمعلومات، بالإضافة إلى مكافحة الفيروسات الضارة بجميع أنواعه، ولكى يتم تحقيق هذا الهدف بفعالية لا يجب أن يتم استغلال الصلاحيات التي تمنح لمحترفيه في سبيل اختراق القاعدة التي من أساسها تم إنشائه.

لذلك تعد خاصية الامتثال للقوانين والسياسات التشريعية الخاصة بأمن المعلومات واحدة من أهم خصائص الأمن السيبراني، حيث لا يتاح لمصادر خارجية الاطلاع عما يتم مشاركته من معلومات وبيانات حساسة، أو إساءة استغلالها بأي صورة ممكنة، وتتنوع هذه القوانين طبقًا لنوع وطبيعة المجال الذي يتم فيه تطبيق الحماية السيبرانية.

7-التنوع:

يجب أن يمتلك النظام الخاص بالأمن السيبراني حلول مجمعة تتعلق بالتعامل مع التهديدات السيبرانية بحيث لا يكون النظام مفعل للحماية من نوع معين من التهديدات والسماح بأخر، بل عليه أن يحلل ويكتشف ويتعامل ويمنع كل أنواع الهجمات الممكنة والتي تشكل تهديدًا على سلامة وأمن المعلومات.[1]

---

[1] إسماعيل باباكر: خصائص الأمن السيبراني ، موقع الوطن اليوم ، ١٤ يوليو ، ٢٠٢٣، متاح على الرابط : https://alwatannewssd.com/56117/ ، ٢٦ فيفري ٢٠٢٥.

المطلب الرابع: أنواع الأمن السيبيراني

١-أمن الشبكات : عندما يتعلق الأمر بحماية البنية التحتية لشبكات الحاسوب والأجهزة المتصلة بها من أيّ تهديدات وهجماتٍ سيبرانية يأتي دور أمن الشبكات؛ إذ يُوفر حماية شاملة لهذه الشبكات من الوصول غير المصرّح به، أو الهجمات والاختراقات السيبرانية، سواءً كانت شبكة منزلية بسيطة تُستخدم للاتصال بالإنترنت، أو شبكة أكبر تُستخدم في الأماكن العامة والمؤسسات والشركات.

كما يشمل أمن الشبكات بالتأكيد حماية أنظمة التشغيل فيها، والخوادم، وأجهزة الشبكة ككل، مثل أجهزة التوجيه (الراوتر)، ومنع الوصول غير المصرح به إليها، أو انقطاع الخدمة بسبب البرامج الضارة أو الاختراقات، وذلك من خلال الحلول الأمنية المختلفة، ومن أهمها جدران الحماية.

٢الأمن السحابي : تُعد كل من منصة جوجل السحابية "Google Cloud" ومايكروسوفت أزور "Microsoft Azure" وحتى خدمات أمازون ويب "Amazon Web Services" من أضخم الخدمات السحابية التي تُتيح للمستخدم تخزين بياناته بكل سهولة في الخوادم الخاصّة بها، وما يضمن أمان البيانات وحمايتها في تلك الأنظمة هو بالتأكيد الأمن السيبراني؛ إذ يهتم بتشفير البيانات في السحابة وتطبيق ضوابط أمنية للتأكد من هوية المستخدم، وكذلك تطبيق العديد من أنظمة الحماية للبنية التحتية الخاصّة بها.

٣-أمن التطبيقات : في كل مرّة يجري فيها تصفّح الإنترنت أو استخدام أحد التطبيقات على الهاتف الذكي أو جهاز الحاسوب تكون هناك احتمالية للتعرّض للعديد من التهديدات الأمنية، لكن لا داعي للقلق؛ فالأمن السيبراني المختص بأمن التطبيقات يُوفّر الحماية اللازمة؛ إذ يمنع وصول أيّ استخدام غير مصرّح به إلى هذه التطبيقات والبيانات المرتبطة بها.

٤-أمن المعلومات : يهدف هذا النوع بشكلٍ رئيسي إلى حماية المعلومات الرقميّة الخاصّة بالشركات والمؤسسات في مكان العمل، بما في ذلك البيانات المخزّنة في قواعد البيانات، والملفات والوسائط الرقمية المختلفة والخاصّة بها؛ إذ تكمن أهمية الأمن السيبراني في حماية هذه المعلومات وسلامتها من أيّ اختراقات، من خلال استخدام آليات التحكّم بالوصول، مثل: كلمات المرور، أو المصادقة الثنائية، بالإضافة إلى التشفير، وإجراء عمليات النسخ الاحتياطي. ٥-أمن المستخدم النهائي : جهاز الحاسوب الخاصّ والهاتف المحمول وأيّ جهاز لوحي آخر يُستخدَم جميعها تُعد الهدف الأول للكثير من الهجمات الإلكترونية؛ لأنّها ببساطة تُمكّن المتسللين من الوصول بسهولة إلى المعلومات التي يُريدونها عن المستخدم.[١]

---

[١] هالة كمال : أنواع الأمن السيبراني ومجالات تطبيقه والتحديات التي يواجهها ، مجلة الشارقة،م١، العدد ٢٣ يوليو ٢٠٢٤، ص ٥٤.

المطلب الخامس: أهمية وأهداف الأمن السيبيراني

أ/الأهمية:

يظهر جليا الأهمية الأمنية لحماية المعلومات ومصادرها والأنظمة المرتبطة بحفظها وصيانتها واسترجاعها، وهذا ما نلمسه في العناصر التالية:

-السلامة: أي سلامة البيانات والمعلومات وحمايتها من أي هجوم أو خرق أو قرصنة. السرية: تكون كل المعطيات والبيانات والمعلومات في مأمن وغير مرخص أو مسموح لأي كان من الولوج إليها.

-الجاهزية: طالما أنها آمنة ومحمية فهي متاحة وجاهزة للاستعمال حسب الطلب والاتاحة فأهمية الأمن السيبراني تكمن في العديد من الفوائد والميزات أهمها: التقليل من مخاطر التهديدات الأمنية والاختراقات المحتملة للبيانات إلى جانب الحفاظ على سرية المعلومات.

-احلال الحماية الأمنية اللازمة للملفات الشخصية والحساسة لمنع الوصول غير المصرح إليها.

-ضمان استمرارية عمل المؤسسات المؤمنة وتجنب تعطيل مصالحها المتصلة بالاستخدام السيبراني لشبكة الانترنت مع تقليل وقت التوقف عن الخدمات الرقمية خاصة الحساسة منها.[1]

ب/الاهداف:

- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات، وما تحتويه من بيانات.
- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
- توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.
- صمود البنى التحتية الحساسة للهجمات الإلكترونية.
- توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
- مقاومة البرمجيات الخبيثة وما تستهدفه من إحداث أضرار بالغة بالمستخدمين وأنظمة المعلومات.
- الحد من التجسس والتخريب الإلكتروني على مستوى الحكومات والأفراد.
- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.[2]

---

[1] حميدي حياة ، طابلي نسيمة : مدخل مفاهيمي حول الأمن السيبيراني ، مدار للدراسات الاتصالية الرقمية ن م٠٢، العدد٠٢، نوفمبر ٢٠٢٢، ص ١١.

[2] وفاء بنت حسن عبد الوهاب : وعي أفراد الاسرة بمفهوم الأمن السيبيراني وعلاقته باحتياطاتهم الأمنية والجرائم الالكترونية المجلة العربية للعلوم الاجتماعية ، م٠٢، جزء٠١، ص٣٥.

المطلب السادس: إجراءات تعزيز الامن السيبيراني

هناك العديد من الإجراءات التي يمكن لكل مستخدم أنترنت أن يقوم بفعلها لتعزيز الأمن السيبيراني لديه لعل ابرزها ما يلي :

-اختيار كلمات مرور قوية، وعمليات تحقق أمنية لمواقع التواصل الاجتماعي، والبريد الإلكتروني، والحسابات الشخصية على الحاسوب أو الهواتف الذكية.

- عدم الاستجابة لأي رسائل مجهولة المصدر ترد إلى البريد الإلكتروني.

- استخدام برامج الحماية ومضادات الفيروسات وتحديثها باستمرار. حماية المعلومات الشخصية ومنع الآخرين . من الاطلاع عليها.

- تحديث كلمات المرور بشكل مستمر على الأقل مرة أو مرتين شهريا.

- عدم إرسال أي معلومات شخصية عبر البريد الإلكتروني، أو الإفصاح عن معلومات خاصة عبر مواقع التواصل الاجتماعي.

- تدريب وتأهيل المستخدمين وتوعيتهم وتدريبهم على استخدام نظم المعلومات التي تتمتع بمزايا الأمن والسرية.

- تأمين وتحديد إمكانية الوصول إلى النظام، فالدخول إلى أنظمة الشبكة: الحاسوب وقواعد البيانات ونظم المعلومات ومواقع المعلوماتية عموماً، يمكن تقييده بالعديد من وسائل التعرف على شخصية المستخدم وتحديد نطاق الاستخدام.[1]

---

[1] ماجد بن عبد الله الحبيب : مرجع سابق، ص،١٩.

المبحث الثاني : ماهية المعلومات الرقمية

المطلب الأول: تعريف المعلومات الرقمية

أدت التطورات التكنولوجية الحاصلة في البيئة الرقمية ، إلى مخاطر تهدد سلامة المعلومات وأمنها ، وهي مشكلة لاتزال تؤرق الجميع لاسيما الطلبة الجامعيين ، لما لها من تداعيات على سلامة المجتمع، في الجهة المقابلة لم يتوقف التطور هنا فحسب ، وإنما شمل تطوير أساليب جديدة لحماية المعلومات الرقمية والحفاظ عليها ، وفي ما يلي تعريف للمعلومات الرقمية وأساليب لحمايتها .

هي تلك الأعمال التي يتم إنشاؤها أو تسجيلها واختزانها، والبحث عنها واسترجاعها وتناقلها واستخدامها رقميًا باستخدام الحاسب الآلي والتجهيزات الملحقة به، سواء كانت متاحة عبر الشبكات، وهي الإتاحة عن بعد، أو قواعد البيانات على الخط المباشر، أو محملة على أحد الوسائط التخزينية (أقراص مرنة، أقراص مدمجة، أقراص صلبة، إلخ)، أو الإتاحة المباشرة. وقد أُغفِلت هذه الأعمال بسبب الالتباس والغباء والأداة في الوسائط المباشرة. إغفال ما تتمتع به من مزايا فيما يتعلق بالانتشار والتداول والبحث والاسترجاع نتيجةً لتقدم على مستوى الحاسب وتقنيات تكنولوجيا الاتصالات، ويتم اتخاذ حق الطبع والنشر عليها، سواء كانت معلومات رقمية أو الإتاحة المباشرة، سواء كانت أعمالًا مستقلة بذاتها، أو كانت أجزاء من أعمال أكبر. ومن خلال العرض السابق لتعريفات مصادر المعلومات الرقمية يلاحظ أن جميعها يركز على أنها عمل علمي، يتم التعامل معه بواسطة الحسابات الإلكترونية، سواء من خلال شبكات معلومات أو من خلال مصادر أخرى يمكن من خلالها الحصول على هذه المصادر الإلكترونية.[1]

المطلب الثاني: التقنيات المستحدثة لضمان أمن المعلومات الرقمية

مع تزايد القيمة الاقتصادية والمالية للمعلومات ، وشيوع وتنامي التطبيقات العملية لفكرة راس المال الفكري والاقتصاد القائم على المعرفة او الاقتصاد الرقمي ،وجب العمل على توفير الحماية التقنية لنظم المعلومات وهو ما ادى الى ابتكار وسائل تقنية مستحدثة ، حيث يتوجب اولا تحديد العناصر الضرورية لاي نظام الامني للمعلومات وهي:

– القدرة على اثبات شخصية الطرف الاخر على الشبكة Authentication وبنفس الوقت اثبات شخصية الموقع للمستخدم .

– الخصوصية او حماية بيانات المستخدم من الافشاء Privacy والاطلاع دون اذن او تخويل

– الصلاحيات وتحديد مناطق الاستخدام المسموحة Access Control لكل مستخدم واوقاته .

– تكاملية او سلامة المحتوى وتتصل بالتأكد من ان المعلومة Integrity التي ارسلت هي نفسها التي تم تلقيها من الطرف الاخر.

---

[1] أمل وجيه حمدي : المصادر الالكترونية للمعلومات ، الاختيار والتنظيم والاتاحة، القاهرة ، الدار المصرية اللبنانية ، ٢٠٠٧، ص٣١.

-عدم الانكار اذ لا يكفي فقط اثبات شخصية Non-repudiation المستخدم او الموقع بل يتعين ضمان عدم انكار منفذ التصرف صدور التصرف عنه .

-استمرارية يكفي الوجود وتقديم الخدمة الالكترونية ووجود النظام الالكتروني ويتعين ضمان استمرار الوجود وحماية النظام من انشطة التعطيل (كهجمات انكار الخدمة).[1]

المطلب الثالث:أنواع برامج أمن المعلومات الرقمية

برامج أمن المعلومات هي البرامج المصممة لحماية وتأمين الخوادم وأجهزة الكمبيوتر المحمولة والأجهزة المحمولة والشبكات من الفيروسات والاختراقات والوصول غير المصرح به، الذي قد يُطال الطالب الجامعي وتشمل تلك البرامج ما يلي:

١-برنامج الحماية من البرامج الضارة: يُعد برنامج الحماية من البرامج الضارة هو الحل الأمني الأفضل لمعالجة دورة الحياة الكاملة لمشكلة البرامج الضارة المتقدمة، إذ يمنع الانتهاكات ويتيح الرؤية والسيطرة للكشف سريعًا عن التهديدات واحتوائها ومعالجتها.

٢-برامج مكافحة الفيروسات هناك العديد من البرامج المستخدمة في مكافحة الفيروسات المهاجمة لأجهزة الكمبيوتر أو الأجهزة المحمولة، إذ تعمل تلك البرامج على تنظيف جميع الأجهزة على الشبكة من الفيروسات لحماية البيانات الحساسة، ومن أمثلة تلك البرامج: Avast free Antivirus، Norton.

٣-Kaspersky مكافحة التجسس في أمن المعلومات :هي البرامج المستخدمة لمكافحة التطفل على أنشطة الضحايا عبر الإنترنت ومعرفة معلوماتهم الشخصية السرية، ومنها أسماء المستخدمين وكلمات المرور، إذ تقوم تلك البرامج باكتشاف وإزالة هذه الأخطاء من النظام والحفاظ عليه آمنًا، من أجل حماية خصوصية المستخدمين والشركات والعملاء.

٤-جدران الحماية : هي برنامج يقوم بتحليل ومسح البيانات الصادرة والداخلة لمنع الدخول غير المصرح به، وهو ما يضمن عدم تعرض بيانات المؤسسة لخطر الاختراق. ويتم تخصيص قواعد وسياسات الجدار الناري وفقًا لتفضيل المستخدم، مثل وضع استثناءات تسمح لتطبيقات معينة بالمرور عبر جدار الحماية دون وضع علامة بأنها إنذارات كاذبة. ومن أمثلة برامج جدران الحماية ManageEngine و SolarWinds Network Firewall و Security Mechanism Ultimate Defense -5SolarWinds Network Firewall Management-5: برامج إدارة كلمات المرور وهي برامج تم تصميمها لتمكين المستخدمين من إعادة ضبط كلمات المرور الخاصة بهم في حالة قفل الحساب، إلى جانب استخدامها في مزامنة كلمات المرور، أي أنها تتيح استخدام نفس كلمة المرور عند تشغيل أكثر من تطبيق. وتفيد تلك البرامج في إنشاء كلمات مرور قوية ومميزة، وهو ما يمنع من اختراقات الحسابات التي تعتمد على ضعف كلمات المرور. ومن أبرز برامج إدارة كلمات المرور: ١Password أو RoboForm أو NordPass أو .DashLane.

٦-برامج الوقاية من التسلل: تم تصميم برامج أو أدوات الوقاية من التسلل من أجل الكشف عن مناطق الضعف والتهديدات في الشبكات، إذ تستهدف تلك التهديدات تطبيقات أو خدمات معينة للسيطرة على البرامج أو الأجهزة، ولذلك فإن برامج الوقاية من التسلل تقوم بحماية النظام من خلال العمل كطبقة إضافية لتحليل البيانات التي يحتمل أن

---

[1] المركز الوطني ايمني للمعلومات ، الاعمال الالكترونية وامن لمعلومات ، مداخلة برسم الندوة الموسومة ب" تنظيم الاتفاقيات والعقود والرخص في عصر المعلوماتية "،اليمن ، مارس ٢٠٠٥،د ص.

تكون خطرة، مع فحص جميع حركات المرور التي تمر عبر الشبكات. ومن أبرز تلك البرامج شبكة FireEye، ومنصة أمان شبكة McAfee، ونظام منع اختراق شبكة iSensor.[1]

المطلب الرابع:خصائص أمن المعلومات الرقمية

في ظل التطور التكنولوجي المتسارع واعتماد المؤسسات والأفراد بشكل متزايد على الأنظمة الرقمية، أصبحت حماية المعلومات الرقمية أمرا بالغ الأهمية. أمن المعلومات الرقمية يهدف إلى ضمان سرية وسلامة وتوافر البيانات، بالإضافة إلى ضمان مصداقية العمليات الرقمية. و

فيما يلي نستعرض الخصائص الأساسية لأمن المعلومات الرقمية التي تشكل الركائز الرئيسية لحماية البيانات في البيئات الرقمية.

١-السرية (Confidentiality) مثل :

. ضمان أن المعلومات لا يتم الكشف عنها إلا للأشخاص المصرح لهم بذلك.

. استخدام تقنيات التشفير (Encryption) لحماية البيانات من الوصول غير المصرح به.

٢- السلامة (Integrity) مثل :

.التأكد من أن المعلومات تبقى صحيحة وكاملة دون تغيير غير مصرح به.

.استخدام تقنيات التحقق من سلامة البيانات مثل التوقيعات الرقمية (Digital Signatures) والهاش (Hash Functions).

٣- التوافر (Availability) مثل :

.ضمان أن المعلومات والخدمات الرقمية متاحة عند الحاجة إليها.

.حماية الأنظمة من هجمات التعطيل مثل هجمات انكار الخدمة (DDoS).

٤- المصادقة (Authentication) مثل :

.التأكد من هوية المستخدمين أو الأجهزة قبل منحهم الوصول إلى النظام.

.استخدام طرق مثل كلمات المرور، البصمة الحيوية، أو المصادقة الثنائية (Two-Factor Authentication).

٥-التحكم في الوصول (Access Control) مثل :

.تحديد الصلاحيات والوصول إلى المعلومات بناءً على أدوار المستخدمين.

---

[1] بكة : أمن المعلومات وأهميته والأنواع والعناصر والاستراتيجيات والبرامج والأهداف، موقع بكة ، ٠٧ جانفي ٢٠٢٥، متاح على الرابط : https://bakkah.com/ar/knowledge-center/%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA ، ٢٨ قيفري ٢٠٢٥.

.ضمان أن كل مستخدم يمكنه الوصول فقط إلى البيانات التي يحتاجها لأداء مهامه.

٦- عدم الإنكار (Non-Repudiation) مثل :

.ضمان أن الأطراف المشاركة في العملية الرقمية لا يمكنها إنكار حدوثها.

.استخدام التوقيعات الرقمية والسجلات الزمنية (Timestamps) لإثبات العمليات.

٧- التقييم المستمر للمخاطر (Risk Assessment) مثل :

.تحديد التهديدات المحتملة ونقاط الضعف في النظام.

.تطوير استراتيجيات للتخفيف من هذه المخاطر.

٨- التحديث والتطوير المستمر (Continuous Improvement) مثل :

.مواكبة التطورات التكنولوجية والتهديدات الأمنية الجديدة.

.تحديث الأنظمة والبروتوكولات الأمنية بشكل دوري.[١]

---

[١] بكة : مرجع سابق ، متاح على الرابط : https://bakkah.com/ar/knowledge-center/%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A%D8%AA ٩

المبحث الثالث : الدراسات السابقة

في القيام بأي دراسة أو بحث، الاقتناع بأن عمله هذا هو عبارة عن حلقة متصلة بمحاولات كثيرة، فكل عمل علمي من هذا القبيل لابد وأن سبقته جهود أخرى مجسدة في شكل دراسات سابقة أو مشابهة يلجأ إليها الباحثون للتعرف على طبيعة مشكلتهم البحثية وكيفية تناولها، وفيما يلي توضيح لذلك

أولا : دراسة حول درجة الوعي بالأمن السيبيراني ودور تكنولوجيا التعليم في تنميته لدى طلبة كلية التربية الأساسية بجامعة الكويت

1-تعريف الدراسة: جاءت هذه الدراسة للباحثة عايدة عبد الكريم العيدان بعنوان درجة الوعي بالأمن السيبيراني ودور تكنولوجيا التعليم في تنميته لدى الطلبة كلية التربية بدولة الكويت. وهي دراسة منشورة في مجلة كلية التربية بجامعة الإسكندرية.[1]

كانت إشكالية الدراسة كالاتي: مادرجة وعي طلبة كلية التربية الاساسية بالأمن السيبيراني ؟ وتفرعت إلى الأسئلة التالية :

أ- ما المخاطر والانتهاكات السيبيرانية التي يتعرض لها الطلبة أثناء التعامل مع الفضاء السيبيراني ؟

ب- ما اسهامات دراسة مقررات تكنولوجيا التعليم في تنمية الوعي بالامن السيبيراني لدى طلبة كلية التربية الأساسية ؟

واعتمدت الدراسة على المنهج المسحي ،كما اعتمد على منهج تحليل المضمون وهو شائع الاستخدام في البحوث الاجتماعية وبالتحديد الدراسات التي تتعلق بتحديد الرسالة الاعلامية وأبعادها ودلالتها.

كما بلغ حجم العينة في الدراسة بلغ ١٧٣٣ طالبًا وطالبة، منهم ١٣٧٧ في الفصل الدراسي الأول من العام الدراسي ٢٠٢٠/٢٠١٤. كما يشير النص إلى استخدام معادلة "ستيتش تأميسون" لحساب حجم العينة التي تمثل هذه الدراسة، حيث بلغ حجم العينة ١٧٨١.

2- نتائج الدراسة:

- تشير نتائج اختبار شيفيه في جدول (١) إلى أن الفروق كانت لصالح مجموعة الطلبة في الفترتين الثالثة والرابعة مقابل مجموعات الطلبة في الفترتين الدراسيتين الأولى والثانية. ويستدل من ذلك على أن طلبة الفترتين الثالثة والرابعة يتمتعون بوعي بمستوى أعلى بالأمن السيبراني ولديهم تقديرات أعلى ومعرفة بسبل

---

[1] عايدة عبد الكريم العيدان : درجة الوعي بالأمن السيبيراني ودور تكنولوجيا التعليم في تنميته لدى طلبة كلية التربية الأساسية بجامعة الكويت، مجلة كلية التربية الأساسية ، م٣٤، العدد٠٤، الجزء٠٢، ٢٠٢٤. منشورة على الرابط الآتي: https://journals.ekb.eg/article_393474_b990008638a0776a0fb59bcb7b7098fe.pdf .

تنمية هذا الوعي في الكلية، وأيضًا يقدرون دورًا أعلى لإسهام دراسة مقررات في تكنولوجيا التعليم في تنمية هذا الوعي، مقارنة بالطلبة في الفترتين الأولى والثانية.

– تشير نتائج تحليل التباين الأحادي في جدول (٧) إلى أنه لا توجد فروق دالة إحصائيًا بين متوسطات درجات العينة حول تقديراتهم بمخاطر وتهديدات الأمن السيبراني تبعًا لاختلاف التخصص الدراسي، حيث كانت قيم (ف) غير دالة عند مستوى (م). في هذا السياق، يُستدل من ذلك على أن أفراد العينة من طلبة الأقسام العلمية المختلفة لديهم تقديرات متشابهة حول تعرضهم للمخاطر والانتهاكات والتهديدات السيبرانية.

– أنه لا توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات العينة حول الوعي بالأمن السيبراني في جميع المحاور تبعًا لاختلاف النوع، وذلك استنادًا إلى قيم (ت) حيث كانت غير دالة عند مستوى (م). ويُستدل من ذلك على أن أفراد العينة من الجنسين لديهم نفس مستوى الوعي بالأمن السيبراني وبمخاطره والتهديدات السيبرانية، وكذلك حول سبل تنميته في كلية التربية الأساسية بدولة الكويت.

٣–التعقيب عن الدراسة :

تشابهت الدراسة التي تحمل عنوان "درجة الوعي بالأمن السيبيراني ودور تكنولوجيا التعليم في تنميته لدى طلبة كلية التربية الأساسية بجامعة الكويت" مع دراستنا حول "الوعي بالأمن السيبيراني والمعلمات الرقمية لدى طلبة الإعلام والاتصال بجامعة الوادي" من حيث موضوع الدراسة، حيث ركزت كلتا الدراستين على قياس مستوى الوعي بالأمن السيبيراني لدى فئة محددة من الطلبة. إلا أن هناك عدة فروق منهجية وأدوات بحثية بين الدراستين. أولا، من حيث منهج الدراسة، اختلفت الدراستان في المنهج المتبع. حيث اعتمدت دراسة الاولى على المنهج المسحي لقياس درجة الوعي بالأمن السيبيراني ودور تكنولوجيا التعليم في تنميته، في حين أن دراستنا اتبعت المنهج الوصفي التحليلي لدراسة الوعي بالأمن السيبيراني والمعلمات الرقمية. ثانيا، من حيث أداة جمع البيانات، استخدمت دراسة السابقة أداة الاستبيان كأداة رئيسية لجمع البيانات، وهو ما يتشابه مع دراستنا التي اعتمدت أيضا على الاستبيان كأداة رئيسية. إلا أن دراسة جامعة الكويت ركزت بشكل أكبر على دور تكنولوجيا التعليم في تنمية الوعي الأمني، بينما ركزت دراستنا على الجانب الرقمي والمعلمات المرتبطة بالأمن السيبيراني. أخيرا، من حيث عينة الدراسة، اختلفت الدراستان في الفئة المستهدفة. حيث تناولت دراسة الأولى طلبة كلية التربية الأساسية، بينما ركزت دراستنا على طلبة الإعلام والاتصال، مما يعكس اختلافا في الخلفية المعرفية والتخصصية للعينة المدروسة.

ثانيا : دراسة حول درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات

1-تعريف الدراسة: جاءت هذه الدراسة للباحثة فاطمة يوسف المنتشري بعنوان وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. وهي دراسة منشورة في مجلة العربية للتربية النوعية بجامعة دار الحكمة في جدة بالسعودية.[1]

وكانت إشكالية الدراسة كالاتي: ؟ ما درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات؟ وتفرعت إلى الأسئلة التالية :

أ- .ما درجة وعي معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة بمفاهيم الأمن السيبراني؟

ب- هل توجد فروق ذات دالة إحصائية عند مستوى ٠,٠٥ بين متوسطات تقديرات المعلمات ؟

ت- ما درجة تعرض معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة الانتهاكات الأمن السيبراني؟

واتبعت الدراسة المنهج الكمي الوصفي التحليلي، كما تكون مجتمع الدراسة من جميع معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة، خال الفصل الأول من العام الدراسي ١٤٤١هـ، ويبلغ عددهن ٤٥٢٥ معلمة.

2- نتائج الدراسة:

-أن المعلمات الحاصلات على درجة البكالوريوس يمثلن ٥٣ %من أفراد العينة، أما باقي أفراد العينة من المعلمات الحاصلات على درجة البكالوريوس والدبلوم التربوي فيمثلن ٣٦ ،%أما الحاصلات على الماجستير فنسبتهن ١١ .%

- أن جميع فقرات الاستبانة ترتبط بمعامل ارتباط دالة، عند مستوى دالة ٠.٠١ مع المحور الذي تنتمي إليه، وتم كذلك حساب معاملات الارتباط بين درجة كل محور والدرجة الكلية لاستبانة.

-اتضح من تلك الاستجابات أن درجة وعي المعلمات بانتهاكات الأمن السيبراني درجة متوسطة بشكل عام، وهو ما يعني احتمال تعرضهن لقدر كبير من انتهاكات الأمن ، وتتعلق هاتين الفقرتين السيبراني، حيث جاءت الاستجابات على فقرتين بدرجة كبيرة بالإجراءات التي يُمكن أن تتخذها إدارة المدرسة.

---

[1] يوسف المنتشري : وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة ، مجلة العربية للتربية النوعية بجامعة دار الحكمة ، السعودية ، ٢٠٢٠ ، منشورة على الرابط الآتي :
https://search.shamaa.org/PDF/Articles/EGAjqe/AjqeVol4No14Y2020/ajqe_2020-v4-n14_095-140.pdf

– أن درجة وعي المعلمات بانتهاكات الأمن السيبراني درجة متوسطة بشكل عام، وهو ما يعني احتمال تعرضهن لقدر كبير من انتهاكات الأمن السيبراني.

٣–التعقيب عن الدراسة :

تشابهت الدراسة التي تحمل عنوان درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلماتمع دراستنا حول"الوعي بالأمن السيبيراني والمعلمات الرقمية لدى طلبة الإعلام والاتصال بجامعة الوادي من حيث موضوع الدراسة، حيث ركزت كلتا الدراستين على قياس مستوى الوعي بالأمن السيبيراني لدى فئة محددة من الأفراد (المعلمات في دراسة جدة، وطلبة الإعلام والاتصال في دراستنا). إلا أن هناك عدة فروق منهجية وأدوات بحثية بين الدراستين. أولا، من حيث منهج الدراسة، اختلفت الدراستان في المنهج المتبع. حيث اعتمدت دراسة السابقة على منهج وصفي الكمي التحليلي لقياس درجة وعي المعلمات بالأمن السيبراني، وهو ما يتشابه مع دراستنا التي اتبعت أيضا المنهج الوصفي التحليلي. ومع ذلك، ركزت الدراسة الاولى على وجهة نظر المعلمات في المدارس العامة، بينما ركزت دراستنا على طلبة الإعلام والاتصال، مما يعكس اختلافا في العينة. ثانيا، من حيث أداة جمع البيانات، استخدمت دراسة الاولى أداة الاستبيان كأداة رئيسية لجمع البيانات، وهو ما يتشابه مع دراستنا التي اعتمدت أيضا على الاستبيان. إلا أن دراسة جدة ركزت على قياس وعي المعلمات بالأمن السيبراني في البيئة التعليمية، بينما ركزت دراستنا على الجانب الرقمي والمعلمات المرتبطة بالأمن السيبيراني لدى طلبة الإعلام والاتصال. كما اختلفت الدراستان في الفئة المستهدفة. حيث تناولت دراسة جدة معلمات المرحلة المتوسطة في المدارس العامة بمدينة جدة، بينما ركزت دراستنا على طلبة الإعلام والاتصال بجامعة الوادي.

ثالثا : دراسة حول الوعي الاجتماعي بالأمن السيبراني لدى طلبة كلية الامام الكاظم انموذجا.

–1تعريف الدراسة: جاءت هذه الدراسة للباحثة هديل تومان محمد البعاج بعنوان الوعي الاجتماعي بالأمن السيبراني لدى طلبة كلية الامام الكاظم انموذجا. وهي دراسة منشورة في ملتقى وطني بالعراق.[١] وكانت إشكالية الدراسة كالاتي: هل هناك وعي لدى طلبة كلية الامام الكاظم بمفاهيم الامن السيبراني ؟ وتفرعت إلى الأسئلة التالية :

[١] هديل تومان محمد البعاج: :الوعي الاجتماعي بالأمن السيبراني لدى طلبة كلية الامام الكاظم انموذجا، وقائع المؤتمر العلمي السابع تحت شعار العلوم الإنسانية بين التحديات الراهنة والافاق المستقبلية كلية الآداب ، جامعة الامام كاظم ، ٢٠٢٣ ، منشورة على الرابط الآتي :
https://lark.uowasit.edu.iq/index.php/lark/article/view/3161/1959

أ- هل هناك وعي لدى طلبة كلية الامام الكاظم بتطبيقات الأمن السيبراني ؟

ب- هل هناك وعي لدى طلبة كلية الامام الكاظم بكيفية تعزيز الوعي بالامن السيبراني ؟

اتبعت الباحثة المنهج الوصفي التحليلي، وقد شمل مجتمع البحث جميع طلبة كلية الامام الكاظم كما تم استخدام الاستبانة كأداة لجمع البيانات الدراسة الحالية، وتم تطبيقها إلكترونيا بهدف ضمان سهولة وسرعة الحصول على النتائج.

٢- نتائج الدراسة:

- افراد عينة البحث لا يملكون درجة عالية من الوعي بمفاهيم الامن السيراني ، وهذا يشير الى محدودية اطلاع افراد العينة على خطورة الامن السيراني واهمية الوعي به.

- تبين ان افراد العينة يملكون درجة متوسطة من الوعي بمفاهيم الامن السيراني في العبارات التالية النتائج المتعلقة بالمحور الثاني الذي يقيس درجة الوعي بتطبيقات الامن السيراني لدى طلبة كلية الامام الكاظم / أقسام واسط.

-أفراد عينة البحث يملكون درجة متوسطة من الوعي بتطبيقات الأمن السيبراني .

-تبين ان افراد العينة يملكون درجة عالية من الوعي نحو العبارة (اتجنب فتح روابط من مصادر مجهولة ، حيث جاءت بالمرتبة الأولى بينما جاءت (احدث جهازي بصفة مستمرة) اذ .جاءت بالمرتبة الثانية.

٣-التعقيب عن الدراسة :

اتفقت الدراسة التي تحمل عنوان "الوعي الاجتماعي بالأمن السيبراني لدى طلبة كلية الإمام الكاظم أنموذجا مع دراستنا حول "الوعي بالأمن السيبيراني والمعلمات الرقمية لدى طلبة الإعلام والاتصال بجامعة الوادي" من حيث موضوع الدراسة، حيث ركزت كلتا الدراستين على قياس مستوى الوعي بالأمن السيبيراني لدى فئة محددة من الطلبة. إلا أن هناك عدة فروق منهجية وأدوات بحثية بين الدراستين. أولا، من حيث منهج الدراسة، تتشابه الدراستان في المنهج المتبع. حيث اعتمدت دراسة كلية الإمام الكاظم على المنهج الوصفي التحليلي لقياس الوعي الاجتماعي بالأمن السيبراني، وهو ما يتشابه مع دراستنا التي اتبعت أيضا المنهج الوصفي التحليلي. ومع ذلك، ركزت الدراسة الأولى على الجانب الاجتماعي للوعي بالأمن السيبراني، بينما ركزت دراستنا على الجانب الرقمي والمعلمات المرتبطة بالأمن السيبيراني. ثانيا، من حيث أداة جمع البيانات، استخدمت الدراسة السابقة أداة الاستبيان كأداة رئيسية لجمع البيانات، وهو ما يتشابه مع دراستنا التي اعتمدت أيضا على الاستبيان. إلا أن دراسة كلية الإمام الكاظم ركزت على قياس الوعي الاجتماعي بالأمن السيبراني، بينما ركزت دراستنا على الجانب الرقمي والمعلومات المرتبطة بالأمن السيبيراني لدى طلبة الإعلام والاتصال بذات الجامعة.

رابعا : دراسة حول درجة وعي المعلمين بالأمن السيبيراني بالمدارس الاردنية

1-تعريف الدراسة: جاءت هذه الدراسة للباحث خالد سليمان سمحان درجة وعي المعلمين بالأمن السيبيراني. دراسة ميدانية من وجهة نظر معلمي المدارس الأردنية، وهي دراسة منشورة في مجلة اتحاد الجامعات العربية للبحوث في التعليم العالي ، بالأردن ، ٢٠٢٣.[١]

وكانت إشكالية الدراسة كالاتي: مامدى ادراك المعلمين بالامن السيبيراني وجهة نظرهم ؟ وتفرعت إلى الأسئلة التالية :

أ- ما مدى إدراك المعلمين مفاهيم الأمن السيبراني من وجهة نظرهم؟

ب- ما دور الإدارة المدرسية في نشر ثقافة الأمن السيبراني لدى الطلبة من وجهة نظر المعلمين؟

ت- هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (α: 0.05) لدرجة وعي المعلمين بالأمن السيبراني تعزى للمتغيرات الديمغرافية لعينة الدراسة؟

واعتمدت الدراسة على المنهج الوصفي التحليلي لغرض قياس درجة وعي معلمي المدارس الأردنية بالأمن السيبراني، وتم اتباع أسلوب العينة العشوائية الطبقية المتناسبة بحيث تم اختيار مجموعة من معلمي ومعلمات مدارس مديرية تربية لواء القويرة لتُمثل عينة الدراسة. وتكون مجتمع الدراسة من جميع المعلمين والمعلمات الذين يدرّسون في مدارس مديرية تربية لواء القويرة ويبلغ عددهم (٤٠٣٦) معلماً ومعلمة (٢٦٦٤ ذكور، و١٣٧٢ إناث).

٢- نتائج الدراسة:

-توجد العديد من معوقات نشر ثقافة الأمن السيبراني في المدارس الأردنية من وجهة نظر عينة الدراسة؛ حيث جاءت الدرجة الكلية لهذا المحور مرتفعة بمتوسط حسابي (٤.٩٣) وانحراف معياري (١.٣٥).

- لا توجد فروق دالة إحصائياً عند مستوى الدلالة (α=0.05) في درجة وعي المعلمين بالأمن السيبراني تعزى لمتغير الجنس.

- لا توجد فروق دالة إحصائيا عند مستوى الدلالة (α=0.05) في درجة وعي المعلمين بالأمن السيبراني تعزى لمتغير التخصص الأكاديمي.

---

[١] خالد سليمان سمحان: درجة وعي المعلمين بالأمن السيبيراني. دراسة ميدانية من وجهة نظر معلمي المدارس الأردنية، مجلة اتحاد الجامعات العربية للبحوث في التعليم العالي ، الأردن ، ٢٠٢٣، منشورة على الرابط الآتي : https://digitalcommons.aaru.edu.jo/cgi/viewcontent.cgi?article=1465&context=jaaru_rhe

– لا توجد فروق دالة إحصائيا عند مستوى الدلالة (α=0.05) في درجة وعي المعلمين بالأمن السيبراني تعزى لمتغير سنوات الخبرة.

٣– التعقيب عن الدراسة:

تتفق الدراسة السابقة مع دراستنا من حيث موضوع الدراسة، حيث ركزت كلتا الدراستين على قياس مستوى الوعي بالأمن السيبيراني لدى فئة محددة من الأفراد (المعلمين في الدراسة الأردنية، وطلبة الإعلام والاتصال في دراستنا). وتتشابه الدراستان في المنهج المتبع. وقد اعتمدت الدراسة الأولى على المنهج الوصفي التحليلي لقياس درجة وعي المعلمين بالأمن السيبيراني، وهو ما يتشابه مع دراستنا التي اتبعت أيضا نفس المنهج. ومع ذلك، ركزت الدراسة الأردنية على المعلمين في المدارس الأردنية، بينما ركزت دراستنا على طلبة الإعلام والاتصال. واستخدمت كلتا الدراستين نفس الأداة وهو الاستبيان كأداة رئيسية لجمع البيانات. إلا أن الدراسة الأردنية ركزت على قياس وعي المعلمين بالأمن السيبيراني في البيئة التعليمية، بينما ركزت دراستنا على الجانب الرقمي والمعلمات المرتبطة بالأمن السيبيراني لدى طلبة الإعلام والاتصال. كما اختلفت الدراستان في مجتمع البحث وتاريخ اجراء الدراسة.


الإطـــار الـمـــيـــداني

تمهيد :

تكون هذا الفصل من مبحثين حيث تطرقنا في المبحث الأول إلى طريقة أدوات الدراسة المستخدمة، والمتمثلة في الملاحظة والمقابلة والاستبيان، وتطرقنا في المبحث الثاني إلى مناقشة وتفسير النتائج في ضوء الدراسات السابقة وكذا في ظل محاور الاستبيان ، حيث تمت معالجة البيانات عن طريق برنامج الرزم الإحصائية للعلوم التربوية والإجتماعية.حيث استخدمنا التكرارات والنسب المئوية.

المبحث الأول : منهجية الدراسة وأدواتها

المطلب الأول : المنهج المستخدم وأدواته

١-المنهج المستخدم:

هو الطريق المؤدي إلى الكشف عن الحقيقة في العلوم بواسطة طائفة من القواعد العامة التي تهيمن على سير العقل وتحديد عملياته، يصل إلى النتائج المعلومة.[١]

ولقد اقتضت دارستنا إلى استخدام المنهج المسح الوصفي بغية تحقيق أهداف الدراسة وإعطاء لمحة على موضوع دراستنا المتعلقة بشأن وعي وإدراك الطالب الجامعي بالأمن السيبراني والمعلومات الرقمية.

إذ يعرف المنهج المسح الوصفي بأنه أسلوب من أساليب التحليل المرتكز على معلومات كافية ودقيقة عن ظاهرة أو موضوع محدد عبر فترة أو فترات زمنية معلومة وذلك من اجل الحصول على نتائج علمية تم تفسيرها بطريقة موضوعية تنسجم مع المعطيات الفعلية للظاهرة.[٢]

٢- أدواته :

لقد اعتمدنا في موضوع دراستنا على أداة الاستبيان، فهو من أدوات البحث المهمة والشائعة استعمالها في ميدان العلوم الإنسانية وخاصة علوم الإعلام والاتصال. وتعد استمارة البحث من أكثر أدوات جمع البيانات شيوعا في البحوث الاجتماعية، هذا ما يدفع الباحث إلى بذل الجهد من اجل صياغة استمارة البحث بصورة تؤدي إلى تحقيق أهداف الدراسة.[٣]

كما كانت الملاحظة إحدى أدوات جمع البيانات التي اعتمدنا عليها، وتعني الانتباه والنظر لشيء ما وهي أداة من أدوات البحث العلمي تجمع بواسطتها المعلومات التي تمكن الباحث من الاجابة عن أسئلة البحث واختبار فروضه. وتعرف أيضا بأنها التنبه للظواهر أو الحوادث بقصد تفسيرها واكتشاف أسبابها وعواملها والوصول إلى القوانين التي تحكمها.[٤]

واستخدمنا الملاحظة تلقائيا في الظروف الطبيعية للظاهرة كاستطلاع أولي من خلال معاينة تزايد ظاهرة نقص الوعي بالأمن السيبراني لدى الطلبة الجامعيين.

---

[١] عبد الرحمن بدوي مناهج البحث العلمي وكالة المطبوعات، الكويت ١٩٧٧،ص١-٥

[٢] فارس رشيد البياتي، الحاوي في مناهج البحث العلمي، دار السواقي العلمية، ط ١ ، عمان ٢٠١٨، ص٩٣

[٣] حمد مرسلي، مناهج البحث العلمي في علوم الاعلام والاتصال، ديوان المطبوعات الجامعية، ط ٤ ، الجزائر ٢٠١٠ ص ٢٢٠.

[٤]عبد الله باشيوة وآخرون: البحث العلمي مفاهيم. أساليب. تطبيقات، الوراق للنشر والتوزيع، الأردن، 2009، ص378.

المطلب الثاني : مجتمع البحث وعينته

يعرف مجتمع الدراسة بـ المجتمع الاحصائي الذي تجرى عليه الدراسة ويشمل كل أنواع المفردات مثل الأشخاص، السيارات، الشوارع.. الخ.

وحسب قراوتز فإن مجتمع البحث هو مجموعة منتهية أو غير منتهية من العناصر المحددة مسبقا والتي ترتكز عليها الملاحظات وهو مجموعة عناصر لها خاصية، عدة خصائص مشتركة تميزها عن غيرها من العناصر الأخرى والتي يجرى عليها البحث.[1]

وعليه يكون مجتمع بحثنا لهذه الدراسة هو طلبة وطالبات قسم الاعلام والاتصال بجامعة الوادي ، وكان اختيارنا لهذا المجتمع مبنيا على مجموعة من الاعتبارات والمتمثلة في امكانية الوصول إلى المجتمع المتناول بالدراسة، ومنه القدرة على التعامل معه ميدانيا. حيث بلغ حجم العينة ٥٠ مفردة ، تم اختيارهم بأسلوب العينة القصدية وهي عينة يتم اختيارها على أساس من الخبرة السابقة فقد يلاحظ الباحث من الدراسات السابقة أن مجموعة من المفردات يتمثل فيها من الخصائص ما يجعل نتائجها قريبة من المجتمع ككل، ومن الملاحظ أن العينة القصدية هي أكثر العينات استخداما نظرا لسهولة الوصول إلى المفردات بالإضافة إلى اعتقاد الباحث بأن هذه المفردات تحديدا هي الأقدر على تزويده بالبيانات التي يحتاجها في دراسته.

المطلب الثالث : أدوات جمع البيانات

تعرف أدوات البحث بأنها الوسيلة أو الطريقة التي يستطيع بها الباحث حل مشكلته مهما كانت تلك الأدوات حيث أن المشكلة المطروحة هي التي تحدد الأدوات التي يستعملها الباحث في بحثه مما تتناسب مع أداة المشكلة "[2]

انطلاقا من إشكالية الدراسة وتساؤلاتها والأهداف المسطرة للدراسة يتضح أن دراستنا اشتملت على أدوات بحثية ساعدتنا في جمع البيانات في إطار المنهج المسح الوصفي وتتمثل هذه الأداة في استمارة استبيان والملاحظة.

١- الاستبيان:

تعرف استمارة الاستبيان بأنها "عبارة عن سلسلة من الأسئلة يصيغه الباحث بعناية فائقة، وتختلف الاستبيانات من حيث الحجم، الشكل، والمضمون، والهدف، والتنظيم، فبينما توجد استبيانات من عدة صفحات يصمم بعض الباحثين استبيانات تزيد عن عشر صفحات، بعضها مطبوع والبعض الآخر

---

[1] منى عبد الله السمحان : مرجع سابق ، ص١٢.

[2] سعد سلمان المشهداني: مناهج البحث الإعلامي، ط 1، دار الكتاب الجامعي، الجمهورية اللبنانية، 2017، ص 42.

مكتوب باليد على ورق أبيض أو ملون، وتوزع بالبريد العادي أو الإلكتروني أو شخصيا أو تنشر في الصحف أو تملى هاتفيًا أو تذاع في الإذاعة أو تعرض في التلفزيون، وتستخدم لأغراض تحديد رغبات المستهلكين أو قياس انطباعات الطلبة وأولياء الأمور ومختلف فئات المجتمع.[1]"

وقد قمنا ببناء نموذج الاستمارة على الشكل التالي، حيث قسمت إلى ثلاثة محاور أساسية:

في المحور الأول تم عنوانه بدرجة وعي الطلبة بمفهوم الأمن السيبيراني ويحتوي على ٠٧ أسئلة

وفي المحور الثاني مدى اطلاع الطالب الجامعي على القوانين والنظم التي تواجه مخاطر الامن السيبيراني ويحتوي على ٠٧ أسئلة ، وفي المحور الأخير طرق وأساليب مواجهة الأمن السيبيراني بحسب تصورات مجتمع البحث يحتوي هو الآخر على ٠٧ أسئلة.

المطلب الرابع : إجراءات الصدق والثبات

١-الصدق

فالصدق يعني "صدق أسئلة الاختبار من حيث صياغتها ومحتواها وطريقة تطبيقها على المبحوثين لتحقيق الهدف من الاختبار "

2-الثبات

إن كلمة الثبات قد تعني الاستقرار بمعنى أنه لو كررت عمليات قياس الفرد الواحد لأظهرت درجته شيئا من الاستقرار كما أن الثبات قد يعني الموضوعية، بمعنى أن الفرد قد يحصل على نفس الدرجة مهما اختلف الباحث الذي يطبق الاختبار أو الذي يصححه وفي هذه الحالة يكون اختبار الثابت اختبار يقدر الفرد تقديرا لا يختلف في حسابه اثنان، فالثبات يعني أن تكون النتائج التي تظهرها الأداة ثابتة، بمعنى تشير إلى النتائج نفسها لو أعيد تطبيقها على العينة نفسها وفي نفس الظروف ولو بعد مدة زمنية ملائمة فإذا لم تتغير النتائج بعد إعادة تطبيق الأداة ولا تختلف استجابة المبحوثين فهذا يعني أن الأداة ثابتة. و المقياس الثابت هو "المقياس الذي يعطي النتائج نفسها إذا قاس الشيء نفسه مرات متتالية تحت الظروف نفسها، أي عدم تناقض المقياس مع نفه، ولا تصل المقاييس النفسية إلى دقة مقياس الظواهر المادية المختلفة كالطول والوزن والزمن.[2]

---

[1] اسماعيل ابراهيم: مناهج البحوث الإعلامية، ط1، دار الفجر للنشر والتوزيع، مصر، 2017، ص114.

[2] حنان بشتة ، نعيم بوعموشة: الصدق والثبات في البحوث الاجتماعية،مجلة دراسات في علوم الانسان والمجتمع،مجلد03. عدد02جوان، جامعة جيجل،2020.ص10.

3–الاتساق الداخلي: يمكن تسميته بصدق الدراسة هو أن تؤدي وتقيس أسئلة الاستبيان ما تم وضعه لقياسه فعلاً، ويقصد به وضوح الاستبيان ومفرداته وفقرات الاستبيان ومفهومه لأفراد عينة الدراسة الذين سوف يشملهم الاستبيان.

4– معامل ألفا كرونوباخ: هو عبارة عن معامل مقياس أو مؤشر لثبات بطارية الاختبار والاستبيان.[1]

المبحث الثاني : تحليل ومناقشة نتائج الدراسة

المطلب الأول: عرض وتحليل البيانات

الجدول 01 : يوضح قيمة معامل الثبات ألفا كرونوباخ

البيان	عدد العبارات	معامل ألفا كرونوباخ
معامل ثبات لجميع فقرات الاستبيان	25	0.698

المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

يتبين من الجدول رقم ٠١ الخاص بمعاملات الثبات للاستبيان المستخدم في هذه الدراسة يقدر بـ (0.698) بعد الاعتماد على معامل ألفا كرونوباخ وهذا يعني أن المقياس يتمتع بدرجة جيدة من الثبات، فهذا المعامل مقبول بالقدر الذي يسمح لنا بقبولها واعتبار الاستبيان ثابت.

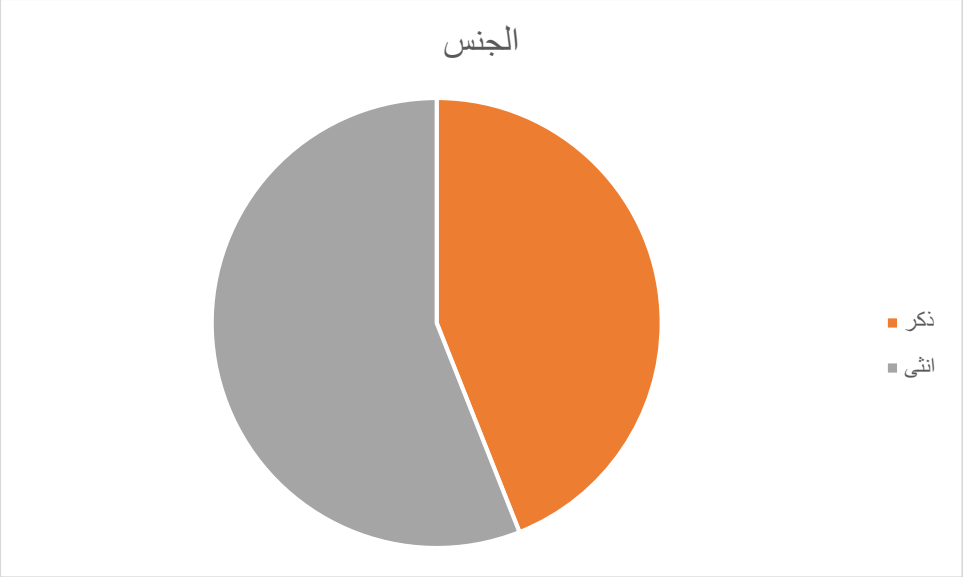
توزيع افراد العينة حسب الجنس

الجدول رقم (٢): توزيع أفراد عينة الدراسة حسب الجنس

الرقم	المتغير	الفئة	التكرار	النسبة
01	الجنس	ذكر	22	44.0
		انثى	28	56.0
المجمـــــــــــوع			50	١٠٠ %

المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

[1] المنارة للاستشارات الأكاديمية:الاتساق الداخلي للاستبيان
https://www.manaraa.com/post/6590/، 25 فيفري 2025، 15:00



المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

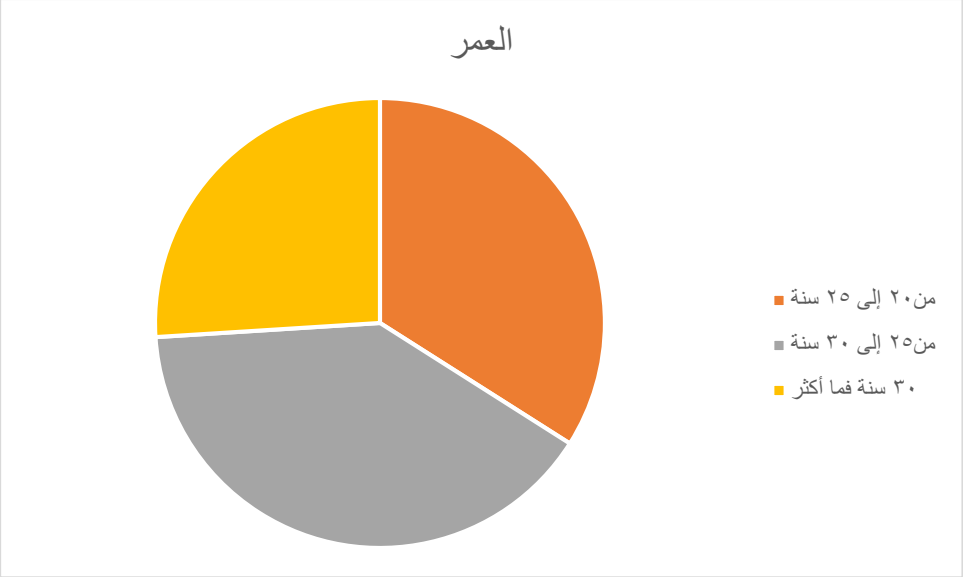
حسب قراءتنا للجدول يتّضح أن نسبة **الإناث** في عينة الدراسة بلغت **56%** (28 طالبة)، وهي النسبة الغالبة، مقابل **44%** من **الذكور** (22 طالبا). مما يظهر تفوقا نسبيا لمشاركة الإناث في هذا الاستبيان.

توزيع افراد العينة حسب العمر

الجدول رقم (٣): توزيع أفراد عينة الدراسة حسب العمر

الرقم	المتغير	الفئة	التكرار	النسبة
02	**العمر**	من20 إلى 25 سنة	17	34.0
		من25 إلى 30 سنة	20	40.0
		30سنة فما أكثر	13	26.0
المجمـــــــــــوع			50	**%100**

المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.



المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

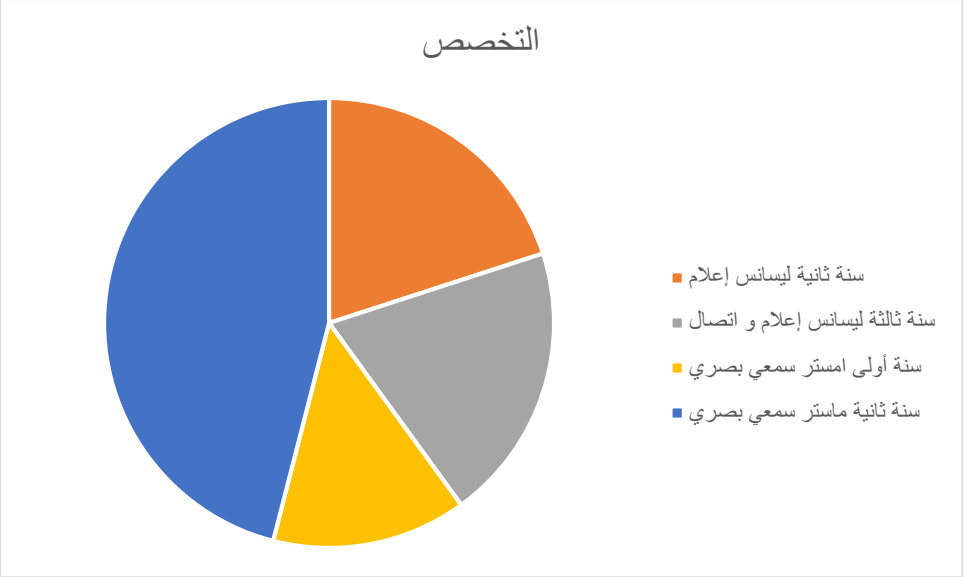
حسب الجدول الموضح أعلاه تشير النتائج إلى أن الفئة العمرية الأكثر تمثيلا في العينة هي فئة **من 25 إلى 30 سنة**، بنسبة **40%** (20 مشاركًا)، تليها فئة **من 20 إلى 25 سنة** بنسبة **34%** (17 مشاركًا)، أما الفئة التي تفوق أعمارها **30 سنة**، فقد شكّلت نسبة **26%** (13 مشاركا). ويُفهم من ذلك أن أغلب العينة هم من فئة الشباب.

توزيع افراد العينة حسب التخصص الجامعي

الجدول رقم (٤): توزيع أفراد عينة الدراسة حسب المستوى الدراسي

الرقم	المتغير	السنوات	التكرار	النسبة
03	التخصص الجامعي	سنة ثانية ليسانس إعلام	10	20.0
		سنة ثالثة ليسانس إعلام واتصال	10	20.0
		سنة أولى ماستر سمعي بصري	7	14.0
		سنة ثانية ماستر سمعي بصري	23	46.0
المجمـــــــــــوع			50	**%100**

المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.



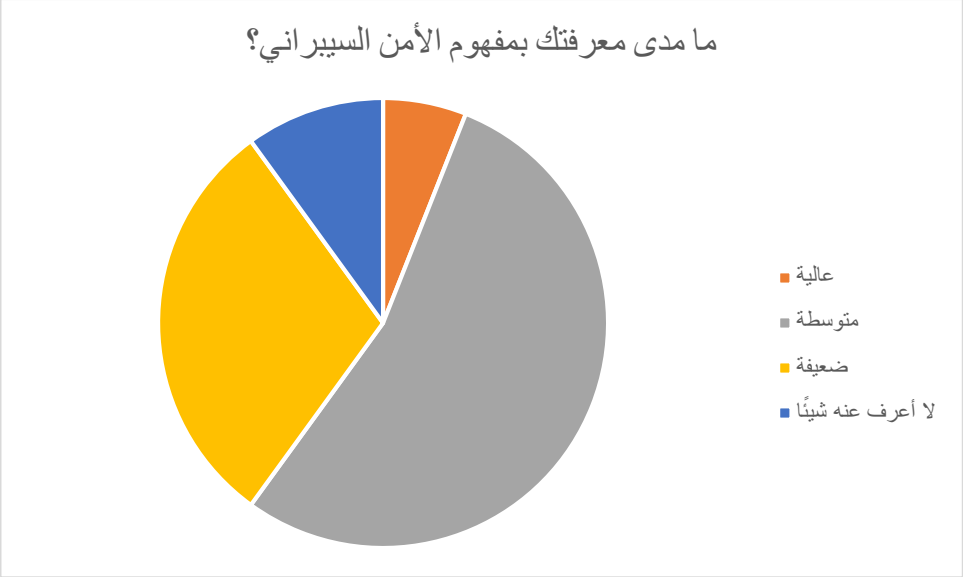
المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

أظهرت النتائج أن النسبة الأكبر من العينة تنتمي إلى **السنة الثانية ماستر تخصص سمعي بصري** بنسبة **46%** (23 طالبا/طالبة)، تليها كل من **السنة ثانية ليسانس إعلام** و**السنة ثالثة ليسانس إعلام واتصال** بنسبة متساوية تقدر بـ **20%** لكل منهما (10 مشاركين لكل فئة)، أما **السنة أولى ماستر سمعي بصري** فشكّلت أقل نسبة وهي **14%** (7 مشاركين).

وهذا يظهر تنوعا في المستويات الدراسية داخل نفس المجال التخصصي، ما يعطي نظرة شاملة ومتوازنة حول الموضوع المدروس.

جدول رقم (٥): نتائج تحليل إجابات أفراد العينة على العبارة الأولى

العبارة	الاجابة	التكرار	النسبة
ما مدى معرفتك بمفهوم الأمن السيبراني؟	عالية	3	6.0
	متوسطة	27	54.0
	ضعيفة	15	30.0
	لا أعرف عنه شيئًا	5	10.0
المجمـــــــــــوع		50	**%100**



المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

حسب قراءتنا للجدول تشير النتائج إلى أن أغلب الطلبة يتمتعون بمعرفة متوسطة بمفهوم الأمن السيبراني، حيث بلغت نسبتهم 54% من إجمالي العينة، وذلك راجع إلى ضعف ال أما الطلبة الذين صرحوا بأن معرفتهم ضعيفة فقد شكلوا نسبة 30%، في حين بلغت نسبة الذين يمتلكون معرفة عالية 10%. ومن الملفت أن 6% من الطلبة لا يعرفون شيئًا عن هذا المفهوم، ما يدل على وجود فجوة معرفية تستدعي تعزيز التوعية في هذا المجال.

جدول رقم (٦): نتائج تحليل إجابات أفراد العينة على العبارة الثانية

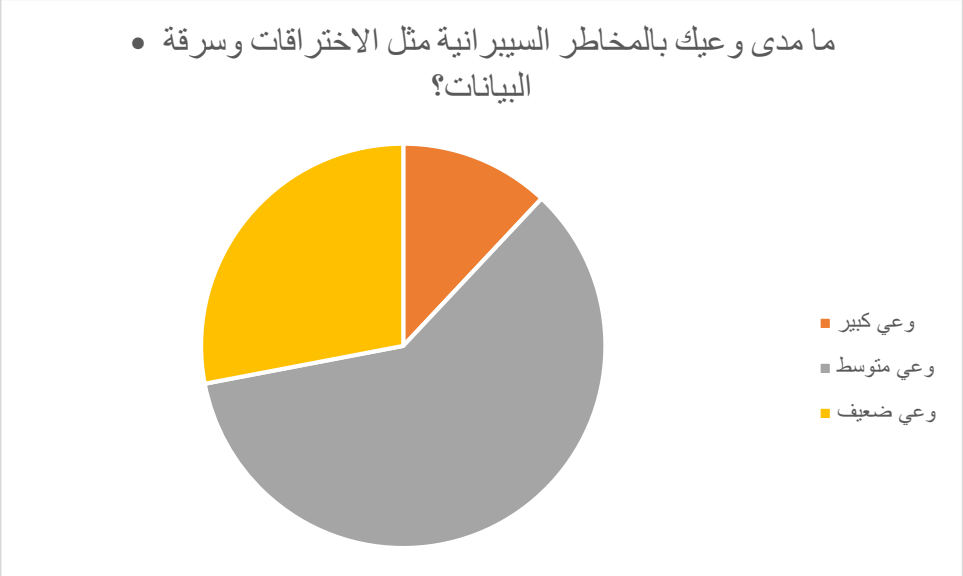
العبارة	الاجابة	التكرار	النسبة
• هل تعتقد أن الأمن السيبراني ضروري في حياتنا اليومية؟	نعم، بشكل كبير	40	80.0
	لا أعلم	8	16.0
	ليس ضروريًا	2	4.0
المجمـــــــــــوع		50	**%100**

يتضح من الجدول أن نسبة كبيرة جدا من أفراد العينة، قدرت بـ 80%، يرون أن الأمن السيبراني ضروري بشكل كبير في حياتنا اليومية ، كون أن عمليات الإختراق أصبحت تتزايد بشكل كبير بين الحين والآخر ، الأمر الذي إلى وجود وعي كبير لأهمية وجدية هذا الأمر. في المقابل، 16% أعربوا عن عدم علمهم بمدى ضرورته، بينما اعتبر 4% فقط أنه ليس ضروريا، ما يبرز وعيا جيدا لدى الأغلبية بأهمية الأمن الرقمي.

جدول رقم (٧): نتائج تحليل إجابات أفراد العينة على العبارة الثالثة

العبارة	الاجابة	التكرار	النسبة

• ما مدى وعيك بالمخاطر السيبرانية مثل الاختراقات وسرقة البيانات؟	وعي كبير	6	12.0
	وعي متوسط	30	60.0
	وعي ضعيف	14	28.0
المجمـــــــــــوع		50	%100

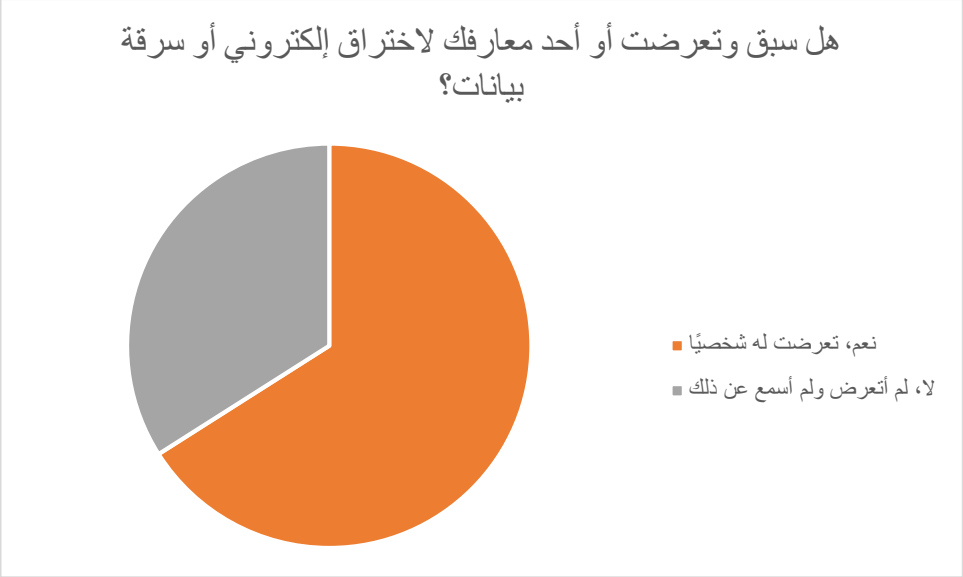


المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

أظهرت النتائج أن الوعي لا يزال بحاجة إلى تعزيز، حيث صرح 60% من المشاركين أن وعيهم بالمخاطر السيبرانية ضعيف، بينما 28% أفادوا بأن وعيهم متوسط، في حين أن فقط 12% من العينة يعتبرون وعيهم كبيرًا، وهو ما يبيّن أن أغلب الطلبة قد لا يكونون على دراية كافية بمخاطر الفضاء الرقمي.

جدول رقم (٨): نتائج تحليل إجابات أفراد العينة على العبارة الرابعة

العبارة	الاجابة	التكرار	النسبة
هل سبق وتعرضت أو أحد معارفك لاختراق إلكتروني أو سرقة بيانات؟	نعم، تعرضت له شخصيًا	33	66.0
	لا، لم أتعرض ولم أسمع عن ذلك	17	34.0
المجمـــــــــــوع		50	%100

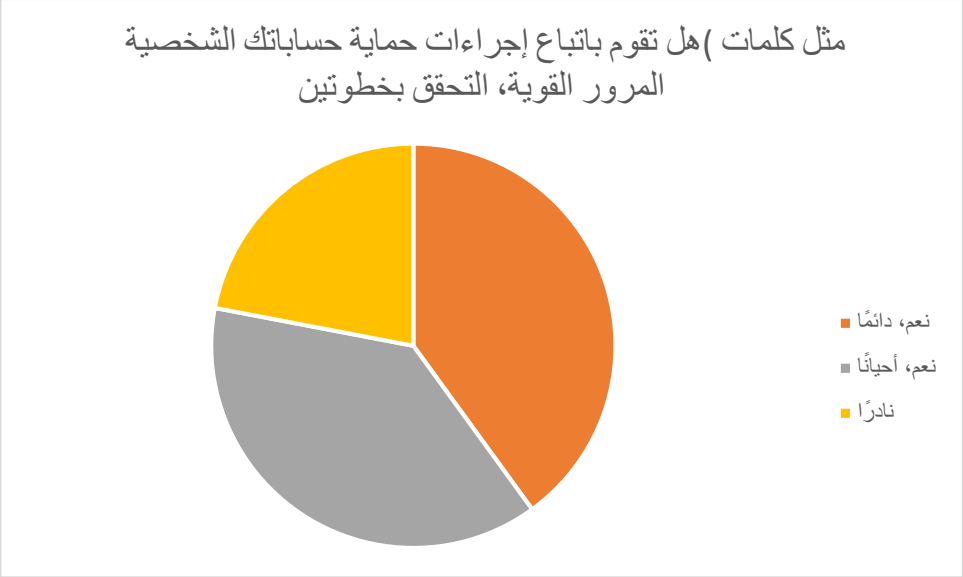


المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

يتضح من الجدول أن 66 بالمئة من المبحوثين تعرضوا إلى اختراق إلكتروني وتمت سرقة بياناتهم الشخصية في حين أن 34 بالمئة صرحوا أنهم لم يتعرضوا إلى أية اختراقات ، وهذا ما يحيلنا على أن اغلب أفراد عينة الدراسة تعرضوا لعملية الاختراق ما يظهر الحاجة الماسة إلى رفع وعيهم عبر اتخاذ إجراءات أمنية.

جدول رقم (٩): نتائج تحليل إجابات أفراد العينة على العبارة الخامسة

العبارة	الاجابة	التكرار	النسبة
هل تقوم باتباع إجراءات حماية حساباتك الشخصية (مثل كلمات المرور القوية، التحقق بخطوتين)؟	نعم، دائمًا	20	40.0
	نعم، أحيانًا	19	38.0
	نادرًا	11	22.0
المجمـــــــــــوع		50	**%100**

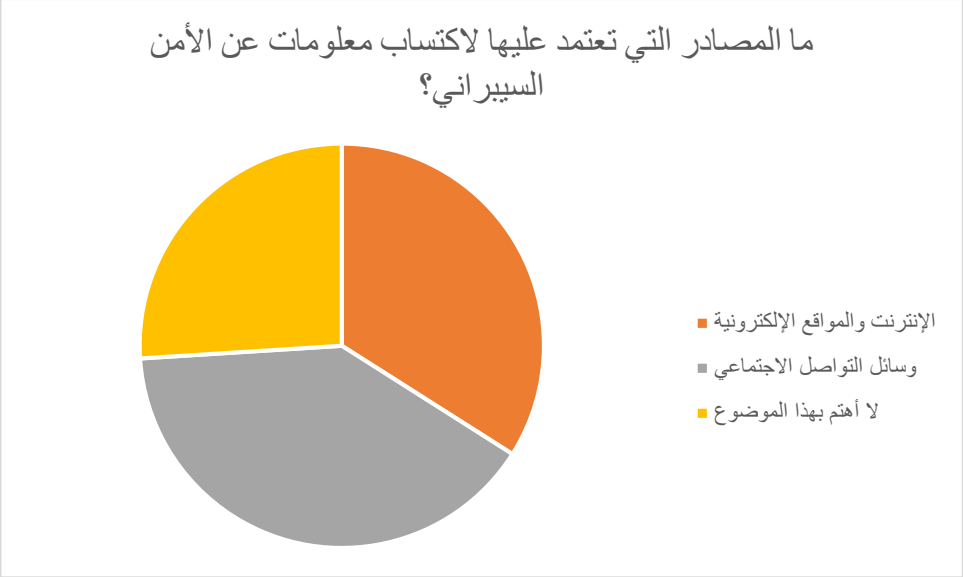


المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

بيّنت النتائج أن 40% من العينة يتبعون دائما إجراءات حماية لحساباتهم مثل كلمات مرور قوية وخطوات التحقق، و22% أفادوا بأنهم أحيانًا يتبعون هذه الإجراءات، بينما 38% من الطلبة لا يقومون باتباع أي خطوات لحماية حساباتهم، وهو مؤشر على نقص الوعي بالممارسات الأمنية الأساسية.

جدول رقم (10): نتائج تحليل إجابات أفراد العينة على العبارة السادسة

العبارة	الاجابة	التكرار	النسبة
ما المصادر التي تعتمد عليها لاكتساب معلومات عن الأمن السيبراني؟	الإنترنت والمواقع الإلكترونية	17	34.0
	وسائل التواصل الاجتماعي	20	40.0
	لا أهتم بهذا الموضوع	13	26.0
المجمـــــــــــوع		50	**%100**



المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول ، يتضح أن غالبية أفراد العينة، وعددهم ١٧ من أصل ٥٠ طالبا وطالبة، أي بنسبة **٣٤%**، يعتمدون على **الإنترنت والمواقع الإلكترونية** كمصدر أساسي لاكتساب معلومات حول الأمن السيبراني، ما يدل على توجه واضح نحو المصادر الرقمية الذاتية في البحث عن المعرفة.

يليهم في المرتبة الثانية الطلبة الذين يعتمدون على **وسائل التواصل الاجتماعي**، حيث بلغ عددهم ١٣، بنسبة **٢٦%**، وهو ما قد يعكس مدى تأثر الطلبة بالمحتوى المتداول عبر هذه المنصات، سواء كان موثوقا أم لا.

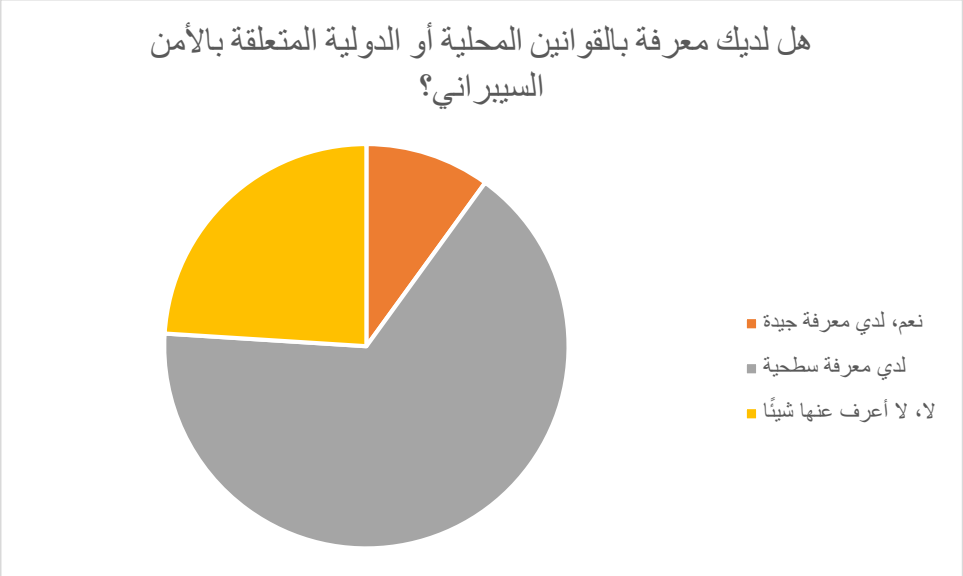
أما **المحاضرات الجامعية** فكانت مصدرًا للمعلومة بالنسبة لـ ١٠ طلبة فقط، أي ما يمثل **٢٠%**، مما يشير إلى ضعف تكامل الأمن السيبراني في البرامج التعليمية الرسمية.

في حين أن **20%** من أفراد العينة، أي 10 طلبة، **لا يعلمون شيئًا عن هذا الموضوع**، وهو مؤشر يستوجب الوقوف عنده، باعتباره يعكس نقصًا حادًا في التوعية بهذا المجال.

جدول رقم (11): نتائج تحليل إجابات أفراد العينة على العبارة السابعة

العبارة	الاجابة	التكرار	النسبة
هل لديك معرفة بالقوانين المحلية أو الدولية المتعلقة بالأمن السيبراني؟	نعم، لدي معرفة جيدة	5	10.0
	لدي معرفة سطحية	33	66.0
	لا، لا أعرف عنها شيئًا	12	24.0

المجمـــــــــــوع	50	%100



المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

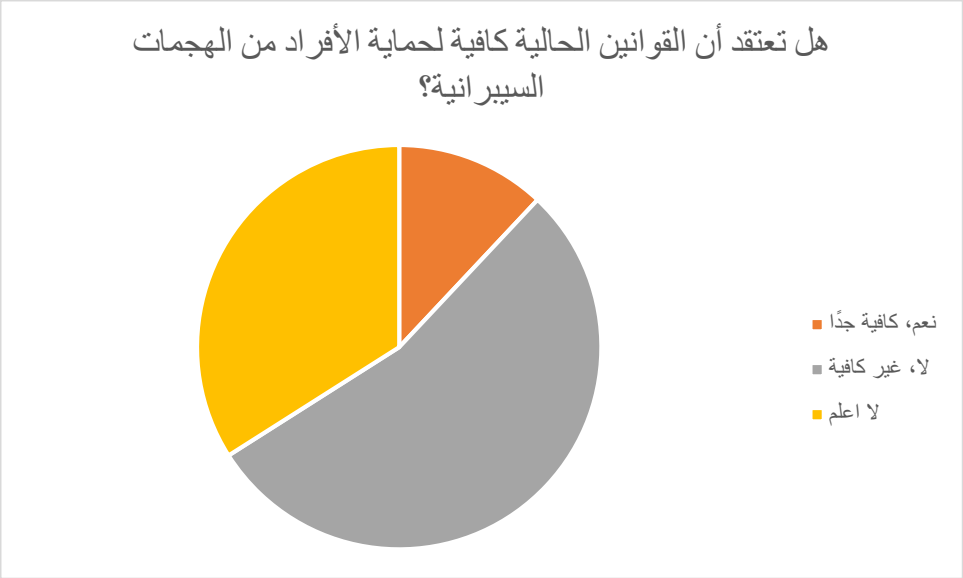
من خلال قراءتنا للجدول رقم (٢)، يتّضح أن غالبية أفراد العينة، وعددهم ٣٣ من أصل ٥٠ طالبًا وطالبة، أي بنسبة **٦٦%**، صرّحوا أنهم **لا يعرفون شيئا** عن القوانين المتعلقة بالأمن السيبراني، **مما** يدل على فجوة معرفية كبيرة في الجانب القانوني المرتبط بالفضاء السيبراني.

بينما أقر **٢٤%** منهم، أي **١٢ طالبا**، بامتلاكهم **معرفة سطحية فقط**، وهو ما يشير إلى إدراك جزئي أو محدود بالإطار القانوني لهذا الموضوع.

أما النسبة الأقل، والمتمثلة في **10%** فقط، أي **5 طلبة**، فقد أبدوا امتلاكهم **معرفة جيدة** بالقوانين المعنية، وهي نسبة ضعيفة تعكس الحاجة إلى إدماج هذا النوع من المعارف بشكل أوسع في المناهج.

جدول رقم (12): نتائج تحليل إجابات أفراد العينة على العبارة الثامنة

العبارة	الاجابة	التكرار	النسبة
هل تعتقد أن القوانين الحالية كافية لحماية الأفراد من الهجمات السيبرانية؟	نعم، كافية جدًا	6	12.0
	لا، غير كافية	27	54.0
	لا اعلم	17	34.0
المجمـــــــــــوع		50	**%100**



المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

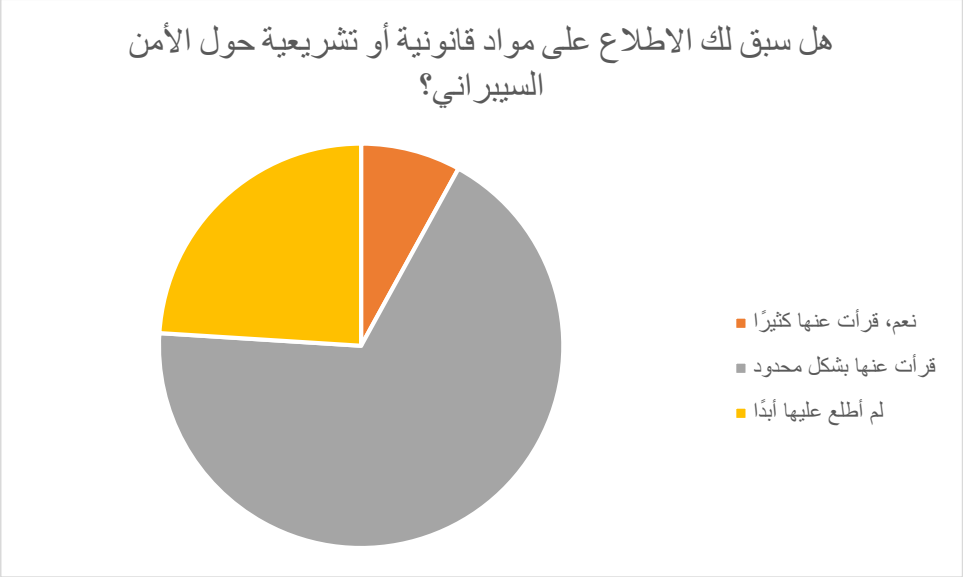
من خلال قراءتنا للجدول رقم (٣)، يتّضح أن أغلبية الطلبة، وعددهم ٢٧ من أصل ٥٠، أي بنسبة **٥٤%**، يعتقدون أن القوانين الحالية **غير كافية** لحماية الأفراد من الهجمات السيبرانية، ما يعكس عدم الثقة في المنظومة القانونية الحالية لمواجهة التحديات الإلكترونية والحاجة الماسة إلى سن قوانين أكثر جدية ضد المخترقين.

في حين أن **٣٤%** من أفراد العينة، أي **١٧ طالبا**، صرّحوا بأنهم **لا يعلمون** مدى كفاية تلك القوانين، مما يعكس مرة أخرى نقصًا في التوعية القانونية.

أما فقط **٦ طلبة**، أي **١٢%**، فقد عبّروا عن اعتقادهم بأن القوانين **كافية جدا**، وهي نسبة قليلة توحي بوجود إجماع نسبي على ضرورة تطوير الأطر التشريعية الحالية.

جدول رقم (13): نتائج تحليل إجابات أفراد العينة على العبارة التاسعة

العبارة	الاجابة	التكرار	النسبة
هل سبق لك الاطلاع على مواد قانونية أو تشريعية حول الأمن السيبراني؟	نعم، قرأت عنها كثيرًا	4	8.0
	قرأت عنها بشكل محدود	34	68.0
	لم أطلع عليها أبدًا	12	24.0
المجمـــــــــــوع		50	**%100**



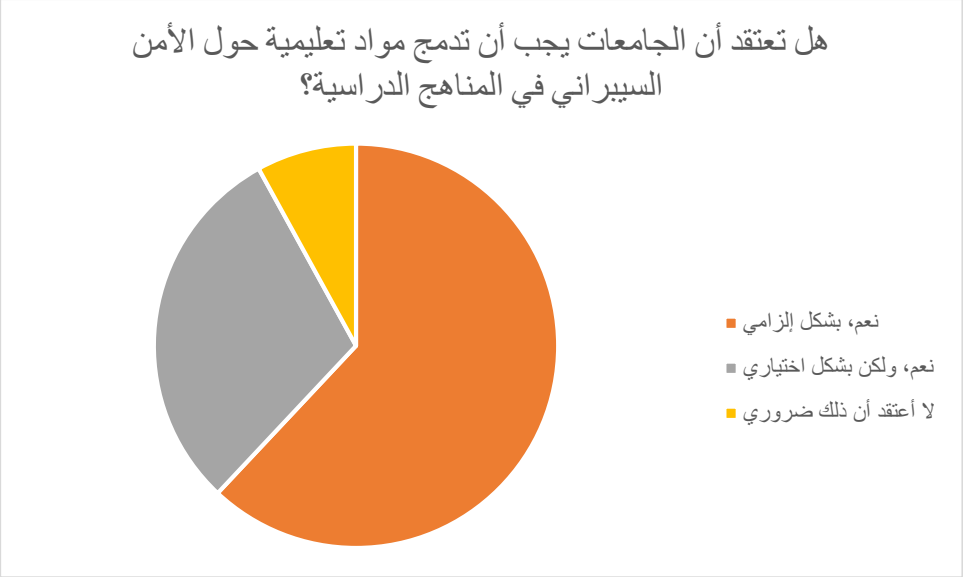
المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (٤)، يتّضح أن أغلب أفراد العينة، وعددهم ٣٤ من أصل ٥٠، أي بنسبة **٦٨%**، لم يسبق لهم أن **اطلعوا على أي مواد قانونية أو تشريعية** متعلقة بالأمن السيبراني، وهو ما يبين بوضوح غياب هذا النوع من المحتوى في المسارات التعليمية أو ضعف الوصول إليه.

أما **١٢ طالبا**، أي بنسبة **٢٤%**، فأشاروا إلى أنهم **قرأوا عنها بشكل محدود**، فيما صرّح فقط **٤ طلاب**، أي بنسبة **٨%**، أنهم **اطلعوا عليها جيدا**، وهي نسبة تعكس ضعفا عاما في الثقافة القانونية المرتبطة بالأمن الرقمي.

جدول رقم (١٣): نتائج تحليل إجابات أفراد العينة على العبارة العاشرة

العبارة	الاجابة	التكرار	النسبة
هل تعتقد أن الجامعات يجب أن تدمج مواد تعليمية حول الأمن السيبراني في المناهج الدراسية؟	نعم، بشكل إلزامي	31	62.0
	نعم، ولكن بشكل اختياري	15	30.0
	لا أعتقد أن ذلك ضروري	4	8.0
المجمـــــــــــوع		50	**%100**



المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

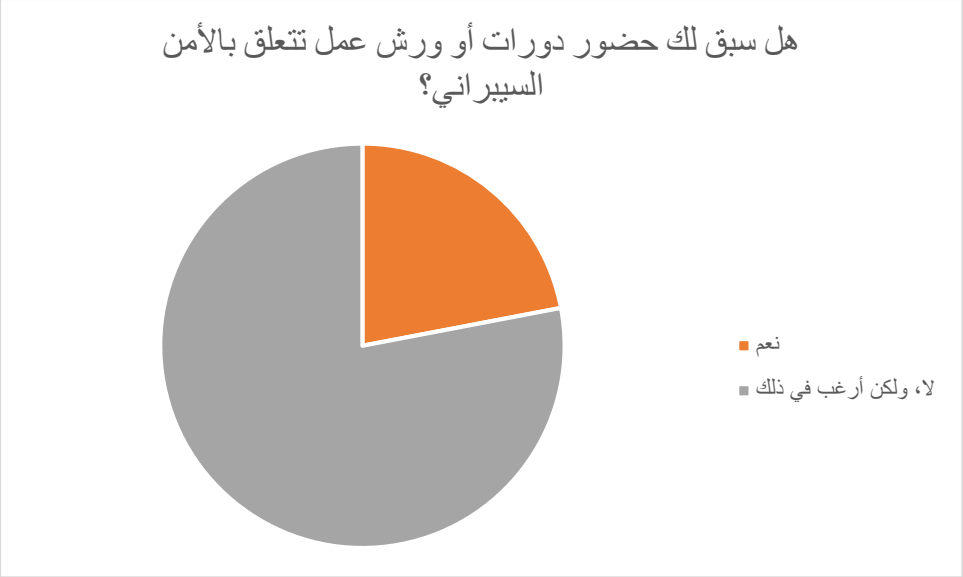
من خلال قراءتنا للجدول رقم (٥)، يتّضح أن الغالبية العظمى من الطلبة، وعددهم ٣١ من أصل ٥٠، أي بنسبة **٦٢%**، يعتقدون أنه من **الضروري إدماج مواد تطبيقية حول الأمن السيبراني** ضمن المناهج الجامعية، ما يدل على وعي متزايد بأهمية التكوين الأكاديمي في هذا المجال.

بينما وافق **١٥ طالبا**، أي بنسبة **٣٠%**، على الفكرة لكنهم اعتبروها **غير أساسية**، وهو ما يشير إلى اختلاف في أولويات بعض الطلبة.

أما **4 طلبة** فقط، أي بنسبة **8%**، فقد عبّروا عن عدم اقتناعهم بهذه الفكرة، وهي نسبة ضئيلة تعكس غالبًا ضعف اهتمامهم أو عدم وعيهم بأهمية الموضوع.

جدول رقم (13): نتائج تحليل إجابات أفراد العينة على العبارة الحادية عشر

العبارة	الاجابة	التكرار	النسبة
هل سبق لك حضور دورات أو ورش عمل تتعلق بالأمن السيبراني؟	نعم	11	22.0
	لا، ولكن أرغب في ذلك	39	78.0
المجمـــــــــــوع		50	**%100**



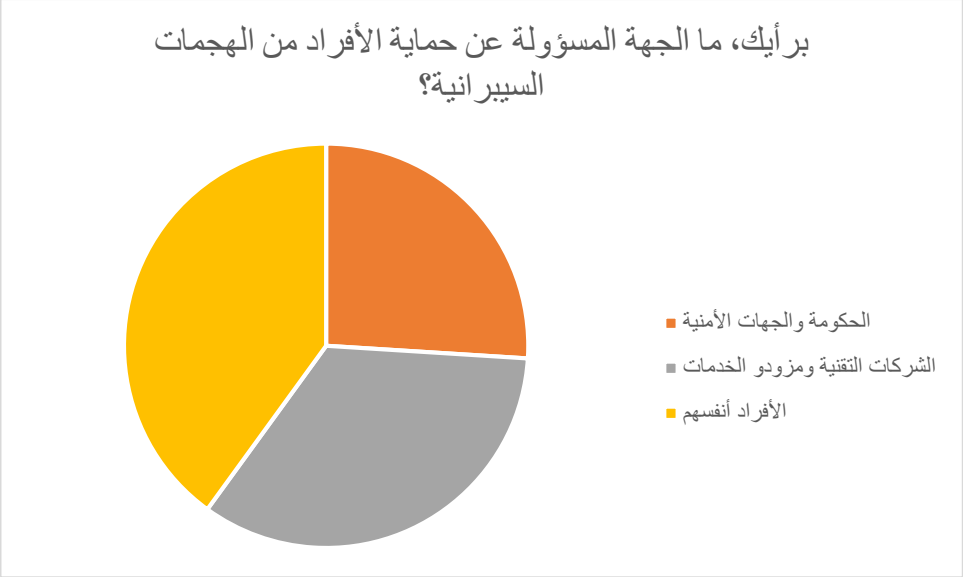
المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (٦)، يتّضح أن الغالبية العظمى من الطلبة، وعددهم ٣٩ من أصل ٥٠، أي بنسبة **٧٨%**، لم يسبق لهم **حضور أي دورات أو ورش عمل** حول الأمن السيبراني، وهو ما يشير إلى نقص واضح في المبادرات التكوينية بهذا المجال أو عدم اهتمام الطلبة بالالتحاق بها لكنهم يريدون أن يتعلمون في مجال الأمن السيبيراني لدوره الكبير في حماية بيانات المستخدم.

بينما صرّح **١١ طالبا** فقط، أي بنسبة **٢٢%**، أنهم سبق لهم حضور **دورات أو ورش عمل**، وهي نسبة ضعيفة تعكس قلة الفرص أو ضعف الإقبال عليها.

جدول رقم (14): نتائج تحليل إجابات أفراد العينة على العبارة الثانية عشر

العبارة	الاجابة	التكرار	النسبة
برأيك، ما الجهة المسؤولة عن حماية الأفراد من الهجمات السيبرانية؟	الحكومة والجهات الأمنية	13	26.0
	الشركات التقنية ومزودو الخدمات	17	34.0
	الأفراد أنفسهم	20	40.0
المجمـــــــــــوع		50	**%100**



المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

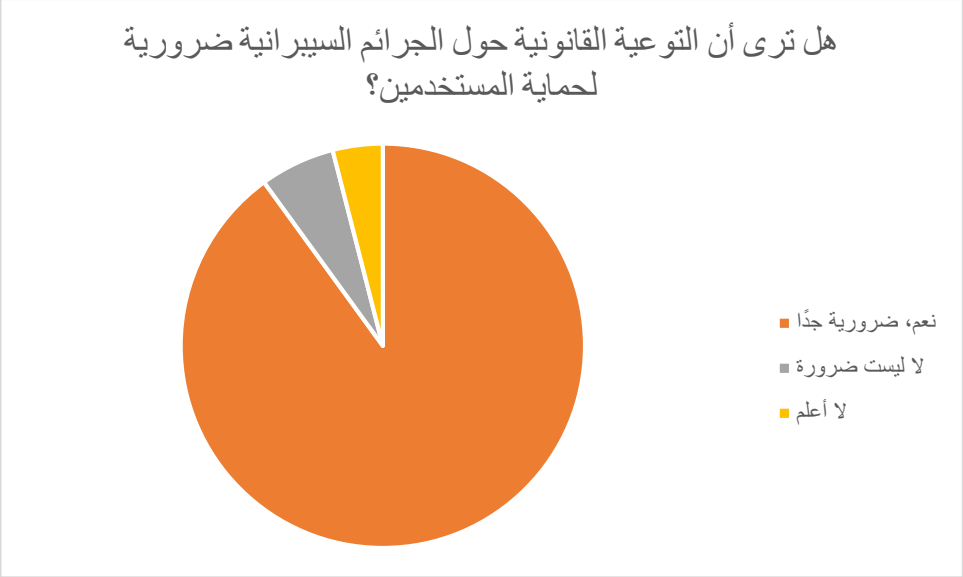
من خلال قراءتنا للجدول رقم (٧)، نلاحظ تباينا في تصورات أفراد العينة، حيث اعتبر **٤٠%** منهم، أي **٢٠ طالبا**، أن **الأفراد أنفسهم** مسؤولون عن حمايتهم من الهجمات السيبرانية، وهو ما يعكس توجها نحو تحميل الفرد مسؤولية حماية نفسه رقميا ، كونه هو المتحكم في حاسوبه ولا تتحمل الشركات التقنية و الحكومة أية مسؤولية جراء دخول الفرد إلى مواقع غير موثوقة.

بينما رأى **١٧ طالبا**، بنسبة **٣٤%**، أن **الشركات الكبرى ومزودي الخدمات** يتحملون المسؤولية، مما يشير إلى توقعات بدور أكبر من القطاع الخاص مثل تخصيص أجهزة وحواسيب ذات نظام عالي من الحماية بحيث لا يستطيع أي أحد الولوج لها أو سرقة البيانات للمستخدم.

أما **١٣ طالبا**، أي بنسبة **٢٦%**، فقد أشاروا إلى أن المسؤولية تقع على عاتق **الحكومة والجهات الأمنية**، وهو ما يدل على وعي بدور الدولة في التشريع والحماية.

جدول رقم (15): نتائج تحليل إجابات أفراد العينة على العبارة الثالثة عشر

العبارة	الاجابة	التكرار	النسبة
هل ترى أن التوعية القانونية حول الجرائم السيبرانية ضرورية لحماية المستخدمين؟	نعم، ضرورية جدًا	45	90.0
	لا ليست ضرورة	3	6.0
	لا أعلم	2	4.0
المجمـــــــــــوع		50	%100



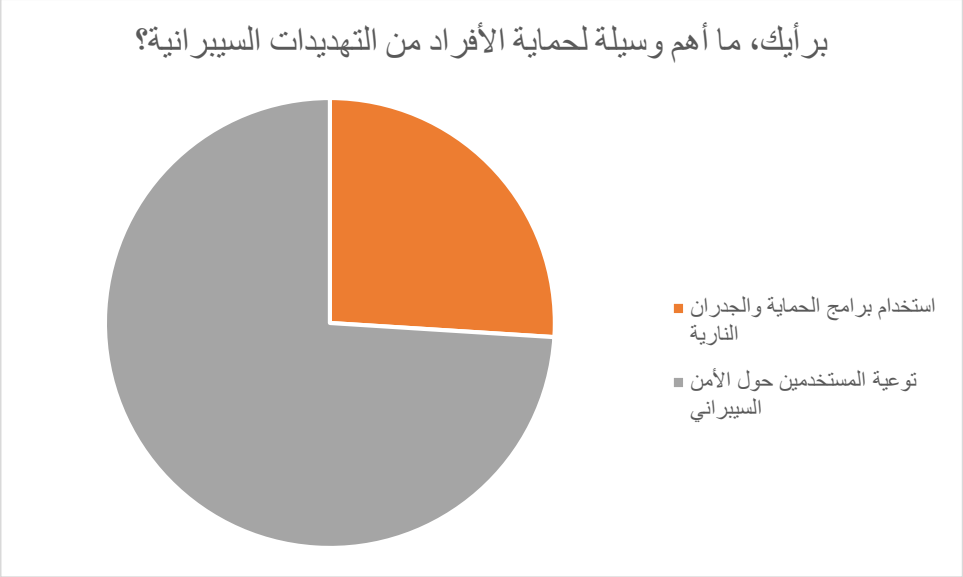
المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (٨)، نلاحظ اتفاقا شبه تام بين أفراد العينة، حيث صرّح **٤٥ طالبا** من أصل ٥٠، أي بنسبة **٩٠%**، بأن **التوعية القانونية ضرورية جدا** لحماية المستخدمين من الجرائم السيبرانية، مما يدل على وعي مرتفع بأهمية الجانب القانوني في الوقاية.

في المقابل، رأى **3 طلبة فقط**، أي بنسبة **6%**، أنها **ليست ضرورية**، بينما **طالبان فقط**، بنسبة **4%**، صرحا بأنهم **لا يعلمون**، ما يعني أن الرفض شبه منعدم، والتردد محدود جدا.

جدول رقم (16): نتائج تحليل إجابات أفراد العينة على العبارة الرابعة عشر

العبارة	الاجابة	التكرار	النسبة
برأيك، ما أهم وسيلة لحماية الأفراد من التهديدات السيبرانية؟	استخدام برامج الحماية والجدران النارية	13	26.0
	توعية المستخدمين حول الأمن السيبراني	37	74.0
المجمـــــــــــوع		50	**%100**



المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

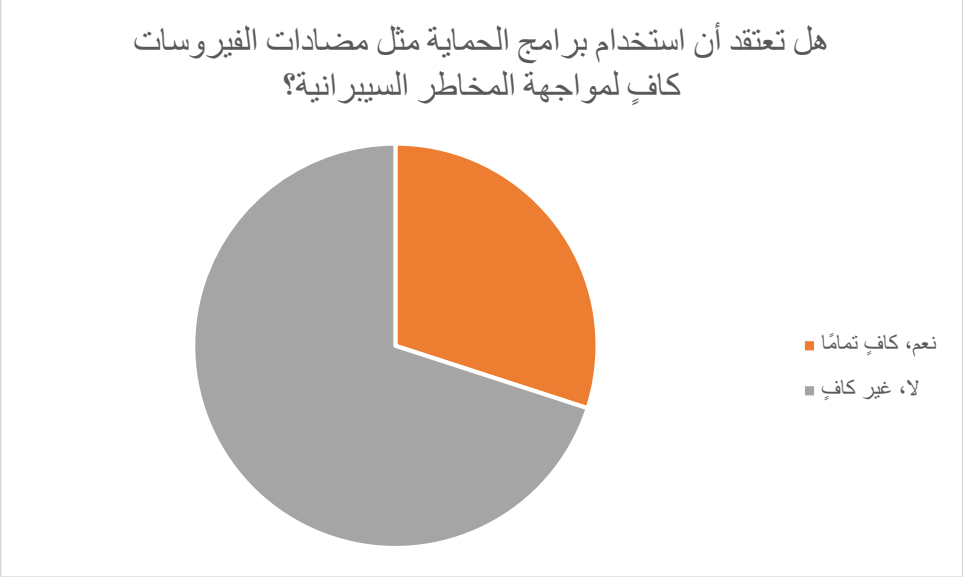
من خلال قراءتنا للجدول رقم (٩)، يتّضح أن نصف العينة، أي **٢٥ طالبا** بنسبة **٥٠%**، يعتقدون أن **توعية المستخدمين حول الأمن السيبراني** هي الوسيلة الأهم للحماية، مما يعكس إدراكا لأهمية الجانب التوعوي والتثقيفي من حملات تحسيسية وانشاء ورشات عمل وتدريب لتعزيز هذا الأمر .

في حين رأى **١٣ طالبا**، بنسبة **٢٦%**، أن **استخدام برامج الحماية والجدران النارية** يمثل الوسيلة الأهم، ما يعكس توجهًا نحو الحلول التقنية.

أما **١٢ طالبا**، أي بنسبة **٢٤%**، فقد اعتبروا أن **تفعيل القوانين الصارمة ضد المخترقين** هو الوسيلة الأهم، في إشارة إلى أهمية الردع القانوني.

جدول رقم (17): نتائج تحليل إجابات أفراد العينة على العبارة الخامسة عشر

العبارة	الاجابة	التكرار	النسبة
هل تعتقد أن استخدام برامج الحماية مثل مضادات الفيروسات كافٍ لمواجهة المخاطر السيبرانية؟	نعم، كافٍ تمامًا	15	30.0
	لا، غير كافٍ	35	70.0
المجمـــــــــــوع		50	%100



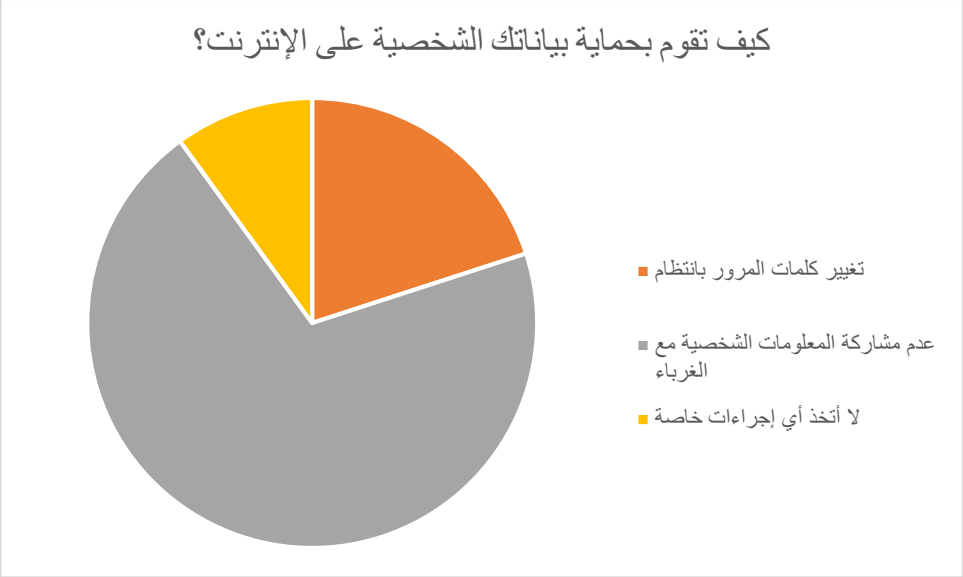
المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (١٠)، نلاحظ أن أغلب أفراد العينة، وعددهم ٣٥ من أصل ٥٠، أي بنسبة **٧٠%**، يعتقدون أن **برامج الحماية غير كافية** لمواجهة المخاطر السيبرانية، مما يدل على وعي بوجود تهديدات تتجاوز قدرة البرامج التقنية وحدها.

بينما يرى **15 طالبا** فقط، أي بنسبة **30%**، أن **تلك البرامج كافية تمامًا**، وهو ما يعكس اختلافًا في التقدير بين الحلول التقنية وحدها وبين أهمية الحلول الشاملة التي تشمل التوعية والقوانين أيضا.

جدول رقم (18): نتائج تحليل إجابات أفراد العينة على العبارة السادسة عشر

العبارة	الاجابة	التكرار	النسبة
كيف تقوم بحماية بياناتك الشخصية على الإنترنت؟	تغيير كلمات المرور بانتظام	10	20.0
	عدم مشاركة المعلومات الشخصية مع الغرباء	35	70.0
	لا أتخذ أي إجراءات خاصة	5	10.0
المجمـــــــــــوع		50	**%100**



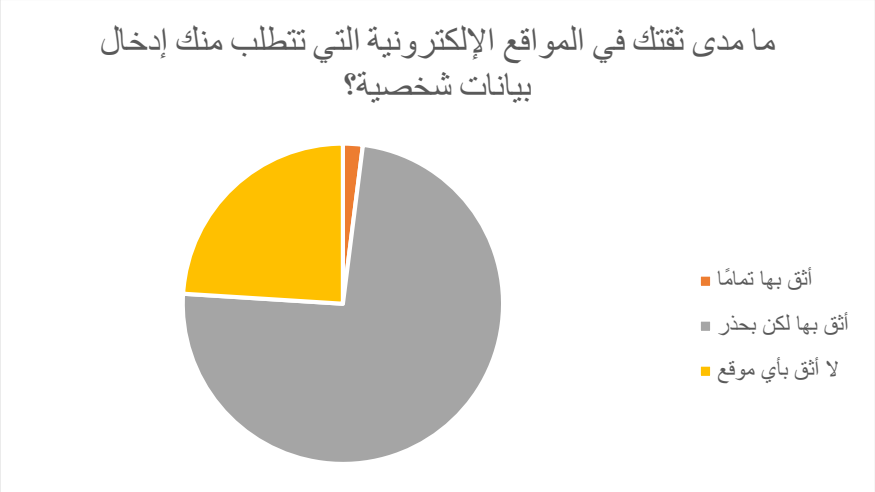
المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (١١)، نلاحظ أن الغالبية، وعددهم **٣٥ طالبا** من أصل ٥٠، أي بنسبة **٧٠%**، صرّحوا بأنهم **لا يتخذون أي إجراءات خاصة** لحماية بياناتهم، وهو ما يعد مؤشرا خطيرا على غياب الثقافة الوقائية الرقمية.

بينما أشار **١٠ طلبة**، بنسبة **٢٠%**، إلى أنهم يعتمدون على **عدم مشاركة المعلومات الشخصية نهائيًا**، في حين اكتفى **٥ طلاب فقط**، أي بنسبة **١٠%**، بذكر أنهم يقومون **بتغيير كلمات المرور بانتظام**.

جدول رقم (19): نتائج تحليل إجابات أفراد العينة على العبارة السابعة عشر

العبارة	الاجابة	التكرار	النسبة
ما مدى ثقتك في المواقع الإلكترونية التي تتطلب منك إدخال بيانات شخصية؟	أثق بها تمامًا	1	2.0
	أثق بها لكن بحذر	37	74.0
	لا أثق بأي موقع	12	24.0
المجمـــــــــــوع		50	**%100**



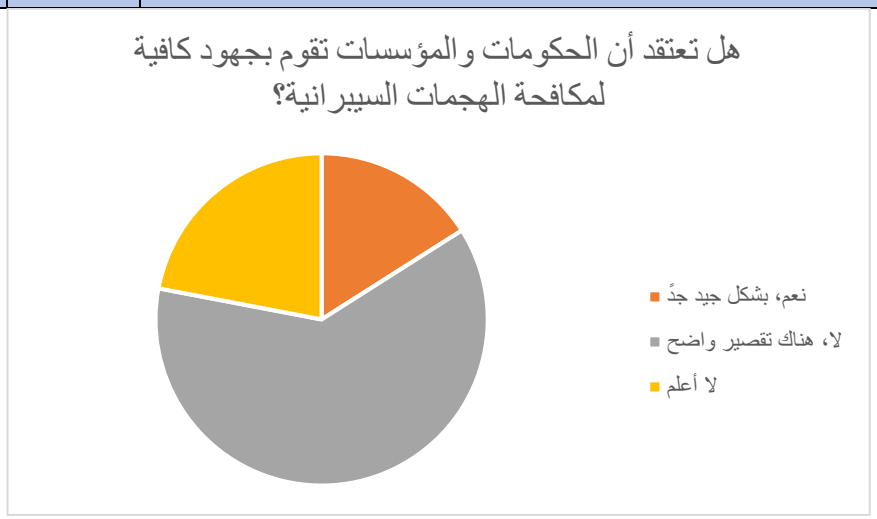
المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (١٢)، نجد أن النسبة الأكبر، والمقدرة بـ **٧٤%** (٣٧ طالبا)، **لا يثقون بأي موقع** يطلب إدخال بياناتهم، وهو ما يعكس حالة من الحذر أو فقدان الثقة العامة بالمواقع بسبب ما تقدمه من فيروسات وأضرار على الأجهزة بالإضافة إلى سرقة بيانات الخاصة بالمستخدم.

بينما صرّح **12 طالبا**، بنسبة **24%**، أنهم **يثقون لكن بحذر**، في حين أن **طالبًا واحدًا فقط**، بنسبة **2%**، صرح بأنه **يثق بها تماما**، ما يعزز فكرة وجود تحفظات كبيرة لدى المبحوثين في هذا الجانب.

جدول رقم (20): نتائج تحليل إجابات أفراد العينة على العبارة الثامنة عشر

العبارة	الاجابة	التكرار	النسبة
هل تعتقد أن الحكومات والمؤسسات تقوم بجهود كافية لمكافحة الهجمات السيبرانية؟	نعم، بشكل جيد جدً	8	16.0
	لا، هناك تقصير واضح	31	62.0
	لا أعلم	11	22.0
المجمـــــــــــوع		50	**%100**



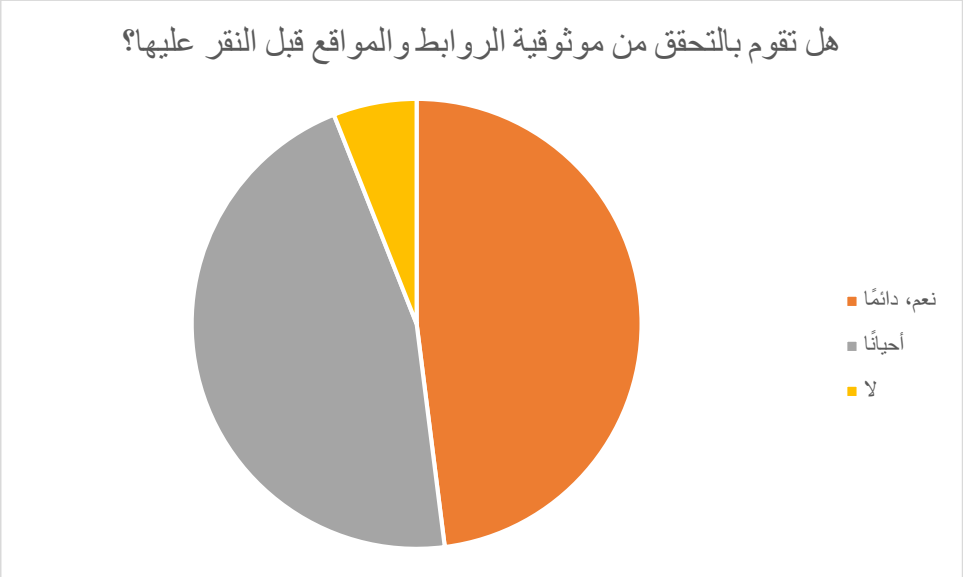
المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (١٣)، يتّضح أن **٣١ طالبا** من أصل ٥٠، بنسبة **٦٢%**، يعتقدون أن هناك **تقصيرا أو برامج غير كافية** من طرف الحكومات والمؤسسات في مجال مكافحة الهجمات السيبرانية.

بينما عبّر **١١ طالبًا**، بنسبة **٢٢%**، عن عدم معرفتهم أو وضوح الرؤية لديهم، واكتفى **٨ منهم فقط**، بنسبة **١٦%**، بالإجابة بـ"نعم بشكل جيد جدًا"، ما يعكس حالة من عدم الرضا أو ضعف الثقة في الجهود الرسمية المبذولة ، الأمر الذي يستدعي الحاجة إلى بذل المزيد من الجهود .

جدول رقم (21): نتائج تحليل إجابات أفراد العينة على العبارة التاسعة عشر

العبارة	الاجابة	التكرار	النسبة
هل تقوم بالتحقق من موثوقية الروابط والمواقع قبل النقر عليها؟	نعم، دائمًا	24	48.0
	أحيانًا	23	46.0
	لا	3	6.0
المجمـــــــــــوع		50	%100



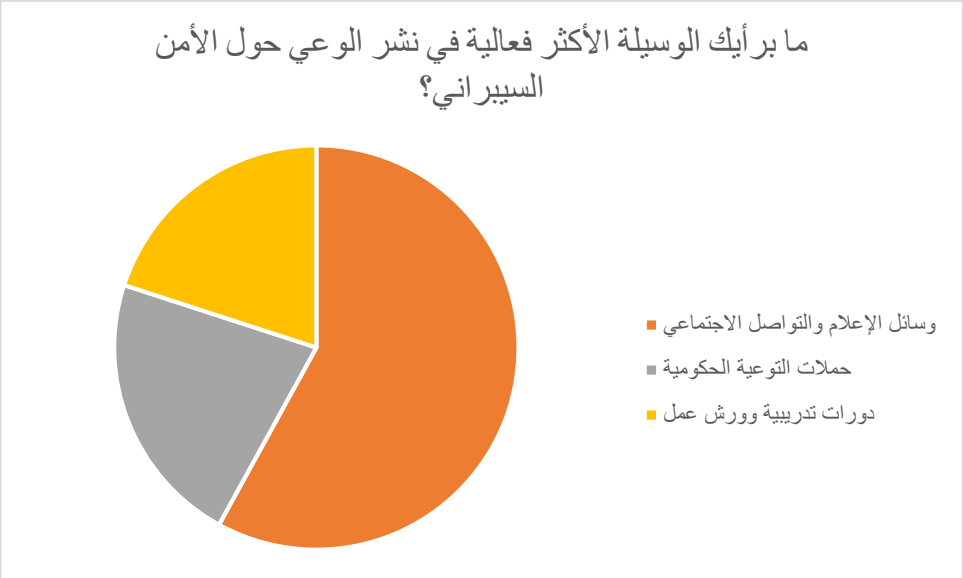
المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (١٤)، نلاحظ أن **٤٨%** من المبحوثين، أي **٢٤ طالبا**، **يتحققون دائما** من موثوقية الروابط والمواقع قبل التفاعل معها وهو ما يدل على أن اغلب المبحوثين على علم بكواليس هذه المواقع وما تقدمه من فيروسات على الأجهزة.

في المقابل، قال **٢٣ طالبا**، بنسبة **٤٦%**، إنهم **يفعلون ذلك أحيانا فقط**، بينما أجاب **٣ طلبة فقط**، بنسبة **٦%**، أنهم **لا يقومون بأي تحقق**، وهو ما يشير إلى وعي متوسط إلى مرتفع بهذا السلوك الوقائي.

جدول رقم (22): نتائج تحليل إجابات أفراد العينة على العبارة العشرين

العبارة	الاجابة	التكرار	النسبة
ما برأيك الوسيلة الأكثر فعالية في نشر الوعي حول الأمن السيبراني؟	وسائل الإعلام والتواصل الاجتماعي	29	58.0
	حملات التوعية الحكومية	11	22.0
	دورات تدريبية وورش عمل	10	20.0
المجمـــــــــــوع		50	**%100**



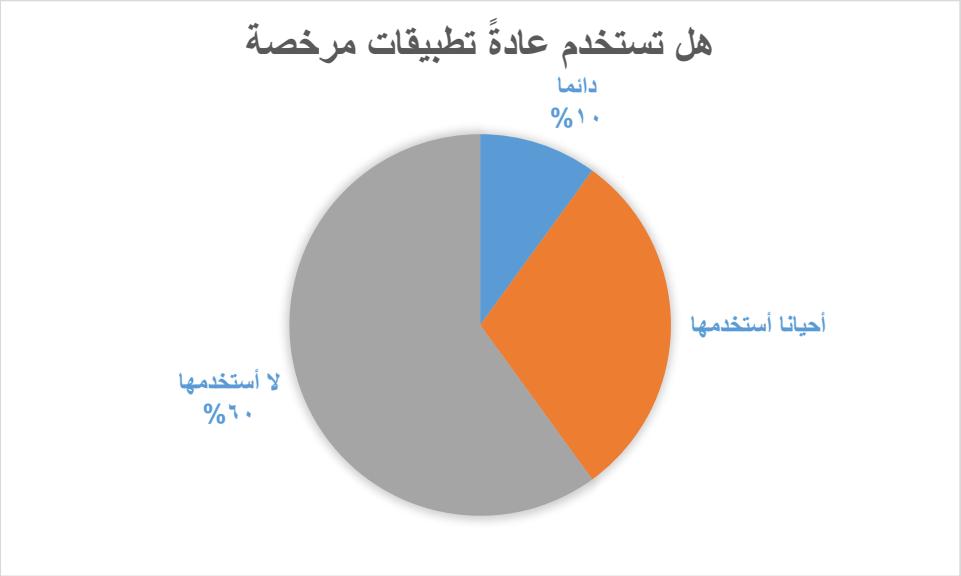
المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (١٥)، نلاحظ أن النسبة الأكبر من المبحوثين، وعددهم **٢٩ طالبًا** من أصل ٥٠، أي بنسبة **٥٨%**، يرون أن **وسائل الإعلام ووسائل التواصل الاجتماعي** هي الأداة الأكثر فعالية في نشر الوعي حول الأمن السيبراني وذلك بسبب الدور الكبير التي تلعبه هذه الوسائل في التوعية كون لها تأثير ثوي على الأفراد في شتى المجالات.

بينما اختار **11 طالبا**، بنسبة **22%**، **الدورات التدريبية وورش العمل**، في حين فضّل **10 طلبة**، بنسبة **20%**، **حملات التوعية الحكومية**، ما يعكس تنوعا في وجهات النظر وتقديرا لدور مختلف الوسائل.

جدول رقم (23): نتائج تحليل إجابات أفراد العينة على العبارة الواحدة والعشرين

العبارة	الاجابة	التكرار	النسبة
هل تستخدم عادةً تطبيقات مرخصة (مثل Microsoft Office، Adobe) في أعمالك الدراسية؟	دائما	05	10.0
	أحيانا	15	30.0
	لا أستخدمها	30	60.0
المجمـــــــــــوع		50	%100



المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

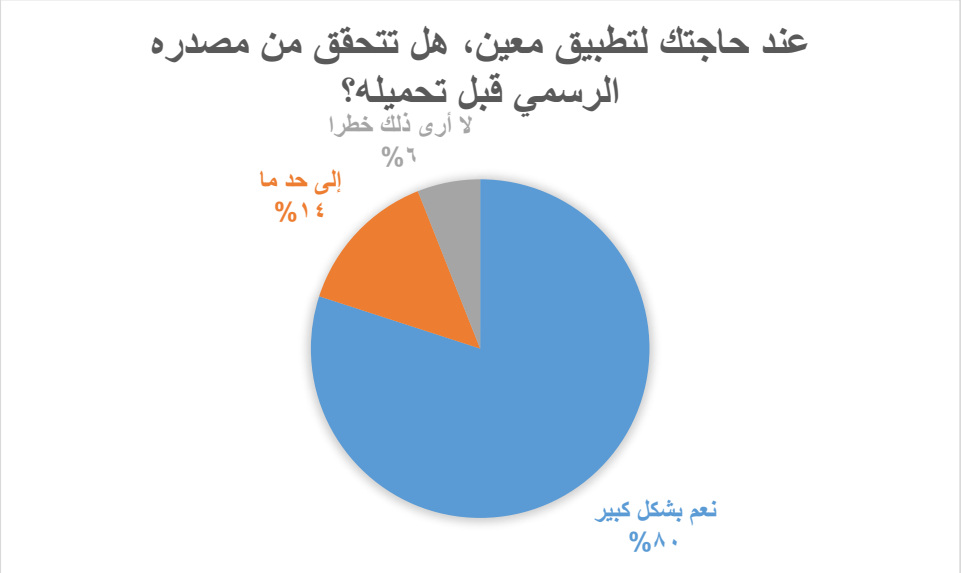
من خلال قراءتنا للجدول رقم (٢٣)، نلاحظ أن النسبة الأكبر من المبحوثين، وعددهم ٣٠ طالبًا من أصل ٥٠، أي بنسبة ٦٠%، صرّحوا بأنهم لا يستخدمون عادة التطبيقات المرخصة (مثل Microsoft Office وAdobe) في أعمالهم الدراسية، وهو ما يدل على وجود عزوف ملحوظ عن استخدام البرمجيات الأصلية، إما بسبب ارتفاع تكلفتها أو توافر بدائل مجانية تسد احتياجاتهم. في المقابل، نجد أن ١٥ مبحوثا، أي بنسبة ٣٠%، أفادوا بأنهم يستخدمون هذه التطبيقات أحيانا، ما يشير إلى اعتماد انتقائي أو محدود على البرمجيات المرخصة، قد يكون مرتبطًا بتوفرها في الحرم الجامعي أو خلال بعض المهام الأكاديمية فقط. أما الفئة التي تستخدمها دائمًا فتمثل الأقلية، وعددها ٥ فقط من أصل ٥٠، أي بنسبة ١٠%، وهي نسبة ضعيفة قد تعكس وعيا رقميا أعلى أو قدرة على تحمل تكاليف هذه البرمجيات.

جدول رقم (24): نتائج تحليل إجابات أفراد العينة على العبارة الثانية والعشرين

العبارة	الاجابة	التكرار	النسبة
	دائما	10	20.0

عند حاجتك لتطبيق معين، هل تتحقق من مصدره الرسمي قبل تحميله؟	أحيانا	10	20.0
	لا اهتم بذلك	30	60.0
المجمـــــــــــوع		50	%100

المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

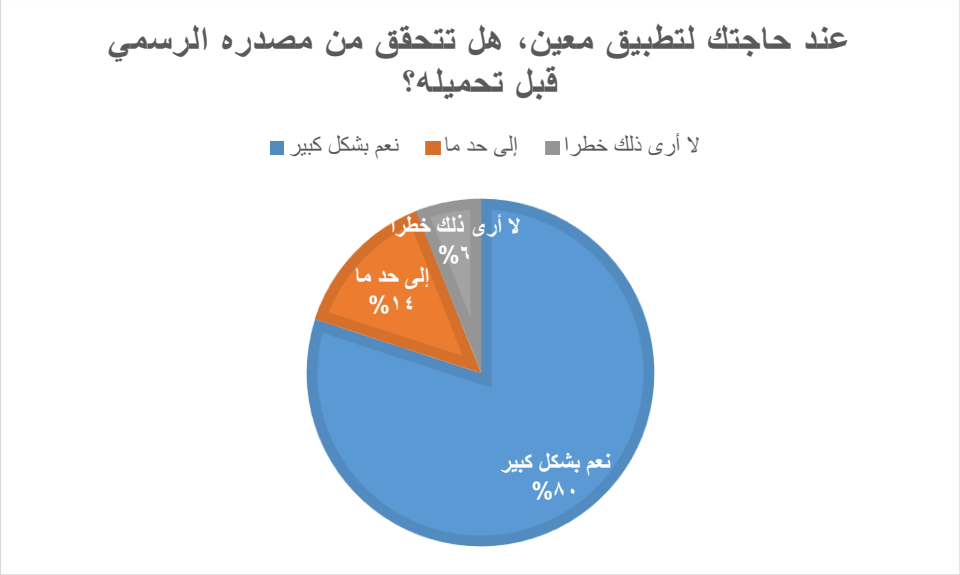


المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (١٦)، نلاحظ أن النسبة الأكبر من المبحوثين، وعددهم ٣٠ طالبًا من أصل ٥٠، أي بنسبة ٦٠%، أفادوا بأنهم لا يهتمون بالتحقق من المصدر الرسمي عند تحميل التطبيقات، وهو ما يكشف عن ضعف واضح في الوعي الرقمي والأمن السيبراني لدى هذه الفئة، خاصة في ظل الانتشار الواسع للتطبيقات المزيفة والبرمجيات الخبيثة التي قد تستهدف بيانات المستخدمين. في المقابل، نجد أن هناك ١٠ مبحوثين فقط (أي بنسبة ٢٠%) يتحققون دائمًا من مصدر التطبيق قبل تحميله، ما يدل على وجود وعي أمني جيد لدى هذه الفئة، بينما اختار نفس العدد (١٠ أفراد بنسبة ٢٠%) خيار "أحيانًا"، ما يعكس سلوكًا متذبذبًا في التعامل مع مصادر التطبيقات قد يرتبط بعوامل مثل الاستعجال أو الثقة المسبقة ببعض المتاجر.

جدول رقم (25): نتائج تحليل إجابات أفراد العينة على العبارة الثالثة والعشرين

العبارة	الاجابة	التكرار	النسبة
هل ترى أن استخدام تطبيقات غير مرخصة يُعرّض جهازك ومعلوماتك للخطر؟	نعم بشكل كبير	40	80.0
	إلى حد ما	07	14.0
	لا أرى ذلك خطرا	03	6.0
المجمـــــــــــوع		50	%100

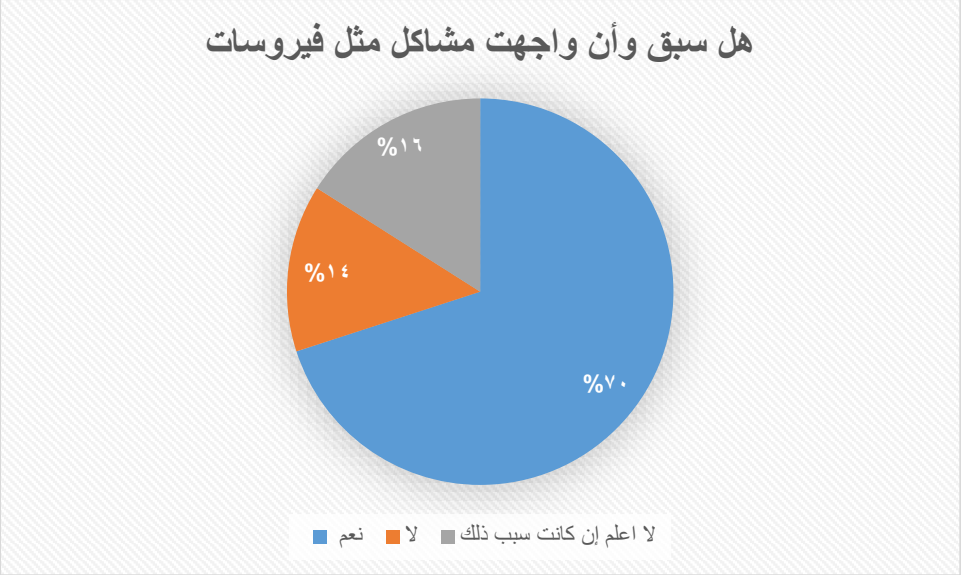


المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (١٧)، نلاحظ أن النسبة الساحقة من المبحوثين، وعددهم ٤٠ طالبًا من أصل ٥٠، أي بنسبة ٨٠%، يرون أن استخدام تطبيقات غير مرخصة يُعرّض أجهزتهم ومعلوماتهم الشخصية للخطر بشكل كبير، ما يعكس وعيًا متقدمًا بخطورة البرمجيات المقرصنة وتأثيرها على أمن المعلومات وسلامة الأجهزة الرقمية. كما تشير النتائج إلى أن ٧ مبحوثين فقط (أي بنسبة ١٤%) يرون أن هذا الخطر موجود "إلى حد ما"، وهو ما يمكن تفسيره بوجود تصور جزئي أو محدود للمخاطر الرقمية، قد يكون ناتجًا عن تجارب سابقة أو عن معلومات غير مكتملة حول هذا الموضوع. أما النسبة المتبقية، وعددها ٣ فقط (٦%)، فتعتقد أنه لا توجد مخاطر حقيقية مرتبطة باستخدام هذه التطبيقات، وهو ما يدل على ضعف كبير في الإدراك الأمني الرقمي، وقد يعرضهم لمشكلات تتعلق بالاختراقات أو فقدان البيانات.

جدول رقم (26): نتائج تحليل إجابات أفراد العينة على العبارة الرابعة والعشرين

العبارة	الاجابة	التكرار	النسبة
هل سبق وأن واجهت مشاكل (مثل فيروسات، فقدان بيانات) بسبب استخدام برامج غير رسمية؟	نعم	35	70.0
	لا	07	14.0
	لا اعلم إن كانت سبب ذلك	08	16.0
المجمـــــــــــوع		50	**%100**



المصدر: من إعداد الطلبة بناء على مخرجات برنامج SPSS V29.

من خلال قراءتنا للجدول رقم (٢٦)، نلاحظ أن غالبية المبحوثين، وعددهم ٣٥ طالبًا من أصل ٥٠، أي بنسبة ٧٠%، صرّحوا بأنهم سبق وأن واجهوا مشاكل مثل الفيروسات أو فقدان البيانات بسبب استخدامهم لبرامج غير رسمية. هذا المعطى يعكس بشكل مباشر التأثيرات السلبية الواقعية والمباشرة التي قد تنتج عن اللجوء إلى البرمجيات غير المرخصة، ويؤكد مدى هشاشة هذه البرمجيات من الناحية الأمنية. وفي المقابل، صرّح ٧ مبحوثين فقط، أي بنسبة ١٤%، بأنهم لم يواجهوا مثل هذه المشاكل، ما قد يشير إلى استخدام حذر أو محدود لهذه البرامج، أو ربما إلى اعتمادهم على وسائل حماية فعّالة. أما الفئة المتبقية، وعددها ٨ طلاب بنسبة ١٦%، فأفادت بأنها لا تعلم ما إذا كانت المشاكل التي تعرضت لها ناتجة عن استخدام برامج غير رسمية، ما يكشف عن نقص في الثقافة التقنية أو عدم القدرة على تحديد مصادر الخلل الرقمي بدقة.

المطلب الثاني: مناقشة نتائج الدراسة في ضوء الدراسات السابقة والتساؤلات الفرعية

أ/ في ضوء الدراسات السابقة:

بعد التطرق لنتائج التي توصلت إليها الدراسة في ضوء التساؤلات للتعرف على درجة وعي بالأمن السيبيراني والمعلومات الرقمية لدى طلبة الإعلام والاتصال بجامعة الوادي، ومن خلال التعرض إلى مختلف ما أوردته الدراسات السابقة في بيئات أخرى حول موضوع الذي تعالجه هذه الدراسة، سوف نناقش نتائج الدراسة الحالية مع الدراسات السابقة من خلال التطرق إلى أهم الدراسات السابقة التي تتشابه وتختلف نتائجها مع نتائج الدراسة الحالية، وتقترب منها وهي كالآتي:

فيما يخص دراسة عايدة عبد الكريم العيدان ، حول درجة الوعي بالأمن السيبيراني ودور تكنولوجيا التعليم في تنميته لدى طلبة كلية التربية الأساسية بجامعة الكويت فقد توصلت إلى أن أفراد العينة من طلبة الأقسام العلمية المختلفة لديهم تقديرات متشابهة حول تعرضهم للمخاطر والانتهاكات والتهديدات السيبرانية وهو ما أثبتته دراستنا.

أما في ما يتعلق بدراسة فاطمة يوسف المنتشري حول درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات فقد توصلت الدراسة إلى نتائج أهمها أن اتضح من تلك الاستجابات أن درجة وعي المعلمات بانتهاكات الأمن السيبراني درجة متوسطة بشكل عام، وهذا ما توافق مع نتائج دراستنا كون ان أكثر من نصف الطلبة صرحوا أن لديهم وعي متوسط تجاه موضوع الأمن السيبيراني.

أما الدراسة الثالثة لصاحبتها هديل تومان محمد البعاج حول الوعي الاجتماعي بالأمن السيبراني لدى طلبة كلية الامام الكاظم انموذجا ، فقد خلصت الدراسة إلى نتيجة رئيسية وهي ان افراد العينة يملكون درجة عالية من الوعي نحو العبارة (اتجنب فتح روابط من مصادر مجهولة وهذا ما اتفق عليه افراد عينة الدراسة حول موضوعنا كون أن أكثر من غالبية المبحوثين يتجنبون فتح روابط مواقع غير موثوقة.

أما الدراسة الأخيرة لصاحبها خالد سليمان سمحان حول درجة وعي المعلمين بالأمن السيبيراني بالمدارس الأردنية فقد توصلت الدراسة إلى أن الوسيلة الأكثر تأثيرا حول وعي الأفراد هي وسائل التواصل لاحتماعي وهو ما اتفقت عليه دراستنا تماما حيث اتفق 58 بالمئة من أفراد العينة على أن وسائل التواصل الاجتماعي أكثر وسيلة يرونها مناسبة لنشر الوعي حول موضوع الأمن السيبيراني.

ب/ مناقشة نتائج الدراسة في ظل محاور الاستبيان

فيما يتعلق بالمحور الأول: درجة وعي الطلبة بمفهوم الأمن السيبيراني

بينت نتائج الدراسة أن:

- أغلبية طلبة قسم الاعلام والاتصال بجامعة الشهيد حمة لخضر يتمتعون بمعرفة متوسطة حول مفهوم الأمن السيبيراني.

-أغلبية الطلبة يعتقدون أن الأمن السيبيراني ضروري جدا في حياتهم اليومية.

-66 بالمئة من افراد العينة صرحوا أنهم تعرضوا لعمليات اختراق أو تمت سرقة بياناتهم.

فيما يتعلق بالمحور الثاني: مدى اطلاع الطالب الجامعي على القوانين والنظم حول مخاطر الامن السيبيراني

بينت نتائج الدراسة أن:

-توصلت النتائج على أن أفراد العينة ليست لديسهم أدنى معرفة بقوانين ونظم الأمن السيبيراني.

-٧٨ بالمئة من المبحوثين لم يحضروا أية ورشات تدريبية أو ورشات عمل تتعلق بالأمن السيبيراني.

-أكدت الدراسة على أن الأفراد أنفسهم هم المسؤولين بشكل رئيسي حول الهجمات السيبيرانية التي يتعرضون لها.

فيما يتعلق بالمحور الثالث: طرق وأساليب لتعزيز الأمن السيبيراني .

بينت نتائج الدراسة أن:

-نصف العينة يعتقدون ان توعية الأفراد عبر حملات تحسيسية هي اهم طريقة لتعزيز الأمن السيبيراني.

-يعتقد أفراد العينة أن استخدام برامج الحماية غير كافية تماما لمواجهة المخاطر السيبيرانية.

-٧٤ بالمئة من المبحوثين لا يثقون في المواقع الالكترونية التي تطلب منهم إدخال بياناتهم الشخصية.

فيما يتعلق بالمحور الرابع: مدى مدى التزام الطالب بالتطبيقات المحرفة المرخصة لحماية بياناته

بينت نتائج الدراسة أن:

-صرح أغلب أفراد العينة بأنهم سبق وأن واجهوا مشاكل مثل الفيروسات أو فقدان البيانات بسبب استخدامهم لبرامج غير رسمية.

- يرى أفراد العينة أن استخدام تطبيقات غير مرخصة يُعرّض أجهزتهم ومعلوماتهم الشخصية للخطر بشكل كبير.

بعد مناقشة النتائج في ضوء محاور الاستبيان، نجيب على التساؤل الرئيسي: **هل لطلبة قسم الإعلام والاتصال بجامعة الوادي وعي بموضوع الأمن السيبيراني والمعلومات الرقمية ؟**

حيث أظهرت نتائج الدراسة أن:

درجة وعي طلبة قسم الإعلام والاتصال بجامعة الوادي حول مفهوم الأمن السيبيراني والمعلومات الرقمية متوسطة ، كما أن أفراد عينة الدراسة بحاجة إلى رفع هذا الوعي عن طريق حملات تحسيسية وورشات تدريبية حول هذا الأمر وغيرها ...

المطلب الثالث: الاستنتاجات العامة

ومن خلال دراستنا لهذا الموضوع وعي الطلبة الجامعيين بالأمن السيبيراني والمعلومات الرقمية، وأخذنا عينة الدراسة طلبة وطالبات علوم الاعلام والاتصال، ومن خلال اطلالتنا على فصول الدراسة بدءا بالإطار النظري المتعلق بمتغيري الدراسة الأمن السيبيراني والمعلومات الرقمية وصولا إلى الجانب التطبيقي. قد توصلنا إلى مجموعة من النتائج نلخصها في النقاط التالية:

-خلصت الدراسة إلى أن غالبية الطلبة يتمتعون بمعرفة متوسطة حول مفهوم الأمن السيبيراني.

-بينت الدراسة أن أكثر من نصف المبحوثين درجة وعيهم ضعيفة بمخاطر الأمن السيبيراني وسرقة البيانات.

-يرى أغلب أفراد عينة الدراسة أنهم لا يعرفون القوانين المحلية أو الدولية المرتبطة بالأمن السيبيراني.

-78 بالمئة من المبحوثين لم يسبق لهم حضور أية ورشات تدريبية أو عمل تتعلق بالأمن السيبيراني.

-استخدام برامج الحماية مثل مضادات الفيروسات غير كافي لمواجهة المخاطر السيبيرانية بحسب أغلب أفراد العينة.

-يعتقد أكثر من نصف المبحوثين أنهم لا يولون أية ثقة بالمواقع الإلكترونية التي تطلب منهم إدخال بيانات شخصية.

-58 بالمئة من افراد العينة يرون أن وسائل الإعلام ووسائل التواصل الاجتماعي هي الأداة الأكثر فعالية في نشر الوعي بالأمن السيبيراني.

خلاصة الفصل :

من خلال هذا الفصل حاولنا عرض وتحليل البيانات الواردة في الاستمارة التي تم توزيعها على المبحوثين عند إجراء الدراسة الميدانية، ليتم بعد مرحلة تحليل البيانات مناقشة وتفسير نتائج الدراسة في ظل الدراسات السابقة وتساؤلات الدراسة ، وفي الأخير تم استعراض النتائج العامة التي تم التوصل إليها.

الخـــاتمة العـــــامة

بناء على ما سبق ذكره عن التأصيل النظري لمفهوم الأمن السيبراني ومختلف المصطلحات المتصلة والتي تشكل في مجملها علاقة المعلومات والبيانات بمالكها وصانع ومستخدمها المشروع، فقد بدى جليا أهمية الوسائل والتطبيقات الرقمية في تحصين المعلومات والبيانات بنفس وسائل واليات الاختراق.

لذلك توجب على المستخدم أن يكون ايجابيا في الاستخدام من خلال اكتساب ثقافة رقمية تسمح له بالإحاطة بواجبات وحقوق الاستخدام وعدم الوقوع ضحية لضعف أو انعدام الأمن السيبراني في وسائلهم المستخدمة.

فالثقافة الرقمية هي السلاح السابق لمختلف التهديدات السيبرانية، يليها شرط الإلمام بأبجديات الرقمنة وحدود الاستخدام العقلاني والمشروع ومن ثم الاستعانة ببرامج الحماية التي تسمح بحد معقول من الحصانة الرقمية للملفات والبيانات الشخصية للأفراد والطلبة الجامعيين.

وكلما زادت أهمية هذه الملفات والمعلومات كلما زادت الحاجة إلى تأمين أكبر وأعلى فعالية وقوة لأن أغلب ضحايا التهديدات السيبرانية عادة ما يكونون من فئة الاشخاص المعلومين ذوي الصلة بالمجرم الالكتروني، أو ذوي النفوذ المالي والسياسي ابتغاء تحقيق أهداف الإبتزاز والجرم الإلكتروني عليهم.

قـائـمة المـصادر والـمـراجـع

أولا :الكتب

-عبد الرحمن بدوي، مناهج البحث العلمي، وكالة المطبوعات، الكويت،.1977

-فارس رشيد البياتي، الحاوي في مناهج البحث العلمي، دار السواقي العلمية، عمان،.2018

-حمد مرسلي، مناهج البحث العلمي في علوم الإعلام والاتصال، ديوان المطبوعات الجامعية، الجزائر، 2010.

-عبد الله باشيوة وآخرون، البحث العلمي :مفاهيم .أساليب .تطبيقات، الوراق للنشر والتوزيع، الأردن،.2009

-أمل وجيه حمدي، المصادر الإلكترونية للمعلومات :الاختيار والتنظيم والإتاحة، الدار المصرية اللبنانية، القاهرة،.2007

-سعد سلمان المشهداني، مناهج البحث الإعلامي، دار الكتاب الجامعي، الجمهورية اللبنانية، 2017.

-إسماعيل إبراهيم، مناهج البحوث الإعلامية، دار الفجر للنشر والتوزيع، مصر،.2017

ثانيا: المقالات والمجلات العلمية

-سعود شباب سدر العتيبي،" مدى توفر الوعي بالأمن السيبيراني لدى أفراد الأسر في المجتمع السعودي– دراسة استطلاعية"-، المجلة الدولية لنشر البحوث والدراسات، جامعة الملك عبد العزيز، السعودية،.2022

-منى عبد الله السمحان،" متطلبات تحقيق الأمن السيبراني في الأنظمة المعلومات الإدارية بجامعة الملك سعود"، مجلة كلية التربية، جامعة المنصورة،.2020

-عبير أحمد عبد الرحمن،" درجة الوعي بالأمن السيبراني لدى المعلمين في مديرية التربية والتعليم قصبة الكرك"، مجلة الزرقاء للبحوث والدراسات الإنسانية،.2023

-هالة كمال،" أنواع الأمن السيبراني ومجالات تطبيقه والتحديات التي يواجهها"، مجلة الشارقة، العدد 23،.2024

-حميدي حياة، طابلي نسيمة،" مدخل مفاهيمي حول الأمن السيبيراني"، مدار للدراسات الاتصالية الرقمية، العدد02 ،.2022

-وفاء بنت حسن عبد الوهاب،" وعي أفراد الأسرة بمفهوم الأمن السيبيراني وعلاقته باحتياطاتهم الأمنية والجرائم الإلكترونية"، المجلة العربية للعلوم الاجتماعية.

-حنان بشتة، نعيم بوعموشة،" الصدق والثبات في البحوث الاجتماعية"، مجلة دراسات في علوم الإنسان والمجتمع، جامعة جيجل،.2020

-خالد سليمان سمحان،" درجة وعي المعلمين بالأمن السيبيراني :دراسة ميدانية من وجهة نظر معلمي المدارس الأردنية"، مجلة اتحاد الجامعات العربية للبحوث في التعليم العالي، الأردن،.2023

ثالثا: الأطروحات والرسائل الجامعية

-ماجد عبد الله الحبيب،" درجة الوعي بالأمن السيبيراني لدى طلبة الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود وسبل تعزيزهم من وجهة نظرهم"، السعودية،.2018

-عايدة عبد الكريم العيدان،" درجة الوعي بالأمن السيبيراني ودور تكنولوجيا التعليم في تنميته لدى طلبة كلية التربية الأساسية بجامعة الكويت"، مجلة كلية التربية الأساسية،.2024

-يوسف المنتشري،" وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة"، مجلة العربية للتربية النوعية، جامعة دار الحكمة، السعودية،.2020

-هديل تومان محمد البعاج،" الوعي الاجتماعي بالأمن السيبراني لدى طلبة كلية الإمام الكاظم : أنموذجًا"، وقائع المؤتمر العلمي السابع، جامعة الإمام كاظم،.2023

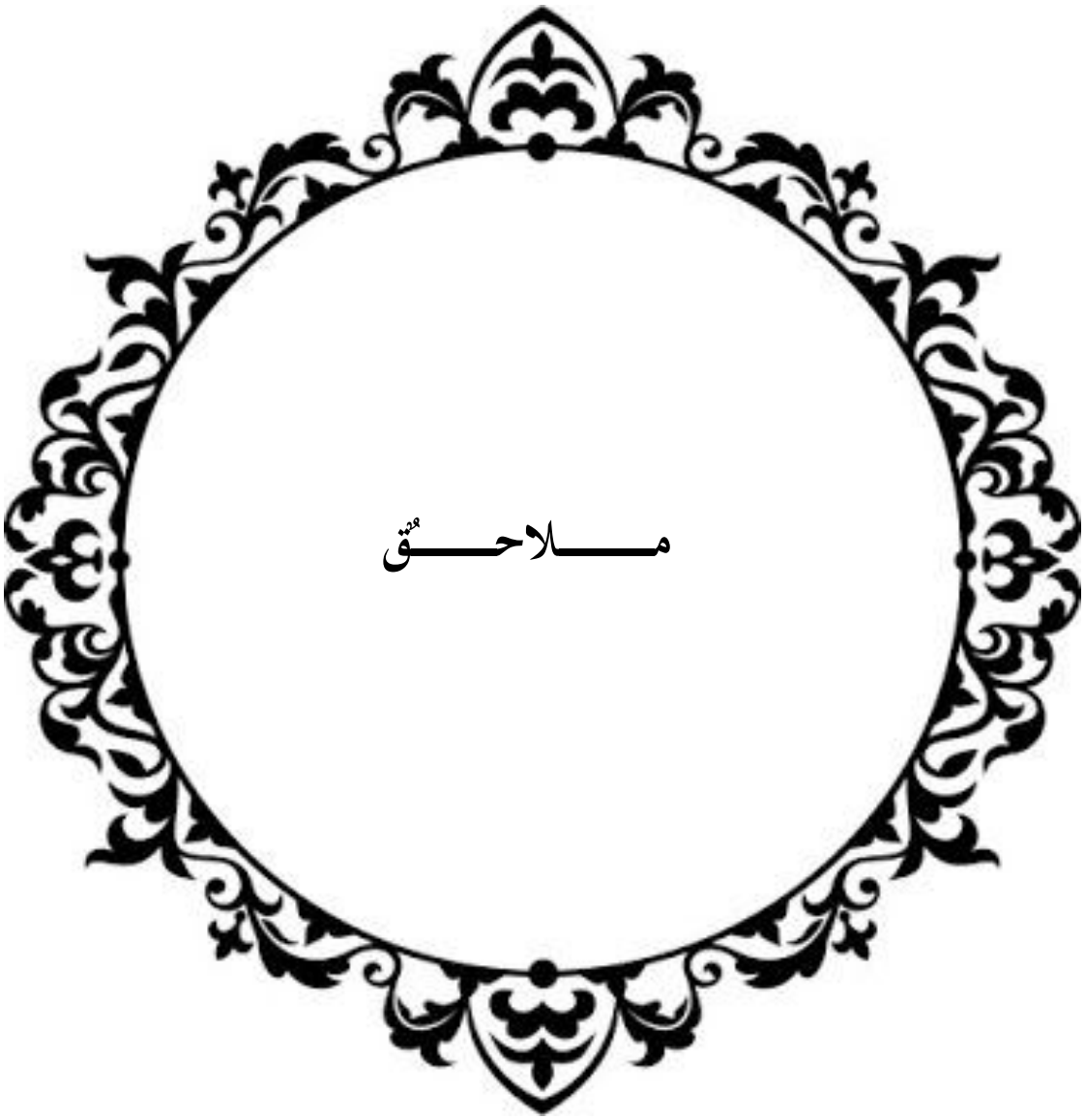
رابعا :المواقع الإلكترونية

-سليم عبد الرحمن،" الأمن السيبراني :مفهومه وتاريخه"، موقع الجزيرة للدراسات،2024 ، متاح على الرابط.https://www.aljazeera.net/encyclopedia/2024/9/19 :

-إسماعيل باباكر،" خصائص الأمن السيبيراني"، موقع الوطن اليوم،2023 ، متاح على الرابط : https://alwatannewssd.com/56117/.

-بكة،" أمن المعلومات وأهميته والأنواع والعناصر والاستراتيجيات والبرامج والأهداف"، موقع بكة، 2025، متاح على الرابط.https://bakkah.com/ar/knowledge-center :

-المركز الوطني لأمن المعلومات،" الأعمال الإلكترونية وأمن المعلومات"، ندوة تنظيم الاتفاقيات والعقود والرخص في عصر المعلوماتية، اليمن،.2005



مـــــلاحـــــقٌ

استمارة استبانة

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة الشهيد حمة لخضر– الوادي –

كلية العلوم الإنسانية والاجتماعية

قسم علوم الإعلام والاتصال

استبيان حول: الوعي بالأمن السيبيراني والمعلومات الرقمية لدى طلبة الإعلام والاتصال بجامعة الوادي

إعداد الطلبة:

سلامة يوسف الصديق

إشراف الاستاذ

محمودي محمد البشير

تساؤلات الدراسة

التساؤل الرئيسي:

هل لطلبة قسم الإعلام والاتصال بجامعة الوادي وعي بموضوع الأمن السيبيراني والمعلومات الرقمية ؟

التساؤلات الفرعية

أ ماهي درجة وعي الطلبة بمفهوم الأمن السيبيراني ؟

ب ما مدى اطلاع الطالب الجامعي على القوانين والنظم التي تواجه مخاطر الامن السيبيراني ؟

ت ماهي طرق وأساليب تعزيز الأمن السيبيراني بحسب تصورات مجتمع البحث ؟

عزيزي الطالب/عزيزتي الطالبة،

هذا الاستبيان يهدف إلى قياس درجة وعي الطلبة بمفهوم الأمن السيبراني ومدى اطلاعهم على القوانين والنظم المرتبطة به، بالإضافة إلى استكشاف تصوراتهم حول أساليب تعزيزه .نرجو منك الإجابة بصدق، حيث ستستخدم نتائج هذه الدراسة لأغراض بحثية فقط.

المحور الأول :درجة وعي الطلبة بمفهوم الأمن السيبراني

.ما مدى معرفتك بمفهوم الأمن السيبراني؟

- ☐عالية
- ☐متوسطة

- ☐ضعيفة
- ☐لا أعرف عنه شيئا

•هل تعتقد أن الأمن السيبراني ضروري في حياتنا اليومية؟

- ☐نعم، بشكل كبير
- ☐لا أعلم
- ☐ليس ضروريًا

•ما مدى وعيك بالمخاطر السيبرانية مثل الاختراقات وسرقة البيانات؟

- ☐وعي كبير
- ☐وعي متوسط
- ☐وعي ضعيف
- ☐لا أعلم عنها شيئًا

•هل سبق وتعرضت أو أحد معارفك لاختراق إلكتروني أو سرقة بيانات؟

- ☐نعم، تعرضت له شخصيًا
- ☐لا، لم أتعرض ولم أسمع عن ذلك
- ☐لا أعلم

•هل تقوم باتباع إجراءات حماية حساباتك الشخصية) مثل كلمات المرور القوية، التحقق بخطوتين(؟

- ☐نعم، دائمًا
- ☐نعم، أحيانًا
- ☐نادرًا

•ما المصادر التي تعتمد عليها لاكتساب معلومات عن الأمن السيبراني؟

- ☐المحاضرات الجامعية
- ☐الإنترنت والمواقع الإلكترونية
- ☐وسائل التواصل الاجتماعي
- ☐لا أهتم بهذا الموضوع

المحور الثاني :مدى اطلاع الطالب الجامعي على القوانين والنظم التي تواجه مخاطر الأمن السيبراني

•هل لديك معرفة بالقوانين المحلية أو الدولية المتعلقة بالأمن السيبراني؟

- ☐نعم، لدي معرفة جيدة
- ☐لدي معرفة سطحية
- ☐لا، لا أعرف عنها شيئًا

•هل تعتقد أن القوانين الحالية كافية لحماية الأفراد من الهجمات السيبرانية؟

- ☐نعم، كافية جدا
- ☐لا، غير كافية
- ☐لا أعلم

•هل سبق لك الاطلاع على مواد قانونية أو تشريعية حول الأمن السيبراني؟

- ☐نعم، قرأت عنها كثيرًا
- ☐قرأت عنها بشكل محدود
- ☐لم أطلع عليها أبدًا

•هل تعتقد أن الجامعات يجب أن تدمج مواد تعليمية حول الأمن السيبراني في المناهج الدراسية؟

- ☐نعم، بشكل إلزامي
- ☐نعم، ولكن بشكل اختياري
- ☐لا أعتقد أن ذلك ضروري

•هل سبق لك حضور دورات أو ورش عمل تتعلق بالأمن السيبراني؟

- ☐نعم
- ☐لا، ولكن أرغب في ذلك
- ☐لا، ولا أرى أنها ضرورية

•برأيك، ما الجهة المسؤولة عن حماية الأفراد من الهجمات السيبرانية؟

- ☐الحكومة والجهات الأمنية
- ☐الشركات التقنية ومزودو الخدمات

- ☐الأفراد أنفسهم

•هل ترى أن التوعية القانونية حول الجرائم السيبرانية ضرورية لحماية المستخدمين؟

- ☐نعم، ضرورية جدا
- ☐لا ليست ضرورة
- ☐لا أعلم

المحور الثالث :طرق وأساليب لتعزيز الأمن السيبراني بحسب تصورات مجتمع البحث

•برأيك، ما أهم وسيلة لحماية الأفراد من التهديدات السيبرانية؟

- ☐استخدام برامج الحماية والجدران النارية
- ☐توعية المستخدمين حول الأمن السيبراني
- ☐تطبيق القوانين الصارمة ضد المخترقين

•هل تعتقد أن استخدام برامج الحماية مثل مضادات الفيروسات كافٍ لمواجهة المخاطر السيبرانية؟

- ☐نعم، كافٍ تماما
- ☐لا، غير كافٍ

•كيف تقوم بحماية بياناتك الشخصية على الإنترنت؟

- ☐تغيير كلمات المرور بانتظام
- ☐عدم مشاركة المعلومات الشخصية مع الغرباء
- ☐لا أتخذ أي إجراءات خاصة

•ما مدى ثقتك في المواقع الإلكترونية التي تتطلب منك إدخال بيانات شخصية؟

- ☐أثق بها تماما
- ☐أثق بها لكن بحذر
- ☐لا أثق بأي موقع

•هل تعتقد أن الحكومات والمؤسسات تقوم بجهود كافية لمكافحة الهجمات السيبرانية؟

- ☐نعم، بشكل جيد جد
- ☐لا، هناك تقصير واضح

- ☐لا أعلم

•هل تقوم بالتحقق من موثوقية الروابط والمواقع قبل النقر عليها؟

- ☐نعم، دائما
- ☐أحيانا
- ☐لا أهتم بذلك

•ما برأيك الوسيلة الأكثر فعالية في نشر الوعي حول الأمن السيبراني؟

- ☐وسائل الإعلام والتواصل الاجتماعي
- ☐حملات التوعية الحكومية
- ☐دورات تدريبية وورش عمل

المحور الرابع :مدى استخدام التطبيقات المحترفة المرخصة لحماية البيانات

•هل تستخدم عادة تطبيقات مرخصة (مثلMicrosoft Office ، Adobeفي أعمالك الدراسية؟

- دائما
- أحيانا
- لا أستخدمها

. عند حاجتك لتطبيق معين، هل تتحقق من مصدره الرسمي قبل تحميله؟

- نعم، دائما
- أحيانا فقط
- لا أهتم بذلك كثيرا

. هل تعتمد على النسخ المقرصنة أو المعدّلة من البرامج؟

- لا، أحرص على استخدام النسخ الأصلية
- أحيانا، إذا لم أجد البديل
- نعم، بشكل دائم تقريبا

هل ترى أن استخدام تطبيقات غير مرخصة يُعرّض جهازك ومعلوماتك للخطر؟

- نعم، بشكل كبير
- إلى حد ما
- لا أرى ذلك خطرا كبيرت

هل سبق وأن واجهت مشاكل (مثل فيروسات، فقدان بيانات) بسبب استخدام برامج غير رسمية؟

- نعم
- لا
- لا أعلم إن كانت بسبب ذلك

شكرا لك على وقتك ومشاركتك في هذا الاستبيان!

جميع إجاباتك ستظل سرية وتستخدم فقط لأغراض البحث العلمي.