تنمية وعي الشباب بمخاطر الأمن السيبراني من منظور طريقة تنظيم المجتمع

إعداد

د/ صارفيناز محمد جمال الدين عبد المنصف سيد

مدرس بقسم تنظيم المجتمع

بالمعهد العالي للخدمة الاجتماعية بالإسكندرية

ملخص الدراسة

تسعى الدراسة الحالية إلى تحقيق هدف رئيسي التوصل برنامج وقائي مقترح من منظور طريقة تنظيم المجتمع لتنمية وعي الشباب بمخاطر الأمن السيبراني وذلك من خلال مجموعة من الأهداف الفرعية تحديد مستوى المخاطر الاجتماعية للأمن السيبراني على الشباب وتحديد مستوى المخاطر النفسية للأمن السيبراني على الشباب وتحديد مستوى المخاطر الأمنية للأمن السيبراني على الشباب وتحديد مستوى المخاطر الأخلاقية للأمن السيبراني على الشباب والتوصل لبرنامج وقائي مقترح من منظور طريقة تنظيم المجتمع لتوعية الشباب بمخاطر الأمن السيبراني، وتعتبر الدراسة من الدراسات الوصفية لكونها أنسب أنواع الدراسات ملائمة لطبيعة وموضوع الدراسة، والتي اعتمدت على منهج المسح الاجتماعي عن طريق العينة من الشباب الأعضاء بمركز الشباب. تكونت عينة البحث من (٢٨٠) مفردة.وتوصلت الدراسة إلى أهم النتائج منها أن مستوى المخاطر على الشباب ككل: (مرتفع) حيث بلغ المتوسط الحسابي (٢.٧٩)، ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: جاء في الترتيب الأول المخاطر الأمنية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٨٢),وانحراف معياري(٠.٤٤) يليه الترتيب الثاني المخاطر النفسية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٨٢), وانحراف معياري (٠.٤٦) وجاء في الترتيب الثالث المخاطر الأخلاقية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٧٨)، وجاء في الترتيب الثالث المخاطر الاجتماعية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٧٦).

الكلمات المفتاحية : تنمية وعي – مخاطر – الأمن السيبراني

Abstract:

The current study seeks to achieve the main objective of reaching a proposed preventive program from the perspective of the method of community organizing to develop youth awareness of the risks of cybersecurity through a set of sub-objectives to determine the level of social risks of cybersecurity on young people, determine the level of psychological risks to cybersecurity on young people, determine the level of security risks of cybersecurity on young people, determine the level of ethical risks of cybersecurity on young people, and to reach a proposed preventive program from the perspective of the method of community organization to raise awareness among young people of the risks of cybersecurity. The study is considered one of the descriptive studies because it is the most appropriate types of studies appropriate to the nature and subject of the study, which relied on the social survey method through the sample of young members Youth Center. The research sample was made up of (280) individuals. The study reached the most important results, including that the level of risks to young people as a whole: (high) where the arithmetic average reached (2.79), and indicators of this according to the order of the arithmetic average: the first ranked included the security risks of cybersecurity on young people with an arithmetic average (2.82), and a standard deviation (0.44) followed by the second order, the psychological risks of cybersecurity on young people with an arithmetic average (2.82), and a standard deviation (0.46) and the third rank came in the moral risks of cybersecurity on young people with an arithmetic average (2.78), and the third ranked the social risks of cybersecurity on young people with an arithmetic average (2.76.)

Keywords: Developing Awareness - Risks - Cyber Security

أولاً- مدخل مشكلة الدراسة:

يعد الأمن السيبراني مكونًا أساسيًا من مكونات ومتطلبات أي تحول رقمي حيث إن حماية البيانات والبنية التحتية ستكون مصدر قلق كبير وبسبب نمو الهجمات السيبرانية أصبح من الضروري التعامل مع مثل هذه الهجمات ومعالجتها بشكل مبتكر ويعد الأمن السيبراني الحل الأمثل لمتابعة الاستخدام الواسع للإنترنت وتطبيقاته وأنظمته المختلفة وللتقليل من المخاطر التى تنشا من سوء الاستخدام حيث توجد محتويات غير مشروعة وغير مرغوب بها ذات تأثير سلبي على أخلاقيات وقيم المجتمع والتي بدورها تؤدى الى تغييرات في شخصية الافراد وتعزز ميلهم للانحراف (الصانع، وآخرون، ٢٠٢٠، ص ٤٩).

ويمثل الأمن السيبراني واحداً من المخاطر الأساسية التي تواجه العالم، حيث لم تعد الهجمات السيبرانية نتاج عمل فردي أو مجموعة من القراصنة، لكنها أصبحت تضم متخصصين في ذلك النوع من الجرائم ولديهم قدرات تعادل – إن لم تكن الأفضل – من كيانات مؤسسية بدول العالم المختلفة، ومن هنا لم يعد أمن المعلومات رفاهية بل قضية أمن قومي، وهو ما دعا أربع هيئات مهنية كبرى إلى إصدار مجموعة من الأطر المعايير التي تتعلق بالأمن السيبراني من زوايا مختلفة هي: (عطية، ٢٠٢١، ص ٥٤)

١- جمعية المراجعة والرقابة على نظم المعلومات (ISACA) التي طورت إطاراً إدارة تكنولوجيا المعلومات لتمكين الإدارة من عبور الفجوة بين متطلبات الرقابة، والمسائل الفنية، ومخاطر الأعمال في وقت واحد.

٢- المنظمة الدولية للمعايرة (ISO) التي طورت سلسلة ٢٧٠٠٠ (ISO) وهي معايير تمكن المنظمة من تطبيق ضوابط رقابية تدعم مبادئ أمن المعلومات فيها.

٣- معهد المحاسبين القانونيين الأمريكي (AICPA) الذي طور إطاراً للتقرير عن إدارة المخاطر السيبرانية يوفر للمنظمة معلومات مناسبة ومفيدة حول درجة فعالية برامجها لإدارة المخاطر السيبرانية ويطلق على الهيكل الرئيسي لهذا الإطار (SOC)

٤- المعهد الوطني للمعايير وتكنولوجيا المعلومات(NIST) الذي أصدر إطاراً لتحسين البنية التحتية للأمن السيبراني مبني على المعايير والإرشادات والممارسات القائمة بهدف توجيه منظمات الأعمال لمحاولة خفض الآثار المحتملة للمخاطر السيبرانية.

حيث يعتبر البعض أن الأمن السيبراني مشكلة تقنية فقط، لكن واقعيا الحلول تتطلب مقاربة متكاملة تغطي الأشخاص والعمليات والتكنولوجيا، فالأشخاص يمكن اعتبارهم مفتاح مهم لتحسين الأمن السيبراني ويمكن تمييز ثلاث مجموعات رئيسية من الأشخاص المعنيين

المستخدمون وصناع القرار وخبراء الأمن السيبراني ويجب أن يزداد الوعي لدى هؤلاء بالمخاطر المهددة، وذلك بتزويدهم بمعلومات حول الإجراءات الممكنة، علما أن حملات التوعية والتدريب والتمارين تساعد المستخدمين وصناع القرار واتخاذ الإجراءات المناسبة لمواجهة المخاطر السيبرانية، حيث أن مصدر الاختراق غالباً ما يكون عالي التقنية. أما فيما يخص خبراء الأمن السيبراني فأي نقص في كفاءتهم ومهاراتهم يعد مصدر قلق خطير لكل من الشركات والحكومات (زمورة وبن عيسي، ٢٠٢٢، ص ٤٢٠).

هذا ويعمل الأمن السيبراني على حماية الأفراد من الأفكار المتعصبة والدخيلة على المجتمع، ومن تدمير الانتماء الوطني واختراق معلومات أمنية أو شخصيه تؤثر على الدولة والمجتمع وغيرها من الأخطار، وتأتي هذه الحماية من خلال استراتيجيات هامة تقوم بها الجهة المسئولة عن الأمن السيبراني في الدول كمحاولة منهم للتقليل من مخاطر الأنترنت بكافه أشكاله (السواط، وآخرون، ٢٠٢٠، ص ٢٨٣).

حيث أصبحت الجريمة السيبرانية الإلكترونية أحد أهم الأخطار التي تواجه الدول المتقدمة والنامية على حد سواء حيث تكلف العالم ٤٠٠ مليار دولار سنويا، فهي عالمية بلا حدود، وترتكب من قبل الأفراد وقد ترتكب من قبل مراكز البحوث، ومن متخصصين في علوم الحاسوب ومديرين يبحثون عن القراء أو من قبل مؤسسات ومنظمات تبحث عن معلومات تجارية عند منافسها، وعلى الرغم أن بعض الدول المتقدمة قد أصدرت التشريعات والقوانين الهادفة للحد من تلك الجرائم، إلا أنها لم تتمكن من منع ارتكاب تلك الجرائم (العقبي، صالح،٢٠٢٢، ٢٩).

فالرقمنة جزءا لا يتجزأ من الأنشطة البشرية في العصر الحديث حيث يدخل التعامل الرقمي في مجالات الحياة المهنية والشخصية و تحتاج كل المؤسسات الى أنظمة تكنولوجية المعلومات وبالتالي ينبغي عليها حماية أصولها المعلوماتية من خلال التفاعل البشري (Begishev, lldar , 2021,p 207,220).

حيث تواكب الدولة التطورات التكنولوجية والمعرفية، عليها أن تتحمل دوراً أساسياً في مواجهة هذه التغييرات حتى تستطيع تحقيق أهدافها المتمثلة في إعداد الشباب المتخصصين في المجالات المختلفة، وتأهيلهم لإجراء البحوث العلمية، بالإضافة الى نشر المعرفة وإنتاجها وتوليد الأفكار المتجددة وربط العلم والمعرفة بسوق العمل ، وفتح مسارات ومساقات جديدة للتعلم وتنمية المهارات اللازمة التي يحتاجها الشباب اثناء عملية التعليم والتعلم، وتطوير شخصية الشباب المتكاملة في ظل متغيرات العصر العلمي والانفجار المعرفي المتزايد (عبد الصادق، ٢٠١٧، ص ٣٨١).

لذلك تهتم الدولة برعاية شبابها باعتبارهم أحد الطاقات الإنسانية للنهوض بالمجتمع فالشباب هم طليعة المجتمع، وعموده الفقري وقوته النشطة والفاعلة لذا لا تنهض أمة من الأمم غالبًا إلا بمشاركتهم في البناء المجتمعي، فالشباب هم الفئة الأكثر أهمية في المجتمع فهم يمثلون اليوم نصف المجتمع ولكنهم في القريب يمثلون كل المستقبل (المصري، ٢٠١٢، ص ٤٦٤).

ويعتبر الشباب هم سواعد التنمية في أي دولة وهم مستقبل البشرية وقوة المجتمع ككل حيث أنهم أكثر الفئات العمرية حيوية وقدرة على العمل والنشاط وهم المصدر الأساسي للتغيير في المجتمع لكونهم الفئة الأكثر رغبة في التجديد والتطلع إلى الحديث (فهيم، ٢٠٠٠، ص ٩).

ولذلك يعد الاهتمام بفئة الشباب عملية استثمارية على المدى البعيد بقدر ما نعطي الشباب ونرعاهم نعدهم الإعداد السليم بقدر ما يرتد عائد هذا العطاء سخيًا على شكل خبرات بشرية أصبحت ثورة العصر، وعده الأمة في حاضرها ومستقبلها لمواجهة التحديات الداخلية والخارجية (الخالدي، ٢٠١٥، ص ١٠٠).

وتحقيقًا لذلك فقد اهتمت الدولة بإنشاء العديد من المؤسسات التي تهتم برعاية الشباب وتعتبر مراكز الشباب من أهم تلك المؤسسات حيث تسهم في إعداد الشباب من خلال ممارسة الأنشطة والبرامج التي تنمي روح الانتماء والتعاون، وتقدم خدماتها في شكل برامج وأنشطة تهدف إحداث تغيير في الشباب من خلال إكسابهم العديد من المهارات وتنمية مواهبهم وحل مشكلاتهم واستغلال كافة إمكانيات المجتمع لمواجهتها لإعداد مواطن لديه القدرة على مواجهة المشكلات المجتمعية والمشاركة في تنمية وطنه في ضوء المتغيرات المجتمعية الحديثة (بندق، ٢٠١١، ص ٣٠).

وقد أكدت دراسة (Checkoway, B., & Gutierrez, L. M., 2006) على أهمية مراكز الشباب كمؤسسات تساعد على إكساب الشباب المهارات المهنية من خلال إعداد البرامج التدريبية التي تؤهلهم لدخول سوق العمل في ضوء التغيرات المجتمعية الرقمية السريعة، كما تساعدهم على تعزيز الثقة بالنفس والقدرة على اتخاذ القرارات المهنية من خلال تعزيز مهارة القيادة لديهم.

كما أشارت دراسة (Glovert, D., 2004) إلى أهمية تأثير مراكز الشباب على اكتساب الشباب القدرة على فهم وتقبل الثقافات المختلفة وما يصاحبها من تطورات تكنولوجية يتم استخدامها بشكل مختلف بين الدول وقد أشارت الدراسة إلى أن البرامج الثقافية والاجتماعية التي تقدم للشباب تساعدهم على التفاعل الاجتماعي وتعزز من الفهم المتبادل بين الشباب المنتمين لخلفيات ثقافية مختلفة.

هذا وتعد الخدمة الاجتماعية السيبرانية عملية تدريب وتعليم، وإدارة وممارسة مهنة الخدمة الاجتماعية بالاعتماد على التكنولوجيا المعلوماتية والاتصالية، وتوظيف الشبكات

المعلوماتية الدولية (الإنترنت) في عملية التواصل مع المستفيدين من الخدمات الاجتماعية، ومحاولة تقديم المساعدات والتدخلات المهنية لهم عن بعد، فضلاً عن تحقيق التواصل مع الأخصائيين الاجتماعيين الآخرين سواء كانوا بنفس البلد أو خارجه أو التواصل مع متخصصين بمهن أخرى لأجل التعاون وإجراء البحوث والدراسات الخاصة بمهنة الخدمة الاجتماعية (أبو النصر، ٢٠٢٠، ص ٥٦).

وقد أدى استخدام التقنية بشكل عام والإنترنت بشكل خاص إلى تغيير في أدوار الأخصائيين الاجتماعيين في الممارسة، مما استدعى ضرورة التكيف مع المطالب الجديدة للممارسة في عصر المعلومات، وهذا يتوجب من الأخصائيين الاجتماعيين اكتساب المهارات الكافية لاستخدام التقنية بشكل مناسب لضمان المحافظة على الممارسة المهنية الأخلاقية، وهنا توجد العديد من القضايا التي يجب معالجتها ومنها أن هناك العديد من التقنيات الحديثة لكنها في الوقت نفسه ذات طبيعة خصوصية غير مرتفعة، فضلاً عن ضياع المعلومات أو التعرض إلى الاختراق، فإن مواقع الويب لا توفر كلها مستوى معينًا من الحماية والخصوصية، وهناك العديد من الثغرات التقنية عند ممارسة الخدمة الاجتماعية الإلكترونية، فقد تكون الأجهزة تالفة، كما قد تصعب المحافظة والالتزام بالسرية التامة أو تحديد المسؤولية الأخلاقية والقانونية في تسرب المعلومات واختراقها (العبد الكريم، ٢٠١٧، ص ٢٤).

وبالرغم من أن ممارسة مهنة الخدمة الاجتماعية بصفة عامة وطريقة تنظيم المجتمع عبر التقنيات الإلكترونية لها فوائد، إلا أنها تواجه العديد من المعوقات المتعلقة بإدارة المخاطر والأخلاقيات المتعلقة بكفاءة الممارسين وخصوصية سرية العمل وتضارب المعالج، كما توجد معوقات خاصة بعدم التزام كثير من الأخصائيين بالقوانين التي تحكم ممارسة الخدمة الاجتماعية الإلكترونية بالمؤسسة (حسانين، ٢٠٢٢، ص ٩٤).

وقد أشارت دراسة (الكواري، ٢٠٢٠) إلى استحداث مجالات للممارسة المهنية في حقل الخدمة الاجتماعية لتقديم خدماتها على نحو أكثر فاعلية مع الفقراء، والمرضى، والعجزة، وتوظيف التقنيات الحديثة في الارتقاء بالخدمة الاجتماعية المقدمة إذ تتحدد أهمية الدراسة بتوضيح إستراتيجية دولة قطر الرقمية لعام (٢٠٢٠) الخاصة بالخدمات الإلكترونية المقدمة لأفراد المجتمع، وتهدف الدراسة لتحديد متطلبات تفعيل ممارسة الخدمة الاجتماعية في مجالات الممارسة المهنية ضمن المجتمع القطري من خلال تحقيق عدد من الأهداف الفرعية التي تتمظهر بتحديد عدد من المتطلبات لتفعيل ممارسة مهنة الخدمة الاجتماعية في المجتمع القطري.

كما أشارت (UNODC, 2013) إلى أن الجريمة الإلكترونية تنتشر انتشاراً واسعاً عبر أعمال مدفوعة ماليا وأعمال ذات صلة بمحتوى الكمبيوتر، وكذلك العمل ضد السرية والسلامة والوصول إلى أنظمة الكمبيوتر. تختلف تصورات المخاطر والتهديد النسبي بين الحكومات ومؤسسات القطاع الخاص، ويرى ثلثي الدول أن أنظمتها غير كافيه لإحصاءات الشرطة في تسجيل الجريمة الإلكترونية، وترتبط سجلات الشرطة للجريمة الإلكترونية مع مستويات الدولة التنموية وقدرة الشرطة المتخصصة.

وأشارت دراسة (K. Jones, J. P. Ashby & M. Krwe, 2019) إلى وجود تصنيفًا شاملاً لأنواع المخاطر السيبرانية في العصر الرقمي، مع التركيز على المخاطر الشائعة مثل التّصيد، والبرمجيات الحديثة وتوضح الدراسة أساليب وتقنيات مواجهة المخاطر مع عرض استراتيجية الحماية المتعددة الطبقات وأهمية الوعي الأمني في الحد من المخاطر وركزت الدراسة على تقديم تصنيف متكامل للمخاطر السيبرانية، بتحليل أدوات وتقنيات الحماية، وأهمية رفع الوعي السيبراني بالمؤسسات.

واستهدفت دراسة (Dreger, P., & Kreutzfeld, C., 2016) دراسة التهديدات والمخاطر السيبرانية المتقدمة والمستمرة وتأثيرها على الأمن السيبراني كما ركزت الدراسة على العلاقة بين الهجمات المستمرة والجاسوسية السيبرانية، موضحة كيف يتم تنفيذ هذه الهجمات من قبل جهات متطورة بهدف سرقة المعلومات والبقاء غير مكتشفين لفترات طويلة.

كما أشارت دراسة (Jackson, Jennifer T,2017) إلى أن هناك مجموعة من السلوكيات الخطأ تنتج عن تعامل الشباب مع شبكة الانترنت العالمية ولابد من التدخل بشأن تعديلها، ويمكن تلخيص هذه الجرائم في الآتي (الكذب والغش، اعطاء معلومات غير صحيحة، التجسس والتطفل، الاعتداء على الخصوصية، الابتزاز والتهديد، التعامل مع الصور الخليعة، ادمان التعامل مع الإنترنت)، وتمثل الجريمة الإلكترونية في وقتنا الحالي تهديدًا كبيراً للمجتمع الحديث والتي تستمر في النمو حيث يتم دمج التكنولوجيا بشكل أكبر في حياتنا وذلك يمكن مرتكبي الجرائم عبر الإنترنت من استغلال الثغرات الأمنية للوصول إلى أنظمة الحوسبة ونشر البرامج الضارة عليه.

وهدفت دراسة (فوزي، ٢٠١٩) إلى التحليل السوسيولوجي لأبعاد الأمن السيبراني المصري وتحديد أهم ركائز وممارسات الأمن السيبراني اجتماعيًا ومجتمعيًا وأشارت الدراسة إلى تأثير المخاطر الاجتماعية والنفسية والتهديدات السيبرانية في تشكيل بنية المجتمع وتهديدها لقيم وأخلاقيات المجتمع واستهداف الأمن القومي وتصدير أزمة ثقة في الحكومة.

كما أشارت دراسة (الحياري، ٢٠٢٢) إلى أن أهم التهديدات والمخاطر التي تنتج عن انتهاك الأمن السيبراني هي التصيد وهو شكل من أشكال الاحتيال وذلك بقصد سرقة البيانات الحساسة واستخدامها والنصب بها على الأشخاص نفسيًا واجتماعيًا، وأشارت الدراسة إلى ضرورة اتخاذ الحكومات تدابير إضافية لضمان مستوى حماية أعلى بالرغم من أنه لا يمكن تجنب المخاطر السيبرانية بشكل مثالي.

واستهدفت دراسة (عبدالله، ٢٠١٧) إلى معرفة دور العلاقات العامة في التوعية بالجرائم الإلكترونية بالتطبيق على عدة هيئات تمثلت في وزارة الداخلية، وزارة الاتصالات وتكنولوجيا المعلومات وزارة العدل، والهيئة القومية للاتصالات، وتوصلت نتائج الدراسة أهمية نجاح الإدارات في عقد شراكات واتفاقيات بخصوص التوعية بمخاطر الجرائم الإلكترونية، ومن أكثر الوسائل الإعلامية كانت الصحف والتليفزيون لكنها لم تهتم باستخدام الإعلام الرقمي في التوعية، كما توصلت أن هناك اتفاقيات بين إدارة العلاقات العامة بالجهات التشريعية والتنفيذية لتكوين هيئات للتوعية بقضايا استخدام التكنولوجيا والمخاطر المرتبطة بها.

وهدفت دراسة (العريشي، الدوسري، ٢٠١٨) إلى تحديد دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع وتحديد آليات تعزيزها بين الشباب والتعرف على أنواع المخاطر الإلكترونية التي تهدد الأمن المعلوماتي في الفضاء السيبراني، والتدابير التي ينبغي اتباعها، وتوصلت الدراسة إلى أن أبرز أدوار الجامعة في تعزيز ثقافة أمن المعلومات في المجتمع تتمثل في تنمية الفكر الثقافي بأهمية أمن المعلومات والإسهام في توعية المجتمع بالمخاطر السيبرانية.

وقد أشارت دراسة (Kondo etal., 2018) إلى أن الجريمة السيبرانية هي ثاني أكبر الجرائم المبلغ عنها خلال عام ٢٠١٧م وتعد أخطر الجرائم على كل شركة بالعالم، وقد تصل الأضرار الناتجة عن الجريمة السيبرانية إلى خسائر اقتصادية أكبر إذا لم تصدر قوانين وتشريعات للحد منها، وفي هذا الصدد ورغم الأرقام المروعة إلا أنه وإلى الآن لم يعمل الكثير للحد منها.

كما سعت دراسة (Maranga & Nelson, 2019) إلى تعرف طرق تأمين الجامعات من الهجمات السيبرانية، والآليات التي تتبعها الجامعات في مجال التخطيط لآليات الأمن السيبراني، والتي من أهمها توعية أعضاء هيئة التدريس والطلاب من خلال البرامج التبادلية بين الجامعات لأعضاء هيئة التدريس والطلاب، وكذلك المؤتمرات والندوات العلمية التي تناقش موضوعات الأمن السيبراني ومفاهيمه، وإمداد إدارة الجامعات بأدوات الحماية الرقمية.

وهدفت دراسة (الجندي ومحمد ٢٠١٩) الى التحقق من دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العلمي للأمن المعلوماتي لدى طالبات الجامعة وتم

الاعتماد على المنهج التكنولوجي التطويري المنظومي, وتوصلت النتائج الى وجود دور مهم في الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة.

كما أوضحت(دراسة Rubasundram &ponnusamy ٢٠١٩). إلى تحديد خطر الإرهاب السيبراني ، وتوصلت إلى عدة نتائج ، أهمها أن تهديد الهجمات الارهابية عبر الانترنت سيزداد باستمرار نظرا لتزايد انتشار مستخدمي الإنترنت بشكل مستمر واعتماد الأفراد والمؤسسات على الإنترنت بشكل مضطرد وأنه بالرغم من إنشاء آلية دفاعيه متعددة بالفعل فإن تهديد الإرهاب السيبراني مستمر في الزيادة بسبب التطور المستمر للمنصات القائمة على الانترنت ، اضافه الى أنه تقع على عاتق المسئولين مسئولية تطوير تقنيات أمنه قادره على تحديد الأنشطة المشبوهة من خلال تحليل البيانات العامة والخاصة ، إضافة إلى ضرورة التعاون الدولي والتنسيق لزيادة تعزيز التحقيق وجمع المعلومات.

كما اهتمت دراسة (L. A. Gordan & M. P. Leob, 2002) بالعوامل الاقتصادية التي يجب الاهتمام بها عند الاستثمار في الأمن السيبراني حيث يقدم الباحثون نموذجاً اقتصادياً يعرف باسم Gordon-Loed Model والذي يهدي إلى توجيه الشركات في اتخاذ قرارات الاستثمار في الحماية السيبرانية بناء على مستوى الخطر المحتمل.

وأوضحت دراسة (Puhakainen, S., & Siponen, M., 2010) أهمية تدريب الأفراد على الوعي السيبراني كجزء من استراتيجيات الحماية. وتناولت الدراسة تأثير برامج التدريب على سلوك المستخدمين وتفاعلهم مع التهديدات السيبرانية وتقنيات التوعية الناجحة في تغيير سلوك الأفراد.

واستهدفت دراسة (علي، ٢٠٢٢) إلى تحديد مستوى وعى الشباب بمخاطر الجرائم الإلكترونية، وتحديد المعوقات التي تحد من التخطيط لتنمية وعي الشباب بمخاطر الجرائم الإلكترونية، وتحديد المقترحات التي تساعد على التخطيط لتنمية وعى الشباب بمخاطر الجرائم الإلكترونية، وصولاً إلى التوصل لرؤية مستقبلية لدور التخطيط الاجتماعي في تنمية وعى الشباب بمخاطر الجرائم الإلكترونية، وتوصلت نتائج الدراسة إلى أن مستوى وعى الشباب بمخاطر الجرائم الإلكترونية متوسط، كما توصلت نتائج الدراسة إلى أن لا توجد فروق جوهرية دلالة إحصائياً بين استجابات الطلاب وفقاً لمتغير النوع ذكور وإناث في تحديدهم لمستوى تنمية وعى الشباب بمخاطر الجرائم الإلكترونية، وأن توجد فروق معنوية دالة إحصائياً بين استجابات الطلاب وفقاً للمرحلة الجامعية في تحديدهم المستوى تنمية وعى الشباب بمخاطر الجرائم الإلكترونية.

وأشارت دراسة (سليمان، ٢٠٢١) في ظل التقدم الهائل في علم البرمجيات والتقنية المتسارعة في النظم المعلوماتية. ومع تزايد الاعتماد على الحواسب الآلية والشبكات المعلوماتية ظهر ما يسمى بالجرائم الإلكترونية والتي يطلق عليها الجرائم السيبرانية والتي تعد من أخطر التحديات التي تواجه المعاملات الالكترونية وبالرغم من الآثار الإيجابية للتطور التكنولوجي إلا أن اختراق الإنترنت للحدود وظهور العوالم الافتراضية العابرة للحدود نتج عنه ما يسمى بالإرهاب الإلكتروني، فلم تعد الجريمة الالكترونية تتمركز في دولة أو مجتمع معين بل أصبحت تهدد أمن واستقرار العديد من الدول خاصة مع صعوبة اكتشاف تلك الجرائم وإثباتها، وهو الأمر الذي يتطلب معه تضافر الجهود الدولية في التصدي لمثل هذه الجرائم وقد مهدت ثورة المعلومات والقدرة على استخدام التكنولوجيا إلى بروز أشكال جديدة ومتنوعة من القوة الإلكترونية، والتي أصبح لها انعكاس مباشر على المستوى المحلي والدولي، فمن ناحية أدت إلى إعادة توزيع القوة وانتشارها بين أكبر عدد من الفاعلين وهذا ما جعل قدرة الدولة في السيطرة على هذا المجال موضوع شك مقارنة بالمجالات الأخرى للقوة.

وسعت هدفت (Ulven & Wangen, 2021) إلى وضع منهجية لمواجهة مخاطر الأمن السيبراني في التعليم العالي، وتعرف متطلبات الأمن السيبراني ومصادره، وتوصلت إلى أن الأمن السيبراني له أهمية كبيرة في حماية وأمن المعلومات،

وهدفت دراسة (التيماني، ٢٠٢١) إلى معرفة واقع الأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بأمن المعلومات، وترجع أهمية هذا البحث لتفاقم التهديدات وكثرة الاختراقات وتواترها على كل الأصعدة وعلى كافة المستويات من الفرد إلى المؤسسات والوزارات والشركات – فقد بدأت الحكومات والشركات تعني تدريجياً أخطار الجرائم السيبرانية وأهمية الأمن المعلوماتي على الأمن الاقتصادي والسياسي للبلد، وعلى المصالح العامة فقد يبدو الإنترنت جنة لمخترقي الشبكات بسبب ظهورهم عليها ظهوراً افتراضياً دون اسم، وقد بات هؤلاء يعون ارتفاع عوائد الجرائم السيبرانية، وتدني أخطار ونسب اكتشافها، وصعوبة إثباتها في بعض الدول، لما تتسم به الجرائم السيبرانية من السرعة التي تتم بها، إذ قد تحدث الأضرار حتى قبل أن تعي الضحية استهدافها، كما توصلت الدراسة إلى أن أكثر العوامل التي تزيد من فرصة حدوث الجرائم السيبرانية هو ضعف الوعي لدى الأفراد ومشاركتهم المعلومات الشخصية مع الآخرين دون دراية ومعرفة بطبيعة عمل هؤلاء الأشخاص.

كما اهتمت دراسة (E., Kamiga & L. Schindler, 2017) بتحليل تأثير الخروقات الأمنية السيبرانية على الأسواق المالية واستعرض الباحثان بالدراسة حالات خرق بيانات الشركات الكبرى وتأثيرها على أسعار الأسهم والثقة العامة. وأوضحت الدراسة العلاقة بين قوة الهجوم السيبراني والتقلبات في الأسواق، وأشارت الدراسة إلى ضرورة السرعة في اتخاذ التدابير الأمنية والتشريعية للحد من تأثير الهجمات على الأسواق.

كما هدفت دراسة (عبداللطيف، ٢٠٢٢) الى الكشف عن دور برامج الثقافة الأمنية ومبادرات التوعية الالكترونية في توعية المواطنين وخاصة طلاب الجامعة من مخاطر الجرائم الالكترونية المهددة للأمن السيبراني، والتعرف على طرق توعية طلاب الجامعة من مخاطر الجرائم الالكترونية المهددة للأمن السيبراني المستخدمة في برامج الثقافة الأمنية الالكترونية ورفع مستوى وعى هذا القطاع الهام من قطاعات المجتمع بالأمن السيبراني وبمخاطر الجرائم الإلكترونية التي قد يتعرضون لها اثناء استخدامهم للأنترنت ، نظرا لخطورتها البالغة على الشباب والمجتمعات العربية ، والكشف عن عناصر التدعيم والوسائط المتعددة المستخدمة في توعية طلاب الجامعة من الجرائم الالكترونية ، كما توصلت نتائج الدراسة الى أهمية دور برامج الثقافة الأمنية في التوعية الالكترونية من مخاطر الجرائم الإلكترونية المهددة للأمن السيبراني والكشف عن سمات ومخاطر هذه الجرائم ،واهمية تأهيل طلاب الجامعة ومواطنين لديهم الوعى الكافي حول سلوكيات استخدام الانترنت بطريقة أمنة وحماية انفسهم في البيئة الرقمية حتى لا يكونوا ضحايا للعديد من الجرائم الإلكترونية.

وقد أسفر تحليل الدراسات والبحوث السابقة عن مجموعة من المؤشرات والتوجهات البحثية فيما يلي:

١- ركزت العديد من الدراسات على أهمية مرحلة الشباب، كأحد أهم فئات المجتمع فهم الثروة البشرية التي يعتمد عليها المجتمع المصري في سعيه لتحقيق التنمية الشاملة والمستدامة.

٢- أشارت بعض الدراسات إلى أهمية استخدام الأمن السيبراني والاعتماد عليه فالأمن السيبرالي الناجح ينتهج منهجًا معينًا يتكون من استراتيجيات وأجهزة عالية الحماية والجودة، كما أشارت الدراسات إلى أن الأمن السيبراني يمكن الإشارة إليه كوسيط تعمل فيه كافة الشبكات والحاسبات والبرمجيات لضمان حماية المعلومات ونظم الاتصالات من مختلف الانتهاكات وتقليل الخسائر المالية المرتبطة بتلك الانتهاكات.

٣- أكدت العديد من الدراسات على المخاطر الناتجة من استخدام الأمن السيبراني من هجمات إلكترونية وانتهاك البيانات وسرقة المعلومات، وقد أشارت الدراسات إلى الإجراءات الضرورية التي يجب أن تتخذها الدول لحماية المستخدمين للمعلومات والبيانات الإلكترونية من أخطار الهجمات السيبرالية والتي تتميز بالسرعة والدقة والغموض.

٤- تختلف الدراسة الحالية عن الدراسات السابقة في السعي إلى وضع برنامج مقترح لتنمية وعي الشباب بمخاطر الأمن السيبراني في (المخاطر الاجتماعية، المخاطر النفسية، المخاطر الأخلاقية، المخاطر الأمنية) من منظور طريقة تنظيم المجتمع.

٥- استفادت الدراسة الحالية من الدراسات والبحوث السابقة في تصميم أدوات الدراسة الحالية وفي تحديد وصياغة مشكلة الدراسة وإجراءاتها المنهجية وإطارها النظري وفي تحديد المفاهيم وتحليل النتائج وتفسيرها.

وتأسيسًا على ما تقدم وما أوضحته الدراسات العربية والأجنبية من أهمية الأمن السيبراني والمخاطر والتهديدات التي يمكن أن يتعرض لها الأفراد والمؤسسات والدول، واعتمادًا على النظريات المفسرة للدراسة الحالية وارتباط تخصص الباحثة وهو طريقة تنظيم المجتمع يمكن صياغة مشكلة الدراسة الحالية في:

التوصل إلى برنامج مقترح من منظور طريقة تنظيم المجتمع لتنمية وعي الشباب بمخاطر الأمن السيبراني.

ثانياً- أهمية الدراسة:

١- اهتمام العالم بالتطور والتغير السريع فقد أصبحت شبكات التواصل الاجتماعي الإلكترونية واقعًا مفروضًا على المجتمع وجزأ لا يتجزأ عنه، فهي قادرة على اختراق الحواجز الزمنية والمكانية والوصول إلى كل البشر في جميع اتجاهات العالم مكونة مجتمعًا آخر افتراضيًا.

٢- يعد الأمن السيبراني ركيزة أساسية لسياسة الأمن للمؤسسات والأفراد والدول كما أصبح الأمن السيبراني أحد مجالات الخدمة الرقمية الذي أصبح ضرورة حتمية تحفظ الدول والمؤسسات والأفراد من خلال مجموعة من الإجراءات المتخذة من مجموع الأدوات والسياسات والمفاهيم الأمنية والضمانات والتوجيهات والتقنيات التي يتم نهجها للدفاع ضد أي هجمات غير قانونية تواجه المعاملات الإلكترونية.

٣- تعتبر المخاطر السيبرانية الدافع الأساسي للاهتمام بتوعية أفراد المجتمع بأهمية الأمن السيبراني للحماية من الابتزاز واختراق البيانات والمعلومات، فالجرائم والمخاطر السيبرانية تعتبر مخاطر مستحدثة، ويمكن تسميتها بالجرائم المعلوماتية أو الجرائم الإلكترونية أو الجرائم السيبرانية وأصبحت تلك الجرائم تحديًا للأمن السيبراني والتي تعد من أخطر التحديات التي تواجه المعاملات الإلكترونية.

٤- إلقاء الضوء على فئة الشباب فهي فئة لها دور الفاعل بالمجتمع وتعتبر من أكثر فئات المجتمع اهتمامًا بثورة المعلومات لما لديها القدرة على استخدام التكنولوجيا الرقمية الحديثة بكفاءة وقدرة عالية.

٥- تشكل مراكز الشباب إحدى المؤسسات الرئيسية التي تتخذها المجتمعات لترسيخ قيمها الثقافية والحضارية ومبادئ ومقومات الانتماء للمجتمع والحفاظ عليه، كما تعتبر من

المؤسسات التربوية التي يقع على كاهلها مسئولية إعداد وتنشئة الشباب تنشئة إيجابية تجاه المجتمع بما يشكل هويته الثقافية والفكرية.

٦- ندرة الدراسات التي تناولت مخاطر الأمن السيبرالي وإعداد برنامج وقائي مقترح من منظور تنظيم المجتمع لتنمية وعي الشباب بمخاطر الأمن السيبراني وذلك في حدود علم الباحثة.

ثالثاً- أهداف الدراسة :

تسعى الدراسة الحالية الي تحقيق هدف رئيسي مؤداه:

التوصل برنامج وقائي مقترح من منظور طريقة تنظيم المجتمع لتنمية وعي الشباب بمخاطر الأمن السيبراني وذلك من خلال مجموعة من الأهداف الفرعية :

١- تحديد مستوى المخاطر الاجتماعية للأمن السيبراني على الشباب

٢- تحديد مستوى المخاطر النفسية للأمن السيبراني على الشباب

٣- تحديد مستوى المخاطر الأمنية للأمن السيبراني على الشباب

٤- تحديد مستوى المخاطر الأخلاقية للأمن السيبراني على الشباب

٥- محاولة التوصل لبرنامج وقائي مقترح من منظور طريقة تنظيم المجتمع لتوعية الشباب بمخاطر الأمن السيبراني

رابعاً- تساؤلات الدراسة :

تسعى الدراسة الحالية الي تحقيق تساؤل رئيس مؤداة : ما البرنامج الوقائي المقترح من منظور طريقة تنظيم المجتمع لتنمية و الشباب بمخاطر الأمن السيبراني وذلك من خلال مجموعة من التساؤلات الفرعية :

١- ما مستوى المخاطر الاجتماعية للأمن السيبراني على الشباب.

٢- ما مستوى المخاطر النفسية للأمن السيبراني على الشباب.

٣- ما مستوى المخاطر الأمنية للأمن السيبراني على الشباب.

٤- ما مستوى المخاطر الأخلاقية للأمن السيبراني على الشباب.

٥- ما البرنامج الوقائي المقترح من منظور طريقة تنظيم المجتمع لتنمية توعية الشباب بمخاطر الأمن السيبراني؟

خامساً- مفاهيم الدراسة وإطارها النظري:

(١) مفهوم تنمية الوعي:

يقصد بالوعي في معجم مصطلحات الخدمة الاجتماعية إدراك المرء لذاته ولما يحيط به إدراكًا مباشرًا (الدخيل، ٢٠١٢، ص ٥٢).

كما يقصد بالوعي بأنه ذلك الإدراك الذهني أو هو ذلك الجزء من العقل الذي يتوسط بين البيئة والمشاعر والأفكار (علي، ٢٠١٦، ص ٤٣٥).

كما يشير الوعي إلى حالة من اليقظة يدرك فيها الإنسان نفسه وعلاقته بمن حوله من زمان ومكان وأشخاص، كما يمكنه أن يستجيب للمؤثرات استجابة صحيحة، وإذا اضطرب الوعي اضطرب معه الانتباه وإدراك البيئة (مدكور، ١٩٧٥، ص ٣٨٢).

أما فيما يتعلق بمفهوم تنمية الوعي فهو يشير إلى عملية المساعدة التي يصبح الفرد أو الجماعة من خلالها أكثر إدراكًا وإحساسًا بوضع اجتماعي أو أثرًا أو فكرة معينة لها الأولوية في الوقت الحاضر على الرغم من الاهتمام الضعيف تجاهه (عبد العزيز، ٢٠٢١، ص ٢٠).

ويقصد بتنمية الوعي في الدراسة الحالية:

هي العملية التي يكون عليها الشباب على دراية كافية بالأمور المحيطة بهم وتهدف هذه العمليات مساعدة الشباب على الإدراك الكامل لمخاطر اختراق الأمن السيبراني سواء كانت مخاطر اجتماعية أو مخاطر نفسية أو صحية فهي ذروة القوة والحيوية.

(٢) مفهوم الشباب:

الشباب مصطلح يطلق على مرحلة عمرية من عمر الانسان هي ذروة القوه والحيوية والنشاط بين جميع مراحل العمر لدى البشر، ويعتبر معدل النضج عند الفرد قد لا يتوافق مع عمره الزمني (حسانين، ٢٠١٤، ص ٢٨).

ويشير مفهوم الشباب إلى فترة عمرية تمتد بين أواخر المراهقة وأوائل العشرينات، تتميز بالانتقال من مرحلة التبعية إلى مرحلة الاستقلال، حيث يواجه الشباب تحديات متعددة تشمل اتخاذ القرارات التعليمية والمهنية، وتكوين الهويات الشخصية والاجتماعية، والبحث عن الاستقلال المالي والعاطفي.

ويعرف الشباب بأنه الفئة العمرية بين سن١٨ و٢٤ عامًا، حيث يخوض الأفراد مرحلة جديدة من حياتهم تتميز بالاستقلالية، والتفاعل الاجتماعي، والتعلم الأكاديمي، هذه المرحلة تعتبر حرجة في تكوين الهوية والقدرات الشخصية والمهنية (Arnett, J., 2000, p. 469).

وتعتبر فترة الجامعة مرحلة حرجة في تطوير القدرات الشخصية والاجتماعية من خلال التفاعل مع بيئة جديدة وأصدقاء جدد، يكتسب الشباب الجامعي مهارات جديدة في التواصل الاجتماعي وحل المشكلات والوعي الذاتي، مما يؤدي إلى تطور هويتهم الشخصية واستقلالهم الاجتماعي (Pascarella, E., & Terenzini, P., 2005).

والشباب هو مصطلح يشير إلى الطلاب الذين يدرسون في مؤسسات التعليم العالي، حيث يلعبون دورًا مهمًا في المجتمع من خلال استكشاف المعرفة، وتطوير المهارات، والتفاعل مع قضايا العالم المعاصر (Hemsley-Brown, J., & Oplatka, I., 2015, p. 169).

والشباب يُعتبرون كفئة اجتماعية حيوية يتميزن بالتفاعل الثقافي والاجتماعي، حيث يواجهون تحديات جديدة تتعلق بالهوية، والتمييز، والمشاركة في القضايا السياسية والاجتماعية (Youniss, J., & Yates, M., 1997, p. 101).

يشير الشباب إلى الفئة العمرية التي تسعى إلى تحقيق الذات من خلال التعليم العالي، حيث تشمل هذه المرحلة تحديات أكاديمية ونفسية مهمة، تؤثر على تطورهم الاجتماعي والشخصي (Chickering, A., & Reisser, L., 1993, p. 105).

ويُنظر إلى الشباب الجامعي كفئة تسعى لتطوير هويتها المهنية من خلال التعليم والتدريب، مما يسهم في تعزيز قدراتهم على التأقلم مع متطلبات سوق العمل (Savickas, M., 2002, p. 149).

كما يعرف الشباب على أنه المرحلة التي يتم فيها الإنسان اكتمال الجسم من الناحية العضوية والوظيفية والتي تقع بين مرحلتي المراهقة والنضج وتتم فيها عمليات التغير في البناء الداخلي للشخص وتتكون الذات وتتجه القدرات العقلية نحو الإكمال ونحو المعايير الاجتماعية (السنهوري، ١٩٩١، ص ٢٣).

والشباب هو مرحلة من مراحل العمر تقع بين الطفولة والشيخوخة تتميز من الناحية البيولوجية بالاكتمال العضوي ونضوج القوة كما تتميز من الناحية الاجتماعية بأنها المرحلة التي يتحدد فيها مستقبل الإنسان سواء مستقبله المهني أو العائلي (فهمي، ٢٠٠٧، ص ١٩).

وتعرف الباحثة الشباب في الدراسة الحالية بأنه:

- هم الشباب من الذكور والإناث الأعضاء بمركز شباب الأنفوشي.
- الشباب المقيدون بالمعاهد العليا وبالجامعات المصرية.
- يتميزون بالنضج البدني والنفسي والاجتماعي.
- مشاركون في أنشطة المركز ومهتمين باستخدام التكنولوجيا الحديثة.

(٣) الأمن السيبراني:

أ- مفهوم الأمن السيبراني:

يعرف الأمن السيبراني: يهتم بأمن المعلومات والبيانات والعمليات التي يتم من خلالها حماية معدات الحاسب والمعلومات والخدمات من أي تدخل غير مشروع حيث يتم استخدام مجموعة من وسائل التقنية لمنع الاستخدام غير المصرح به, ومنع سوء استغلال المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها (ماجد، ٢٠١٨، ص٤).

ويعرف أيضاً بأنه: حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمة 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 الالكتروني والأمن الرقمي (هيئة الاتصالات وتقنية المعلومات، ٢٠٢٠، ص ٥).

يعرف الأمن السيبراني على أنه مجموعة تقنيات وإجراءات وسياسات تهدف إلى حماية المعلومات الرقمية والأنظمة الحيوية من الوصول غير المصرح به من التهديدات السيبرانية. (International Telecommunication Union, 2018).

كما يعرف على أنه استخدام استراتيجيات دفاع متعددة الطبقات في الأمن السيبراني مثل الجدران النارية، أنظمة كشف التسلل، والمراقبة المستمرة لخلق بيئة رقمية قادرة على مقاومة التهديدات المختلفة (European Union Agency for Cybersecurity, 2019).

ويشير الأمن السيبراني إلى مجموعة الأدوات والمبادئ الأمنية والإجراءات والتقنيات المستخدمة لحماية الأصول الإلكترونية من الوصول غير المصرح به من الهجمات السيبرانية والأضرار المحتملة (National Institute of staudards and Technology, 2018).

ويعرف الأمن السيبراني في الدراسة الحالية بأنه:

هو نظام تقني أمني حديث يشمل مجموعة إجراءات وسياسات لحماية المعلومات الرقمية للأشخاص والجماعات والمؤسسات من سوء الاستغلال والاختراق والسرقة للمعلومات الإلكترونية وحمايتها من الهجمات والتهديدات الإلكترونية.

ب-أهداف الأمن السيبراني:

يمكن حصر أهم أهداف الأمن السيبراني فيما يلي:

١- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
٢- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
٣- توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات.
٤- صمود البنى التحتية الحساسة للهجمات الإلكترونية.
٥- توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين
٦- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها
٧- سد الثغرات في أنظمة أمن المعلومات
٨- مقاومة البرمجيات الخبيثة وما تستهدفه من إحداث أضرار بالغة للمستخدمين.
٩- الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.
١٠- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.
١١- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة (جاب الله، ٢٠٢٢، ٢٢٤٨: ٢٢٤٩).

ج- أبعاد الأمن السيبراني بتطبيقات الإعلام الأمني:

يعتمد الأمن السيبراني على أجهزة وشبكات يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من اي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث وقد يعتمد الأمن السيبراني على مجموعة ابعاد تتمثل في التالي:

- **الأبعاد العسكرية:** تتمثل في قدرتها على ربط الوحدات العسكرية ببعضها مما يسمح بسهولة تبادل المعلومات والسرعة في اتخاذ القرارات العسكرية وتدمير الأهداف عن بعد، وفي المقابل يمكن تعطيل قدرة الدولة.
- **الأبعاد الاقتصادية:** يرتبط الأمن السيبراني ارتباطاً وثيقاً بالاقتصاد القومي حيث تتنافس الشركات على إصدار تطبيقات تسمح بآليات دفع أمنه، ووضعت بعض الدول تشريعات خاصه بحماية أموالها والحد من بعض الجرائم الاقتصادية العابرة للحدود مثل الإرهاب الالكتروني، وغسيل الأموال، والتجارة بالبشر وغيرها.
- **الأبعاد الاجتماعية:** حيث تسهم وسائل الإعلام وشبكات التواصل الاجتماعي في فتح المجال للأفراد للتعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية بأشكال مختلفة، وتبادل الخبرات والأفكار وتكوين الصداقات بين أفراد المجتمعات الأخرى.
- **الأبعاد السياسية:** وتعني حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية، حيث أصبح بإمكان الفرد المشاركة في صناعة القرار السياسي، والاطلاع على خلفيات ومبررات القرارات السياسية التي تتخذها حكومته عبر الكم الهائل من المعلومات التي يمكنه الوصول إليها (الداغر، ٢٠٢١، ص ٣٧).
- **الأبعاد القانونية:** تشمل المخاطر القانونية بشكل أساسي في غياب الإطارين التشريعي والتنظيمي المناسبين للتعامل مع نتائج الأعمال القانونية وغير القانونية منها، والتي تتم في القضاء السيبرالي ويتطلب النشاط الاقتصادي والتجاري وغيرهما تحديدًا واضحًا للواجبات والحقوق فمستخدمو هذه التقنيات عبر القضاء السيبراني بحاجة إلى إطار يؤمن حماية استخدامهم، ففي حالة غياب الأطر التشريعية تؤثر الجرائم السيبرانية على عمليات معلوماتية تخص حقوق الإنسان الدولية وتدفع على العنف وتسبب ضررًا اقتصاديًا خطيرًا. فضمان إدارة مخاطر الأمن السيبراني على منهج يهدف إلى حماية الأصول المعلوماتية والتقنية وفقًا للسياسات والإجراءات التنظيمية والمتطلبات التشريعية (فوزي، ٢٠١٩، ص ١١٤).

د- الجهود المصرية في دعم الأمن السيبراني في ضوء الاستراتيجية الوطنية لرؤية مصر ٢٠٣٠:

يتمثل الهدف الاستراتيجي لها في مواجهة المخاطر السيبرانية وتعزيز الثقة في البنى التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها في شتى القطاعات الحيوية وتأمينها من

اجل تحقيق بيئة رقمية أمنة وموثوقة للمجتمع المصري بمختلف اطيافه وتشتمل هذه الاستراتيجية على مجموعة من العناصر تتلخص في:

١-التحديات والاخطار السيبرانية والتي تتمثل في خطر اختراق وتخريب البنى التحتية للاتصالات وتكنولوجيا المعلومات وخطر الإرهاب والحرب السيبرانية وخطر سرقة الهوية الرقمية والبيانات الخاصة.

٢-أهم القطاعات الحيوية المستهدفة وتشمل:

- القطاع الأمني
- قطاع الطاقة والخدمات الحكومية.
- قطاع الاتصالات وتكنولوجيا المعلومات.
- قطاع النقل والمواصلات.
- قطاع الصحة وخدمات الإسعاف العاجل.
- قطاع الاعلام والثقافة.
- المواقع الرسمية للدولة.
- القطاعات ذات التأثير على النشاط الاقتصادي

٣-العناصر الرئيسية لخطورة التهديدات السيبرانية تكمن في استنادها الى تقنيات متقدمة ومتطورة وأنها ذات سرعة وسهولة في الانتشار، وأنها ذات نطاق واسع للتأثير.

٤-قامت مصر بتأسيس المركز المصري للاستجابة لطوارئ الإنترنت والحاسب " المجلس الأعلى للأمن السيبراني" التابع لوزارة الاتصالات وتكنولوجيا المعلومات بجمهورية مصر العربية وهو مسئولا عن الاستجابة لحوادث أمن الكمبيوتر والمعلومات وتوفير الدعم والدفاع والتحليل في مجال الهجمات السيبرانية والتعاون مع الهيئات الحكومية والمالية وأي قطاعات معينة بالبنية التحتية المعلوماتية الحرجة. كما يوفر المركز أيضًا الإنذار المبكر ضد انتشار البرمجيات الخبيثة والهجمات السيبرانية الضخمة ضد البنية التحتية للاتصالات في مصر (المجلس الأعلى للأمن السيبراني ،٢٠١٧، ص ٢-١٤).

(٤) مخاطر الأمن السيبراني:

أ- مفهوم مخاطر الأمن السيبراني:

تشير المخاطر السيبرانية إلى إمكانية حدوث اختراقات أو تهديدات إلكترونية قد تؤدي إلى خسائر مادية، أو اختراقات للبيانات أو انقطاع في الأعمال، أو ضرر للسمعة (World Economic Forum, 2020, p. 25).

وتتعلق المخاطر السيبرانية بالخسارة المالية أو الاضطراب أو الأضرار بسمعة منظمة بسبب شكل من أشكال فشل نظام تكنولوجيا المعلومات الخاص بها (Moulton, 2020, p. 20).

كما تشير المخاطر السيبرانية إلى مجموعة الهجمات الإلكترونية والمستمرة والمعتمدة التي تهدف إلى الوصول للأنظمة الحسابية أو الشبكات وذلك باستخدام تقنيات متعددة وخطوات مراقبة دقيقة (Mandiant, 2020, p. 70).

وتعرف مخاطر الأمن السيبراني في الدراسة الحالية:

هي مجموعة المخاطر التي يتعرض لها الشباب نتيجة اختراق نظام الأمن السيبراني للأجهزة والبرمجيات والشبكات وتشمل تلك المخاطر المخاطر الاجتماعية، النفسية، الأمنية، الأخلاقية.

ب- عوامل تنامي التهديدات السيبرانية:

لقد ساعدت عدة عوامل من تنامي التهديدات السيبرانية من هذه العوامل ما يلي:

١- تزايد ارتباط العالم بالفضاء الإلكتروني (السيبراني)، الأمر الذي اتسع معه خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية في الفضاء السيبراني.

٢- تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الاستراتيجية مع تصاعد أدوار الشركات متعددة الجنسيات، خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء السيبراني.

٣- تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية، الأمر الذي جعل من الممكن الإضرار بمصالحها من خلال الهجمات الإلكترونية في حالات العداء.

٤- قلة تكلفة الحروب السيبرانية مقارنة بنظيراتها التقليدية، مع إمكانية شن الهجوم في أي وقت، بحيث لا يتطلب تنفيذه سوى وقت محدود.

٥- تحول الحروب السيبرانية إلى إحدى أدوات التأثير في المعومات المستخدمة في مستويات ومراحل القتال الإلكترونية والصراع المختلفة، سواء على الصعيد الاستراتيجي أو التكتيكي العملياتي بهدف التأثير بشكل سلبي على هذه المعلومات ونظم عملها.

٦- توظيف الفضاء السيبراني في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهر ما يسمى الاستراتيجية السيبرانية للدول.

٧- اتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون، سواء من الدول أو من غير الدول في الحروب السيبرانية، فقد تشن الهجمات الإلكترونية عبر أجهزتها الأمنية الدفاعية، كما قد تلجأ إلى تجنيد قراصنة أو موالين لشن هجمات ضد الخصوم دون أي ارتباط رسمي (كلاع، ٢٠٢٢، ص ٢٩٩، ٣٠٠).

ج-أنواع الجرائم السيبرانية:

من أهم أنواع الجرائم السيبرانية في ما يلي:

١- **القرصنة:** وهي الوصول إلى جهاز الكمبيوتر ومشاهدته، أو النسخ منه أو إنشاء بيانات بغرض تدمير البيانات، أو إلحاق الضرر بالكمبيوتر.

٢- **نشر الفيروسات:** هي برامج يمكن أن تصيب برامج شرعية أخرى عن طريق تعديلها لتشمل نسخة قد تكون تطورت، وبالتالي تسبب فيروسات الكمبيوتر أضراراً اقتصادية تقدر بمليارات الدولارات في كل عام ويعود ذلك بسبب الفشل في الأنظمة الخاصة بالحماية وإهدار موارد الحاسب وإفساد البيانات وزيادة تكاليف الصيانة.

٣- **الاحتيال:** وهو محاولة الحصول على معلومات مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقات الائتمان، وذلك عن طريق التنكر وعادة ما يحدث ذلك عن طريق البريد الإلكتروني.

٤- **المطاردة:** وهي استخدام الانترنت أو غيره من الوسائل السيبرانية المضايقة الأفراد أو المنظمات وقد يشمل اتهامات كاذبة أو بيانات غير صحيحة عن الواقع، أو التهديد أو سرقة الهوية.

٥- **الإرهاب الإلكتروني:** وهو استخدام الهجمات السيبرانية في الأنشطة الإرهابية على سبيل المثال تعطيل شبكات الكمبيوتر عن طريق نشر الفيروسات، وبالذات على الأجهزة المتصلة بالإنترنت والهدف هو إطلاق الإنذارات والهلع بين الناس.

٦- **المواد الإباحية عبر الإنترنت:** وهي تلك المواد الإباحية التي يمكن الوصول إليها عبر الإنترنت عن طريق مواقع الويب، أو مشاركة الملفات مع الأقران، حيث أتاح الإنترنت وصول الأطفال لتلك المواقع الإباحية رغم التقييدات القانونية والاجتماعية (الشلوى، ٢٠٢٢، ٥٩: ٦٠).

د- خصائص الجريمة الإلكترونية:

للجرائم الإلكترونية خصائص متعددة لجعلها اختلف عن الجرائم العادية وهذه الخصائص هي:

١- جريمة عابرة للحدود وذات بعد دولي أي أنها جرائم لا تعترف بالحدود الجغرافية للدول وحتى بين القارات، وذلك بسبب الربط الإلكترونية بين جميع الدول والقارات

٢- لا يتم في الغالب الإبلاغ عن جرائم الانترنت اما لعدم اكتشاف الضحية لها وإما خشيته من التشهير.

٣- تتصف بصعوبة الإثبات فهي تفتقر للإثبات بالعامل المادي التقليدي فيصعب متابعتها واكتشافها لاعتمادها على الذكاء والخداع والخبرة الفنية مع صعوبة الاحتفاظ بأثار الجريمة

٤- جرائم ناعمة بعيدة عن العنف في الغالب فهي لا تحتاج جهد عضلي بل تعتمد على التفكير العلمي المدروس القائم على معرفة الوسائل الإلكترونية.

٥- مرتكب الجريمة شخص من بين ملايين المستخدمين فيصعب معرفة.

٦- صعوبة تحديد حجم الضرر الواقع قياسا بالجرائم العادية.

٧- سهولة إتلاف الأدلة من قبل الفاعل.

٨- مرتكب الجريمة الإلكترونية شخص يتميز بالذكاء وذو مهارات التقنية عالية ودراية في مجال أنظمة الحاسب الآلي وكيفية تشغيله وكيفية تخزين المعلومات وطرق الحصول عليها (النويران، ثامر على ، ٢٠١٥ ص١٧٤).

هـ- مرتكبي الجرائم السيبرانية: تشمل العناصر الآتية:

١- **المخترقون**: هم هواة بارعون يمتلكون مواهب عالية، ليس لديهم نوايا خبيثة وإنما يخترقون الأنظمة لاكتشاف الثغرات ونقاط الضعف حتى يتم سدها أو بدافع حب الاستطلاع والقضاء على الملل ولكن هذا مما لا شك فيه انتهاك للخصوصية.

٢- **القراصنة:** يمتلكون مهارات متقدمة ودافعهم تخريبي حيث يقومون بحذف وتغيير المعلومات وإسقاط الخادمات وإثارة الفوضى بين مستخدمي الشبكات.

٣- **الموظفون الساخطون:** قد لا يمتلكون تلك المهارات العالية، ولكن منصبهم الوظيفي يخولهم الاطلاع على المعلومات الحساسة فقد يقومون بسرقتها لابتزاز الشركة، ومنحها لشركة منافسة مقابل إغراء مادي أو تدميرها بغرض الانتقام.

٤- **الإرهابيون:** غالباً ما يكونوا متخصصين، لديهم مهارات متطورة جداً دافعهم الأيديولوجي، يصنعون برامج الاختراق الخاصة بهم، يستهدفون البنية التحتية للشبكات والمجتمع بأكمله لنشر أفكارهم، تشويه ونشر معلومات مغلوطة عن الجهات المناوئة لهم، غالباً ما تكون هجماتهم مفاجئة وتفصل بينها مدة طويلة يستعدون خلالها للهجمة القادمة.

٥- **الأعداء الشخصيون:** يستهدفون شخص بعينه ويخترقون جهازه لانتهاك أسراره وسرقة معلوماته الخاصة بغرض التشهير والابتزاز (كامل، ٢٠١٩، ١١).

و- آليات تنمية وعي الشباب بمخاطر الأمن السيبراني:

١- تنمية القاعدة المعرفية للشباب لكي يتم تمكينهم من أن يناقشوا ويفكروا بشكل مستقل ويتم هذا من خلال:

أ- تطوير القاعدة المعرفية للشباب بتزويدهم بمعلومات عن حقوقهم المشروعة داخل مجتمعهم والوقوف على مخاطر الوسائل التكنولوجية الحديثة.

ب-استشارة الشباب ليشعروا بضرورة إحداث تغييرات مقصودة في الأحوال غير المرغوبة في مجتمعهم

٢- مساعدة الشباب على إكساب المهارات التكنولوجية من خلال إقامة اتصالات مع الهيئات الحكومية وغير الحكومية ذات الصلة بتحديد مخاطر الوسائل التكنولوجية بغرض تنمية مهاراتهم في التعامل مع تلك المخاطر.

٣- مساعدة الشباب على تنظيم أنفسهم لإيجاد تنظيمات جديدة تناقش مخاطر الوسائل التكنولوجية.

٤- الوقوف على عوامل وقوع الكثير من الفتيات والشباب ضحية لوسائل التكنولوجية الحديثة والحرص على معالجة الأسباب والقضاء على العوامل التي تهيئ المناخ المناسب لها.

٥- تنمية المراقبة الذاتية لدى الأفراد مع تفعيل أساليب الوقاية والحماية من الآثار السلبية لوسائل التكنولوجيا الحديثة.

٦- تدعيم دور الأسرة والمجتمع للحد من المشكلات المترتبة على استخدام الشباب لوسائل التكنولوجيا الحديثة.

٧- تفادي الروابط الوهمية والتأكد من أي مصدر لتفادي النصب والاحتيال (السيد، ٢٠٢١، ص ٨١٢).

سادسًا- الموجهات النظرية للدراسة:

(١) نظرية الأنساق الإيكولوجية:

ظهر مفهوم النسق الإيكولوجي كمنظور يقوم على أساس مشترك بين علم الإيكولوجيا البشرية ونظرية الأنساق، ويختص بالتلازم والتكيف بين الكائنات والبيئات التي تعيش فيها الكائنات بالشكل الذي يحقق توازنًا ديناميكيًا بين الأطراف (النوحي، ٢٠٠١، ص ٣٦١).

وتساعد النظرية على فهم القناعات المختلفة بين الناس وبيئاتهم الاجتماعية ومعرفة العوامل الداخلي والخارجية المؤثرة في سلوكهم فهذه النظرية تركز على الإنسان والبيئة معًا وعلى العلاقة بينهما.

وتعرف الأنساق الإيكولوجية بأنها إطار ديني يستخدم في فهم الفرد والأسرة والمجتمع والوقائع من أشكال السلوك بالمنظمات والمجتمع، ويؤكد على التعامل المتبادل بين الأفراد وبيئاتهم، وتعتبر نقطة البداية لهذا الإطار هي النظرة الإيجابية للإنسان والفكرة المركزية التي ينطلق منها هي فكرة التغيير (علي، ٢٠١٠، ص ٢٧٩).

(٢) النظرية الموحدة لقبول واستخدام التكنولوجيا:

تعد النظرية الموحدة لقبول واستخدام التكنولوجيا إحدى التوجهات النظرية الحديثة التي تهدف إلى تفسير نية وسلوك الاستخدام للتكنولوجيا الحديثة وتقترح النظرية أن توقع الآراء، توقع

الجهات، التأثير الاجتماعي، الاستخدام الفعلي بشكل غير مباشر في حين أن التسهيلات المتاحة تؤثر على سلوك الاستخدام الفعلي بشكل مباشر.

ظهرت النظرية الموحدة لقبول واستخدام التكنولوجيا من تنقيح ودمج العديد من النظريات والنماذج المنبثقة منها قبل نظرية الفعل المبرر، نموذج قبول التكنولوجيا، نظرية السلوك المخطط، نظرية الإدراك الاجتماعي (البطاينة، العقيف، ٢٠١٨، ص ٢٣٢٩).

ووفقًا للنظرية الموحدة لقبول واستخدام التكنولوجيا يتحدد سلوك الاستخدام الفعلي للتطبيقات التكنولوجية من خلال متغير نسبة الاستخدام للتكنولوجيا (الاتجاه نحو الاستخدام) وتتأثير نية الاستخدام بعدة متغيرات تؤثر على استخدام التقنية وهي:

١- الآداء المتوقع من التقنية المستخدمة Performance Expectance: يعتبر أقوى مؤثر يؤثر على نية الاستخدام وهو الدرجة التي يعتقد الفرد أن استخدام نظام معين سوف يساعده على تحقيق مكاسب في الأداء.

٢- الجهد المبذول وهو مدى سهولة أو صعوبة التطبيق التعليمي المستخدم.

٣- التسهيلات المتاحة: وهي الدرجة التي يعتقد الفرد فيها أن هناك بنية تحتية موجهة لدهم استخدام التقنية.

٤- التأثير الاجتماعي وهو الدرجة التي يدركها الفرد أن الآخرين يعتقدون ألا يجب استخدام نظام معين (مؤيد، ٢٠١٧، ص ٢٠٠).

سابعًا- الإجراءات المنهجية للدراسة:

١- **نوع الدراسة** : تنتمي الدراسة الحالية لنمط الدراسات الوصفية لكونها أنسب أنواع الدراسات ملائمة لطبيعة وموضع الدراسة التي تستهدف الي التوصل برنامج وقائي مقترح من منظور طريقة تنظيم المجتمع لتنمية وعي الشباب بمخاطر الأمن السيبراني.

٢- **المنهج المستخدم:** المسح الاجتماعي بالعينة باعتباره من أنسب المناهج لهذه الدراسة.

٣- **أدوات الدراسة:** استمارة استبيان لتحديد مخاطر الأمن السيبراني من اعداد الباحثة

وقد تم تصميم أدة الدراسة وفقا للخطوات التالية :

(أ) مرحلة تصميم الأداة وفي هذه المرحلة تم الاتي

- قامت الباحثة بتصميم استمارة استبيان وذلك بالرجوع إلى التراث النظري، والدراسات السابقة المرتبطة بموضوع الدراسة.
- اشتملت استمارة استبيان على المحاور التالية: البيانات الأولية، تحديد المخاطر الاجتماعية للأمن السيبراني على الشباب ، تحديد المخاطر النفسية للأمن السيبراني على

الشباب، تحديد المخاطر الأمنية للأمن السيبراني على الشباب، تحديد المخاطر الأخلاقية للأمن السيبراني على الشباب

- اعتمدت الباحثة على الصدق المنطقي لاستمارة استبيان من خلال الاطلاع على الأدبيات والكتب، والأطر النظرية، والدراسات والبحوث السابقة التي تناولت أبعاد الدراسة، وتحليل هذه الأدبيات والبحوث والدراسات وذلك لتحديد **وعي الشباب بمخاطر الأمن السيبراني**

(ب) الخصائص السيكومترية للاستبيان :

(١)الصدق الظاهري:

أجرت الباحثة الصدق الظاهري لاستمارة استبيان بعد عرضها على (٥) محكمين من أعضاء هيئة التدريس في تخصص الخدمة الاجتماعية لإبداء الرأي في صلاحية الأداة من حيث السلامة اللغوية للعبارات من ناحية وارتباطها بأبعاد الدراسة من ناحية أخرى، وقد تم الاعتماد على نسبة اتفاق لا تقل عن (٨٠%) ، وقد تم حذف بعض العبارات وإعادة صياغة البعض، وبناء على ذلك تم صياغة الاستمارة في صورتها النهائية.

٢-الصدق الإحصائي :

تم حساب الصدق الذاتي (الإحصائي) للاستبيان بحساب الجذر التربيعي لمعامل الثبات وبحساب الجذر التربيعي لمعامل ثبات أداة القياس باستخدام برنامج الحزم الإحصائية للعلوم الإجتماعية Spss فقد بلغت قيمة معامل الصدق الإحصائي للمقياس للكل (٠.٩٠) ، وتعد هذه القيمة مرتفعة مما يؤكد على صلاحية أداة القياس وإمكانية تطبيقها.

جدول رقم (١)

يوضح معاملات الصدق الإحصائي لاستمارة استبيان (ن=١٠)

المتغيرات	معامل ثبات الفا كرونباخ	الجذر التربيعى لمعامل (الثبات)	الدلالة
المخاطر الاجتماعية للأمن السيبراني على الشباب	٠.٨٨	٠.٩٣	دالة عند ٠١.
المخاطر النفسية للأمن السيبراني على الشباب	٠.٩٠	٠.٩٤	دالة عند ٠١.
المخاطر الأمنية للأمن السيبراني على الشباب	٠.٩٣	٠.٩٦	دالة عند ٠١.
المخاطر الأخلاقية للأمن السيبراني على الشباب	٠.٩٢	٠.٩٥	دالة عند ٠١.
الاستبيان ككل	٠.٩٠	٠.٩٤	دالة عند ٠١.

ويتضح من الجدول السابق أن قيمة معامل الصدق الإحصائي لاستمارة استبيان بلغت (٠.٩٠) وتعد هذه القيم مرتفعة وتفي بأغراض الدراسة.

(٣) ثبات الاداة :

تم حساب ثبات الأداة باستخدام معامل ثبات (ألفا .كرونباخ) لقيم الثبات التقديرية، وذلك بتطبيقها على عينة قوامها (١٠) مفردة من االشباب من غير العينة الاساسية وتنطبق عليهم نفس الشروط ، وتم استبعادهم بعد ذلك من العينة الاساسية للدراسة الحالية، وقد جاءت النتائج كما يلي:

جدول رقم (٢)

نتائج ثبات الاستبيان باستخدام معامل (ألفا .كرونباخ)

(ن=١٠)

م	الأبعاد	معامل (ألفا .كرونباخ)
١	المخاطر الاجتماعية للأمن السيبراني على الشباب	٠.٨٨
٢	المخاطر النفسية للأمن السيبراني على الشباب	٠.٩٠
	المخاطر الأمنية للأمن السيبراني على الشباب	٠.٩٣
٣	المخاطر الأخلاقية للأمن السيبراني على الشباب	٠.٩٢
الاستبيان ككل		٠.٩٠

يوضح الجدول السابق أن:

معاملات الثبات للأبعاد تتمتع بدرجة عالية من الثبات، وبذلك يمكن الاعتماد على نتائجها وأصبحت الأداة في صورتها النهائية.

(٤) تحديد مستوى المتوسطات الحسابية للاستجابات

جدول رقم (٣)

يوضح مستويات المتوسطات الحسابية لأبعاد الدراسة

القيم	المستوى
إذا تراوحت قيمة المتوسط للعبارة أو البعد من ١ إلى ١.٦٧	**مستوى منخفض**
إذا تراوحت قيمة المتوسط للعبارة أو البعد من ١.٦٨ إلى ٢.٣٤	**مستوى متوسط**
إذا تراوحت قيمة المتوسط للعبارة أو البعد من ٢.٣٥ إلى ٣	**مستوى مرتفع**

(٥) أساليب التحليل الإحصائي المستخدمة في الدراسة :

تم معالجة البيانات من خلال الحاسب الآلي باستخدام برنامج (SPSS .V. 24.0) الحزم الإحصائية للعلوم الاجتماعية، وقد طبقت الأساليب الإحصائية التالية :

١– التكرارات والنسب المئوية : وذلك لوصف خصائص أفراد عينة الدراسة .
٢– المتوسط الحسابى، والانحراف المعياري، وذلك لتحديد النسبة التقديرية لاستجابات المبحوثين وترتيب العبارات حسب أعلى نسبة.
٣– معامل ثبات (ألفا . كرونباخ): لحساب قيم الثبات التقديرية لأدوات الدراسة.
٤– الصدق الإحصائي: ويتم حسابه من خلال الجذر التربيعى لمعامل الثبات.

سابعًا– مجالات الدراسة:

١– **المجـال المكـاني:** تـم تطبيـق الدراسـة الميدانيـة بمركـز شـباب الأنفوشـي بمحافظـة الإسكندرية.

أسباب اختيار المجال المكاني:

– موافقة المسؤولين بمركز شباب الأنفوشي بالتعاون مع الباحثة لتطبيق الجزء الميداني للدراسة الحالية.
– تجمع وتواجد الشباب الجامعي في مركز الشباب والذي يعتبر أهم المؤسسات التي تهتم برعاية وتنشئة الشباب وتنمية مهاراتهم في ضوء المتغيرات المجتمعية الرقمية السريعة.
– اهتمام المركز بتقديم الخدمات والبرامج الثقافية والاجتماعية التوعوية المختلفة لاستخدام الوسائل التكنولوجية الحديثة وعرض آثارها السلبية والإيجابية على المجتمع.

٢– **المجال البشري:** تم اختيار عينة من الشباب الجامعي من أعضاء مركز شباب الأنفوشي عن طريق المسح الاجتماعي بالعينة من الأعضاء المقيدين بمركز شباب الأنفوشي وعددهم (٢٨٠) مفردة، وتم سحب هذه العينة من إطار المعاينة والبلغ عدده (١٠٣١) مفردة من خلال تطبيق معادلة ستيفن ثامبسون Thompson (2012) لتحديد الحجم العينة المناسب للدراسة وهى كما يلى :– (Steven K,2012,p59;60)

$$n=\frac{N\times p(1-p)}{\left[\left[N-1\times\left(d^2\div z^2\right)\right]+p(1-p)\right]}$$

حيث :–

n= الحجم الأمثل للعينة المطلوبة.
N= حجم المجتمع الأصلى .
P= القيمة الاحتمالية = 0.50
D= نسبة الخطا التى يمكن التجاوز عنها =0.05
Z= الدرجة المعيارية المقابلة لمستوى المعنوية ٠.٠٥ ومستوى ثقة ٠.٩٥ وتساوى ١.٩٦

٣- **المجـــال الزمنـــي:** تمثـل المجـال الزمنـي فـي إجـراء الدراسـة الميدانيـة فـي الفتـرة مـن ٢٠٢٢/١٠/١٥ حتى ٢٠٢٢/١٢/١٧.

أولاً – البيانات الأولية لعينة الدراسة من الشباب:

جدول رقم (٤)

يوضح البيانات الأولية لعينة الدراسة من الشباب.

م	المتغير	الإستجابة (ن =280)	ك	%
١	**النوع**	ذكر	١٠٤	٣٧.٩
		انثي	١٧٦	٦٢.١
المجموع			**٢٨٠**	**١٠٠ %**
٢	**السن**	أقل من 22 سنة	١٥٦	٥٥.٢
		من 22 لأقل من 23 سنة	٩٠	٣١.٩
		من 23 سنة فأكثر	٣٤	١٢.٩
المجموع			**٢٨٠**	**%١٠٠**
٣	**الفرقة الدراسية**	الأولي	٨١	٢٨.٦
		الثانية	٧٥	٢٦.٧
		الثالثة	٧٢	٢٥.٣
		الرابعة	٥٢	١٨.٤
المجموع			**٢٨٠**	**١٠٠ %**

- **يتضـح مـن بيانـات الجـدول السـابق**أن البيانـات الأوليـة لعينـة الدراسـة مـن الشباب جـاءت كالآتي:
- **النوع:** جاء توزيع عينة الدراسة من حيث النوع كالآتي من هم ذكور بنسبة ٣٧.٩ %، بينما الإناث بنسبة ٦٢.١ %.
- **السن** : جاء توزيع عينة الدراسة من حيث السن كالآتي من هم بسن أقل من ٢٢ سنة بنسبة ٥٥.٢ % ، بينما من هم بسن من ٢٢ لأقل من ٢٣ سنة بنسبة ٣١.٩ % ، بينما من هم بسن من ٢٣ سنة فأكثر بنسبة ١٢.٩ % .
- **الفرقـة الدراسـية:** جاء توزيـع عينـة الدراسة من حيث المؤهل العلمي كـالآتي من هو بالفرقة الأولـي بنسبة ٢٨.٦ % ، بينمـا مـن هـو بالفرقـة الثانيـة بنسبة ٢٦.٧ % ، بينمـا مـن هـو بالفرقة الثالثة بنسبة ٢٥.٣ % ، بينما من هو بالفرقة الرابعة بنسبة ١٨.٤ %.

(ب): نتائج الدراسة في ضوء تساؤلات الدراسة :

(١) ما مستوى المخاطر الاجتماعية للأمن السيبراني على الشباب.

جدول رقم (٥)

المخاطر الاجتماعية للأمن السيبراني على الشباب (ن=٢٨٠)

م	العبارات	الاستجابات						المتوسط الحسابي	الانحراف المعياري	الترتيب
		نعم		إلى حد ما		لا				
		ك	%	ك	%	ك	%			
١	أنتهاك الخصوصية لدى الشباب	٢٣٠	٨٢.١	٤٥	١٦.١	٥	١.٨	٢.٨٠	٠.٤٤	٢
٢	التطفل من جانب الهاكر على الشباب	٢٣٤	٨٣.٦	٤١	١٤.٦	٥	١.٨	٢.٨٢	٠.٤٣	١
٣	التجسس على العلاقات الاجتماعية لدى الشباب	٢٢٩	٨١.٨	٤٣	١٥.٤	٨	٢.٩	٢.٧٩	٠.٤٧	٣
٤	أنتحال شخصية الضحية من الشباب	٢٢٠	٧٨.٦	٥٥	١٩.٦	٥	١.٨	٢.٧٧	٠.٤٦	٤
٥	أستغلال شبكة العلاقات الاجتماعية الإلكترونية لدى الشباب	٢١٧	٧٧.٥	٥٢	١٨.٦	١١	٣.٩	٢.٧٤	٠.٥٢	٦
٦	أزمة الثقة في الآخرين لدى الشباب	٢٢٣	٧٩.٦	٣٩	١٣.٩	١٨	٦.٤	٢.٧٣	٠.٥٧	٧
٧	نشر المعلومات المضللة بين الشباب	٢١٦	٧٧.١	٥٠	١٧.٩	١٤	٥.٠	٢.٧٢	٠.٥٥	٨
٨	التنصت على شبكة العلاقات الاجتماعية لدى الشباب	٢١٩	٧٨.٢	٥٢	١٨.٦	٩	٣.٢	٢.٧٥	٠.٥٠	٥
٩	العزلة الاجتماعية لدى الشباب	٢١٠	٧٥.٠	٥٨	٢٠.٧	١٢	٤.٣	٢.٧١	٠.٥٤	٩
المتغيير ككل								٢.٧٦	٠.٥٠	مرتفع

يوضح الجدول السابق أن:

مستوى المخاطر الاجتماعية للأمن السيبراني على الشباب: (مرتفع) حيث بلغ المتوسط الحسابي (٢.٧٦)، ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: جاء في الترتيب الأول التطفل من جانب الهاكر على الشباب بمتوسط حسابي (٢.٨٢)، يليه الترتيب الثاني أنتهاك الخصوصية لدى الشباب بمتوسط حسابي (٢.٨٠)، وجاء في الترتيب الثالث التجسس على العلاقات الاجتماعية لدى الشباب بمتوسط حسابي (٢.٧٩)، وجاء في الترتيب الرابع أنتحال شخصية الضحية من الشباب بمتوسط حسابي (٢.٧٧)، وجاء في الترتيب الخامس التنصت على شبكة العلاقات الاجتماعية لدى الشباب بمتوسط حسابي (٢.٧٥)، وجاء في الترتيب السادس أستغلال شبكة العلاقات الاجتماعية الإلكترونية لدى الشباب بمتوسط حسابي (٢.٧٤)، وجاء في الترتيب السابع أزمة الثقة في الآخرين لدى الشباب بمتوسط حسابي (٢.٧٣)، وجاء في الترتيب الثأمن نشر المعلومات المضللة بين الشبابمتوسط حسابي (٢.٧٢)، وجاء في الترتيب الاخير العزلة الاجتماعية لدى الشباب بمتوسط حسابي (٢.٧١) . ويمكن تفسير ذلك بان المخاطر الاجتماعية للأمن السيبراني على الشباب متعددة الاشكال وتتطلب تنمية الوعي لدى الشباب

بطبيعة تاثيراتها المختلفة على النواحي الاجتماعية لديه وكيفية التعامل معها بشكل إيجابي. وهو ما أشارت إليه دراسة كل من (Puhakainene, S., & Siponen, M., 2010)، ودراسة (عبد الله، ٢٠١٧)، (العريشي، الدوسري، ٢٠١٨)، ودراسة (سليمان، ٢٠١٩)، (الحياري، ٢٠٢٢).

(٢) ما مستوى المخاطر النفسية للأمن السيبراني على الشباب.

جدول رقم (٦)

المخاطر النفسية للأمن السيبراني على الشباب (ن=٢٨٠)

م	العبارات	الاستجابات						المتوسط الحسابي	الانحراف المعياري	الترتيب
		نعم		إلى حد ما		لا				
		ك	%	ك	%	ك	%			
١	التعرض للابتزاز من جانب الهاكرز	٢٣٨	٨٥.٠	٣٣	١١.٨	٩	٣.٢	٢.٨٢	٠.٤٦	٤
٢	الضغط النفسي عند تسريب معلومات خاصة	٢٣٥	٨٣.٩	٣٤	١٢.١	١١	٣.٩	٢.٨٠	٠.٤٩	٦
٣	القلق الدائم من الفضيحة بين الزملاء والأهل	٢٤٠	٨٥.٧	٣٢	١١.٤	٨	٢.٩	٢.٨٣	٠.٤٥	٣
٤	التوتر الدائم عند استخدام التكنولوجيا الرقمية	٢٤٤	٨٧.١	٣٠	١٠.٧	٦	٢.١	٢.٨٥	٠.٤١	١
٥	الخوف من قبول صداقات جديدة	٢٣٠	٨٢.١	٤٨	١٧.١	٢	٠.٧	٢.٨١	٠.٤١	٥
٦	التشكك الدائم في الآخرين عند التعامل الإلكتروني	٢٣٣	٨٣.٢	٣٥	١٢.٥	١٢	٤.٣	٢.٧٩	٠.٥٠	٧
٧	الاكتئاب بعد التعرض لمساومات من جانب الهاكرز	٢٤١	٨٦.١	٣٣	١١.٨	٦	٢.١	٢.٨٤	٠.٤٢	٢
٨	تقديم تنازلات عند التعرض لاختراق الحسابات الشخصية	٢٢٩	٨١.٨	٤١	١٤.٦	١٠	٣.٦	٢.٧٨	٠.٤٩	٨
	المتغيير ككل							٢.٨٢	٠.٤٦	مرتفع

يوضح الجدول السابق أن:

مستوى المخاطر النفسية للأمن السيبراني على الشباب: (مرتفع) حيث بلغ المتوسط الحسابي (٢.٨٢)، وانحراف معياري(٠.٤٦) ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: جاء في الترتيب الأول التوتر الدائم عند استخدام التكنولوجيا الرقمية بمتوسط حسابي (٢.٨٥)، يليه الترتيب الثاني الاكتئاب بعد التعرض لمساومات من جانب الهاكرز بمتوسط حسابي (٢.٨٤)، وجاء في الترتيب الثالث القلق الدائم من الفضيحة بين الزملاء والأهل بمتوسط حسابي (٢.٨٣)، وجاء في الترتيب الرابع التعرض للابتزاز من جانب الهاكرز بمتوسط حسابي (٢.٨٢)، وجاء في الترتيب الخامس الخوف من قبول صداقات جديدة بمتوسط حسابي (٢.٨١)، وجاء في الترتيب السادس الضغط النفسي عند تسريب معلومات خاصة بمتوسط حسابي (٢.٨٠)، وجاء في الترتيب السابع التشكك الدائم في الآخرين عند التعامل الإلكتروني بمتوسط حسابي (٢.٧٩)،

وجاء في الترتيب الثأمن والاخير تقديم تنازلات عند التعرض لاختراق الحسابات الشخصية بمتوسط حسابي (٢.٧٨)، ويمكن تفسير ذلك بان المخاطر النفسية للأمن السيبراني على الشباب متعددة الاشكال وتتطلب تنمية الوعي لدى الشباب بطبيعة تاثيراتها المختلفة على النواحي النفسية لديه وكيفية التعامل معها بشكل إيجابي. وهو ما أشارت إليه دراسة (Kondaa et al., 2018)، (فوزي، ٢٠١٩)، (L. A. Gordon & M. P. Loeb, 2002)، (الحياري، ٢٠٢٢).

(٣) ما مستوى المخاطر الأمنية للأمن السيبراني على الشباب

جدول رقم (٧)

المخاطر الأمنية للأمن السيبراني على الشباب (ن=٢٨٠)

م	العبارات	الاستجابات						المتوسط الحسابي	الانحراف المعياري	الترتيب
		نعم		إلى حد ما		لا				
		ك	%	ك	%	ك	%			
١	ضعف الوعي بآليات التشفير الخوارزمي لتأمين الاتصالات لدى الشباب	٢٥٢	٩٠.٠	٢٦	٩.٣	٢	٠.٧	٢.٨٩	٠.٣٣	١
٢	مراقبة نشاط الشباب على الأنترنت	٢٣٥	٨٣.٩	٣٩	١٣.٩	٦	٢.١	٢.٨٢	٠.٤٤	٦
٣	الاستيلاء على البيانات السرية للشباب الجامعي	٢٣٠	٨٢.١	٣٥	١٢.٥	١٥	٥.٤	٢.٧٧	٠.٥٣	١١
٤	وصول رسائل عشوائية للاختراق الأمني لدى الشباب	٢٣٧	٨٤.٦	٣٧	١٣.٢	٦	٢.١	٢.٨٣	٠.٤٣	٥
٥	اختراق الحسابات الشخصية لدى الشباب	٢٣٣	٨٣.٢	٤٢	١٥.٠	٥	١.٨	٢.٨١	٠.٤٣	٧
٦	اختراق الحسابات المالية الإلكترونية للشباب الجامعي	٢٢٥	٨٠.٤	٤٨	١٧.١	٧	٢.٥	٢.٧٨	٠.٤٧	١٠
٧	ضعف برامج الحماية الإلكترونية لدى الشباب	٢٢٩	٨١.٨	٤٥	١٦.١	٦	٢.١	٢.٨٠	٠.٤٥	٨
٨	عدم استخدام البرامج الأصلية المصدر من جانب الشباب	٢٤٠	٨٥.٧	٣٧	١٣.٢	٣	١.١	٢.٨٥	٠.٣٩	٣
٩	غياب التحديثات المستمر للبرامج لدى الشباب	٢٣٩	٨٥.٤	٣٧	١٣.٢	٤	١.٤	٢.٨٤	٠.٤٠	٤
١٠	وجود ثغرات أمنية في شبكات الاتصال لدى الشباب	٢٢٥	٨٠.٤	٥٠	١٧.٩	٥	١.٨	٢.٧٩	٠.٤٥	٩
١١	أنتشار البرامج الضارة على الأجهزة الشخصية	٢٤٨	٨٨.٦	٢٩	١٠.٤	٣	١.١	٢.٨٨	٠.٣٦	٢
١٢	أنشار لينكات الهاكر على وسائل التواصل الاجتماعي لدى الشباب	٢٢٣	٧٩.٦	٤٨	١٧.١	٩	٣.٢	٢.٧٦	٠.٤٩	١٢
	المتغيير ككل							٢.٨٢	٠.٤٤	مرتفع

يوضح الجدول السابق أن:

مستوى المخاطر الأمنية للأمن السيبراني على الشباب: (مرتفع) حيث بلغ المتوسط الحسابي (٢.٨٢)، وانحراف معياري (٠.٤٤) ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: جاء في الترتيب الأول ضعف الوعي بآليات التشفير الخوارزمي لتأمين الاتصالات لدى الشباب بمتوسط حسابي (٢.٨٩)، يليه الترتيب الثاني أنتشار البرامج الضارة على الأجهزة الشخصية بمتوسط حسابي (٢.٨٨)، وجاء في الترتيب الثالث عدم استخدام البرامج الأصلية المصدر من جانب الشباب بمتوسط حسابي (٢.٨٥)، وجاء في الترتيب الرابع غياب التحديثات المستمر للبرامج لدى الشباب بمتوسط حسابي (٢.٨٤)، وجاء في الترتيب الخامس وصول رسائل عشوائية للاختراق الأمني لدى الشباب بمتوسط حسابي (٢.٨٣)، وجاء في الترتيب السادس مراقبة نشاط الشباب على الأنترنت بمتوسط حسابي (٢.٨٢)، وجاء في الترتيب السابع اختراق الحسابات الشخصية لدى الشباب بمتوسط حسابي (٢.٨١)، وجاء في الترتيب الثأمن ضعف برامج الحماية الإلكترونية لدى الشباب بمتوسط حسابي (٢.٨٠)، وجاء في الترتيب التاسع وجود ثغرات أمنية في شبكات الاتصال لدى الشباب بمتوسط حسابي (٢.٧٩)، وجاء في الترتيب العاشر اختراق الحسابات المالية الإلكترونية للشباب الجامعي بمتوسط حسابي (٢.٧٨)، وجاء في الترتيب الحادي عشر الاستيلاء على البيانات السرية للشباب الجامعي بمتوسط حسابي (٢.٧٧)، وجاء في الترتيب الاخير أنشار لينكات الهاكر على وسائل التواصل الاجتماعي لدى الشباب بمتوسط حسابي (٢.٧٦)، ويمكن تفسير ذلك بان المخاطر الأمنية للأمن السيبراني على الشباب متعددة الاشكال وتتطلب تنمية الوعي لدى الشباب بطبيعة تاثيراتها المختلفة على النواحي الأمنية لديه وكيفية التعامل معها بشكل إيجابي. وهو ما أشارت إليه دراسة (علي، ٢٠٢٢)، (التيماني، ٢٠٢١)، (عبد اللطيف، ٢٠٢٢)، (Ponnusamy & Rubasundram, 2019)، (E. Kamiya & L. Schindler, 2017)، (سليمان، ٢٠٢١)، (K. Jones, J. P. Ashby & M. Kruse, 2017).

(٤) ما مستوى المخاطر الأخلاقية للأمن السيبراني على الشباب

جدول رقم (٨)

المخاطر الأخلاقية للأمن السيبراني على الشباب (ن=٢٨٠)

م	العبارات	الاستجابات						المتوسط الحسابي	الانحراف المعياري	الترتيب
		نعم		إلى حد ما		لا				
		ك	%	ك	%	ك	%			
١	أنتشار المحتويات الغير أخلاقية بين الشباب	٢٣٠	٨٢.١	٤٣	١٥.٤	٧	٢.٥	٢.٨٠	٠.٤٦	٢
٢	تضليل الضحايا من الشباب	٢٢٩	٨١.٨	٤٣	١٥.٤	٨	٢.٩	٢.٧٩	٠.٤٧	٣
٣	طلب صور غير أخلاقية من الضحية من الشباب	٢٢٥	٨٠.٤	٤٧	١٦.٨	٨	٢.٩	٢.٧٨	٠.٤٨	٤
٤	عمليات النصب المالية لدى الشباب	٢١٨	٧٧.٩	٥٩	٢١.١	٣	١.١	٢.٧٧	٠.٤٥	٥
٥	الترويج لمحتويات جنسية بين الشباب	٢١٨	٧٧.٩	٥٥	١٩.٦	٧	٢.٥	٢.٧٥	٠.٤٩	٧
٦	انتحال شخصيات للنصب على الآخرين من الشباب	٢٢٠	٧٨.٦	٥٢	١٨.٦	٨	٢.٩	٢.٧٦	٠.٤٩	٦
٧	استغلال احتياجات الضحية من الشباب	٢٣٣	٨٣.٢	٤١	١٤.٦	٦	٢.١	٢.٨١	٠.٤٤	١
المتغيير ككل								٢.٧٨	٠.٤٧	مرتفع

يوضح الجدول السابق أن:

مستوى المخاطر الأخلاقية للأمن السيبراني على الشباب: (مرتفع) حيث بلغ المتوسط الحسابي (٢.٧٨)، ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: جاء في الترتيب الأول استغلال احتياجات الضحية من الشباب بمتوسط حسابي (٢.٨١)، يليه الترتيب الثاني أنتشار المحتويات الغير أخلاقية بين الشباب بمتوسط حسابي (٢.٨٠)، وجاء في الترتيب الثالث تضليل الضحايا من الشباب بمتوسط حسابي (٢.٧٩)، وجاء في الترتيب الرابع طلب صور غير أخلاقية من الضحية من الشباب بمتوسط حسابي (٢.٧٨)، وجاء في الترتيب الخامس عمليات النصب المالية لدى الشباب بمتوسط حسابي (٢.٧٧)، وجاء في الترتيب السادس انتحال شخصيات للنصب على الآخرين من الشباب بمتوسط حسابي (٢.٧٦)، وجاء في الترتيب الاخير الترويج لمحتويات جنسية بين الشباب بمتوسط حسابي (٢.٧٥)، ويمكن تفسير ذلك بان المخاطر الأخلاقية للأمن السيبراني على الشباب متعددة الاشكال وتتطلب تنمية الوعي لدى الشباب بطبيعة تاثيراتها المختلفة على النواحي الأخلاقية لديه وكيفية التعامل معها بشكل إيجابي. وهو ما أشارت إليه دراسة كل من (Puhakainene, S., & Siponen, M., 2010)، دراسة (Dreger, P. & Kreutzfeld, C., 2016).

مستوى المخاطر ككل

جدول رقم (٩)

يوضح مخاطر الأمن السيبراني على الشباب.

م	الأبعاد	المتوسط الوزني	الانحراف المعياري	المستوي	الترتيب
١	**المخاطر الاجتماعية للأمن السيبراني على الشباب**	٢.٧٦	٠.٥٠	مرتفعة	٤
٢	**المخاطر النفسية للأمن السيبراني على الشباب**	٢.٨٢	٠.٤٦	مرتفعة	٢
٣	**المخاطر الأمنية للأمن السيبراني على الشباب**	٢.٨٢	٠.٤٤	مرتفعة	١
٤	**المخاطر الأخلاقية للأمن السيبراني على الشباب**	٢.٧٨	٠.٤٧	مرتفعة	٣
المجموع الكلي		٢.٧٩	٠.٤٦	**مرتفعة**	

يوضح الجدول السابق أن:

مستوى المخاطر للأمن السيبراني على الشباب ككل: (مرتفع) حيث بلغ المتوسط الحسابي (٢.٧٩)، ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: جاء في الترتيب الأول المخاطر الأمنية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٨٢)، وانحراف معياري(٠.٤٤) يليه الترتيب الثاني المخاطر النفسية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٨٢)، وانحراف معياري(٠.٤٦) وجاء في الترتيب الثالث المخاطر الأخلاقية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٧٨), وجاء في الترتيب الثالث المخاطر الاجتماعية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٧٦).

النتائج العامة للدراسة :

- مستوى المخاطر الاجتماعية للأمن السيبراني على الشباب: (مرتفع) حيث بلغ المتوسط الحسابي (٢.٧٦)، ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: جاء في الترتيب الأول التطفل من جانب الهاكر على الشباب بمتوسط حسابي (٢.٨٢), يليه الترتيب الثاني أنتهاك الخصوصية لدى الشباب بمتوسط حسابي (٢.٨٠), وجاء في الترتيب الثالث التجسس على العلاقات الاجتماعية لدى الشباب بمتوسط حسابي (٢.٧٩)، وجاء في الترتيب الاخير العزلة الاجتماعية لدى الشباب بمتوسط حسابي (٢.٧١).

- مستوى المخاطر النفسية للأمن السيبراني على الشباب: (مرتفع) حيث بلغ المتوسط الحسابي (٢.٨٢)، وانحراف معياري(٠.٤٦) ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: جاء في الترتيب الأول التوتر الدائم عند استخدام التكنولوجيا الرقمية بمتوسط حسابي (٢.٨٥), يليه الترتيب الثاني الاكتئاب بعد التعرض لمساومات من جانب الهاكرز بمتوسط حسابي (٢.٨٤), وجاء في الترتيب الثالث القلق الدائم من الفضيحة بين الزملاء والأهل بمتوسط حسابي (٢.٨٣), وجاء في الترتيب الثأمن والاخير تقديم تنازلات عند التعرض لاختراق الحسابات الشخصية بمتوسط حسابي (٢.٧٨).
- مستوى المخاطر الأمنية للأمن السيبراني على الشباب: (مرتفع) حيث بلغ المتوسط الحسابي (٢.٨٢)، وانحراف معياري(٠.٤٤) ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: جاء في الترتيب الأول ضعف الوعي بآليات التشفير الخوارزمي لتأمين الاتصالات لدى الشباب بمتوسط حسابي (٢.٨٩), يليه الترتيب الثاني أنتشار البرامج الضارة على الأجهزة الشخصيةبمتوسط حسابي (٢.٨٨), وجاء في الترتيب الثالث عدم استخدام البرامج الأصلية المصدر من جانب الشباب بمتوسط حسابي (٢.٨٥), وجاء في الترتيب الاخير أنشار لينكات الهاكر على وسائل التواصل الاجتماعي لدى الشباب بمتوسط حسابي (٢.٧٦).
- مستوى المخاطر الأخلاقية للأمن السيبراني على الشباب: (مرتفع) حيث بلغ المتوسط الحسابي (٢.٧٨)، ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: جاء في الترتيب الأول استغلال احتياجات الضحية من الشباب بمتوسط حسابي (٢.٨١), يليه الترتيب الثاني أنتشار المحتويات الغير أخلاقية بين الشباب بمتوسط حسابي (٢.٨٠), وجاء في الترتيب الثالث تضليل الضحايا من الشباب بمتوسط حسابي (٢.٧٩)، وجاء في الترتيب الاخير الترويج لمحتويات جنسية بين الشباب بمتوسط حسابي (٢.٧٥).
- مستوى المخاطر على الشباب ككل: (مرتفع) حيث بلغ المتوسط الحسابي (٢.٧٩)، ومؤشرات ذلك وفقاً لترتيب المتوسط الحسابي: جاء في الترتيب الأول المخاطر الأمنية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٨٢),وانحراف معياري(٠.٤٤) يليه الترتيب الثاني المخاطر النفسية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٨٢), وانحراف معياري(٠.٤٦) وجاء في الترتيب الثالث المخاطر الأخلاقية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٧٨), وجاء في الترتيب الثالث المخاطر الاجتماعية للأمن السيبراني على الشباب بمتوسط حسابي (٢.٧٦).

البرنامج المقترح من منظور طريقة تنظيم المجتمع لتنمية وعي الشباب بمخاطر الأمن السيبراني

أولاً– الركائز والأسس التي اعتمد عليها البرنامج المقترح من منظور طريقة تنظيم المجتمع لتنمية وعي الشباب بمخاطر الأمن السيبراني:

- نتائج وتوصيات الدراسات والبحوث السابقة التي تناولت مخاطر الأمن السيبراني وأنواعها.
- نتائج الدراسة الحالية والمرتبطة بتوعية الشباب بمخاطر الأمن السيبراني.
- الاتجاهات الحديثة في طريقة تنظيم المجتمع وتناول موضوع مخاطر الأمن السيبراني.

ثانيًا– أهداف البرنامج المقترح:

- يسعى البرنامج المقترح إلى تحقيق هدف رئيس وهو تنمية وعي الشباب بمخاطر الأمن السيبراني. ويتم تحقيق الهدف الرئيسي من خلال مجموعة أهداف فرعية تحددت في:
  - تحديد مستوى المخاطر الاجتماعية للأمن السيبراني على الشباب.
  - تحديد مستوى المخاطر النفسية للأمن السيبراني على الشباب.
  - تحديد مستوى المخاطر الأمنية للأمن السيبراني على الشباب.
  - تحديد مستوى المخاطر الأخلاقية للأمن السيبراني على الشباب.

ثالثًا– أهمية البرنامج المقترح:

- تحديد أشكال المخاطر التي يتعرض لها الشباب من هجمات الأمن السيبراني (الاجتماعية – النفسية – الأمنية – الأخلاقية).
- تحديد أهداف وأبعاد (القانونية – العسكرية – الاقتصادية – الاجتماعية – السياسية) للأمن السيبراني.
- تحديد جهود الدولة بمؤسساتها للحد من مخاطر الهجمات السيبرانية.
- تحديد المعوقات التي تحد من حماية المؤسسات والأفراد من التهديدات والهجمات السيبرانية.

رابعًا– الأنساق التي يتعامل معها البرنامج المقترح:

- الشباب المقيد بالجامعات وأعضاء بمراكز الشباب.
- المتخصصين في تكنولوجيا المعلومات.
- الباحثة والمتخصصين في الخدمة الاجتماعية والتكنولوجيا الحديثة.

خامسًا– محتويات البرنامج المقترح:

١– تنمية وعي الشباب بالمخاطر الاجتماعية للأمن السيبراني.

- تعلم فنيات الحفاظ على الخصوصية لدى الشباب.

- غلق البيانات التي تسمح بالتطفل من جانب الهاكر والتجسس على الشباب.
- كيفية التصرف عند انتحال الهاكرز للحسابات.
- بناء الثقة وفقًا للأمن السيبراني عند التعامل الإلكتروني مع الآخرين.
- توعية الشباب الجامعي من مخاطر المعلومات المضللة.

٢- تنمية وعي الشباب بالمخاطر النفسية للأمن السيبراني.

- كيفية التعامل نفسيًا التعرض للابتزاز من جانب الهاكرز.
- مهارة الصمود النفسي عند تسريب معلومات خاصة.
- خفض التوتر الدائم من استخدام التكنولوجيا الرقمية.
- الحد من التشكك الدائم في الآخرين عند التعامل الإلكتروني بناء على الوعي المعرفي.
- عدم تقديم تنازلات عند التعرض لاختراق الحسابات الشخصية.
- توفير دوائر دعم نفسي.

٣- تنمية وعي الشباب بالمخاطر الأمنية للأمن السيبراني.

- الوعي بآليات التشفير الخوارزمي لتأمين الاتصالات لدى الشباب.
- مراقبة نشاط الشباب على الإنترنت.
- الحفاظ على البيانات السرية للشباب.
- تجنب الرسائل عشوائية للاختراق الأمني لدى الشباب.
- كيفية استعادة الحساب عند اختراق الحسابات الشخصية لدى الشباب.
- كيفية إيقاف اختراق الحسابات المالية الإلكترنية للشباب.
- شراء برامج الحماية الإلكترونية.
- استخدام البرامج الأصلية المصدر من جانب الشباب.
- التحديثات المستمرة للبرامج لدى الشباب.
- غلق الثغرات أمنية في شبكات الاتصال لدى الشباب.
- تنظيف البرامج الضارة على الأجهزة الشخصية.
- تجنب فتح لينكات الهاكر على وسائل التواصل الاجتماعي لدى الشباب.

٤- تنمية وعي الشباب بالمخاطر الأخلاقية للأمن السيبراني.

- تجنب المحتويات الغير أخلاقية بين الشباب.
- الوعي بأساليب تضليل الضحايا من الشباب.
- عدم الانسياق وراء طلب صور غير أخلاقية من الضحية من الشباب.
- تجنب عمليات النصب المالية لدى الشباب.

- البعد عن منصات الترويج لمحتويات جنسية بين الشباب.

سادسًا- استراتيجيات البرنامج المقترح:

(استراتيجية التفاوض- الإقناع- الضغط- تغيير السلوك- استراتيجية بناء الاتصالات)

سابعًا- تكنيكات البرنامج المقترح:

(حل المشكلة – التعاون – الشرح والتوضيح – العلاقة المهنية).

ثأمنا- أدوات البرنامج المقترح:

(دور المساعد – المرشد – المخطط – المنسق – الخبير – المنمي).

تاسعًا- أدوات البرنامج المقترح:

(قواعد البيانات الإلكترونية- المناقشات الجماعية- المقابلات- الندوات – المقابلات)

عاشرًا- المهارات المهنية للبرنامج المقترح:

(مهارة ممارسة الأدوار – الاتصال – الملاحظة – الإنصاف الواعي – مهارة المشورة المهنية).

مراجع الدراسة

- أبو النصر، مدحت (٢٠٢٠). الخدمة الاجتماعية الإلكترونية، بحث منشور، المجلة العربية للمعلوماتية وأمن المعلومات، العدد (١).
- أبو النيل، مرفت أحمد (٢٠١٣). تنمية وعي الشباب بمعنى المواطنة وكيفية المطالبة بحقوقهم الإنسانية من منظور الخدمة الاجتماعية، مجلة دراسات في الخدمة الاجتماعية والعلوم الإنسانية، جامعة حلوان، العدد (٣٤).
- البطاينة، محمد، العقيف، محمد (٢٠١٨). التسوق عبر الإنترنت، مدخل نظر النظرية الموحدة لقبول واستخدام التكنولوجيا، مجلة جامعة النجاح للأبحاث (العلوم الإنسانية)، جامعة جريش، الأردن، ع(١٢).
- بندق، حسام طلعت (٢٠١١). مراكز الشباب وتنمية قيمة المواطنة لدى المرأة المصرية، دراسة وصفية مطبقة على مركز شباب مدينة المحلة الكبرى محافظة الغربية، مجلة دراسات في الخدمة الاجتماعية والعلوم الإنسانية، كلية الخدمة الاجتماعية، جامعة حلوان.
- التيماني، مداخل زيد عبد الرحيم (٢٠٢١). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني، مجلة الخدمة الاجتماعية، العدد (١).
- جاب الله، عادل موسى عوض (٢٠٢٢). وسائل حماية الأمن السيبراني: دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة مجلة كلية الشريعة والقانون بأسيوط، العدد (٣٤).
- الجندي، علياء بنت عبدالله ومحمد ، نهير طه (٢٠١٩). دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلومات لدى طالبات الجامعة ، مجلة عالم التربية ،المؤسسة العربية للاستثمارات العلمية وتنمية الموارد البشرية، العدد (٦٧).
- حسانين. أسامة محمد عبد الرحمن (٢٠١٤). دور الفيس بوك في إمداد الشباب بالمعلومات حول قضايا الفساد المصري، رسالة دكتوراه غير منشوره، جامعة عين شمس، معهد الدراسات العليا للطفولة، قسم الإعلام وثقافة الأطفال.
- حسانين، أمل عبد الكريم (٢٠٢٢). سياسة الخدمة الاجتماعية الإلكترونية في عصر العولمة، المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للعلوم والآداب، العدد (٩).
- الحياري، عبد المجيد صالح (٢٠٢٢). مركز البحث وتطوير الموارد البشرية، المجلة العربية للنشر العلمي، العدد (٤١).
- الخالدي، أيمن على عيد (٢٠١٥). دور المراكز الشبابية في تنمية المسئولية الاجتماعية لدى الشباب المنتمين إليها في محافظة المفرق، رسالة دكتوراه، كلية الدراسات العليا، الجامعة الأردنية، الأردن.
- الخضري، جيهان سعد محمد وكليبي ،نعمة ناصر مدبش و سلامي، هدى جبريل على (٢٠٢٠) الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية دراسة مقارنة مجلة تطوير الأداء الجامعي، العدد(٢).
- الداغر، مجدي محمد عبد الجواد (٢٠٢١). اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبراني في مصر، دراسة ميدانية ، المجلة العربية لبحوث الإعلام والاتصال، العدد (٣٣)، ٤-١١٠.

- الدخيل، عبد العزيز عبد الله (٢٠١٢). معجم مصطلحات الخدمة الاجتماعية والعلوم الاجتماعية، دار المناهج للنشر والتوزيع، عمان.
- زمورة، جمال، وبن عيسى، ليلى (٢٠٢٢). أهمية حوكمة الأمن السيبراني لضمان تحول رقمي أمن للخدمات العمومية في الجزائر، مجلة البحوث الاقتصادية المتقدمة، العدد (٢)، ٤١٤ – ٤٢٩.
- سليمان، ايناس ممدوح محمد محمد (٢٠٢١). دور الأمن السيبراني في مواجهة الإرهاب الالكتروني مجلة العلوم القانونية والاقتصادية، ١١– ٥٢ مسترجع من:
- http://search.mandumah.com/Record/1294728
- السواط ، عواطف وآخرون (٢٠٢٠). العلاقة بين الوعي الأمن السيبراني والقيم الوطنية والأخلاقية لتلاميذ المرحلتين الابتدائية والمتوسطة، بحث منشور مجله البحث العلمي في التربية، العدد (٤)، الطائف السعودية.
- السيد، فاطمة أنور محمد (٢٠٢١). آليات تنمية وعي الشباب بمخاطر الوسائل التكنولوجية الحديثة، المؤتمر البيئي الأول، التنمية المستدامة وبناء الإنسان في ظل تحديات العصر، كلية التربية، قطاع خدمة المجتمع، تنمية البيئة، جامعة الفيوم.
- الشلوي راشد حمدان عيد (٢٠٢٢). المتطلبات الحديثة لمكافحة الجريمة السيبرانية في المملكة العربية السعودية: دراسة تطبيقية على ضباط شرطة محافظة الطائف عالم التربية، العدد (٧٦)، ٤٨–١٠٥.
- الصانع، نورة عمر وسليمان، ايناس السيد محمد وعسران، عواطف سعد الدين والسواط، حمد بن حمودة ، وأبو عيشة ،زاهدة جميل (٢٠٢٠). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية، جامعة المنصورة، عدد (١١١).
- عبد الصادق، عادل (٢٠١٧). الفضاء الالكتروني والعلاقات الدولية، دراسة في النظرية والتطبيق، القاهرة، الهيئة المصرية العامة للكتاب.
- عبد العزيز، أبو بكر على (٢٠٢١). برنامج مقترح لتنمية وعي الشباب الجامعي بحقوق الإنسان من منظور الخدمة الاجتماعية، مجلة العلوم الإنسانية، جامعة المرقب، كلية الآداب بالحمص، العدد (٢٢).
- العبد الكريم (٢٠١٧). أخلاقيات ممارسة الخدمة الاجتماعية الإلكترونية، الجمعية المصرية للأخصائيين الاجتماعيين، مجلة الخدمة الاجتماعية، حلوان، العدد (٥٧).
- عبداللطيف، سماح محمد لطفي (٢٠٢٢). دور برامج الثقافة الأمنية في توعية طلاب الجامعة من مخاطر الجرائم الإلكترونية المهددة للأمن السيبراني، دراسة تحليلية ،مجلة بحوث كلية الآداب، كلية الآداب، جامعة المنوفية، العدد (١٢٩).
- عبدالله، ميادة بشير محمد (٢٠١٧). توظيف برامج العلاقات العامة في النوعية بمخاطر الجرائم الإلكترونية، رسالة ماجستير، دراسة تحليلية وصفية على الإدارات المسؤولة عن الجرائم الإلكترونية، جامعة السودان، للعلوم والتكنولوجيا.
- العريشي، جبريل والدوسري، سلمى (٢٠١٨). دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع مجلة مكتبة الملك فهد الوطنية مكتبة الملك فهد الوطنية بالرياض، العدد(٢٤)، ٣٧٣–٣٠٢.
- عطية، أحمد محمد صلاح (٢٠٢١). التحول الرقمي في مصر: هلي يلقي بمسئوليات جديدة على المراجع؟. مجلة البحوث التجارية، العدد (١).

- العقبي، طه أحمد منص، و صالح عبد الله مقبل على (٢٠٢٢). الأحكام المتعلقة بالأمن السيبراني في الشريعة الإسلامية وتطبيقاته المعاصرة مجلة مركز جزيرة العرب للبحوث التربوية والإنسانية، العدد (١٣).
- علي، ماهر أبو المعاطي (٢٠١٠). الاتجاهات الحديثة في الخدمة الاجتماعية، المكتب الجامعي الحديث، القاهرة.
- علي، هالة مصطفي محمد (٢٠٢٢). التخطيط لتنمية وعى الشباب بمخاطر الجرائم الإلكترونية، مجلة دراسات في الخدمة الاجتماعية، جامعة حلوان، كلية الخدمة الاجتماعية، العدد (٦٠).
- علي، هيام على حامد (٢٠١٦). تصور مقترح لدور جماعات الأسر الطلابية في تنمية وعي الشباب الجامعي لمشكلة التحرش الجنسي، الجمعية المصرية للأخصائيين الاجتماعيين، مجلة الخدمة الاجتماعية.
- فهيم، كلير (٢٠٠٧). طريقة نجاح الشباب في الحياة، مكتبة الأنجلو المصرية، القاهرة.
- فوزي، إسلام (٢٠١٩). الأمن السيبراني: الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي، المجلة الاجتماعية القومية، المركز القومي للبحوث الاجتماعية والجنائية، ع (٢).
- كلاع، شريفة (٢٠٢٢). الأمن السيبراني وتحديات الجاسوسية والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجفلة، ع (٢).
- الكواري، كلثم جبر(٢٠٢٠) ممارسة الخدمة الاجتماعية الرقمية في الوطن العربي دولة قطر انموذجاً، بحث منشور، مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية، جامعة الفيوم، العدد ٢٧.
- ماجد، احمد. (٢٠١٨). الذكاء الاصطناعي بدولة الامارات، إدارة الدراسات والسياسات الاقتصادية، دبى.
- المجلس الأعلى للأمن السيبراني (٢٠١٧). رئاسة الجمهورية، مجلس الوزراء، الاستراتيجية الوطنية لأمن السيبراني.
- مدكور، إبراهيم (١٩٧٥). معجم العلوم الاجتماعية، الهيئة المصرية العامة للكتاب، القاهرة.
- المصري، محمد عزت (٢٠١٢). تخطيط لتفعيل دور مراكز الشباب في تعزيز ثقافة التغير السلمي كأحد مبادئ بناء الدولة المدنية، المؤتمر الدولي رقم ٢٥، كلية الخدمة الاجتماعية، جامعة حلوان، ج ١١.
- مطروح، وفاء و أونيس ، ابتسام (٢٠٢٢) تداعيات جائحة كوفيد ١٩ وتأثيرها على تحقيق الأمن السيبراني في الجزائر، المجلة الدولية للاتصال الاجتماعي مجلد٩،ع٢، ٦٥٧ – ٦٨٠،متاح على الرابط التالي http://search.mandumah.com/Record/1282558
- مؤيد، هيثم جودة (٢٠١٧). تبني أخصائي الإعلام التربوي تكنولوجيًا، النشر الإلكتروني لإنتاج وتقييم الموارد الإعلامية المطبوعة، المجلة العلمية لبحوث الصحافة، كلية الإعلام، جامعة القاهرة، القاهرة.
- النوحي، عبد العزيز فهمي إبراهيم (٢٠٠١). المؤسسة العامة في الخدمة الاجتماعية، عملية حل المشكلة ضمن إطار تقني إيكولوجي، دار الأقصى، القاهرة.
- نهى، محمد سيد (٢٠٠١). العمل مع جماعات الشباب ودعم الانتماء الوطني في ظل العولمة، مجلة دراسات للعلوم الاجتماعية والإنسانية، كلية الخدمة الاجتماعية، جامعة حلوان، عدد (١٠).
- النويران، ثامر على (٢٠١٥). الجرائم الإلكترونية وطرق الحد منها: تجربة الأردن، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC المملكة العربية السعودية، الرياض، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات.

- هيئة الاتصالات وتقنية المعلومات (٢٠٢٠). إجراءات التعامل مع حوادث الأمن السيبراني في قطاع الاتصالات وتقنية المعلومات والبريد. الرياض، المركز الإعلامي للهيئة.

- Arnett, J. J. (2000). Emerging Adulthood: A theory of development from the late Teens through the Twenties. American Psychologist, 55 (4), 469-480. DOI: 10.1037/0003-066X.55.5.469.
- Begishev, I1dar. (2021).Cyber-Security Culture: Psychological and Legal Aspects Psychology and Law ,Volume11(4) ,207,220 , DO110.17759/psychology.2021110415
- Chickering, A. W., & Reisser, L. (1993). Education and Identity. San Francisco: Jossey-Bass.
- Dreger, P., & Kreulzfeld, C. (2016). Advanced Persistent Threats: A Symbiotic Relationship with Cyber espionage. Cybersecurity Journal, 12 (2), 45-63.
- ENISA (European Union Agency for Cyber security) (2019). ENISA Threat Landscape Report 2019. Retrieved from ENISA website.
- ENISA (European Union Agency for Cybersecurity) (2019). ENISA Threat Landscape Report 2019. Retrieved from ENISA websit.
- Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investments. ACM Transactions on Information and System Security (TISSEC), 5 (4), 438-457.
- Hemsley-Bron, J., & Oplatka, I. (2015). University Marketing: A Review of the Literature and future research directions. Journal of Marketing for Higher Education, 25 (2), 169-196. DOI:10.1080/08841241.2015.1081665.
- Insurance Purchasing in US Organizations. (Doctoral dissertation, Wilmington University-Delaware).
- International Institute of Standards and Technology (NIST) (2018). Framework for Improving Critical Infrastructure Cyber security. NIST. Retrieved from NIST website.
- International Telecommunication Union (ITU) (2018). Global Cyber Security Index (GCI). Retrieved from ITU website.
- International Telecommunication Union (ITU) (2018). Global Cyber security Index (GCI). Retrieved from ITU website.
- Jackson, Jennifer T.(2017) A biodiversity approach to cyber security, Thesis (Ph.D.), University of Warwick , available at , https://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.752472
- Kamiya, E., & Schindler, L. (2017). Understanding the impact of Cybersecurity Breaches on financial markets. Journal of Financial Economics, 126 (2), 500-517.

- Kondo. T ; Katsenga. N. Zvidzayi T.(2018): Bercrime and Human Rights: A case for the due process of internet criminals, orensic Research & Criminology International Journal
- Mandiant (FireEye) (2020). M-Trends 2020 Report: Insights into Today's Cyber Attack Trends. FireEye. Retrieved from Mandiant website.
- Maranga, M. & Nelson, M. (2019): Emerging Issues in Cyber Security for Initiutions of Higher Education. International Journal of Computer Science & Network. 8(4) August, pp 371-379
- Moulton, P. (2021). Decision Factors Used by Risk Managers for Cyber.
- National Institute of Standards and Technology (NIST) (2018). Framework for improving critical infrastructure Cybersecurity NIST. Retrieved from NIST website.
- National Institute of Standards and Technology (NIST) (2021). NIST special publication 800.
- Pascarella, E. T., & Terenzini, P. T. (2005). How College Affects Students: A Third decade of research. Jossey-Bass.
- Ponnusamy, Suhannia & Geetha A. Rubasundramk (2019)K An international study on the Risk of Cyber Terrorismk international journal of Recent technology and Engineering (URTE). volume -7 issue -5S, January 2019.
- Puhakainen, S., & Siponen, M. (2010). Cybersecurity Awareness Training: A study on effectiveness and user behavior. Information & Computer Security, 18 (4), 265-276.
- Savickas, M. L. (2002). Career Construction: A developmental theory of career counseling. In D. Brown & Associates (eds.), career development and counseling: Putting theory and research to work (pp. 149-208). Hoboken, NJ: John Wiley & Sons.
- Ulven, J, B. & Wangen, G. (2021): A Systematic Review of Cybersecurity Risks in Higher Education, Faculty of Information Technology and Electrical Engineering, Future Internet, 13(2), 39, pp2-40
- UNICEF, Lao PDR (2020). Keeping children safe online during the COVID-19pandemic. UNICEF
- UNODC United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. United nations
- World Economic Forum (WEF) (2020). The Global risks report 2020. WEF. Retrieved from WEF website.
- Youniss, J., & Yates, M. (1997). Community Service and social responsibility in youth. Chicago: University of Chicago Press.