تعزيز ثقافة الأمن السيبراني
لدى طالبات جامعة القاهرة
لمواجهة العنف الرقمي

إعداد
د/ نهى عادل مجاهد
مدرس بقسم أصول التربية

كلية الدراسات العليا للتربية –جامعة القاهرة

مستخلص البحث:

يهدف البحث الحالي إلى تعرف الإطار الفكري للعنف الرقمي، والإطار المفاهيمي للأمن السيبراني، والاطلاع على أبرز جهود جامعة القاهرة في مواجهة العنف الرقمي ضد الطالبات، وكذلك تعرف مستوى وعي طالبات جامعة القاهرة بثقافة الأمن السيبراني لمواجهة العنف الرقمي، وصولا لوضع تصور مقترح لتعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي.

واتبعت الباحثة **"منهج دراسة الحالة"**، وتطبيقًا لهذا المنهج بالبحث الحالي تم تحديد الحالة ممثلة في طالبات جامعة القاهرة، وتعزيز ثقافة الأمن السيبراني لديهن حتى يتمكن من مواجهة العنف الرقمي، ومن ثم تم جمع البيانات والمعلومات باستخدام أداة **"المقابلة"**، والتي تكونت من عدد (١٠) أسئلة، مقسمة في محورين: أسئلة تتعلق بفهم الأمن السيبراني، وأسئلة تتعلق بالعنف الرقمي، والتي هدفت لتعرف مستوى وعي طالبات جامعة القاهرة بثقافة الأمن السيبراني لمواجهة العنف الرقمي. وطبق البحث على عينة قوامها (١٢٤) طالبة من جامعة القاهرة بالمرحلة الجامعية الأولى من كليات (الآداب، التجارة، الإعلام، دار العلوم) كنماذج للكليات النظرية، ومن كليات (العلوم، والحاسبات والذكاء الاصطناعي) كنماذج للكليات العملية. بالإضافة إلى عينة من طالبات كلية الدراسات العليا للتربية بجامعة القاهرة كنموذج لطالبات الدراسات العليا.

وتوصل البحث إلى مجموعة من النتائج من أهمها:

- أجمعت آراء عدد كبير من طالبات كليات (الآداب- التجارة- دار العلوم) حول نقص امتلاكهن لمهارات الأمن السيبراني، في حين أكدت طالبات كلية (الحاسبات والذكاء الاصطناعي) على امتلاكهن لمعظم مهارات الأمن السيبراني ومعرفتهن لها نظرًا لطبيعة

دراستهن، في حين أجمعت آراء طالبات كليتي (العلوم والإعلام) وطالبات الدبلوم العامة بكلية الدراسات العليا للتربية على معرفتهن المتوسطة لها.

- تبين تعرض نسبة (٦ , ٥٥٪) من الطالبات عينة البحث أو من يعرفونهم لأشكال من العنف الرقمي مثل التحرش أو التهديدات عبر الإنترنت؛ والذي كان له آثاره السلبية على نفسيتهن وتعرضهن للاكتئاب والعزلة والإحباط والقلق والخوف واضطرابات النوم والشهية وعدم الثقة بالنفس، والتأثير على صحتهن النفسية ومستواهن الأكاديمي وتحصيلهن الدراسي.

وتوصل البحث إلى وضع تصور مقترح لتعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي.

الكلمات المفتاحية: الأمن السيبراني- طالبات الجامعة- العنف الرقمي.

Research abstract

The current research aims to identify the intellectual framework of digital violence, the conceptual framework of cybersecurity, and review the most prominent efforts of Cairo University in confronting digital violence against female students, as well as identifying the level of awareness of Cairo University students of the culture of cybersecurity to confront digital violence, in order to develop a proposed vision to enhance the culture of cybersecurity among Cairo University students to confront digital violence. The researcher followed the "case study approach", and in application of this approach in the current research, the case was identified represented by Cairo University students, and the culture of cybersecurity was enhanced among them so that they could confront digital violence, and then data and information were collected using the "interview" tool, which consisted of (10) questions, divided into two axes: questions related to understanding cybersecurity, and questions related to digital violence, which aimed to identify the level of awareness of Cairo University students of the culture of cybersecurity to confront digital violence. The research was applied to a sample of (124) female students from Cairo University in the first university stage from the faculties of (Arts, Commerce, Media, Dar Al-Ulum) as models for theoretical faculties, and from the faculties of (Science, Computers and Artificial Intelligence) as models for practical faculties. In addition to a sample of female students from the Faculty of Graduate Studies for Education at Cairo University as a model for female graduate students.

The research achieved a set of results, the most important of which are:

- A large number of female students from the Faculties of Arts, Commerce, and Dar Al-Ulum agreed on their lack of cybersecurity skills, while female students from the Faculty of Computers and Artificial Intelligence confirmed that they possess most of the cybersecurity skills and know them due to the nature of their studies, while the opinions of female students from the Faculties of Science

and Media and General Diploma students at the College of Graduate Studies for Education agreed on their average knowledge of them.

- It was found that (55.6%) of the female students in the research sample or those they know were exposed to forms of digital violence such as harassment or threats via the Internet; which had negative effects on their psychology and exposed them to depression, isolation, frustration, anxiety, fear, sleep and appetite disorders, and lack of self-confidence, and affected their psychological health, academic level, and academic achievement.

The research reached a proposed vision to enhance the culture of cybersecurity among female students at Cairo University to confront digital violence.

Keywords: Cybersecurity - female university students - digital violence.

مقدمة:

في ظل ما يمر به العصر الحالي من ثورة رقمية وتطور كبير في تقنية المعلومات والاتصالات، وانتشار سريع للإنترنت، وظهور وسائل الإعلام الجديد وشبكات التواصل الاجتماعي المتنوعة، وما وفرته من تسهيل وسرعة في عمليات التواصل والوصول إلى مصادر المعلومات، فإنه قد ينتج عن استخدامها سلوكيات تتباين بين الإيجابية إذا استغلت على الوجه الأمثل، والسلبية إذا تمرد مستخدموها على القواعد والضوابط القانونية التي تنظم شؤون الحياة، والفرق بينهما هو كيفية استخدام الفرد لها. حيث إن استخدام التقنية دون وعي بشكل غير آمن في ظل غياب المسئولية تجاه الآخرين، ومع غياب القوانين والعقوبات الرادعة وانتشار ضعاف النفوس، مما يؤدي إلى التزايد المستمر في نسب الجريمة الإلكترونية، والتي تشكل خطرًا حقيقيًا على المجتمعات وتهدد أفراده (مريم بنت محمد فضل الشهري، ٢٠٢١م، ص٨٤).

فضلا عن ذلك أسهمت التكنولوجيا الحديثة بانتشار نوع جديد من العنف ضد الفتيات والذي عُرف بـ (العنف الرقمي)، ومن أبرز صوره الابتزاز الإلكتروني، والتحرشات الجنسية الإلكترونية، والمراقبة والتجسس على أجهزة الحاسوب والهواتف النقالة واختراقها واستخدام الصور ومقاطع الفيديوهات وتحريفها من أجل استخدامها كوسيلة للتهديد والابتزاز (علي صلاح الحديثي، عامر عاشور عبد الله، م٢٠١٩، ص٢٠٠).

فالعنف الرقمي ضد الفتيات هو فعل من أفعال العنف القائم على النوع الاجتماعي الذي يُرتكب بشكل مباشر أو غير مباشر من خلال تكنولوجيا المعلومات والاتصالات والذي يؤدي أو من المرجح أن يؤدي إلى أذى، أو معاناة جسدية، أو جنسية، أو نفسية، أو اقتصادية للفتيات، بما في ذلك التهديد بمثل هذه الأفعال، سواء حدثت في الحياة العامة أو الخاصة، أو عوائق أمام استخدام حقوقهن وحرياتهن الأساسية. ولا يقتصر العنف الرقمي ضد الفتيات على انتهاكات الخصوصية،

والمطاردة، والمضايقة، وخطاب الكراهية القائم على النوع الاجتماعي، ومشاركة المحتوى الشخصي دون موافقة، والإساءة الجنسية القائمة على الصور، والقرصنة، وسرقة الهوية، والعنف المباشر، بل يشملها أيضًا. فالعنف الرقمي هو جزء من استمرارية العنف ضد المرأة: فهو لا يوجد في فراغ؛ بل إنه ينبع من أشكال متعددة من العنف غير المتصل بالإنترنت ويدعمها في نفس الوقت **(Polyzoidou, V., 2024, P.1784).**

لذلك فمن الضروري توعية الطالبات ومساعدتهن على الاستخدام الآمن للتكنولوجيا في الجامعة، والمنزل على النحو الملائم، وهو ما يُعرف بـ "الأمن السيبراني"، والذي يُسهم في تنمية الوعي والإدراك لديهن، ومساعدتهن ليصبحن مثقفات من الناحية التقنية، وتجاوز مرحلة الوعي المعرفي الأساسية لأجزاء الحاسب الآلي وبرامجه، إلى معرفة الاستخدام الملائم لهذه التقنيات الرقمية، كما يعمل على تنمية مهارات الممارسة الموجهة التي تساعدهن على تمييز وممارسة الاستخدام الآمن؛ بحيث يتم منح الطالبات التعلم في بيئة تشجع على الاكتشاف، كما يقدم التغذية الراجعة والتحليل ومناقشة استخدام التقنيات الرقمية داخل وخارج الجامعة، من خلال الأنشطة التي تشارك فيها الطالبات؛ بحيث يمكن استخدام التقنيات الرقمية بشكل فعال وآمن (محمد إبراهيم عبده السيد، وليد سعيد أحمد سيد، ٢٠٢٢م، ص٣٦١).

وتأسيسا على ما سبق، أطلقت مصر الاستراتيجية الوطنية للأمن السيبراني (٢٠٢٣-٢٠٢٧)، والتي تهدف إلى التصدي للحوادث السيبرانية التي تزايدت من حيث عددها ومصادرها (جمهورية مصر العربية، رئاسة مجلس الوزراء، المجلس الأعلى للأمن السيبراني، ص٣).

وتحقيقًا لأهداف هذه الاستراتيجية سعى البحث الحالي إلى تسليط الضوء على أهم الطرق والوسائل التي يمكن من خلالها تعزيز ثقافة الأمن السيبراني لدى طالبات الجامعة في مصر، والذي يُعد خطوة حيوية لمواجهة التحديات المتعلقة بالعنف الرقمي وحماية الفتيات من المخاطر التي قد يتعرضن لها عبر الإنترنت.

الدراسات والبحوث السابقة

فيما يلي عرضًا لأبرز الدراسات والبحوث السابقة العربية والأجنبية ذات الصلة بموضوع الدراسة، مرتبة وفقًا للتسلسل الزمني من الأقدم إلى الأحدث، والتي تنقسم في محورين:

- الدراسات والبحوث السابقة ذات الصلة بالعنف الرقمي.
- الدراسات والبحوث السابقة المرتبطة بالأمن السيبراني.

أولا: الدراسات والبحوث السابقة ذات الصلة بالعنف الرقمي

(١) دراسة (ريهام السيد عبد الجليل إبراهيم، ٢٠١٧م) بعنوان: **"دور الجامعة في مواجهة مخاطر العنف الإلكتروني عبر شبكات التواصل الاجتماعي- دراسة تحليلية"**

استهدف البحث توضيح دور الجامعة في مواجهة مخاطر العنف الإلكتروني التي يتعرض لها الشباب الجامعي، واستخدمت الباحثة المنهج الوصفي لملاءمته لموضوع البحث، وتوصل البحث إلى عدد من النتائج، منها: ظهر العنف الإلكتروني كنتاج طبيعي للتفاعلات الافتراضية على شبكات التواصل الاجتماعي، وله العديد من المظاهر كالمضايقات، والرسائل المزعجة، والافتضاح الإلكتروني، إلخ، وتتنوع وتتعدد مخاطره إلى مخاطر فردية وجماعية، ومنها مخاطر بدنية ونفسية وثقافية واقتصادية، كما يمكن تفعيل دور الجامعة في مواجهة العنف الإلكتروني عبر شبكات التواصل الاجتماعي من خلال تحقيق بعض المتطلبات الخاصة بأعضاء هيئة التدريس، والإدارة الجامعية، والمقررات الدراسية.

(٢) دراسة **(Hassan, F. M.& et.al. 2020)** بعنوان: **"نمط العنف السيبراني والعوامل المرتبطة به: مسح عبر الإنترنت للإناث في مصر"**

استهدفت تلك الدراسة تقييم مشكلة العنف الرقمي ضد النساء في مصر. واستخدمت الاستبانة كأداة للدراسة، وطبقت على عينة قوامها (٣٥٦) أنثى. وتوصلت نتائج الدراسة إلى:

تعرض حوالي ٤١,٦٪ من المشاركات للعنف الرقمي خلال عام٢٠١٩م، وأفادت ٤٥,٣٪ منهن بأنهن تعرضن للعنف عدة مرات. وكانت وسائل التواصل الاجتماعي هي الطريقة الأكثر شيوعًا للتعرض، وكان الجناة غير معروفين لـ ٩٢,٦٪ من الضحايا. وقد شملت أكثر أشكال العنف شيوعًا ٤١,٢٪ من الضحايا تلقي صور أو رموز ذات محتوى جنسي، و٢٦,٤٪ تلقي رسائل إلكترونية أو رسائل مسيئة، و٢٥,٧٪ تلقي منشورات أو تعليقات مسيئة أو مهينة، و٢١,٦٪ تلقي صور غير لائقة أو عنيفة تحط من قدر المرأة، و٢٠,٣٪ تلقي ملفات مصابة عبر رسائل البريد الإلكتروني. وقد عانت أغلب الضحايا (٧٦,٩٪) من التأثيرات النفسية في شكل الغضب والقلق والخوف؛ و١٣,٦٪ من التأثيرات الاجتماعية؛ و٤,١٪ تعرضوا لأذى جسدي؛ و٢,٠٪ أبلغوا عن خسائر مالية. وكان حظر الجاني هو الاستجابة الأكثر شيوعًا للضحايا. وأوصت الدراسة بضرورة تنفيذ برنامج لمكافحة العنف الرقمي.

(٣) دراسة (Malanga, D. F., 2021) بعنوان: " دراسة مسحية حول العنف الإلكتروني ضد المرأة في ملاوي"

استهدفت تلك الدراسة التحقيق في انتشار العنف الإلكتروني ضد النساء في منطقة كارونجا في ملاوي. واعتمدت الدراسة تصميم المسح الوصفي. وشاركت حوالي ٦٧ امرأة في استبانة المسح. واستخدمت الدراسة إطار العنف القائم على النوع الاجتماعي الميسر بالتكنولوجيا. ولاحظت الدراسة أن النساء تعرضن لأشكال مختلفة من العنف الإلكتروني مثل التنمر الإلكتروني والتحرش الإلكتروني والتشهير عبر الإنترنت والملاحقة الإلكترونية والاستغلال الجنسي وخطاب الكراهية عبر الإنترنت والمواد الإباحية الانتقامية. كما استخدم الجناة منصات رقمية مثل **Facebook** و**WhatsApp** والحسابات الشخصية عبر الإنترنت ومواقع المواعدة والهواتف الذكية لتنفيذ أفعالهم الشريرة. ووجدت الدراسة أيضًا أن دوافع الجناة كانت مدفوعة بالانتقام والغضب والغيرة والرغبة الجنسية والأجندة السياسية، بقصد إيذاء الضحايا اجتماعيًا، ونفسيًا، واقتصاديًا،

وجسديًا. واستخدمت النساء تدابير التكيف مثل المواجهة وحظر الجاني أو مغادرة المنصة الإلكترونية. وقد تبين أن النساء لم يكلفن أنفسهن عناء الإبلاغ عن هذه الحوادث إلى الشرطة أو المجتمع لطلب الدعم بسبب نقص الوعي والعوامل الثقافية والذكورية. وفي الختام، وجدت الدراسة أن انتشار العنف الرقمي ضد النساء آخذ في الارتفاع بشكل كبير في ملاوي. وبالتالي، توفر النتائج رؤى لصناع السياسات وممارسي البحث حول كيفية تنفيذ استراتيجيات لمكافحة العنف الرقمي ضد النساء في البلاد.

(٤) **دراسة** (ممدوح الغريب السيد يونس، ٢٠٢٣م) بعنوان: **"العنف الرقمي القائم على النوع الاجتماعي لدى طالبات الجامعات المصرية: دراسة ميدانية في ضوء نظرية بيير بورديو"**

استهدفت تلك الدراسة تعرف واقع العنف الرقمي القائم على النوع الاجتماعي بين طالبات الجامعات المصرية وفق نظرية العنف لبيير بورديو، وتقديم عدة آليات مقترحة يمكن من خلالها مواجهة تلك الظاهرة قبل انتشارها في المجتمع المصري، واستخدمت الدراسة المنهج الوصفي مستعينة بأحد أدواته وهي الاستبانة والتي طبقت على (٧١٢) طالبة من طالبات الجامعات المصرية الحكومية في قطاعات جامعات العاصمة وشمال مصر والدلتا والصعيد، وتوصلت الدراسة إلى أن حجم العنف والإيذاء الرقمي ضد الطالبات بالجامعات المصرية كان متوسطًا من خلال أبعاد نظرية بيير بورديو للعنف، وبخاصة بُعد الإنكار القيمي، وبُعد الاستلاب النفسي، كما توصلت الدراسة إلى وجود فروق ذات دلالة إحصائية لمتغير (الإقامة) للطالبات القاطنات بالمدن طبقًا لبُعد التعبير العدائي المعلن، كما كانت هناك فروق ذات دلالة إحصائية طبقًا لمتغير (الجامعة) للطالبات في جامعات القاهرة عن غيرهن، وكذلك وجود فروق ذات دلالة إحصائية طبقًا لمتغير (المستوى الاقتصادي للأسرة) وذلك للطالبات من الأسر ذات الدخل المنخفض، وتوصلت الدراسة إلى وضع تصور مقترح لمجابهة ظاهرة العنف الرقمي القائم على النوع الاجتماعي بين طالبات الجامعات المصرية.

(٥) دراسة (Mahdi, A. M., & Sheriji, I. L., 2024) بعنوان: **"أسباب وأشكال العنف الافتراضي ضد المرأة"**

استهدف البحث الحالي تعرف أسباب العنف الافتراضي الذي تتعرض له الطالبة الجامعية، وأشكاله. وبناءً على ذلك تكونت العينة من (١٠٠) طالبة جامعية تم توجيههن إلى استبانة استطلاعية مفتوحة حول أسباب العنف الافتراضي الذي يتعرضن له وأشكاله الشائعة، وقد أظهرت النتائج أن أكثر أسباب العنف الرقمي شيوعاً هي: ضعف الرقابة الأسرية والتي جاءت بنسبة ٩٨٪، وأقلها شيوعاً الحاجة إلى الحب بين الفتيات بنسبة ٣٠٪، في حين ظهر أن أكثر أنواع العنف الرقمي شيوعاً هو الابتزاز الإلكتروني. وقدمت الدراسة عددًا من التوصيات للحد من العنف الرقمي، منها: إنشاء وإيجاد مراكز متخصصة في الإرشاد النفسي ترعى ضحايا الجرائم الإلكترونية بشكل عام والنساء بشكل خاص، للحد من حالات الانتحار والهروب من المنزل. وكذلك نشر الوعي بين الأسر العراقية من خلال إقامة ندوات توعوية في وسائل الإعلام تشرح خطورة العنف الرقمي، وأن المرأة يجب أن تكون أكثر حرصًا على الحفاظ على خصوصيتها ومعلوماتها الشخصية. وتعزيز قدرات أفراد الشرطة لمواجهة العنف الرقمي.

ثانيًا: الدراسات والبحوث السابقة المرتبطة بالأمن السيبراني

(١) دراسة (رشا عبد القادر محمد الهندي، ٢٠٢١م) بعنوان: **"تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول"**

استهدف البحث تعرف دور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول، واعتمد البحث على المنهج الوصفي، وتكونت الاستبانة من (٢٥) فقرة، وتم تطبيقها على عينة من طلاب الدراسات العليا (الماجستير- الدكتوراه) بكلية الدراسات العليا للتربية جامعة القاهرة مكونة من (٩٣) طالبًا تم اختيارهم بطريقة عشوائية بنسبة

(٢٣,٣٦٪) من المجتمع الأصلي للطلاب البالغ عددهم (٣٩٨) طالبًا في العام الجامعي ٢٠٢٠/ ٢٠٢١م، وتوصلت نتائج البحث إلى: أن درجة وعي أفراد العينة بمفهوم الأمن السيبراني، وطرق المحافظة عليه جاءا بمستوى عام متوسط. وتوصل البحث إلى تقديم تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول.

(٢) دراسة (مريم بنت محمد فضل الشهري، ٢٠٢١م) بعنوان: **"دور إدارة الجامعة في تعزيز الوعي بالأمن السيبراني لدى طلبة كلية التربية بجامعة الإمام محمد بن سعود الإسلامية"**

استهدفت تلك الدراسة تعرف دور إدارة الجامعة في تعزيز الوعي بالأمن السيبراني لدى طلبة كلية التربية بجامعة الإمام محمد بن سعود الإسلامية، والكشف عن درجة معرفة طلبة كلية التربية في جامعة الإمام محمد بن سعود الإسلامية بالأمن السيبراني، وقد استخدمت الدراسة المنهج الوصفي المسحي، وذلك من خلال توزيع استبانة على عينة من طلبة كلية التربية مكونة من (١٨٨) طالبا وطالبة، وأشارت نتائج الدراسة إلى أن معرفة طلبة كلية التربية في جامعة الإمام محمد بن سعود الإسلامية بالأمن السيبراني جاءت بدرجة متوسطة، وأن ممارسة إدارة الجامعة لدورها في تعزيز الوعي بالأمن السيبراني لدى هؤلاء الطلبة جاءت بدرجة متوسطة، كما قدمت الدراسة مجموعة من التوصيات؛ من أبرزها: دعم وتبني إدارة الجامعة لبرامج وحملات لتوعية طلابها بالأمن السيبراني، ومخاطر الجرائم الإلكترونية، والتساهل في حفظ المعلومات المهمة، وضرورة التنسيق بين إدارة الجامعة والجهات المشرفة على الأمن السيبراني؛ كالهيئة الوطنية للأمن السيبراني؛ لاتخاذ الإجراءات اللازمة لتنمية الوعي لدى طلبة الجامعة في مجال الأمن السيبراني. بالإضافة إلى إقامة ورش عمل ودورات تدريبية لطلبة الجامعة، واستضافة المختصين البارزين في التقنية؛ لنشر ثقافة الأمن السيبراني والاستخدام الأمثل للتقنية، بما يضمن الوقاية والحماية من المخاطر في العالم الرقمي.

(٣) دراسة (محمد إبراهيم عبده السيد، وليد سعيد أحمد سيد، ٢٠٢٢م) بعنوان: **"قيم تعزيز الأمن الرقمي لدى طلاب الجامعات في مصر لمواجهة تحديات الثورة الرقمية"**

استهدف ذلك البحث الوقوف على درجة توفر قيم تعزيز الأمن الرقمي لدى طلاب الجامعات في مصر، لمواجهة مخاطر وتحديات الثورة الرقمية؛ وذلك من خلال إطار مفاهيمي، يعكس ماهية الأمن الرقمي، ويبرز أهم تحديات الثورة الرقمية وانعكاساتها على طلاب الجامعة، واستخدم البحث المنهج الوصفي، واعتمد على الاستبانة كأداة لجمع البيانات، حيث تضمنت خمسة محاور رئيسة هي: حرية الرأي والتعبير الرقمي، والرقابة الذاتية، واحترام الخصوصية الرقمية، واحترام حقوق الملكية الفكرية الرقمية، والحماية من المخاطر والتهديدات الرقمية؛ وطبقت الاستبانة على عينة بلغت (١٠٣٦) طالبًا وطالبة بالجامعات الحكومية المصرية للوقوف على درجة توفر قيم تعزيز الأمن الرقمي لديهم، وتوصلت نتائج البحث إلى أن قيم تعزيز الأمن الرقمي لدى طلاب الجامعة متوفرة بدرجة متوسطة، حيث بلغت نسبة الاستجابة على الاستبانة مجملة (٤٩ , ٦٣٪)؛ كما توصلت النتائج إلى وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة تبعًا لمتغير النوع (ذكور- إناث)، لصالح الإناث؛ وتبعًا لمتغير الجامعة(أزهر- عام) لصالح الأزهر، وتبعًا لمتغير التخصص(نظري- عملي) لصالح العملي، وتبعًا لمتغير محل الإقامة(ريف- حضر) لصالح الحضر؛ وأوصى البحث بضرورة تنمية قيم تعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة تحديات الثورة الرقمية من خلال بعض الآليات الإجرائية المقترحة.

(٤) دراسة **(Mohammed, M., & Bamasoud, D. M., 2022)** بعنوان: **"تأثير تعزيز الوعي بالأمن السيبراني على طلاب الجامعات: دراسة مسحية"**

استهدفت تلك الدراسة تعرف مستوى وعي طلاب الجامعات السعودية بالأمن السيبراني، وتم تصميم استبانة شارك فيها ١٣٦ طالبًا وطالبة، لقياس وعي الطلاب من خلال ثقافتهم وبيئتهم المحيطة ومعرفتهم، بالإضافة إلى سلوك الطلاب. وأشارت النتائج إلى مستوى متوسط من الوعي

بالأمن السيبراني بين الطلاب وأن الأمن السيبراني يحظى باهتمام أكبر بين الطالبات. بالإضافة إلى ذلك، كان لدى طلاب الحاسبات وتقنية المعلومات وعي أعلى مقارنة بالطلاب في الأقسام الأخرى. وأكد الباحثان على أهمية توفير الوعي بالأمن السيبراني لطلاب الجامعات وأنهم يجب أن يكونوا على دراية بالتهديدات المحتملة أثناء استخدام الإنترنت. وأوصت الدراسة بضرورة توفير الوعي بالأمن السيبراني بين طلاب الجامعات، من خلال إنشاء موقع ويب يحتوي على السياسات والممارسات الصحيحة للموضوعات التي يكون الطلاب عُرضة للانتحال من خلالها.

(٥) دراسة (بدر عدنان أحمد سعد محمد الخبيزي، ٢٠٢٣م) بعنوان: **"تحديات وتهديدات الأمن السيبراني وكيفية التغلب عليها"**

استهدف البحث رصد بعض التحديات والتهديدات التي تواجه الأمن السيبراني في الوقت الحالي، وتقديم مجموعة من الإجراءات والتوصيات لكيفية التغلب على هذه التحديات والتهديدات أو التخفيف من حدتها أو تقليل عددها. وهذا تطلب إلقاء الضوء على ماهية الأمن السيبراني وذلك من حيث: التعريف والأهداف والأهمية. وكنوع من التمهيد لكل ذلك تم تعريف مفهوم الأمن وتوضيح أهميته وتحديد أنواعه. أيضا تم تعريف الجريمة السيبرانية وتحديد بعض خصائصها ووسائلها. والبحث يعتبر من البحوث النظرية المكتبية ومن نمط البحوث الوصفية الكيفية. ومن أهم نتائج البحث رصد بعض التحديات والتهديدات التي تواجه الأمن السيبراني في الوقت الحالي، وتقديم مجموعة من الإجراءات والتوصيات لكيفية التغلب عليها.

(٦) دراسة (أسماء مراد صالح، ٢٠٢٤م) بعنوان: **"تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية (تصور مقترح)"**

استهدفت تلك الدراسة الوقوف على الإطار المفاهيمي للتربية الإعلامية الرقمية بالجامعات، وتحديد أهم كفايات التربية الإعلامية الرقمية اللازمة لطلاب الجامعات لتنمية ثقافة

الأمن السيبراني، والكشف عن الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية، وأساليب تنميتها. ووضع تصور مقترح لتنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية. واتبعت الدراسة المنهج الوصفي، واستخدمت الاستبانة كأداة لجمع البيانات. وتكونت عينة الدراسة من (٣٤٧) طالبًا من كليات (التربية، التجارة وإدارة الأعمال، السياحة والفنادق) بجامعة حلوان، وتوصلت الدراسة إلى عدة نتائج من أهمها:

- ضعف تركيز اللوائح والقوانين الجامعية على قضايا وممارسات الأمن السيبراني بالجامعات، مما يعرض الأنظمة والشبكات الجامعية لخطر الاختراق والهجمات السيبرانية.
- نقص المتخصصين في مجال الأمن السيبراني في الجامعات، مما يصعب تنفيذ استراتيجيات الأمن السيبراني بشكل فعال.
- ضعف وعي الطلاب بكيفية استخدام شبكات الإنترنت العامة بشكل آمن ومشفر لحماية بياناتهم الحساسة من الاختراق والسرقة، مما يعرضهم لخطر سرقة الهوية الرقمية واختراق حسابات البريد الإلكتروني والشبكات الاجتماعية والاحتيال الإلكتروني.
- نقص البرامج التعليمية والتدريبية المتخصصة في مجال الأمن السيبراني، مما يؤثر سلبًا على قدرة الطلاب على اكتساب المهارات والممارسات الآمنة في استخدام التكنولوجيا الرقمية.
- ضعف وعي الطلاب بأهمية استخدام كلمات مرور قوية وتغييرها بشكل منتظم لتأمين حساباتهم الشخصية والبيانات الحساسة من التهديدات السيبرانية والاختراقات.
- إغفال بعض الطلاب إجراءات تحديث البرامج والتطبيقات الضرورية لمعالجة الثغرات الأمنية، مما يجعلهم عرضة للهجمات الإلكترونية التي تستهدف النسخ غير المحدثة.

التعقيب على الدراسات والبحوث السابقة

يتضح من العرض السابق للدراسات والبحوث السابقة العربية والأجنبية ذات الصلة بموضوع الدراسة، ما يلي:

- تركز الدراسة الحالية على تعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة باعتباره يمثل حجر الزاوية في مواجهة العنف الرقمي، إذ إن تعزيز الحماية الرقمية، وتعليم الطالبات سبل الوقاية من المخاطر الإلكترونية، يمكن أن يقلل بشكل كبير من التعرض لأشكال مختلفة من العنف الرقمي.
- تتشابه الدراسة الحالية مع الدراسات السابقة المرتبطة بالعنف الرقمي في تناولها لقضية العنف الرقمي ضد الفتيات وطلاب الجامعة، وكذلك تركيزها على تعزيز الأمن السيبراني لدى طلاب الجامعة، وتأكيدها على أهمية تفعيل دور الجامعة في مواجهة العنف الرقمي.
- تختلف الدراسة الحالية عن الدراسات السابقة في إتباعها لمنهج "دراسة الحالة" مستخدمة المقابلة كأداة للدراسة، بينما اتبعت الدراسات السابقة "المنهج الوصفي" واستخدمت الاستبانة كأداة للدراسة.

مشكلة البحث وأسئلته

في ظل التطور التكنولوجي السريع وانتشار الإنترنت، أصبح العالم الرقمي جزءًا أساسيًا من حياة الأفراد، خاصة طالبات الجامعة اللواتي يعتمدن بشكل كبير على الشبكات الرقمية في دراستهن وتواصلهن الاجتماعي. وعلى الرغم من الفوائد العديدة التي توفرها هذه التقنيات، إلا أنها في الوقت ذاته تخلق بيئة خصبة لظهور ظاهرة العنف الرقمي، الذي يشمل التحرش الإلكتروني، التنمر، والتهديدات الرقمية، مما يعرض العديد من الطالبات لمخاطر قد تؤثر على حياتهن الأكاديمية والنفسية.

ووفقًا لبعض الدراسات، تتعرض النساء للعنف الرقمي أكثر من الرجال. ومع ذلك، هناك أيضًا دراسات تشير إلى أن النساء أكثر عرضة لارتكاب العنف الرقمي. وتم التركيز على طالبات الجامعة لأنهن محاطات بالتكنولوجيا ويجب أن يتفاعلن معها بشكل يومي تقريبًا، وبالتالي هن أكثر عرضة لخطر التعرض للإيذاء والعنف من خلال الوسائط التكنولوجية المختلفة ذاتها التي ينبغي أن تسهل تعليمهن. ولذلك تعتقد الفتيات أن سمعتهن تتضرر بسبب مثل هذا العنف الرقمي، مما يؤثر على علاقاتهن مع الأصدقاء، وبشكل عام يتعرضن للعديد من العواقب السلبية؛ كالتأثير السلبي على الأداء الأكاديمي، بما في ذلك انخفاض التركيز، والعزلة، وانخفاض التحصيل الأكاديمي. ويرتبط التهديد أيضًا بنشر وسائط وصور خاصة للضحايا باحتمالات أعلى للأفكار الانتحارية. كذلك له عواقب سلبية على الصحة النفسية والاجتماعية والجسدية لهن (زيد نجم عبد الله العبادي، ٢٠٢٤م، ص٧٢).

وتتمثل مشكلة البحث الحالي في نقص الوعي الكافي لدى العديد من طلاب وطالبات الجامعة بثقافة الأمن السيبراني كأداة مهمة لحماية أنفسهم من مخاطر وتهديدات العنف الرقمي، وهذا ما أكدت عليه العديد من الدراسات السابقة ومنها دراسة (رشا عبد القادر محمد الهندي، ٢٠٢١م) والتي توصلت إلى أن مستوى وعي الطلاب والطالبات بمفهوم الأمن السيبراني، وطرق المحافظة عليه جاءا بمستوى عام متوسط، وكذلك دراسة (أسماء مراد صالح، ٢٠٢٤م) والتي توصلت إلى ضعف وعي طلاب وطالبات الجامعة بثقافة الأمن السيبراني.

فبينما يتزايد استخدام التكنولوجيا في الحياة اليومية، تفتقر الكثير من الطالبات إلى المعرفة والمهارات اللازمة لتأمين بياناتهن الشخصية وحمايتها من الهجمات الإلكترونية.

وبناءً عليه يسعى البحث الحالي إلى الإجابة عن السؤال الرئيس الآتي:

كيف يمكن تعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي؟

ويتفرع من السؤال الرئيس الأسئلة الآتية:

- ما الإطار الفكري للعنف الرقمي؟
- ما الإطار المفاهيمي للأمن السيبراني؟
- ما أبرز جهود جامعة القاهرة في مواجهة العنف الرقمي ضد الطالبات؟
- ما مستوى وعي طالبات جامعة القاهرة بثقافة الأمن السيبراني لمواجهة العنف الرقمي؟
- ما التصور المقترح لتعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي؟

أهداف البحث

تتمثل أهداف البحث الحالي في الآتي:

- تعرف الإطار الفكري للعنف الرقمي.
- تعرف الإطار المفاهيمي للأمن السيبراني.
- الاطلاع على أبرز جهود جامعة القاهرة في مواجهة العنف الرقمي ضد الطالبات.
- تعرف مستوى وعي طالبات جامعة القاهرة بثقافة الأمن السيبراني لمواجهة العنف الرقمي.
- وضع تصور مقترح لتعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي.

أهمية البحث

تتمثل أهمية البحث الحالي في الآتي:

- اهتمامه بشريحة مهمة ومؤثرة في المجتمع وهن طالبات الجامعة، والتي تُسهم في تشكيل حاضره ومستقبله، كما أنهم أكثر عرضة للعنف الرقمي من الذكور، وضرورة توعيتهن بكيفية مواجهته وحماية أنفسهن من مخاطره.
- يعزز هذا البحث أهمية نشر ثقافة الأمن السيبراني بين الطالبات، مما يمكنهن من التعامل بشكل أكثر أمانًا مع التقنيات الحديثة ويحسن من قدرتهن على مواجهة التهديدات الرقمية.

- تفعيل دور الجامعة في تعزيز ثقافة الأمن السيبراني لدى طالباتها.
- يسهم البحث في وضع تصور مقترح لتعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي.

منهج البحث وأداته

تعتمد إجراءات البحث الحالي على استخدام "منهج دراسة الحالة"، والذي يُعرف بأنه "دراسة حالة فرد أو جماعة أو مؤسسة ما، عن طريق جمع المعلومات والبيانات عن الوضع الحالي للحالة، ومعرفة الأوضاع التي أثرت عليها، لفهم الحالة وتفسيرها بشكل صحيح" (عبد الغني محمد إسماعيل العمراني، ٢٠١٣م، ص١٣٦). وتطبيقًا لهذا المنهج بالبحث الحالي تم تحديد الحالة ممثلة في طالبات جامعة القاهرة، وتعزيز ثقافة الأمن السيبراني لديهن حتى يتمكن من مواجهة العنف الرقمي، ومن ثم تم جمع البيانات والمعلومات باستخدام أداة **"المقابلة"**، والتي هدفت لتعرف مستوى وعي طالبات جامعة القاهرة بثقافة الأمن السيبراني لمواجهة العنف الرقمي.

حدود البحث

تتمثل حدود البحث الحالي في:

١. **الحد الموضوعي**: يتمثل في تعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي.
٢. **الحد البشري**: تمثل في عينة من طالبات جامعة القاهرة قوامها (١٢٤) طالبة.
٣. **الحد المكاني**: اقتصر البحث الحالي على عينة من طالبات جامعة القاهرة بالمرحلة الجامعية الأولى من كليات (الآداب، التجارة، الإعلام، دار العلوم) كنماذج للكليات النظرية، ومن كليات (العلوم، والحاسبات والذكاء الاصطناعي) كنماذج للكليات العملية. بالإضافة إلى

عينة من طالبات كلية الدراسات العليا للتربية بجامعة القاهرة كنموذج لطالبات الدراسات العليا.

٤. **الحد الزماني**: تم تطبيق الدراسة الميدانية في الفصل الدراسي الأول من العام الجامعي ٢٠٢٤/ ٢٠٢٥م.

مصطلحات البحث

تحددت المصطلحات المرتبطة بالبحث الحالي في الآتي:

١. **الأمن السيبراني:**

هو جميع إجراءات حماية شبكات المعلومات ضد كافة الأعمال والممارسات التي تستهدف التلاعب بتلك المعلومات وإلحاق الأذى بالمستخدمين، بما يشمل الحماية ضد الاختراق، وبث البرمجيات الخبيثة والفيروسات، والوصول غير المصرح به، وغير ذلك من ممارسات سلبية (شريفة محمد السويدي، زيزيت مصطفى نوفل، ٢٠٢٣م، ص٤٢٨).

ويعرف الأمن السيبراني إجرائيًا بأنه: "مجموعة من الأنشطة الموجهة نحو توفير بيئة آمنة لطالبات الجامعة، من خلال حماية المعلومات الشخصية والعلمية عبر الإنترنت، باستخدام تقنيات الحماية الحديثة وتوعية الطالبات بكيفية تجنب المخاطر والتهديدات السيبرانية".

٢. **العنف الرقمي:**

هو العنف المتصل بالتقنية، وهو جزء من العنف الموجه ضد المرأة في الواقع، ويتضمن مجموعة من الأفعال العنيفة القائمة على النوع الاجتماعي والتي ترتكب أو تحرض أو تتفاقم باستخدام تكنولوجيا المعلومات والاتصالات كالهاتف والإنترنت ومنصات التواصل الاجتماعي، ويشمل هذا النوع التتبع الإلكتروني، التحرش الإلكتروني، خطاب الكراهية (يوسف بلعباس، ٢٠٢٣م، ص٤١).

ويعرف العنف الرقمي إجرائيًا بأنه: "أي شكل من أشكال الإيذاء النفسي أو الاجتماعي الذي يُمارس ضد طالبات الجامعة عبر الإنترنت باستخدام الوسائل الرقمية، سواء من خلال التهديدات أو المضايقات أو التشويه المتعمد للمعلومات الشخصية، مما يتطلب تدابير وقائية وتوعوية لحماية الطالبات من هذه الممارسات".

إجراءات البحث

تمثلت إجراءات البحث الحالي فيما يلي:

الجزء الأول: الإطار النظري للبحث.

الجزء الثاني: الجانب الميداني للبحث.

الجزء الثالث: تصور مقترح لتعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي.

الجزء الأول: الإطار النظري للبحث

يسير وفقًا لمحورين هما: الإطار الفكري للعنف الرقمي، والإطار المفاهيمي للأمن السيبراني، وأبرز جهود جامعة القاهرة في مواجهة العنف الرقمي ضد الطالبات.

المحور الأول: الإطار الفكري للعنف الرقمي

يتعرض كل من النساء والرجال لحوادث العنف والإساءة بين الأشخاص (بما في ذلك عبر الإنترنت)، ويمكن أن يكون الرجال ضحايا أيضًا، ويمكن أن تكون النساء مرتكبات. ومع ذلك، تُظهر الأدلة على المستويات الأوروبية والدولية والوطنية أن النساء والفتيات معرضات بشدة للعنف الرقمي ويتأثرن بشكل خاص بهذه الظاهرة، وأكثر عرضة لتجربة أشكال متكررة وشديدة من الإساءة الجسدية أو النفسية أو العاطفية والمعاناة من عواقب وخيمة. ويشمل العنف الرقمي ضد طالبات الجامعة مجموعة من أشكال العنف المختلفة التي تُرتكب باستخدام وسائل تكنولوجيا

المعلومات والاتصالات. ففي الواقع، هناك مجموعة كبيرة ومتنوعة من السلوكيات الإجرامية التي تتضمن العنف الرقمي ضد الفتيات، وحتى أشكالًا أكثر من العنف الرقمي (مثل انتحال الهوية وسرقة الهوية والتشهير والسخرية والتصيد والعار الجسدي)، أو اعتُبرت "عامة للغاية (مثل التهديدات عبر الإنترنت) أو محددة للغاية (مثل انتحال الهوية) أو تندرج تحت الأحكام العامة بشأن أشكال أخرى من العنف، مثل التحرش الإلكتروني". فالعنف الرقمي ضد الفتيات هو بلا شك بُعد جديد وأعظم من أبعاد العنف القائم على النوع الاجتماعي **(Polyzoidou, V., 2024, P.1784)** .

ونظرًا لخطورة هذه الظاهرة وتأثيرها السلبي على الجوانب الأكاديمية والنفسية والصحية لطالبات الجامعة، فسيتم تناولها بالتفصيل فيما يلي:

(أ) مفهوم العنف الرقمي

يُعرف العنف بأنه شكل محدد من أشكال العلاقات التي يرتبط استخدامها بـ "استخدام القوة"، و"إلحاق الضرر الجسدي والروحي والممتلكات"، و"انتهاك مصالح الفرد وحقوقه"، و"قمع الإرادة الحرة" **(Bjelajac, Ž., & Filipović, M.A., 2021, P.18).**

أما العنف الرقمي فهو شكل من أشكال العنف الذي يتم تنفيذه باستخدام أدوات افتراضية.**(Özsungur, F. 2021, P.663)**

حيث يرتبط العنف الرقمي باستخدام مختلف الوسائل التكنولوجية كالإنترنت والهاتف والتسجيلات الصوتية، وتجاوز الخصوصيات وغيرها، ويشترط في هذا السلوك حدوث التكرار بشكل متعمد، ويتخذ عدة أشكال من بينها المضايقات والتحقير والإهانة والتهديد، لكن ما يميزه عن البقية هو التخفي أي أنه يتخذ هوية مجهولة، ويمتد من فرد يقوم بهذا السلوك إلى جماعة، وقد يقوم به شخص لتخويف نظيره في نفس البيئة والمجتمع، وفي هذه الحالة يتعسر، بل يصعب على الضحايا مواجهة المعنف أو المتنمر فلا يمكنهم الدفاع عن أنفسهم (يوسف بلعباس، ٢٠٢٣م، ص٤١).

ويطلق على العنف الرقمي عدة تسميات منها: العنف التقني والإلكتروني، العنف الرقمي عبر الإنترنت، الاستقواء الإلكتروني، التنمر الإلكتروني. وتكمن خطورة العنف الرقمي في أنه يستخدم فضاءًا واسعًا جدًا هو فضاء الإنترنت، من الصعب التحكم فيما ينشر وخاصة إذا كان الأمر يتعلق بالفتاة، وفي المجتمعات العربية التي لديها منظومة من القيم والأعراف التي لا يسمح بتجاوزها أو اختراقها. فالعنف الرقمي أكثر خطورة من العنف التقليدي بسبب ثلاثة عوامل متمثلة في صعوبة الابتعاد عنه، اتساع الجمهور المحتمل، وعدم مرئية أولئك الذين يقومون بالعنف (فاطمة الزهرة قمقاني، ٢٠٢٣م، ص٦٨).

كما يُعرف العنف الرقمي ضد الفتيات بأنه عنف قائم على النوع الاجتماعي يُرتكب من خلال الاتصالات الإلكترونية والإنترنت. ورغم أن العنف الرقمي قد يؤثر على كل من النساء والرجال، فإن الفتيات يتعرضن لأشكال مختلفة وأكثر صدمة من العنف الرقمي. فهناك أشكال مختلفة من العنف الرقمي الممارس ضدهن، بما في ذلك، على سبيل المثال لا الحصر، الملاحقة الإلكترونية، والشتائم القائمة على النوع الاجتماعي، وخطاب الكراهية والتحرش، و"التشهير بهن، والمواد الإباحية غير المرغوب فيها، و"الابتزاز والتحرش والتهديدات والاستغلال والإذلال والإكراه أو التمييز ضدهن **(European Union's Rights, Equality and Citizenship Programme (2014–2020), P.39).**

(ب) خصائص العنف الرقمي

يتميز العنف الرقمي بالعديد من الخصائص، منها ما يلي (حسين حسين زيدان، هديل علي قاسم، ٢٠٢٣م، ص ص٨٣-٨٤):

- لا يحتاج إلى استعمال القوة والضرب باليد؛ بل يحتاج إلى وجود حاسوب وهاتف متصل بالإنترنت يستعمل به الشخص ألفاظ تمس الطرف المقابل متمثلًا بالقذف والسب والشتم والترويج له.

- يُعد العنف الرقمي جريمة متعدية الحدود ومنتشرة في جميع جوانب الحياة وغير خاضعة لنطاق قانوني.
- صعوبة معرفة الأشخاص الذين يمارسون العنف نتيجة لنقص الخبرة لدى الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من العنف.
- يُسهم العنف الرقمي في قيام بعض الأشخاص باختراق المواقع الرسمية أو الشخصية أو الاستيلاء عليها من أجل الحصول على الأموال.
- إن مرتكبي العنف يكونون في العادة من ذوي الاختصاص في مجال الإنترنت أو على الأقل الأشخاص الذين لديهم معرفة قليلة في التعامل مع الحاسوب وشبكات الاتصال.

كما يمكن إيجاز الخصائص التي يتميز بها العنف الرقمي في الآتي(Kaphle, P., 2019, P.89):

- **عدم الكشف عن الهوية**: يمكن أن يظل الشخص المسيء غير معروف للضحية/ الناجية.
- **العمل عن بعد**: يمكن القيام بالإساءة دون اتصال جسدي ومن أي مكان.
- **الأتمتة**: تتطلب الإجراءات المسيئة باستخدام التقنيات وقتًا وجهدًا أقل.
- **إمكانية الوصول**: إن تنوع العديد من التقنيات وبأسعار معقولة يجعلها في متناول الجناة بسهولة.

(ج) أسباب ودوافع العنف الرقمي

تتعدد أسباب ودوافع العنف الرقمي، وتتمثل في دوافع ذاتية وأخرى خارجية، وهي على النحو التالي (كوكب الزمان بليردوح، وآخران، ٢٠٢٢م، ص ص٣٩٤-٣٩٥):

❖ **الدوافع الذاتية:**

- ✓ في بعض الأحيان العنف وسيلة لإثبات الذات من خلال الإحساس بالقلق الناتج عن وجود بعض الرغبات والحاجات غير مشبعة.

- ✓ أحيانًا العنف ناتج عن اضطراب في شخصية الجاني، فإما أن تكون شخصية سيكوباتية، أو شخصية مدمنة على المخدرات، أو بسبب مرض عقلي أو آخر.
- ✓ غياب معايير عامة لضبط السلوك، وبالتالي انخفاض قيمة احترام الآخر، بسبب ظروف اكتسبها الجاني من التنشئة الأسرية، أو المحيط المدرسي أو الاجتماعي.
- ✓ في بعض الحالات تكون الظروف الاجتماعية المزرية ونمط الحياة المتدني، كالفقر والبطالة، تدفع الآخر إما أن يكون منتقمًا أو ظالمًا لما يحيط من حوله.

❖ **الدوافع الخارجية:**

- ✓ غياب الرقابة في ظل القوانين التي تنظم الفضاء الرقمي.
- ✓ طريقة التعامل بين الإنسان والآلة، ومنها إمكانية إنشاء حسابات وهمية بأسماء مستعارة من أجل التطفل ومضايقة الآخرين، دون القدرة على التعرف إلى هويتهم الحقيقية، وبالتالي لن تطالهم أي عقوبات.

(د) الأساليب المستخدمة في العنف الرقمي

تتنوع الأساليب المستخدمة في العنف الرقمي، ومنها على سبيل المثال (ممدوح الغريب السيد يونس، ٢٠٢٣م، ص٣٤٢):

- ✓ الرسائل الهجومية أو المضايقات عبر الهواتف المحمولة.
- ✓ نشر الشائعات أو التسجيلات المتضمنة مضايقات للفتيات عبر شبكات التواصل الاجتماعي.
- ✓ نشر الصور أو مقاطع الفيديو الخاصة بالضحية.
- ✓ سرقة الهوية الافتراضية للضحية.
- ✓ العمل على الاستيلاء على معلومات البريد الإلكتروني، وذلك من خلال رسائل تهديد أو فتح الروابط التي يرسلها الجاني إلى الضحية والقيام بسرقة البريد الإلكتروني.

- ✓ الرسائل النصية والتي تحمل بداخلها عبارات تهديد للفتيات والتي عانين منها كشكل من أشكال السيطرة من الذكور.

(هـ) أهداف العنف الرقمي

يسعى العنف الرقمي إلى تحقيق مجموعة من الأهداف، من أبرزها (حسين حسين زيدان، هديل علي قاسم ٢٠٢٣م، ص٨٤):

- ✓ نشر القلق الاجتماعي والنفسي بين الأفراد الذين يمارسون الإنترنت وشبكات التواصل.
- ✓ تعرض سلامة الأسرة والمجتمع وأمنه للخطر والانتقام من الخصوم.
- ✓ الدعاية والإعلان وجذب الانتباه وإثارة الرأي العام وجمع الأموال والاستيلاء عليها.
- ✓ الإخلال بالنظام العام لشبكات الإنترنت مما قد يؤدي إلى ممارسة العنف ضد الأفراد.
- ✓ التشهير وتشويه السمعة لدى بعض الأفراد المعرضون للخطر.

(و) أشكال العنف الرقمي

على الرغم من أن العنف الرقمي يمكن أن يؤثر على كل من الرجال والنساء، إلا أن النساء يتعرضن لأشكال مختلفة وأكثر صدمة من العنف الرقمي. وتقدم الأدبيات أشكالًا مختلفة من العنف الرقمي ضد المرأة مثل المطاردة الإلكترونية، والتحرش الإلكتروني، والتنمر الإلكتروني، والتحرش الجنسي عبر الإنترنت، والمواد الإباحية غير التوافقية، وما إلى ذلك. كما تشير لجنة الأمم المتحدة الواسعة النطاق (٢٠١٥) إلى أن النساء اللاتي تتراوح أعمارهن بين ١٨ و٢٤ عامًا تعرضن لبعض أشكال العنف الرقمي في حياتهن، ويعانين بشكل غير متناسب من التنمر الإلكتروني، والتحرش الإلكتروني، والمطاردة الإلكترونية، والتحرش الجنسي عبر الإنترنت، وما إلى ذلك **(Malanga, D. F., 2021, P.624)**

وتتعدد أشكال العنف الرقمي، والتي أجملها كل من (كوكب الزمان بليردوح، وآخران، ٢٠٢٢م، ص٣٩٣)، و **(Karanac, R. & et.al. 2016, P.319)** في الآتي:

- اختراق البريد الإلكتروني لشخص ما، أو السطو على حسابه في موقع ما، ثم إرسال رسائل بذيئة أو صور غير مقبولة إلى الأشخاص المضافين في قائمة الاتصال لديه.
- اختراق موقع يملكه شخص ما وترك رسائل غير مقبولة أو عنيفة لديه.
- نشر رقم هاتف الجوال لشخص ما على شبكة الإنترنت مع رسائل إيحائية، يكون بعدها صاحب هذا الرقم عرضة لرسائل بذيئة من مستخدمي شبكة الإنترنت.
- نشر صور إما حقيقية أو تم التعديل عليها بغرض إلحاق الضرر والحرج لصاحبها.
- إفشاء خصوصيات شخص ما ومناقشتها على شبكات التواصل الاجتماعي، أو إنشاء مجموعات عدائية ضده، أو نشر الشائعات والأكاذيب حوله.
- إرسال برمجيات ضارة (فيروسات) بواسطة البريد الإلكتروني بغرض تدمير البيانات الموجودة في حاسوب الضحية.
- سرقة معلومات مهمة على سبيل المثال: مشروع مهم أو بحث حان موعد تسليمه لجهة ما ثم حذفه نهائيًا من حاسوب الضحية.
- انتشار مقاطع وألعاب عنف وإطلاق النار المتوافرة عبر الأجهزة الذكية.
- انتشار المعلومات المنفلتة التي من شأنها تأجيج النزاعات وخلخلة التماسك والروابط الاجتماعية.
- إرسال رسائل نصية قصيرة تحتوي على محتوى مهين وتهديدي/ إهانات، وتهديدات، ونكات سيئة وما إلى ذلك.
- الإزعاج من خلال المكالمات الهاتفية/ التعريف بالنفس بشكل زائف، والصمت، والإهانة وما إلى ذلك.
- التقاط الصور باستخدام الهاتف المحمول أو الكاميرا، ونقل الصور ووضعها على الإنترنت.

- رسائل البريد الإلكتروني المزعجة/ الإهانات، والتهديدات، والنكات غير اللائقة وما إلى ذلك.
- الإزعاج على شبكات التواصل الاجتماعي/ فيسبوك وما إلى ذلك، وعلى الإنترنت/ إخفاء الهوية، والتعريف الزائف، واستخدام حسابات أشخاص آخرين، وتحميل صور ومقاطع فيديو لأشخاص آخرين دون موافقتهم، وإرسال الفيروسات وما إلى ذلك.

بالإضافة لذلك ذكر كل من **(Un Broadband Commission, 2015, P.22)**، (شيماء كمال عبد العليم حسن، ٢٠٢٣م، ص٨٧٠)، (نوال وسار، ٢٠٢١م، ص ص٢٧٠-٢٧١)، **Malanga, D. (F., 2021, P.624)**، **(Kaphle, P., 2019, PP.88-89)** ، **Duman, M. Ç., 2023, PP.363-364)** أشكال العنف الرقمي، والتي قد تمارس ضد الفتيات وطالبات الجامعة، ويمكن إجمالها في الجدول الآتي:

جدول (١): أشكال العنف الرقمي

م	أشكال العنف الرقمي	مفهومها
١	المطاردة الإلكترونية	تتضمن حوادث متكررة، قد تكون أو لا تكون أعمالاً غير ضارة على حدة، ولكنها مجتمعة تقوض شعور الضحية بالأمان وتسبب الضيق أو الخوف أو الفزع.
٢	التنمر الإلكتروني	يتضمن تلقي رسائل بريد إلكتروني أو رسائل نصية قصيرة غير مرغوب فيها أو مسيئة أو صريحة جنسيًا؛ أو التقديمات غير اللائقة أو المسيئة على مواقع التواصل الاجتماعي أو في غرف الدردشة على الإنترنت.
٣	التحرش الإلكتروني	هو التحرش الذي يتم عن طريق البريد الإلكتروني أو الرسائل النصية أو عبر الإنترنت.
٤	خطاب الكراهية عبر الإنترنت	هو نوع من الخطاب الذي يتم عبر الإنترنت بهدف مهاجمة شخص أو مجموعة بناءً على عرقهم، أو دينهم، أو أصلهم العرقي، أو توجههم الجنسي، أو إعاقتهم، أو جنسهم. وتتم مشاركة خطابات الكراهية هذه من خلال منصات الإنترنت الموثقة في مقاطع الفيديو مما يحقق عددًا كبيرًا من الجماهير. وفي غياب التوازن بين خطاب الكراهية وحرية التعبير، فإن

م	أشكال العنف الرقمي	مفهومها
		الانسجام الاجتماعي والحرية الفردية تكون دائمًا على المحك. وعلى النقيض من ذلك، يتم استخدام خطاب الكراهية لإهانة الأفراد وجذب الدعاية المؤقتة.
٥	التشهير عبر الإنترنت	يتضمن نشر بيان كاذب عن شخص ما عبر الإنترنت مما يؤدي إلى نوع من الضرر، بما في ذلك الخسائر المالية أو الإضرار بسمعة الشخص المعني.
٦	الاستغلال عبر الإنترنت	الشخص الذي يتلقى تهديدات جنسية، أو يُجبر على المشاركة في سلوك جنسي عبر الإنترنت، أو يُبتز بمحتوى جنسي.
٧	إباحية غير توافقية (إباحية انتقامية)	يتضمن توزيع صور أو مقاطع فيديو جنسية عبر الإنترنت دون موافقة الفرد الموجود في الصور، بهدف التشهير به وإذلاله علنًا، بل وحتى إلحاق ضرر حقيقي بحياته "في العالم الحقيقي".
٨	الاختراق	استخدام التكنولوجيا للحصول على وصول غير قانوني أو غير مصرح به إلى الأنظمة أو الموارد لغرض الحصول على معلومات شخصية، أو تغيير، أو تعديل المعلومات، أو التشهير بالضحية وتشويه سمعتها. على سبيل المثال، انتهاك كلمات المرور والتحكم في وظائف الحاسوب، مثل تجميد الحاسوب أو تسجيل خروج المستخدم.
٩	انتحال الشخصية	استخدام التكنولوجيا لانتحال هوية الضحية أو شخص آخر من أجل الوصول إلى معلومات خاصة، أو إحراج الضحية، أو إهانتها، أو الاتصال بها أو إنشاء مستندات هوية مزورة؛ على سبيل المثال، إرسال رسائل بريد إلكتروني مسيئة من حساب البريد الإلكتروني للضحية؛ الاتصال بالضحية من رقم غير معروف لتجنب حظر المكالمة.
١٠	المراقبة/ التتبع	استخدام التكنولوجيا لملاحقة ومراقبة أنشطة وسلوكيات الضحية إما في الوقت الفعلي أو تاريخيًا؛ على سبيل المثال. تتبع نظام تحديد المواقع العالمي (**GPS**) عبر الهاتف المحمول؛ تتبع ضغطات المفاتيح لإعادة إنشاء أنشطة الضحية على الحاسوب.
١١	التحرش/ البريد العشوائي	تكرار الأفعال غير المرغوب بها، بشكل تطفلي محسوس بحيث يسبب إزعاجًا أو تهديدًا، وقد يصاحب هذا الأداء أفعالًا جنسية في بعض الأحيان. أي استخدام التكنولوجيا للتواصل بشكل مستمر مع الضحية، وإزعاجها، وتهديدها، وتخويفها. هذا سلوك مستمر وليس حادثًا معزولًا؛ على سبيل المثال، المكالمات/ الرسائل النصية المستمرة عبر الهاتف المحمول؛ ملء البريد الصوتي بالرسائل حتى لا يتمكن أي شخص آخر من ترك رسالة.

م	أشكال العنف الرقمي	مفهومها
١٢	التجنيد	استخدام التكنولوجيا لجذب الضحايا المحتملين إلى مواقف عنيفة؛ على سبيل المثال، المنشورات والإعلانات الاحتيالية (مواقع المواعدة؛ فرص العمل)؛ المتاجرون الذين يستخدمون غرف الدردشة، ولوحات الرسائل، ومواقع الويب للتواصل/ الإعلان.
١٣	التوزيع الخبيث	استخدام التكنولوجيا للتلاعب وتوزيع المواد التشهيرية وغير القانونية المتعلقة بالضحايا؛ على سبيل المثال، التهديد أو تسريب صور/ فيديوهات؛ استخدام التكنولوجيا كأداة دعاية للترويج للعنف ضد الفتيات.
١٤	المضايقة	ويقصد بها إرسال رسائل عدوانية وجارحة للفرد بشكل دائم ومتكرر على الإنترنت.
١٥	التصيد	يقصد بها عملية الاحتيال التي تمارس ضد الفرد للكشف عن معلومات شخصية خاصة به أو بأحد أفراد أسرته.
١٦	الإقصاء	يقصد به إقصاء شخص ما بتعمد وقسوة من مجموعة ما على الإنترنت.
١٧	تشويه السمعة	تشير إلى تحقير شخص ما على الإنترنت ونشر شائعات عن شخص لإلحاق الأذى به وتشويه سمعته.
١٨	تقليد أو سرقة أو انتحال الهوية	التظاهر بأن شخص آخر هو الذي يقوم بنشر مواد معينة لإيقاع هذا الشخص في مشكلة.
١٩	الابتزاز الإلكتروني	إجبار الشخص على القيام بتصرفات ضد رغبته، عن طريق التهديد والتخويف. فهو الوجه الأعنف للعنف الرقمي الذي يسعى إلى ابتزاز الفرد والتلاعب به وتهديده بهدف الوصول إلى مكاسب مادية أو جنسية ولتشويه سمعته والتشهير به.
٢٠	المطاردة	❖ يقصد بها التوحش الشديد الذي يتضمن تهديدًا بالأذى وخلق خوف شديد للفرد بدرجة عالية عبر الإنترنت. وتصنف المطاردة إلى نوعين: ✓ التنمر المباشر: وهو سلوك يحدث عندما يتعرض شخص بشكل متكرر لسلوكيات أو أفعال سلبية من أشخاص آخرين بقصد ايذائه، ويتضمن عادة عدم التوازن في القوة، وهو إما أن يكون لفظيًا كالتنابز بالألقاب، أو عاطفيًا كالنبذ الاجتماعي، أو يكون جسديًا كالضرب، أو يكون إساءة في المعاملة.

م	أشكال العنف الرقمي	مفهومها
		ويكون على شكل: (إرسال صور أو فيديوهات فاحشة- إرسال ملفات تحمل فيروسات عن قصد- استخدام الإنترنت للتهديد أو الإهانة). ✓ التنمر غير المباشر: وهو الذي يحدث دون أن يلاحظ الضحية، ويكون في حالة تصفح بريد إلكتروني لشخص آخر، ونشر ما يسيء إليه عبر الهاتف المحمول.
٢١	العنف اللفظي الكتابي	يشمل هذا النوع الأفعال التي تستخدم سلوك العنف اللفظي أو المكتوب مثل: الرسائل النصية والمكالمات الهاتفية.
٢٢	العنف البصري	يتضمن هذا النوع الاعتداءات التي تستخدم أشكال بصرية من العنف مثل: نشر صور مخجلة أو مسيئة.
٢٣	الوصول غيرالمسموح/ السيطرة غير المسموحة	هو الهجوم على حسابات الشخص الإلكترونية أو أجهزته الشخصية، ما يعني الحصول على المعلومات والبيانات الخاصة به أو حجب وصول الشخص إلى حساباته الشخصية.
٢٤	السيطرة والتلاعب بالمعلومات	المعلومات المجموعة أو المسروقة تعني فقدان السيطرة عليها من قبل أصحابها أو إمكانية تغييرها والعبث بها.
٢٥	التهديد	هو الخطاب أو المحتوى العنيف سواء كان (كتابة، صورة، شفويًا، أو أي شكل آخر)، للتهديد بالعنف أو الاعتداء الجنسي بحيث يعبر عن نيات صاحب التهديد على إيقاع الضرر بالشخص نفسه، أو عائلته، أو أصدقائه، أو ممتلكاته.
٢٦	المشاركة غير الرضائية للمعلومات الخاصة	نشر أو مشاركة أي نوع من المعلومات الخاصة بالشخص، أو بياناته الخاصة دون رضاه.
٢٧	الذم	السب والقذف والتشهير في مصداقية أو مهنية أو عمل أو في الصورة العامة للشخص عن طريق نشر أخبار كاذبة عنه، أو التلاعب بالحقائق.
٢٨	الهجوم على قنوات الاتصال	الهجوم الدائم على قنوات التواصل، بحيث يبقى الشخص المستهدف خارج دائرة التواصل.
٢٩	الانتهاك والاستغلال الجنسي المرتبط بالتقنية	هو ممارسة القوة على شخص تقوم على استغلاله جنسيًا عن طريق صوره الشخصية على غير إرادته، بحيث تكون التكنولوجيا هي الأداة الأساسية في هذا الاستغلال.
٣٠	القرصنة	هو استخدام التكنولوجيا للحصول على وصول غير قانوني أو غير مصرح به إلى الأنظمة أو الموارد لغرض الحصول على معلومات شخصية، أو تغيير المعلومات، أو تعديلها، أو

م	أشكال العنف الرقمي	مفهومها
		التشهير بالضحية و/ أو منظمات العنف ضد المرأة وتشويه سمعتها. على سبيل المثال، انتهاك كلمات المرور والتحكم في وظائف الحاسوب، مثل تجميد الحاسوب أو تسجيل خروج المستخدم.
٣١	العنف بين الشريكين	هو النوع الذي تستخدم فيه التكنولوجيا للعنف في الأسرة والعنف الزوجي والعلاقات الوثيقة. على سبيل المثال، الكشف عن رسائل الشريك.
٣٢	العنف المبرر ثقافيا ضد المرأة	هو الاستخدام الخبيث للتكنولوجيا لتبرير الثقافة والدين. ويهدف إلى تطبيع العنف ضد المرأة. على سبيل المثال، الرجال أكثر قيمة من النساء.
٣٣	الاغتصاب والاعتداء الجنسي	تتبع تحركات النساء والضحايا، وتوزيعها، وتوفير معلومات عن مواقعهن. على سبيل المثال، استدراج النساء إلى الاعتداء الجنسي.
٣٤	المجتمعات المستهدفة بالعنف	إنه تعرض الأفراد للهجمات الرقمية بسبب جنسهم أو هويتهم الجنسية أو آرائهم السياسية. على سبيل المثال، تعرضت بعض صفحات الويب الخاصة بحقوق المرأة للهجوم بسبب موقفها من عدم المساواة بين الجنسين.

المصدر: راجع كل من:

- شيماء كمال عبد العليم حسن (٢٠٢٣): "العنف الرقمي وعلاقته بالأفكار الانتحارية وهوية الأنا لدى عينة من المراهقين في ضوء بعض المتغيرات الديموجرافية"، **مجلة قطاع الدراسات الإنسانية**، كلية الدراسات الإنسانية، جامعة الأزهر، ع٣٢، ديسمبر، ص٨٧٠.
- نوال وسار (٢٠٢١م): "العنف الرقمي ضد المرأة: امتداد الظاهرة وتمدد الأشكال"، **مجلة الرواق للدراسات الاجتماعية والإنسانية**، المركز الجامعي أحمد زبانة غليزان- مخبر الدراسات الاجتماعية والنفسية والانثروبولوجية، الجزائر، مج٧، ع١، ص ص٢٧٠-٢٧١.
- Un Broadband Commission (2015). Cyber Violence Against Women and Girls. **A Report by the UN Broadband Commission for Digital Development Working Group on Broadband and Gender**. P.22.
- Malanga, D. F. (2021). Survey of cyber violence against women in Malawi. **Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development**, P.624.
- Kaphle, P. (2019). Cyber violence against women and girls in Nepal. **Kathmandu School of Law Review (KSLR),** 7(1), 88-89.

❖ Duman, M. Ç. (2023) DIGITAL VIOLENCE AND WOMEN: SYSTEMATIZATION OF RESEARCHS AND SUGGESTIONS FOR FUTURE RESEARCH. **Anadolu University Journal of Economics and Administrative Sciences**, 24(3), 363-364.

مما سبق عرضه يتبين تنوع أشكال العنف الرقمي التي قد تتعرض لها بعض طالبات الجامعة، والتي لها العديد من الآثار السلبية عليهن، ويمكن تناولها فيما يلي:

(ز) الآثار السلبية للعنف الرقمي ضد طالبات الجامعة

إن تأثيرات العنف الرقمي ضد طالبات الجامعة هي نفسية، واجتماعية، وجسدية، واقتصادية. والأكثر انتشارًا هي التأثيرات النفسية، التي تشعر بها معظم الطالبات اللاتي يتعرضن للعنف الرقمي، ومنها القلق وعدم الراحة وصورة الذات المتضررة والانخراط في سلوك إيذاء النفس، ونوبات الهلع، وتجربة الخوف الشديد الذي يمنعهن من مغادرة منزلهن، ومشاعر الإذلال، وأفكار الانتحار، والاكتئاب، وتقلبات المزاج **(West, J., 2014, PP.14-15).**

وتتمثل الآثار السلبية للعنف الرقمي ضد طالبات الجامعة فيما يلي (فاطمة الزهرة قمقاني، ٢٠٢٣م، ص٧٢):

- ✓ **الآثار النفسية:** ومن أكثر هذه الآثار شيوعًا القلق، وتشوه الصورة الذاتية، وأحيانًا تصل الآثار النفسية إلى أكثر تطرفًا كالأفكار الانتحارية، أو الانخراط في سلوك إيذاء النفس والاكتئاب، والأرق، ونوبات الهلع والخوف الشديد من مغادرة المنزل بالإضافة إلى الشعور بالإذلال.
- ✓ **الآثار الاقتصادية:** قد يؤدي العنف الرقمي والتشهير بالضحية إلى تقليص فرصتها في الالتحاق بالعمل، خاصة إذا كانت هي من تعيل عائلتها.
- ✓ **الآثار الاجتماعية:** عادة ما تفضل أسر الضحايا عدم الإفصاح عن الجرائم الإلكترونية التي تتعرض لها فتياتها خوفًا من نظرة المجتمع والمحيطين وتنامي الشكوك حول سلوكيات هذه الفتيات، فيلجئون إلى الصمت مع الإحساس بالقهر الاجتماعي وعدم القدرة على معاقبة الجناة

الذين أساءوا لهن، وهو الأمر الذي يعمق مشاعر الغضب داخل هذه المجتمعات لا سيما العربية المحافظة؛ فالفتاة رغم أنها تعرضت للعنف وليس لها أي علاقة بالذي عنفها، إلا أنها هي من تنال السخط الاجتماعي من وسطها المقرب، وهذا يدفع بالفتاة في الكثير من الأحيان إلى التمرد والخروج عن القواعد والأعراف.

مما سبق عرضه يتبين الآثار السلبية للعنف الرقمي ضد طالبات الجامعة، والتي يتطلب توعيتهن بكيفية مواجهته من خلال معرفتهن بالتشريعات والإجراءات القانونية اللازمة لمواجهته، والتي سيتم الحديث عنها فيما يلي:

(ح) الإجراءات القانونية للتعامل مع العنف الرقمي في مصر

فيما يتعلق بالقوانين التي تتناول العنف الرقمي، أصدرت مصر العديد من القوانين والتشريعات التي تواجهه، منها ما يلي:

١. القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات:

أصدرت مصر قانونًا عامًا لمكافحة جرائم الإنترنت وجرائم تكنولوجيا المعلومات في عام ٢٠١٨م، ويتضمن القانون ٤٥ مادة تتناول جوانب مختلفة من الجرائم الإلكترونية مع عقوبات تعكس الطبيعة المختلفة لهذه الجرائم، مثل التهديدات والابتزاز والتشهير أو الترهيب. وتشمل العقوبة السجن والغرامة، على سبيل المثال: تبدأ عقوبة الابتزاز الإلكتروني بالسجن لستة أشهر، ويمكن تغريم الجاني حتى ٢٠٠ ألف جنيه مصري. تم تعديل القانون في وقت لاحق لضمان عدم الكشف عن هوية ضحايا هذه الجرائم (رئاسة الجمهورية، ٢٠١٨م).

٢. قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣:

تنص المادة ٢/٧٦ من قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ على أنه مع عدم الإخلال بالحق في التعويض المناسب، يعاقب بالحبس وبغرامة لا تقل عن خمسمائة جنيه ولا تجاوز

عشرين ألف جنيه أو بإحدى هاتين العقوبتين كل من: تعمد إزعاج أو مضايقة غيره بإساءة استعمال أجهزة الاتصالات (جمهورية مصر العربية، المادة ٧٦/ ٢).

٣. الدستور المصري ٢٠١٤:

تنص **المادة (٥٧) في الدستور المصري ٢٠١٤** على أن: (للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك) (**رئاسة الجمهورية: الدستور المصري ٢٠١٤**).

٤. أرقام مكافحة الجرائم الإلكترونية وطرق الإبلاغ عنها في مصر

أقرت الجهات الرسمية لمكافحة الجرائم الإلكترونية بعض الأرقام للتواصل في حالة التعرض لعنف رقمي، أولها الاتصال بالخط الساخن ١٠٨ أو الاتصال على الأرضي ٠٢٢٤٠٦٥٠٥٢ أو الاتصال على ٠٢٢٤٠٦٥٠٥١ للتواصل مباشرة مع إدارة تكنولوجيا المعلومات. أو عن طريق القيام بتقديم بلاغ عن طريق استخدام الموقع المخصص لوزارة الداخلية. والتواصل على رقم المباحث للابتزاز الإلكتروني وهو ١٢٢. كما يمكن التوجه إلى الإدارة العامة لمكافحة جرائم الحاسبات والمعلومات بالمقر الخاص بوزارة الداخلية (**مؤسسة جنوبية حرة، ص٤١**).

مما سبق عرضه لابد من توعية طالبات الجامعة بكيفية اتخاذهن لهذه الإجراءات القانونية عند تعرضهن للعنف الرقمي، وأيضًا توعيتهن بكيفية حماية بياناتهن ومعلوماتهن الشخصية من التهديدات الرقمية المتزايدة، وهذا يتطلب معرفتهن لمفهوم الأمن السيبراني وأهميته لديهن في مواجهة العنف الرقمي، وهذا ما سيتم تناوله في المحور الثاني الآتي:

المحور الثاني: الإطار المفاهيمي للأمن السيبراني

يُعد الأمن السيبراني من الموضوعات المهمة في العصر الحالي؛ حيث أصبح العالم الرقمي جزءًا أساسيًا من الحياة اليومية للأفراد، خاصة طالبات الجامعة اللاتي قد يواجهن العديد من التحديات والمخاطر في الفضاء الإلكتروني، والتي تمثل تهديدًا حقيقيًا على الأمان الشخصي لهن، وتؤثر تأثيرًا سلبيًا على حياتهن الأكاديمية والاجتماعية والنفسية.

وفيما يلي عرضًا للإطار المفاهيمي للأمن السيبراني من خلال الحديث عن مفهومه، والمفاهيم المرتبطة به، ونشأته، وخصائصه، وأهميته، وأهدافه، وعناصره، وأبعاده، وأنواعه، ومجالات استخدامه، وتقنياته، ومخاطره وتهديداته، وتحدياته، وكيفية التغلب عليها، ومتطلبات تطبيقه، وآليات وإجراءات تعزيزه لطالبات الجامعة، والمهارات اللازمة لتحقيقه.

(أ) مفهوم الأمن السيبراني

من الناحية اللغوية، كلمة الأمن جاءت في اللغة العربية ضد الخوف وتعني طمأنينة النفس وزوال الخوف. ويشير أيضًا إلى الحالة التي توفر للفرد الإحساس بعدم الخطر والأمان على نفسه، وممتلكاته، وأمواله. أما كلمة "سيبراني" لغة فجاءت من كلمة "سيبر" وتعني صفة أي شيء مرتبط بثقافة الحواسيب، أو تقنية المعلومات أو الواقع الافتراضي. وفي الاصطلاح، كلمة سيبراني استعملت لأول مرة من قبل عالم الرياضيات الأمريكي Norbert Winner عام ١٩٤٨م، وتعني علم القيادة والتحكم في أجهزة الحاسوب، ودراسة آليات التواصل، والتي تتضمن تكنولوجيا المعلومات، والواقع الافتراضي (سفيان يوسفي، كلثوم مسعودي، ٢٠٢٤م، ص٦٥٦).

ويُعرف الأمن السيبراني بأنه 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(علياء عمر كامل فرج، ٢٠٢٢م، ص٥٢١).

كما يُعرف بأنه عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال، واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني، كما أن الأمن السيبراني هو سلاح استراتيجي بيد الحكومات والأفراد لا سيما أن الحرب السيبرانية أصبحت جزءًا لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول (مصباح أحمد حامد الصحفي، سناء صالح عسكول، ٢٠١٩م، ص٤٩٨).

فالأمن السيبراني هو ممارسة حماية الأنظمة والشبكات والبيانات الرقمية من الوصول غير المصرح به والاختراقات والهجمات. في عالم رقمي متزايد، حيث يتم تخزين المعلومات ونقلها ومعالجتها إلكترونيًا، يؤدي الأمن السيبراني دورًا حاسمًا في حماية المعلومات الحساسة والحفاظ على الخصوصية والحفاظ على سلامة وتوافر الأصول الرقمية **(Sevinch, Q., 2024, P.50)**.

ويشمل الأمن السيبراني الممارسات والتقنيات والعمليات المصممة لحماية الأنظمة والشبكات والبيانات الرقمية من الوصول غير المصرح به أو التلف أو السرقة. فهو ممارسة حماية الأصول الرقمية، مثل أنظمة الحاسوب والشبكات وما إلى ذلك، من الهجمات الرقمية. وتشمل بعض الأنواع البارزة من الأمن السيبراني أمن الشبكات، وأمن التطبيقات، وأمن المعلومات أو البيانات، وأمن السحابة، وأمن الأجهزة المحمولة، وأمن البنية التحتية الحرجة **(Amin, M., 2024, P.494)**.

فالأمن السيبراني بإيجاز هو ممارسة حماية أجهزة الحاسوب والخوادم، والأجهزة المحمولة والأنظمة الإلكترونية، والشبكات والبيانات من الوصول غير المصرح به والسرقة والتلف **(Oladokun, B. & et.al., 2024, P.2)**.

(ب) المفاهيم المرتبطة بالأمن السيبراني

يرتبط مفهوم الأمن السيبراني بعدة مفاهيم، من أبرزها ما ذكره كل من (هاني رزق عبد الجواد الألفي، ٢٠٢٢م، ص ص٧٣٥-٧٣٦)، و(قطاف سليمان، بوقرين عبد الحليم، ٢٠٢٢م، ص٤٩):

- ✓ **الهجمات السيبرانية**: وتعرف بأنها محاولات جادة من قبل المتسللين أو المخربين الإلكترونيين؛ بقصد تخريب أو سرقة، أو تدمير أنظمة الجامعة الإلكترونية وما ترتبط بها من أنظمة فرعية ووثائق وملفات.
- ✓ **الجرائم السيبرانية**: الأعمال والأفعال والممارسات الإجرامية غير القانونية التي تتم بواسطة محترفين بصورة فردية أو يتبعون جهات مختلفة؛ بقصد السيطرة على نظام الجامعة الإلكتروني.
- ✓ **المهاجمين أو المخربين السيبرانيين**: أفراد أو كيانات تقوم بأفعال وسلوكيات مخالفة للقوانين- غالبًا- ما يكونوا على درجة من الاحترافية في التخطيط والتنفيذ للهجمات السيبرانية على المؤسسات ومنها الجامعات.
- ✓ **الردع السيبراني**: إجراءات سريعة وفورية تأتي كرد حاسم على المخربين السيبرانيين؛ بحيث تعمل تلك الإجراءات على منعهم في المستقبل من تكرار تلك الهجمات والعمل على اكتشافهم وفضحهم واتخاذ الإجراءات القانونية تجاههم.
- ✓ **الخطر السيبراني**: مجموعة من الأفعال التي تشكل أو تمثل تحركات ضارة من قبل بعض الجهات غير الواضحة لمسؤولي الجامعة؛ والتي تستلزم اتخاذ قرارات فورية لمواجهة تلك الأفعال والقضاء عليها في مهدها.
- ✓ **الصراع السيبراني**: مع انتشار الفضاء السيبراني وسهولة الدخول، اتسع نطاق النزاعات السيبرانية وازداد عدد المهاجمين. وهناك عاملان رئيسان لتوسع النزاعات السيبرانية: أحدهما هو التغيير الأساسي في منظور الحرب؛ ونمط التحولات بين الناس. ثانيًا، ظهور النزاعات على المستويين المحلي والدولي، وزيادة حدة النزاعات الداخلية وبؤر التوتر بعد الحرب الباردة، كما يوفر السياق الدولي للفضاء السيبراني بيئة مفتوحة للقوى المهمشة في السياسة الدولية.

- ✓ **أمن المعلومات:** يشمل الأمن الحفاظ على سرية المعلومات والبيانات التي يعلقها مستخدمو الإنترنت على مواقع التواصل الاجتماعي وجميع المنصات الإلكترونية، ويستمر في تشكيل حماية المعلومات والبيانات الشخصية من أي محاولة اختراق للنظام الإلكتروني أو التجسس الإلكتروني. وزادت حماية المعلومات من استخدامها مع تطور الإنترنت والتوسع في أساليبها وأنواعها. فأمن المعلومات له أنواع أساسية من المعالجة وهي: نظام حماية نظام التشغيل، ونظام حماية البرامج والتطبيقات، ونظام الحماية البرامجية والإلكترونية والدخول، ونظام حماية الخروج.

(ج) نشأة الأمن السيبراني

يمكن إرجاع بداية مصطلح "الأمن السيبراني" إلى السنوات الأولى لتقنية الحوسبة والشبكات؛ حيث كان الأمن السيبراني في مرحلته الأولى مرتبطًا بشكل أساسي بحماية الأنظمة المادية والبنى التحتية. وخلال الستينيات والسبعينيات من القرن الماضي، عندما كانت أجهزة الحاسوب تستخدم في الغالب للحسابات المعقدة ومعالجة البيانات في الإعدادات الأكاديمية والبحثية، كان التركيز الأساسي على الحفاظ على سلامة الأنظمة وضمان دقة البيانات. وقد أدى ظهور الإنترنت في أواخر الثمانينيات وتوسع الاتصال الرقمي في التسعينيات إلى تحول كبير في مشهد الأمن السيبراني خاصة مع بدء استخدام الإنترنت لأغراض تجارية وحكومية وشخصية مختلفة ليبدأ نطاق الأمن السيبراني في الاتساع مع التركيز ليس فقط على تكامل النظام، ولكن أيضًا على خصوصية البيانات ومصادقة المستخدم. وتطور الأمن السيبراني حديثًا إلى مفهوم شامل يشمل حماية أنظمة المعلومات والشبكات والبيانات من الهجمات الرقمية أو الوصول غير المصرح به بهدف ضمان السرية والنزاهة والتوافر، والذي يشار إليه عادة باسم ثالوث النزاهة والتوافر. وقد جعل التقدم التكنولوجي والاعتماد المتزايد على المنصات الرقمية لمختلف جوانب الحياة الأمن السيبراني مصدر قلق محوري على جميع المستويات، من المستخدمين الأفراد إلى الشركات الكبيرة وحتى الدول (عبير بنت محمد بن ربيع عاتي، ٢٠٢٣م، ص٣).

وبحلول العقد الأول من القرن الحادي والعشرين تنوعت وتضاعفت التهديدات والاختراقات، وكذلك الهجمات الإلكترونية المتعلقة بالأنظمة البنكية التي بدأت كثير من الكيانات الإجرامية القيام بها وبشكل محترف باستخدام تقنيات عالية، الأمر الذي دفع الكثير من الدول والحكومات إلى اتخاذ العديد من القرارات من أجل تضييق الخناق على هذه الجهات. وكان ذلك من خلال العديد من الخطوات مثل؛ سن التشريعات الخاصة بهذا النوع من الجرائم، وإصدار الأحكام الجنائية. وبدأت الارهاصات الأولى لمصطلح الأمن السيبراني في الدول المتقدمة فهي السباقة لتبني أمن سيبراني يهدف إلى حماية الفضاء السيبراني من الهجومات التي قد تطاله خاصة تلك المتعلقة بالأنظمة البنكية؛ وبعدها انتشر الأمن السيبراني وتداعياته في جل العالم (بدر الحيمودي، ٢٠٢٣، ص١٧٦).

(د) خصائص الأمن السيبراني

بما أن الجريمة الإلكترونية تتم بمنهجية وأساليب جديدة ذات بعد تكنولوجي أعلى من الجرائم التقليدية، كان لابد أن يأتي الأمن السيبراني للتغلب على هذه المشكلة مواكبًا للتطور التكنولوجي، ولذا تميز الأمن السيبراني بعدد من الخصائص ذكرها كل من (جيهان سعد محمد الخضري، وآخران، ٢٠٢٠م، ص٢٢٣)، و (الجوهرة بنت عبد الرحمن إبراهيم المنيع، ٢٠٢٢م، ص١٦٤) فيما يلي:

١. **الاكتشاف والتعقب**: حيث يهدف الأمن السيبراني إلى اكتشاف الجريمة الإلكترونية وتعقب أثرها، وبالتالي التغلب عليها.
٢. **السرعة وغياب الدليل**: فصعوبة إثبات الجرائم الإلكترونية نظرًا لاستخدام المخترقين وسائل تقنية حديثة، أتى الأمن السيبراني بتقنيات حديثة عالية تفوق خبرة المجرم.
٣. **ضعف الأجهزة الأمنية والقضائية تجاه التعامل مع الجرائم الإلكترونية**: نتيجة لنقص الخبرة الرقمية لدى الأجهزة الأمنية مما يعزز دور الأمن السيبراني في تحقيق الأمن الرقمي للمؤسسات والأفراد في حماية البيانات والبنى التحتية لها.

كما يتمتع الأمن السيبراني بمجموعة من الخصائص، منها ما يلي (عائشة عبيد الله العازمي، ٢٠٢٤م، ص٣٦):

- ✓ ضمان الوصول المنطقي إلى الأصول المعلوماتية والتقنية للمؤسسة، وذلك لمنع الوصول غير المصرح به، وتقييد الوصول لما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.
- ✓ قدرته على حماية أنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للمؤسسة، وكذلك القدرة على حماية البريد الإلكتروني من المخاطر السيبرانية.
- ✓ لديه قدرة على حماية وإدارة أمن الشبكات.
- ✓ ضمان حماية أجهزة المؤسسة المحمولة بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في المؤسسة.
- ✓ السرية وسلامة البيانات والمعلومات ودقتها وتوافرها وفق السياسات والإجراءات التنظيمية للمؤسسة.

(هـ) أهمية الأمن السيبراني

تتمثل أهمية الأمن السيبراني في الآتي (العنود بنت عبد الله بن محمد الحميد، نورة بنت محمد المطرودي، ٢٠٢٤م، ص٢٣٦):

- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك من العبث بها، وتحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.
- حماية الأجهزة والشبكات ككل من الاختراقات لتكون درع واق للبيانات والمعلومات.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.
- توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية.

(و) أهداف الأمن السيبراني

تتمثل أهداف الأمن السيبراني فيما يلي (عمار حسن صفر، ٢٠٢٤م، ص ص٢٥-٢٦):

- **حماية البيانات والمعلومات:** أحد أهم أهداف الأمن السيبراني هو حماية البيانات والمعلومات الحساسة. تُعد البيانات الحساسة مثل المعلومات الشخصية والمالية والتجارية والحكومية هدفًا للقرصنة والهاكرز والمجرمين الإلكترونيين. يجب توفير الحماية اللازمة لهذه البيانات والمعلومات لمنع الوصول غير المصرح به والاستخدام غير القانوني. وتشمل الإجراءات المهمة لحماية البيانات والمعلومات التشفير، وتقييد الوصول بواسطة طبقات من الحماية ونظم المصادقة الثنائية، وتطبيق السياسات الأمنية المناسبة.
- **ضمان سلامة الأنظمة والشبكات:** تُعد سلامة الأنظمة والشبكات الإلكترونية أحد الأهداف الرئيسة للأمن السيبراني. حيث يهدف الأمن السيبراني إلى حماية الأنظمة والشبكات من الهجمات والاختراقات الإلكترونية التي يمكن أن تتسبب في تعطيل الخدمات أو سرقة البيانات والمعلومات الحساسة. ويجب اتخاذ إجراءات مثل تطبيق الجدران النارية، وتحديث البرامج الأمنية بانتظام، واستخدام أنظمة الكشف عن التسلل للحفاظ على سلامة الأنظمة والشبكات.
- **حماية البنية التحتية الحيوية:** تستهدف استراتيجيات الأمن السيبراني حماية البنية التحتية الحيوية التي تشمل محطات الطاقة والشبكات الكهربائية والمرافق الحيوية الأخرى. ويمكن لهجمات القرصنة الموجهة لهذه البنية التحتية أن تؤدي إلى انقطاع التيار الكهربائي أو تعطيل الخدمات الحيوية الأخرى. ويجب تطبيق الحماية السيبرانية المتقدمة على هذه البُنى التحتية لمنع واستدامة أي هجمات محتملة.

- **التصدي للتهديدات النشطة:** تهدف جهود الأمن السيبراني إلى التصدي للتهديدات النشطة مثل هجمات القرصنة والبرمجيات الخبيثة والاحتيال الإلكتروني. فالقراصنة والمجرمون الإلكترونيون والدول الأعداء والمنافسون يشكلون تهديدًا محتملًا للأنظمة السيبرانية. ويجب توفير أنظمة الكشف المبكر والاستجابة السريعة وتحديثات الأمان المستمرة للحد من هذه التهديدات وتقليل الأضرار المحتملة.
- **تعزيز الوعي والتثقيف السيبراني:** تهدف جهود الأمن السيبراني أيضًا إلى تعزيز الوعي والتثقيف السيبراني لدى المستخدمين. ويُعد التوعية بمفاهيم الأمن السيبراني وممارساته الجيدة مهمًا للغاية في الحد من المخاطر والهجمات. ويجب توفير التدريب والتثقيف المستمر للمستخدمين لتعرف التهديدات الحديثة وكيفية التعامل معها بشكل آمن.

ولتعزيز وعي طالبات الجامعة بأهمية الأمن السيبراني، هناك العديد من الأهداف التي يحققها والتي ذكرها (Odaibat, A. A., & Eyadah, H. T. A., 2024, P.6)، من أهمها:

- الحفاظ على معلومات الطالبات المتوفرة على شبكة المعلومات والاتصالات من أي اختراق محتمل، وذلك بتعريفهم بالتقنيات المتعلقة بأمن المعلومات، وأهمها كشف الرسائل الاحتيالية أو رسائل الاختراق الإلكتروني والعمل على مواجهتها.
- تعريف الطالبات بالبنية التحتية التكنولوجية لأمن المعلومات في الجامعة ليعلموا أن معلوماتهم وبياناتهم تتمتع بحماية خاصة بشرط عدم إساءة استخدامها، وتوعيتهم بالطرق والإجراءات الصحيحة التي يتم اتخاذها في حال اختراق معلوماتهم أو بياناتهم أو حساباتهم.
- تعريف الطالبات بالآثار الاجتماعية والاقتصادية والشخصية والتجارية الناتجة عن الاستخدام غير المشروع للإنترنت، والآثار السلبية الناتجة عن الجرائم الإلكترونية على المجتمع والأفراد،

حيث من المحتمل أن تؤدي الجرائم الإلكترونية إلى إتلاف أو العبث بالبيانات أو المعلومات بالإضافة إلى انتهاك خصوصية وسرية الآخرين.

(ز) عناصر الأمن السيبراني

لابد من توافر مجموعة عناصر تعمل مع بعضها البعض لتحقيق الهدف من الأمن السيبراني، والتي ذكرها كل من (سارة محمد روحي فتحي غزال، ٢٠٢٢م، ص٥٨١)، (عائشة عبيد الله العازمي، ٢٠٢٤م، ص٣٦) فيما يلي:

- **التقنية**: تشكل التقنية والتكنولوجيا دورًا في غاية الأهمية في حياة الأفراد والمؤسسات؛ حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات، واعتمادها على جدران ووسائل الحماية التي ستتطرق إلى توضيحها لاحقًا واستخدام البرامج الضارة ومكافحة الفيروسات.
- **الأشخاص**: يتوجب على كل شخص من مستخدمي البيانات والأنظمة في المؤسسات استخدام مبادئ حماية البيانات الرئيسة لتحديد كلمة مرور قوية، لتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، وعمل نسخ احتياطية للبيانات.
- **الأنشطة والعمليات**: يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني، والتصدي لهجماته بكل كفاءة.
- **البنية التحتية الحرجة**: وهي مجموعة الأنظمة والشبكات الإلكترونية والأصول المادية وغير المادية، أو الأصول السيبرانية والأنظمة التي يعد تشغيلها المستمر ضرورة ضمان أمن الدولة واقتصادها وسلامة المجتمع.

(ح) أبعاد الأمن السيبراني

تتعدد أبعاد الأمن السيبراني، والتي ذكرها كل من (منى عبد الله السمحان، ٢٠٢٠م، ص١٥)، و (ربيعي حسين، سمر محمود، ٢٠٢٢م، ص١٨٠)، و (صلاح الدين محمد توفيق، شيرين عيد مرسي، ٢٠٢٣م، ص ص٧٧٢-٧٧٣) فيما يلي:

١. **الأبعاد العسكرية**: وتتمثل في قدرته على ربط الوحدات العسكرية ببعضها، بما يسمح بسهولة تبادل المعلومات والسرعة في اتخاذ القرارات العسكرية وتدمير الأهداف عن بُعد، وتنشأ أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، واختراقات أنظمة المنشأة النووية، وما قد يحدث عنها من تهديدات لأمن الدول والحكومات ويؤدي إلى كوارث.

٢. **الأبعاد السياسية**: تقوم على أساس حماية نظام الدولة السياسية وكيانها؛ حيث يمكن أن تستخدم التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة لاستقرار أمن الدول والحكومات؛ حيث تصل بسرعة فائقة إلى أكبر شرائح من المواطنين بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها.

٣. **الأبعاد الاقتصادية**: يرتبط الأمن السيبراني ارتباطًا وثيقًا بالحفاظ على المصالح الاقتصادية لكل الدول، فالترابط وثيق بين الاقتصاد والمعرفة؛ فأغلب الدول تعتمد في تعزيز اقتصادها وازدهاره على إنتاج وتداول المعرفة والمعلومات، مما يبرر الدور الخطير للأمن السيبراني في حماية الاقتصاد من السرقة والملكية الفكرية.

٤. **الأبعاد القانونية**: ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقوانين، ومع ظهور المجتمع المعلوماتي ظهرت القوانين الجديدة التي تعد البيئة التنظيمية التشريعية المنظمة لحماية هذا المجتمع، وحفظ الحقوق فيه بكافة ما يتضمن من أبعاد، ويقوم الأمن

السيبراني في هذا البعد على حماية المجتمع المعلوماتي، ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات.

٥. **الأبعاد الاجتماعية**: يرتبط الأمن السيبراني بشبكات التواصل الاجتماعي التي تسمح وتتيح جمع المعلومات المتعلقة بالأفراد، بما أصبح يُعرف "الهندسة الاجتماعية" من خلال معرفة تطلعاتهم السياسية والاجتماعية واستغلالها لتحقيق تطلعاتهم. حيث تسمح طبيعة الإنترنت المفتوحة عبر شبكات التواصل الاجتماعي لكل مواطن بأن يعبر عن أفكاره، والاطلاع على مختلف المعلومات، والانفتاح عبر جميع الثقافات المختلفة، وهنا يكمن دور الأمن السيبراني وأهميته في حماية القيم الجوهرية للمجتمع وصيانتها؛ كالانتماء، والمعتقدات الدينية، والعادات والتقاليد...إلخ. وفي هذا السياق تعمل المنظمات والهيئات على نشر ثقافة الأمن السيبراني، وتطالب بضرورة تعاون كل أفراد المجتمع في تحقيقه، للحد من مخاطر الهجمات والجرائم السيبرانية التي تطول المجتمع ككل، وتهدد أمنه واستقراره، بالعمل على هدم قيمه وضياع هويته الثقافية.

(ط) أنواع الأمن السيبراني

هناك أنواع مختلفة للأمن السيبراني، والتي ذكرها كل من (صلاح الدين محمد توفيق، شيرين عيد مرسي، ٢٠٢٣م، ص٧٦٧)، و (علي آل مداوي، ٢٠٢٣م، ص ص١١٩-١٢٠) فيما يلي:

- **أمن الشبكات (Network Security):** وفيه تتم حماية أجهزة الحاسوب من الهجمات التي قد يتعرض لها داخل الشبكة وخارجها، ومن أبرز التقنيات المستخدمة لتطبيق أمن الشبكات جدار الحماية الذي يعمل واقيًا بين الجهاز الشخصي والأجهزة الأخرى في الشبكة، بالإضافة إلى أمن البريد الإلكتروني. كما أنه يهتم بالاختراقات الخارجية التي تهدد المنظومة الإلكترونية والمواقع التكنولوجية، فهو عملية تهتم بحماية الشبكة من الاختراقات الخارجية والأجهزة.

وهناك عدة أنواع تضمن حصول أمن الشبكة؛ وهي: كلمات مرور جديدة، وبرامج الحماية من الفيروسات، وبرامج مكافحة التجسس، والجدران النارية.

- **أمن التطبيقات (Application Security):** وفيه تتم حماية المعلومات المتعلقة بتطبيق على جهاز الحاسوب، كإجراءات وضع كلمات المرور، وعمليات المصادقة، وأسئلة الأمان التي تضمن هوية مستخدم التطبيق. فهو الاختيار السليم للبرامج التي تحمي الأجهزة والشبكات من عمليات الاختراق الإلكتروني، ولها عدة أنواع معروفة؛ أهمها: برامج مكافحة الفيروسات، والجدران النارية، وبرامج التشفير المعلوماتي. هذه الطرق الثلاثة تضمن حماية المحتوى من عمليات الاختراق الإلكترونية؛ فكلما كان مستخدم الإنترنت أكثر اطلاعًا على برامج الحماية ويستخدمها، كان أبعد عن احتمالية وقوعه رهن الابتزاز والاختراق.
- **الأمن السحابي (Cloud Security):** تُعرف البرامج السحابية بأنها برامج تخزين البيانات وحفظها عبر الإنترنت، ويلجأ الكثير إلى حفظ بياناتهم عبر البرامج الإلكترونية عوضًا عن برامج التخزين المحلية، مما أدى إلى ظهور الحاجة إلى حماية تلك البيانات، فتعني البرامج السحابية بتوفير الحماية اللازمة لمستخدميها. فهو نظام مراقبة وحماية لكل مصادر المعلومات والبيانات التابعة للمستخدم عبر المواقع والمنصات الإلكترونية، ولكن إذا تم تفعيل هذه الخاصية لا يعني أنه بإمكانك تجاهل كل الأمور السيبرانية الأخرى، فمن الضروري الاهتمام بحماية المعلومات والبيانات الخاصة بك بشكل مستمر.
- **الأمن التشغيلي (Operational Security):** وهو إدارة مخاطر عمليات الأمن السيبراني الداخلي، وفيه يوظف خبراء إدارة المخاطر لإيجاد خطة بديلة في حال تعرض بيانات المستخدمين لهجوم إلكتروني، ويشمل كذلك توعية الموظفين وتدريبهم على أفضل الممارسات لتجنب المخاطر.

- **أمن البنية التحتية الحيوية:** يعتمد على البنية التحتية الفيزيائية الإلكترونية للشبكة، وتتواجد عادة في وسائل النقل، والمدارس، والمستشفيات، والدوائر الحكومية، وفي شبكات المراكز التجارية. وهذا النوع يتطلب دراسة إلكترونية لنقاط ضعف المنظومة، والقاعدة الفيزيائية للشبكة لتطويرها وحمايتها من عمليات الاختراق.
- **إنترنت الأشياء:** يشمل عدة منظومات أساسية، مثل: أجهزة التلفاز، وأجهزة الاستشعارات والطابعات، وهذا النوع صنف كنوع من الأمن السيبراني، الذي يحمي البيانات لدى الأجهزة المذكورة، ولكنه كباقي التقنيات؛ إذا لم يتم الاهتمام والمتابعة به يمكن أن يصل المخترق إلى نظام الحماية ويفك شفرته.

كما ذكر (خالد مخلف الجنفاوي، ٢٠٢١م ، ص٨٥) عدة أنواع للأمن السيبراني فيما يلي:

١. **أمن الاتصالات (Communications Security)**: وهو الذي يهدف إلى الحماية من التهديدات المؤثرة على البنية التحتية والتقنية والحفاظ عليها من التلاعب.
٢. **أمن العمليات (Operations Security)**: وهو الذي يهدف إلى حماية التلاعب بالعمليات أو طريقة سير العمل.
٣. **أمن المعلومات (Information Security)**: يحمي أمن المعلومات (المعلومات) من غير المصرح به الوصول إليها، وحماية خصوصيتها، وكذلك المحافظة عليها من السرقة، ومن الأمثلة على أمن المعلومات (استخدام الحماية من خلال التشفير).
٤. **الأمن المادي (Physical Security):** وهو يمثل حماية الأصول المادية المرتبطة والمتعلقة بالنظام السيبراني، وهذه الأصول يمكن أن تكون عبارة عن خوادم وتخزين مكونات الشبكة، وتتضمن حمايتها ضد الوصول غير المصرح به.
٥. **أمن التطبيقات (Application Security):** يحمي أمان التطبيقات من التهديدات التي تحدث بسبب عيوب في تصميم التطبيق أو التطوير أو التثبيت أو التحديث أو الصيانة.

٦. **الأمن العسكري (Military Security):** وهو يمثل نظام حماية من الوصول إلى الأصول المادية ذات الجانب السياسي أو العسكري أو الاستراتيجي.

٧. **أمن الشبكات (Networks Security):** يحمي أمان الشبكة قابلية الاستخدام والسلامة في الشبكة والمكونات المرتبطة بها والاتصال والمعلومات عبر الشركة، ومن الأمثلة على أمان الشبكة (مكافحة الفايروسات ومكافحة برامج التجسس).

مما سبق يتضح أن الأمن السيبراني يتضمن عدة أنواع منها: أمن المعلومات أو البيانات، الحماية من الكوارث، أمن الشبكات والتطبيقات، أمن العمليات، أمن السحابة، أمن البنية الأساسية الحرجة، والتي يوضحها الشكل التالي**(Odaibat, A. A., & Eyadah, H. T. A., 2024, P.4) :**

شكل (١):أ نواع الأمن السيبراني

Source: Odaibat, A. A., & Eyadah, H. T. A. (2024). A Proposed Conception of the Role of the Family in Achieving Digital Security in Light of Achieving Cybersecurity. **International Journal of Latest Research in Humanities and Social Science (IJLRHSS)**, *7*(10), P.4. http://www.ijlrhss.com/paper/volume-7-issue-10/1-HSS-2923.pdf

(ي) مجالات استخدام الأمن السيبراني

يستخدم الأمن السيبراني في مجالات عديدة كما ذكرها كل من (نورة عمر الصائغ، وآخرون، ٢٠٢٠م، ص٥٠)، و (حمد بن حمود السواط، وآخرون، ٢٠٢٠م، ص٢٨٣)، ومن أهمها:

- **حماية الأجهزة الخاصة المحمولة وكذلك وسائط التخزين**: ويعني حماية جميع أنواع الأجهزة والمعدات التقنية من خطر الهجمات الإلكترونية والاختراقات والتدمير الجزئي أو الكلي، والقدرة على التعامل مع هذه البيانات والمعلومات.
- **التعامل الآمن مع خدمات تصفح الإنترنت**: ويعني توعية الأفراد بخطورة الهجمات والجرائم الإلكترونية، ووسائل الخداع والاحتيال وتدمير البيانات الشخصية أو سرقتها وابتزاز أصحابها، وذلك من خلال نشر المعلومات والإجراءات التي تساعدهم على حماية أنفسهم ومعلوماتهم على وسائل التواصل الاجتماعي.

كما تتعدد مجالات الأمن السيبراني، ومنها ما يلي (ريهام عصام سيد أحمد حشيش، محمد خيري محمد فتوح نوح، ٢٠٢٤م، ص ص٣٢٨-٣٢٩):

١. **أمن التطبيقات**: حماية البرمجيات من الثغرات الأنية أثناء التصميم والتشغيل.
٢. **أمن الشبكات**: يهتم بحماية الشبكات من الهجمات مثل حجب الخدمة، والدخول غير المصرح به.
٣. **الأمن السحابي**: يحمي البيانات المخزنة على السحابة من التهديدات، ويعزز أمانها.
٤. **إدارة الهوية والوصول**: تضمن وصول الأفراد المصرح لهم فقط إلى المعلومات الحساسة.
٥. **أمن إنترنت الأشياء**: يحمي الأجهزة المتصلة بالإنترنت من الهجمات الإلكترونية.
٦. **أمن الأجهزة المحمولة**: يعزز أمان الهواتف والحواسيب المحمولة من الهجمات، ويشمل حماية المعلومات الحساسة والوقاية من الاختراقات.
٧. **أمن العمليات**: يميز العمليات الصديقة من الخبيثة التي تسعى للوصول إلى البيانات الحساسة.

٨. **التشفير**: يستخدم لتأمين المعلومات لتحويلها إلى صيغ غير قابلة للقراءة دون مفتاح فك التشفير.

٩. **التعامل مع البرمجيات الخبيثة**: مثل الفيروسات والبرمجيات الخبيثة، والتعرف عليها وإزالتها.

١٠. **الأمن الجنائي الرقمي**: يجمع الأدلة من الجرائم الإلكترونية مثل الاختراقات ويحقق في الهجمات الرقمية لتتبع المجرمين.

(ك) تقنيات الأمن السيبراني

تتعدد تقنيات الأمن السيبراني، ومنها ما يلي (علي بن طراز، ٢٠٢٤م، ص ص٦٦-٦٧):

- ✓ **التحكم في الوصول وأمن كلمة المرور**: إن مفهوم اسم المستخدم وكلمة المرور طريقة أساسية لحماية المعلومات؛ حيث يُعد كأحد الإجراءات الأولى المتعلقة بالأمن السيبراني.
- ✓ **توثيق البيانات**: يجب دائمًا توثيق المستندات التي يتلقاها الأفراد قبل التنزيل، ويجب التحقق مما إذا كانت قد نشأت من مصدر موثوق به، ولم يتم تغييرها، وعادة ما تتم مصادقة هذه المستندات بواسطة برنامج مكافحة الفيروسات الموجود في الأجهزة. وبالتالي فإن برنامج مكافحة الفيروسات الجيد ضروري أيضًا لحماية الأجهزة من الفيروسات.
- ✓ **ماسحات البرامج الضارة**: هذه البرامج تقوم عادةً بمسح جميع الملفات والمستندات الموجودة في النظام بحثًا عن تعليمات برمجية ضارة أو فيروسات ضارة، والفيروسات والديدان وأحصنة طروادة هي أمثلة على البرامج الضارة التي غالبًا ما يتم تجميعها معًا، ويشار إليها باسم البرامج الضارة.
- ✓ **جدران الحماية**: جدار الحماية هو برنامج أو قطعة من الأجهزة التي تساعد على حجب المتسللين والفيروسات والديدان التي تحاول الوصول إلى جهاز الحاسوب الخاص بالفرد عبر الإنترنت، تمر جميع الرسائل التي تدخل الإنترنت أو تغادرها عبر جدار الحماية ومن ثم تؤدي جدران الحماية دورًا مهمًا في اكتشاف البرامج الضارة.

- ✓ **برامج مكافحة الفيروسات**: هي برامج حاسوب تكتشف وتمنع وتتخذ إجراءات وقف البرامج الضارة أو إزالتها، مثل الفيروسات والديدان، تتضمن معظم برامج مكافحة الفيروسات ميزة التحديث التلقائي التي تمكنها من تنزيل ملفات تعريف الفيروسات الجديدة حتى يتمكن من التحقق من الفيروسات الجديدة بمجرد اكتشافها، وبرامج مكافحة الفيروسات أمر لابد منه وضرورة أساسية لكل نظام حالي، والذي يفحص كل رسالة ويحظر تلك التي لا تفي بمعايير الأمان المحددة.

(ل) مخاطر وتهديدات الأمن السيبراني

تتمثل مخاطر وتهديدات الأمن السيبراني في الهجمات السيبرانية التي تقوض من قدرات وظائف الشبكة المعلوماتية من خلال استغلال أحد نقاط الضعف، ما يمنح المهاجم القدرة على التلاعب بالنظام، وهي عملية الاستغلال المتعمد لأنظمة الكمبيوتر والشبكات المعتمدة على التكنولوجيا من خلال البرمجيات الضارة، ويمكن حصر أهم هذه التهديدات كما ذكرها كل من (مشاعل بنت شبيب بن مطيران الظويفري، ٢٠٢١م، ص٦٣٧)، و(عايدة عبد الكريم العيدان، بدور مسعد المسعد، ٢٠٢٤م، ص٤١٥) في الآتي:

- **الأنشطة غير المصرح بها**: التي تستهدف مسح أو تعديل أو إعاقة نظام التشغيل، وتشمل جرائم الدخول غير المشروع إلى نظام معلوماتي أو المكوث فيه، مع التعرض للبيانات المعلوماتية وإعاقة عملها، وقد تتضمن الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح، أو ترخيص مسبق يتيح القيام بالمعالجة، وإنشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليها.
- **البرمجيات الخبيثة**: وتتمثل في التخمين والخداع والبرمجيات الخبيثة، والنفاذ لملف تخزين كلمات المرور والتحكم بالأجهزة.

- **محاولات الاختراق**: وتستهدف هذه الهجمات البنية التحتية للنظام من شبكات اتصالات وأغذية وصرافة، فكلما كانت البُنى التحتية مرتبطة بشكل كبير بالإنترنت كان تأثير هذه الهجمات أقوى على النظام، وتحاول المنظمات تشديد الرقابة على الكهرباء لكونها المشغل الرئيسي لكل الأنظمة، ويجب أن يكون هناك خطط منظمة لحماية البنى التحتية من أي هجوم.
- **الاحتيال الإلكتروني**: وهو نوع من أنواع النصب على الضحية، ويتخذ الاحتيال الإلكتروني أشكالا متعددة؛ منها إيهام الضحية (المجني عليه) بوجود مشروع كاذب، وقد يتخذ اسم أو صفة كاذبة، تمكنه من الاستيلاء على الضحية؛ فيتم التواصل مع الضحية من خلال اتصال الجاني بالضحية عن طريق الشبكة، أو قد يتعامل الجاني مباشرة مع بيانات الحاسب، فيستعمل البيانات الكاذبة التي تساعده في الخداع والاحتيال عليه.

- **انتحال اسم المجال**: يستغل هذا النوع من الهجمات أوجه القصور في بروتوكولات الاستقبال والإرسال لمحاولة التسلل إلى النظام؛ حيث إن آلية عمل معظم البروتوكولات تعد من المعلومات العامة التي يسهل على الجميع معرفتها، فتشمل الهجمات إعادة توجيه الرسائل، أو منع إرسالها إلى طرف معين.
- **الدخول والتعديل**: تتضمن هذه الجرائم كل من قدم أو أنتج أو وزع أو حاز بغرض الاستخدام جهازًا أو برنامجًا معلوماتيًا، أو أي بيانات معلوماتية معدة، أو كلمات سر أو أكواد دخول؛ وذلك بغرض اقتراف الجرائم السيبرانية.
- **هجمات مستهدفة**: هو القيام باختراق شبكة أو جهاز إلكتروني؛ بهدف سرقة المعلومات المخزنة فيه، والتي عادة ما تكون على درجة كبيرة من الأهمية، سواءً أكانت معلومات عسكرية، أم اقتصادية، أم صناعية، أم تجارية، أم غيرها، وهو ما يترتب عليه آثار استراتيجية فادحة في الطرف المستهدف.
- **تسريب البيانات**: إن أشهر الجرائم انتشارًا هي جرائم الدخول غير المشروع إلى البريد الإلكتروني للآخرين، وإنشاء مواقع للتشهير.

- **الهندسة الاجتماعية (اختراق العقول)**: تشير إلى عملية التلاعب بالبشر وخداعهم بهدف الحصول على بيانات أو معلومات؛ كانت ستظل خاصة وآمنة، ولا يمكن الوصول إليها بهدف اختراق النظام. فهي مجموعة من الأساليب التي يستخدمها الجناة لإقناع الضحايا بتنفيذ بعض الإجراءات التي تساعد على اختراق أنظمتهم والإضرار بها.
- **التنمر الإلكتروني**: يُقصد به استخدام تكنولوجيا الاتصالات لأغراض الإيذاء كالتحرش والمضايقة والإزعاج، والتهديد، والابتزاز، وقد انتشر التنمر الإلكتروني كأحد أشكال المخاطر السيبرانية بصورة كبيرة مع انتشار الأجهزة اللوحية والهواتف الذكية.
- **التشهير الإلكتروني**: الذي يقوم على بث أفكار وأخبار من شأنها الإضرار الأدبي أو المعنوي بشخص أو جهة معينة.
- **التصيد الإلكتروني**: وهو أحد أشكال الجرائم السيبرانية يتم من خلاله استهداف المستخدمين وخداعهم للحصول على معلوماتهم الحساسة وسرقة أموالهم وابتزازهم.
- **الإرهاب الإلكتروني**: وهو إحداث الخوف والاضطرابات وزعزعة الأمن والأمان في نفوس الناس من خلال بث الأخبار المحبطة والمسيئة، ونشر الشائعات بغرض الحصول على الأنباء الصحيحة التي تخص هذا الموضوع.
- **التغرير والاستدراج**: حيث يوهم الجناة ضحاياهم من الصغار برغبتهم في تكوين علاقة صداقة على الإنترنت؛ لاستغلالهم وابتزازهم.
- **التجسس الإلكتروني**: حيث يتم بواسطة برامج معينة تقوم بالحصول سرًا على معلومات تخص المستخدم، ومراقبة حركته، ومن ثم يقوم بنقل هذه المعلومات إلى الجهة التي تريد مهاجمته.

(م) تحديات الأمن السيبراني

يواجه الأمن السيبراني العديد من التحديات، منها ما يلي **(ADEJUWON, F. E., & OJEAGBASE, I. O., 2023, PP.166-167):**

١. **الجرائم الإلكترونية**: إن تزايد الجرائم الإلكترونية، بما في ذلك القرصنة واختراق البيانات وهجمات برامج الفدية وسرقة الهوية، لا يعرض خصوصية الأفراد وأمنهم للخطر فحسب، بل يؤثر أيضًا على الشركات والحكومات والبنية التحتية الحيوية. ويمكن لهذه الهجمات أن تعطل الخدمات الأساسية، وتهدد البيانات الحساسة، وتقوض الثقة في الأنظمة الرقمية، وتعطيل الصناعة والابتكار والبنية التحتية. بالإضافة إلى ذلك، يمكن أن تؤدي خروقات البيانات التي تعرض المعلومات الشخصية للخطر إلى سرقة الهوية والخسائر المالية.

٢. **الفجوة الرقمية**: تشير الفجوة الرقمية إلى التفاوت في الوصول إلى التكنولوجيا واستخدامها بين مختلف السكان. ويمكن أن يؤدي عدم كفاية الوصول إلى التكنولوجيا ومحو الأمية الرقمية إلى جعل بعض الفئات أكثر عرضة للتهديدات السيبرانية.

٣. **التقنيات الناشئة**: تقدم التطورات السريعة في التقنيات الناشئة مثل الذكاء الاصطناعي وإنترنت الأشياء والبلوك تشين فرصًا وتحديات. وفي حين يمكن لهذه التقنيات أن تعزز الإنتاجية والكفاءة، فإنها تقدم أيضًا مخاطر جديدة للأمن السيبراني. ويمكن استغلال تدابير الأمن غير الكافية والثغرات في هذه التقنيات من قبل الجهات الفاعلة الخبيثة.

٤. **التهديدات الداخلية**: تنشأ التهديدات الداخلية من أفراد داخل منظمة يسيئون استخدام امتيازات الوصول الخاصة بهم أو يعرضون الأمن للخطر عمدًا. يمكن أن يشمل ذلك الموظفين أو المتعاقدين أو الشركاء ذوي النوايا الخبيثة أو أولئك الذين يخلقون نقاط ضعف عن غير قصد من خلال الإهمال أو الافتقار إلى الوعي، والمساس بسلامة البيانات والسرية والثقة.

٥. **التعاون الدولي**: لا تقتصر التهديدات السيبرانية على الحدود الجغرافية، مما يجعل التعاون الدولي أمرًا بالغ الأهمية للأمن السيبراني الفعال. ومع ذلك، فإن الاختلافات في الأطر القانونية،

والقضائية، والتوترات الجيوسياسية يمكن أن تعيق التعاون وتبادل المعلومات بين الدول لمعالجة التهديدات السيبرانية عبر الحدود.

(ن) كيفية التغلب على تحديات الأمن السيبراني

هناك أمور عديدة إذا تم مراعاتها وتطبيقها يمكن في هذه الحالة الوقاية من تحديات الأمن السيبراني ومواجهته، ومن هذه الأمور ما يلي (بدر عدنان أحمد سعد محمد الخبيزي، ٢٠٢٣م، ص ص٢٤٧-٢٤٨):

١. **الأشخاص**

- ضرورة عقد دورات تدريبية للمستخدمين في مجال الأمن السيبراني، على أن تتناول مفاهيم وأهداف وأهمية وفوائد وأنواع الأمن السيبراني، والتحديات التي تواجهه وكيفية التغلب عليها.
- ضرورة عقد ورش عمل حول إجراءات الحماية ضد تحديات وتهديدات ومخاطر الأمن السيبراني تحت إشراف مدربين مختصين في الأمن السيبراني.
- يجب على المستخدمين فهم المبادئ الأساسية لأمان البيانات والمعلومات والامتثال إليها مثل اختيار كلمات مرور قوية، والحذر من المرفقات الموجودة ضمن البريد الإلكتروني والنسخ الاحتياطي للبيانات.

٢. **العمليات**

- ✓ يجب أن تمتلك المؤسسات إطار عمل حول كيفية التعامل مع الهجمات السيبرانية غير المكتملة أو الناجحة.
- ✓ وضع إطار عمل موحد يوضح كيف يمكن للفرد تحديد الهجمات السيبرانية وحماية الأنظمة، واكتشاف التهديدات والتصدي لها، والتعافي من الهجمات الناجحة.

٣. التقنية

- توفير التكنولوجيا هو أمر ضروري لمنح المؤسسات والأفراد أدوات الأمن السيبراني اللازمة لحماية أنفسهم من الجرائم والهجمات السيبرانية.
- يجب أن توجه الحماية للكيانات التالية: الأجهزة الطرفية مثل أجهزة الحاسوب، والأجهزة الذكية، والموجهات، والشبكات، والسحابة.
- ومن أشكال التكنولوجيا الشائعة المستخدمة لحماية هذه الكيانات، الجيل التالي من الجدران النارية وتصفية DNS، والحماية ضد البرامج الضارة، وبرامج مكافحة الفيروسات، وحلول أمان البريد الإلكتروني.

٤. المجتمع

- ضرورة توعية المجتمع بأهمية الأمن السيبراني وبأساليب الحماية من التهديدات والمخاطر التي تواجه الأمن السيبراني، وذلك من خلال الاتصال الجماهيري وخاصة التلفاز والصحف.
- ضرورة تشجيع المواطنين عن الإبلاغ عن الجرائم السيبرانية.
- ضرورة وضع وتطوير تشريعات حديثة لمكافحة الهجمات والجرائم السيبرانية.
- إعداد مصفوفة للمعايير الأخلاقية فيما يتعلق باستخدام النظم الإلكترونية.
- تخصيص اختصاص قضائي خاص بهذه النوعية من الهجمات والجرائم السيبرانية.
- ضرورة التنسيق بين الأجهزة الأمنية لمكافحة الهجمات والجرائم السيبرانية.
- إنشاء مراكز وطنية مسئولة عن حماية الأمن السيبراني للدولة وتدعيمها بالخبراء من مختلف التخصصات المرتبطة.

(س) متطلبات تطبيق الأمن السيبراني

هناك عدة عناصر ضرورية ومتطلبات مهمة لتطبيق الأمن السيبراني، يمكن إجمالها على النحو الآتي (خالد مخلف الجنفاوي، ٢٠٢١م، ص٨٦):

- **العناصر المادية (Hardware):** وهي عبارة عن الأجهزة والقطع الفنية والإلكترونية والأدوات المادية التي تمثل البنية التحتية الأساسية اللازمة لتشغيل نظم المعلومات.
- **العناصر البرمجية (Software):** وهي المكونات غير المادية والتي تشتمل على النظم والبرمجيات الأساسية والمطلوبة لتشغيل نظم المعلومات.
- **القوى البشرية (Human Resources):** تمثل الأفراد الأكفاء وذوي المهارات في مجال تكنولوجيا المعلومات ونظم المعلومات، الذين يقع على عاتقهم تشغيل النظم وإدامتها في المنظمة.
- **دعم الإدارة العليا لعملية تطبيق نظم المعلومات:** يجب أن يكون هناك اقتناع كامل ودعم مطلق من الإدارة العليا لعمليات تطبيق نظم المعلومات في المنظمة، وعدم تعجل النتائج إلى حين اكتمال حلقة الحوسبة أو الأتمتة للعمليات والوظائف الإدارية في المنظمة.
- **إعادة تصميم الهيكل التنظيمي لتلبية متطلبات تكنولوجيا المعلومات:** وهي عملية إعادة ووصف للوظائف الموجودة في المنظمة، وما يتبعه من إلغاء او استحداث الوظائف على أسس حديثة تأخذ بعين الاعتبار التطورات التكنولوجية المتسارعة واحتياجات تطبيق نظم المعلومات.
- **الشبكات والاتصالات:** وهي الوسيلة التي يتم من خلالها مرور البيانات من مكان لآخر.

ولتحقيق هذه المتطلبات لابد من اتباع مجموعة من الإجراءات لتعزيز الأمن السيبراني، والتي سيتم توضيحها فيما يلي:

(ع) إجراءات تعزيز الأمن السيبراني لطالبات الجامعة

قد تساعد الخطوات البسيطة أدناه طالبات الجامعة في الحفاظ على مستوى جيد من الأمان والسلامة السيبرانية (منى عبد الله السمحان، ٢٠٢٠م، ص١٦):

- **الموثوقية**: وتعني استخدام المواقع الموثوق بها عند تقديم معلومات شخصية، والقاعدة الأساسية هي التحقق من عنوان **.URL**، وإذا كان الموقع يتضمن **https** في بدايته، فهذا يعني أنه موقع آمن، أما إذا كان عنوان **.URL** يحتوي على **http** بدون s؛ فيجب الحذر من إدخال أي معلومات حساسة مثل بيانات بطاقة الائتمان، أو رقم التأمين الاجتماعي... إلخ.
- **البريد الاحتيالي**: ويعني عدم مرفقات البريد الإلكتروني أو النقر فوق روابط الرسائل من المصادر غير المعروفة؛ إذ إن إحدى الطرق الأكثر شيوعًا التي يتعرض فيها الأشخاص للسرقة أو الاختراق هي عبر رسائل البريد الإلكتروني المتخفية على أنها مرسلة من شخص موثوق به.
- **التحديثات**: وتعني الحرص على تحديث الأجهزة؛ فغالبًا ما تحتوي تحديثات البرامج على تصحيحات مهمة لإصلاح مشكلات الأمان، وإن هجمات المخترقين الناجحة تتركز على الأجهزة القديمة بنسبة كبرى، والتي لا تملك أحدث برامج الأمان.
- **النسخ الاحتياطي**: ويتطلب هذا عمل نسخ احتياطية من الملفات بانتظام لمنع هجمات الأمان على الإنترنت.

كما أن هناك العديد من الإجراءات التي يمكن لكل مستخدم للإنترنت ولرواد الفضاء السيبراني اتخاذها، ومن هذه الإجراءات ما ذكره كل من (فاطمة يوسف المنتشري، ٢٠٢٠م، ص٤٦٧)، و **(Odaibat, A. A., & Eyadah, H. T. A., 2024, P.8)** فيما يلي:

١. المحافظة على تحديث جدران الحماية، والتي تمثل أنظمة الدفاع عن البنية التحتية للبيئة المعلوماتية.

٢. التأكد من إعدادات الحاسوب وشبكة الإنترنت.
٣. اختيار كلمات مرور قوية، وعمليات تحقق أمنية لمواقع التواصل الاجتماعي، والبريد الإلكتروني، والحسابات الشخصية على الحاسوب أو الهواتف الذكية.
٤. عدم الاستجابة لأي رسائل مجهولة المصدر ترد إلى البريد الإلكتروني.
٥. استخدام برامج الحماية ومضادات الفيروسات وتحديثها باستمرار.
٦. حماية المعلومات الشخصية ومنع الآخرين من الاطلاع عليها.
٧. تحديث كلمات المرور بشكل مستمر، على الأقل مرة أو مرتين شهريًا.
٨. عدم إرسال أي معلومات شخصية عبر البريد الإلكتروني، أو الإفصاح عن معلومات خاصة عبر مواقع التواصل الاجتماعي.

مما سبق عرضه يتطلب تحقيق هذه الإجراءات امتلاك طالبات الجامعة للعديد من المهارات، والتي سيتم تناولها فيما يلي:

(ف) المهارات اللازمة لتحقيق الأمن السيبراني

تتمثل المهارات اللازمة التي يجب أن تكتسبها طالبات الجامعة لتحقيق الأمن السيبراني في ثلاث مهارات رئيسة، وهي (محمد إبراهيم عبده السيد، وليد سعيد أحمد سيد، ٢٠٢٢م، ص ص٣٦٢-٣٦٣):

١. **مهارات الأمن السيبراني الشخصية**: وهي المهارات ذات العلاقة بالمستخدم شخصيًا، وترتبط بمعلوماته، وبياناته الشخصية، وسلوكه، وأسلوب تعامله أثناء استخدام الأجهزة الإلكترونية وشبكة الإنترنت، وتتمثل هذه المهارات في:

- **حماية المعلومات الشخصية (الخصوصية)**: وتتضمن الوعي بأهمية حفظ المعلومات الشخصية، والصور الخاصة أثناء استخدام الإنترنت، وتعرف أضرار كشف المعلومات الشخصية على المستخدم، وإدراك أهمية حذف الملفات الشخصية عند التخلص من الجهاز.
- **الحماية من الاحتيال وسرقة الهوية**: وتتضمن إدراك أهمية العناية باختيار اسم المستخدم وكلمة المرور، وتعرف أنواع الاحتيال الإلكتروني، والوعي بخطورة نشر المعلومات الخاصة في برامج الألعاب المباشرة، وإدراك إمكانية إبلاغ الجهات المعنية بمحاولات الاحتيال والتصيد الإلكتروني.
- **مواجهة التسلط عبر الإنترنت**: وتتضمن فهم مصطلح التسلط الإلكتروني، ومعرفة كيفية مواجهته، والوعي بأهمية رفض الرسائل والدعوات المشبوهة عبر الإنترنت، وإدراك مخاطر مقابلة جهات الاتصال التي يتم التعرف عليها عن طريق الإنترنت.
- **الحماية من إدمان الإنترنت**: وتتضمن تعرف تأثير الإنترنت على الحياة اليومية والعمل والعلاقات الاجتماعية، وتعرف الأضرار الصحية والعقلية والنفسية، التي يسببها الجلوس والبقاء طويلًا أمام شبكة الإنترنت، وإدراك التأثيرات السلبية لإدمان الألعاب الإلكترونية.
- **التعامل مع المحتوى المعلوماتي على الإنترنت**: وتتضمن القدرة على تقييم مصادر المعلومات عبر الإنترنت، والوعي بأساليب التعامل مع المحتوى غير الملائم عبر الإنترنت، وإدراك مخاطر التعامل مع المواد الإباحية عبر الإنترنت، والتمييز بين العلم النافع والعلم الضار على شبكة الإنترنت.

٢. **مهارات الأمن السيبراني التكنولوجية**: وهي المهارات ذات العلاقة بالحماية المادية للأجهزة والبيانات، والتي ترتبط بالإجراءات التقنية في تعامل المستخدم مع الأجهزة الإلكترونية والشبكات، وتتمثل هذه المهارات في:

- ✓ **المفاهيم الأساسية للأمن الرقمي**: وتتضمن فهم مصطلحات الأمن السيبراني (البيانات والمعلومات، أمن المعلومات، حماية الأجهزة، جرائم الإنترنت)، والتعرف على التهديدات التي تتعرض لها الأجهزة والبيانات، وإدراك أهمية أمن المعلومات في الحياة المعاصرة.
- ✓ **الحماية من الفيروسات**: وتتضمن إدراك مفهوم الفيروسات، وأسباب إصابة الحاسوب بها، وتعرف طرق حماية الأجهزة منها، والأسلوب الأمثل لاستخدام برامج مكافحتها.
- ✓ **الحماية من البرمجيات الخبيثة**: وتتضمن فهم مصطلح البرمجيات الخبيثة، وتعرف أنواعها، ودوافع تطوير واستخدام البرمجيات الخبيثة، وإدراك طرق الحماية منها، والقدرة على التعامل معل ملفات تعريف الارتباط، والإعلانات المنبثقة، والبريد الإلكتروني المزعج.
- ✓ **الاستخدام الآمن للشبكات**: وتتضمن تعرف أنواع الشبكات الشائعة، وإدراك المزايا والمخاطر المرتبطة باستخدام شبكات الحاسب الآلي، والقدرة على التعامل مع الشبكات اللاسلكية بطريقة آمنة، وتعرف طرق منع الوصول غير المصرح به إلى الجهاز والبيانات.
- ✓ **حماية الأجهزة والنسخ الاحتياطي للبيانات**: وتتضمن تعرف تأثير البيئة المحيطة على الأجهزة الإلكترونية، وإدراك أهمية النسخ الاحتياطي للبيانات، وإدراك أهمية إزالة البيانات غير المرغوب فيها.

٣. **مهارات الأمن السيبراني الاجتماعية**: وهي المهارات ذات العلاقة بتأثير الأجهزة الإلكترونية وشبكة الإنترنت على المجتمع، وعلاقة المستخدم بالمجتمع الرقمي المحيط به، وتتمثل هذه المهارات في:

- ➢ **الوعي بالمخاطر المحتملة لاستخدام مواقع التواصل الاجتماعي**: وتتضمن تعرف مميزات مواقع التواصل الاجتماعي، والآثار السلبية لاستخدامها، والوعي بالآثار المترتبة على نشر المعلومات والرسائل عبر المنصات الاجتماعية وتأثيرها على سمعة المستخدم.

- **الحماية من الجماعات التي تدعو إلى التطرف والعنف**: وتتضمن فهم مصطلح الإرهاب والتطرف الإلكتروني، والوعي بأساليب الجهات المشبوهة في شبكة الإنترنت؛ لجذب الشباب نحو ارتكاب أعمال غير قانونية، والوعي بطرق التصدي لتأثيرات الجماعات الإرهابية.
- **الالتزام بالسلوك الاجتماعي والأخلاقي الرقمي**: وتتضمن المحافظة على آداب التعامل والنشر على الإنترنت، وتجنب الكتابة بما يسيء للآخرين عبر الإنترنت، وتقديم الخدمات للمجتمع عبر الحاسب الآلي.
- **احترام حقوق النشر الإلكتروني**: وتتضمن فهم مصطلح حقوق النشر والتأليف، والتمييز بين المحتوى المجاني، والمحتوى الذي يحمل حقوق التأليف والنشر، وتعرف الآثار السلبية لتحميل المحتوى بشكل غير مشروع، واحترام حقوق الملكية الفكرية للآخرين.

إجمالا لما سبق عرضه يتضح أهمية امتلاك طالبات الجامعة لمهارات الأمن السيبراني من أجل مواجهة العنف الرقمي، والذي يُعد قضية حيوية تهدد الصحة النفسية والاجتماعية لهن. فمن الضروري تعزيز الوعي لديهن وتعليمهن كيفية التعامل مع هذه التهديدات عبر الإنترنت. كما ينبغي أن تسعى الجامعات إلى إنشاء بيئة رقمية آمنة، مما يتطلب تكامل الجهود بين الجهات التعليمية، القانونية، والاجتماعية لمكافحة هذا النوع من العنف.

ونظرًا لدور الجامعة المهم في مواجهة العنف الرقمي ضد الطالبات، فسيتم تناول الجهود التي تبذلها جامعة القاهرة في ذلك كما يلي:

المحور الثالث: جهود جامعة القاهرة في مواجهة العنف الرقمي ضد الطالبات

تُعد جامعة القاهرة مركزًا رئيسًا للتعليم العالي؛ حيث تقدم برامج تعليمية متميزة في مختلف المجالات العلمية والإنسانية. إلى جانب دورها في تقديم التعليم، تُسهم بشكل كبير في البحث العلمي من خلال مشاريع وأبحاث تهدف إلى حل القضايا المجتمعية والتحديات الإقليمية. كما تتمتع الجامعة بعلاقات أكاديمية دولية واسعة، مما يعزز من مكانتها كأحد أبرز مراكز الفكر والتعليم في العالم العربي.

كما تؤدي جامعة القاهرة دورًا محوريًا في مواجهة العنف الرقمي ضد الطالبات، من خلال تبني سياسات ومبادرات تهدف إلى حماية حقوق الطالبات والطلاب على حد سواء ورفع الوعي حول أبعاد هذه القضية. وتهتم الجامعة بتوفير بيئة تعليمية آمنة لجميع الطلاب، خاصة الطالبات، عبر إنشاء برامج توعوية وتدريبية تُسهم في تعزيز مفاهيم الحماية الرقمية وتطوير مهارات استخدام التكنولوجيا بشكل آمن. كما تسعى الجامعة إلى وضع آليات للتعامل مع حالات العنف الرقمي من خلال دعم قانوني ونفسي للمتضررات. من خلال هذه الجهود، تعمل جامعة القاهرة على تعزيز ثقافة الاحترام والمساواة، وتوفير بيئة تعليمية خالية من أي أشكال للعنف، مما يُسهم في تمكين الطالبات في جميع المجالات الأكاديمية والمهنية.

ومن أبرز جهود جامعة القاهرة في مواجهة العنف الرقمي ضد الطالبات، ما يلي:

- **إنشاء وحدة مناهضة العنف ضد المرأة بجامعة القاهرة:**

أسست وحدة مناهضة العنف ضد المرأة بجامعة القاهرة في عام ٢٠١٤م، وتُعد أول وحدة رسمية لمناهضة التحرش والعنف في الجامعات المصرية. وبادرت بإصدار سياسة لمناهضة التحرش في الجامعات المصرية من أجل توفير بيئة جامعية آمنة للجميع. وتقوم هذه السياسة على محورين **(https://cu.edu.eg/ar/anti-violence):**

١. اتخاذ التدابير اللازمة للتعامل مع فعل التحرش في حالة حدوثه.

٢. معالجة الآثار المترتبة عليه، والتي تركز على اتخاذ إجراءات للوقاية والتوعية ضد التحرش في المجتمع الأكاديمي من خلال تقديم الدعم النفسي والقانوني.

❖ **إنشاء مركز الدعم النفسي وإعادة بناء الذات بجامعة القاهرة:**

يقدم مركز الدعم النفسي وإعادة بناء الذات بجامعة القاهرة خدمات الدعم النفسي للطلاب والطالبات الذين يتعرضون لأي شكل من أشكال العنف، وذلك بالمجان، وفي سرية تامة؛ حيث يساعد في العلاج النفسي والسلوكي، ويسهم في زيادة فعالية الطلاب والطالبات، وقدرتهم على مقاومة الأمراض النفسية، وتحديات الحياة وضغوطها

.(https://cu.edu.eg/old/ar/Cairo-University-News-15153.html)

إجمالا لما سبق عرضه تبرز أهمية الأمن السيبراني في حماية طالبات الجامعة من العنف الرقمي الذي قد يمارس ضدهن، لذا سيتناول الجزء التالي تعرف مستوى وعي طالبات جامعة القاهرة بثقافة الأمن السيبراني لمواجهة العنف الرقمي.

الجزء الثاني: الجانب الميداني للبحث

يتناول الجزء التالي البحث الميداني من حيث إجراءاته، والتي تشمل هدف البحث الميداني، ومجتمع البحث، وعينة البحث، وتحديد خصائصها، وتصميم أداة البحث وتقنينها، ونتائج البحث الميداني من حيث التحليل والتفسير.

أولًا: إجراءات البحث الميداني

فيما يلي عرض لأبرز إجراءات البحث الميداني، وذلك على النحو التالي:

١. هدف البحث الميداني:

يهدف البحث الميداني إلى تعرف مستوى وعي طالبات جامعة القاهرة بثقافة الأمن السيبراني لمواجهة العنف الرقمي.

٢. مجتمع البحث:

يتكون مجتمع البحث الذي سحبت منه العينة من جميع طالبات جامعة القاهرة البالغ عددهم (٩٨٨٨٤) طالبة، والمقيدات بالعام الجامعي ٢٠٢٤/ ٢٠٢٥م (جمهورية مصر العربية، الجهاز المركزي للتعبئة العامة والإحصاء، نوفمبر٢٠٢٤م، ص٢٦).

٣. عينة البحث (اختيارها، وخصائصها)

أ. اختيار عينة البحث:

تم اختيار عينة عرضية/ متاحة من طالبات جامعة القاهرة بالمرحلة الجامعية الأولى من كليات (الآداب، التجارة، الإعلام، دار العلوم) كنماذج للكليات النظرية، ومن كليات (العلوم، والحاسبات والذكاء الاصطناعي) كنماذج للكليات العملية. بالإضافة إلى عينة من طالبات كلية الدراسات العليا للتربية بجامعة القاهرة كنموذج لطالبات الدراسات العليا.
أما قوام العينة فقد بلغ (١٢٤) طالبة بالفرق الدراسية المختلفة (أولى، ثانية، ثالثة، رابعة، دراسات عليا).

ب. خصائص عينة البحث:

روعي أن تكون عينة البحث ممثلة لمتغيرات الفرقة الدراسية، وطبيعة الدراسة، والكليات، ويتضح ذلك كما في الجداول التالية:

جدول (٢) :توزيع النسبة المئوية للطالبات حسب متغير الفرقة الدراسية

الفرقة الدراسية	التكرار (ك)	النسبة المئوية
أولى	١٧	١٣,٧٪
ثانية	١٦	١٢,٩٪
ثالثة	١٩	١٥,٣٪
رابعة	٢٤	١٩,٤٪
دراسات عليا	٤٨	٣٨,٧٪
المجموع	١٢٤	١٠٠٪

باستقراء بيانات الجدول السابق يتضح أن النسبة المئوية لطالبات الفرقة الأولى ١٣,٧٪، بينما جاءت النسبة المئوية لطالبات الفرقة الثانية ١٢,٩٪، وجاءت النسبة المئوية لطالبات الفرقة الثالثة ١٥,٣٪، وجاءت النسبة المئوية لطالبات الفرقة الرابعة ١٩,٤٪، بينما جاءت النسبة المئوية لطالبات الدراسات العليا ٣٨,٧٪.

جدول (٣): توصيف عينة البحث وفقًا لطبيعة الدراسة

طبيعة الدراسة	التكرار (ك)	النسبة المئوية
نظرية	١٠٠	٨٠,٦٪
عملية	٢٤	١٩,٤٪
المجموع	١٢٤	١٠٠٪

باستقراء بيانات الجدول السابق يتضح أن عينة البحث من الكليات النظرية تتكون من (١٠٠) طالبة بنسبة مئوية ٨٠,٦٪، و(٢٤) طالبة من الكليات العملية بنسبة مئوية ١٩,٤٪.

جدول (٤): توصيف عينة البحث وفقًا للكليات

الكليات	التكرار (ك)	النسبة المئوية
آداب	١٦	١٢,٩٪
تجارة	١٤	١١,٣٪
إعلام	١٢	٩,٧٪
دار العلوم	١٠	٨,١٪
العلوم	١٧	١٣,٧٪
الحاسبات والذكاء الاصطناعي	٧	٥,٦
الدراسات العليا للتربية	٤٨	٣٨,٧٪
المجموع	١٢٤	١٠٠٪

باستقراء بيانات الجدول السابق يتضح أن النسبة المئوية لطالبات كلية الآداب ٩ , ١٢٪، بينما جاءت النسبة المئوية لطالبات كلية التجارة ٣ , ١١٪، وجاءت النسبة المئوية لطالبات كلية الإعلام ٧ , ٩٪، وجاءت النسبة المئوية لطالبات كلية دار العلوم ١ , ٨٪، وجاءت النسبة المئوية لطالبات كليتي العلوم والحاسبات والذكاء الاصطناعي ٧ , ١٣٪، ٦ , ٥٪ على الترتيب، في حين جاءت النسبة المئوية لطالبات كلية الدراسات العليا للتربية ٧ , ٣٨٪ واللاتي يمثلن طالبات الدبلوم العامة من عدة تخصصات مختلفة (دراسات اجتماعية- مواد تجارية- لغات إنجليزية وفرنسية).

جدول (٥): توصيف عينة البحث وفقًا لعدد الساعات التي تقضيها على مواقع التواصل الاجتماعي يوميًا

عدد الساعات	التكرار (ك)	النسبة المئوية
أقل من ساعة	١٨	١٤ , ٥٪
من ساعة إلى ٣ ساعات	٤٢	٣٣ , ٩٪
أكثر من ٣ ساعات	٦٤	٥١ , ٦٪
المجموع	١٢٤	١٠٠٪

باستقراء بيانات الجدول السابق يتضح زيادة عدد الساعات التي تقضيها الطالبات على مواقع التواصل الاجتماعي يوميًا، حيث بلغت النسبة المئوية لعدد الساعات أكثر من ٣ ساعات ٥١ , ٦٪، مما قد يعرضهن للمضايقات والعنف الرقمي، وهذا يتطلب زيادة الوعي بكيفية الاستخدام الأمثل لهذه المواقع، ومعرفة الاحتياطات والتدابير اللازمة لحماية المعلومات الشخصية عبر الإنترنت.

جدول (٦): توصيف عينة البحث وفقًا لنوعية مواقع التواصل الاجتماعي الأكثر استخدامًا لها

النوعية	التكرار (ك)	النسبة المئوية
الفيسبوك	٥٧	٤٥,٩٪
الواتساب	٤٣	٣٤,٧٪
مواقع أخرى كـ (تويتر، انستجرام، تليجرام،...)	٢٤	١٩,٤٪
المجموع	١٢٤	١٠٠٪

باستقراء بيانات الجدول السابق يتضح تعدد وتنوع مواقع التواصل الاجتماعي وكثرة استخدامها، وجاء في مقدمتها الفيسبوك حيث بلغت النسبة المئوية له ٤٥,٩٪ كأكثر مواقع التواصل الاجتماعي استخدامًا، يليها الواتساب بنسبة مئوية ٣٤,٧٪، يليها مواقع أخرى كـ (تويتر، انستجرام، تليجرام،....) بنسبة مئوية ١٩,٤٪.

جدول (٧): توصيف عينة البحث وفقًا للحصول على دورات في الأمن السيبراني

الحصول على دورات في الأمن السيبراني	التكرار (ك)	النسبة المئوية
نعم	١٨	١٤,٥٪
لا	١٠٦	٨٥,٥٪
المجموع	١٢٤	١٠٠٪

باستقراء بيانات الجدول السابق يتضح نقص الوعي بأهمية الحصول على دورات في الأمن السيبراني؛ حيث بلغت نسبة من حصلوا فقط من الطالبات عينة البحث على دورات في الأمن السيبراني ١٤,٥٪، واقتصرت نوعية هذه الدورات عن (أمن الشبكات- مقدمة في الأمن السيبراني- التحول الرقمي- تكنولوجيا المعلومات- البرمجة). مما يستلزم ضرورة توعية الطالبات بأهمية الحصول على دورات في الأمن السيبراني حتى يستطعن حماية أنفسهن من العنف الرقمي، وهذا يستلزم قيام الجامعة بدورها من خلال توفير المزيد من الدورات والبرامج التدريبية في مجال الأمن السيبراني وما يرتبط به.

ثانيًا. أداة البحث الميداني

اعتمد البحث الحالي على استخدام أداة المقابلة، وكان إعدادها على النحو التالي:

أ. خطوات إعداد أداة المقابلة

١. الاطلاع على الأدبيات الخاصة بالأمن السيبراني والعنف الرقمي، من خلال الكتب والمراجع والبحوث، والدراسات النظرية والميدانية ذات الصلة بمجال وموضوع البحث.

٢. تصميم أداة المقابلة في صورتها الأولية، وعرضها على مجموعة من الأساتذة المحكمين، والذين قاموا بدورهم بتحكيم الأداة، وتقديم التوجيهات والتعديلات اللازمة على أسئلتها.

٣. بعد استعادة أداة المقابلة من الأساتذة المحكمين قامت الباحثة بإجراء التعديلات المقترحة سواء بالحذف أو التعديل أو الإضافة على أسئلتها، ومن ثم وضع أداة المقابلة في صورتها النهائية وتطبيقها.

ب. وصف أداة المقابلة

تتكون أداة المقابلة من عدد (١٠) أسئلة، مقسمة في محورين: أسئلة تتعلق بفهم الأمن السيبراني، وأسئلة تتعلق بالعنف الرقمي.

المحور الأول: أسئلة تتعلق بفهم الأمن السيبراني: وتنص على:

١. ما مفهوم الأمن السيبراني من وجهة نظرك؟

٢. ما أهمية الأمن السيبراني من وجهة نظرك؟

٣. ما المهارات التي تمتلكينها في الأمن السيبراني؟

٤. ما التدابير التي يمكنك اتخاذها لحماية معلوماتك الشخصية عبر الإنترنت من وجهة نظرك؟

المحور الثاني: أسئلة تتعلق بالعنف الرقمي: وتنص على:

١. ما أشكال العنف الرقمي التي يمكن أن تتعرض لها الطالبات عبر الإنترنت من وجهة نظرك؟

٢. هل تعرضتِ شخصيًا أو تعرفين أحدًا تعرض لأشكال من العنف الرقمي مثل التحرش أو التهديدات عبر الإنترنت؟

نعم ( ) لا ( )، إذا كانت الإجابة نعم، اذكري أهم هذه المواقف التي تعرضت لها أو تعرض لها من تعرفينهم؟

٣. ما الخطوات التي يمكنك اتخاذها إذا تعرضتِ لتهديدات أو مضايقات عبر الإنترنت من وجهة نظرك؟

٤. هل تعلمين عن أهم قوانين مكافحة الجرائم الإلكترونية؟

نعم ( ) لا ( )، إذا كانت الإجابة نعم، اذكري أهم هذه القوانين.

٥. هل تعلمين بوجود وحدة لمناهضة العنف ضد المرأة داخل جامعة القاهرة؟

نعم ( ) لا ( )، إذا كانت الإجابة نعم، اذكري أدوارها.

٦. ما الدور الذي يمكن أن تقوم به الجامعة في مواجهة العنف الرقمي ضد الطالبات من وجهة نظرك؟

ج. تقنين أداة المقابلة

قامت الباحثة بتقنين أداة المقابلة، وذلك بعرضها على عدد (٨) محكمين من الأساتذة المتخصصين بجامعتي القاهرة والأزهر، وذلك لمعرفة آرائهم حول مدى وضوح وملائمة وصياغة عبارات الأسئلة، حيث تكونت أداة المقابلة في صورتها الأولية من (١١) سؤال، وفي ضوء آراء المحكمين وتعديلاتهم عدلت لتصبح (١٠) أسئلة، وقد عدت الباحثة آراء المحكمين وتعديلاتهم

دلالة صدق كافية لأغراض البحث، مثل: تعديل صياغة بعض الأسئلة، أو حذف البعض الآخر، أو إضافة أسئلة أخرى.

ثالثًا: نتائج البحث الميداني (عرضها، وتحليلها، وتفسيرها)

يتناول الجزء التالي نتائج البحث الميداني من حيث عرضها وتحليلها وتفسيرها؛ حيث يهدف هذا البحث إلى تعرف مستوى وعي طالبات جامعة القاهرة بثقافة الأمن السيبراني لمواجهة العنف الرقمي، مما يفيد في بناء التصور المقترح.

❖ **تفسير نتائج المحور الأول: أسئلة تتعلق بفهم الأمن السيبراني**

- **بالنسبة لاستجابات الطالبات حول السؤال الأول: ما مفهوم الأمن السيبراني من وجهة نظرك؟**

يمكن إيجاز أهم آراء الطالبات حول مفهوم الأمن السيبراني، والتي تمحورت فيما يلي:

- الأمن السيبراني هو حماية مستخدمي الإنترنت من العنف الرقمي والتهديدات الواردة من الهاكرز.
- هو القيام ببعض التدابير لحماية الشخص لنفسه من الآخرين أثناء استخدام شبكة الإنترنت؛ من خلال حماية المعلومات الشخصية مثل الاسم والصور الشخصية وبيانات الدفع للبطاقات الذكية.
- هو حماية الطالبات من التعرض إلى مضايقات أو اختراق حسابها على أي منصة رقمية أو التعرض إلى الابتزاز أو التهديد.
- هو نظام لحماية البيانات عبر الإنترنت.
- هو حماية المعلومات الشخصية الدقيقة والعملية لدى الفرد من الهاكر الإلكتروني من تهديدات وخوف، ويتم عن طريق تدابير وقائية لحماية الأشخاص من هذه التهديدات.

- هو أمن المعلومات وعدم انتشارها إلى أي شخص دون إذن، وإخفاء المعلومات تمامًا إذا توفي الشخص.
- هو مجموعة من الأنشطة الموجهة لطالبات الجامعة لتوفير بيئة آمنة لهم.
- هو كل ما يتعلق بتوفير البيئة الآمنة على جميع المستويات (النفسية، الاجتماعية، ...) في حالة استخدام الشبكة العنكبوتية أو أي شبكة تربط عدد معين من الأفراد.
- هو الحفاظ على بيانات ومعلومات الطالبة من الاختراق، لكي يكون هناك سرية المعلومات الخاصة بها.
- هو مجموعة من التقنيات والممارسات المصممة لحماية الأنظمة والشبكات والبرمجيات والبيانات من الهجمات الإلكترونية، والهدف الأساسي هو ضمان سرية المعلومات وحمايتها من الوصول غير المصرح به والحفاظ على سلامة البيانات وضمان توافرها عند الحاجة إليها.
- الاحتفاظ بالبيانات والمعلومات والسرية التامة للسيرة الذاتية الخاصة بي، وتجعلني أشعر بالأمان المعلوماتي.
- هو توفير الأمن للمعلومات الشخصية وحمايتها عبر الإنترنت، وصعوبة الوصول إليها.
- حماية المعلومات الشخصية عبر الإنترنت من التسرب إلى جهات من الممكن أن تسبب أذى لي.
- هو عملية حماية الأنظمة والبيانات والاتصالات والشبكات من الهجمات الرقمية.
- هو محاولة حماية المعلومات الشخصية والعلمية عبر الإنترنت.

- **بالنسبة لاستجابات الطالبات حول السؤال الثاني: ما أهمية الأمن السيبراني من وجهة نظرك؟ حيث أكدت جميع الطالبات على وجود أهمية كبيرة للأمن السيبراني، وتلخصت أهم آراءهن فيما يلي:**

✓ الحفاظ على أمن الإنترنت، وعلى سلامة مستخدميه، والحفاظ على المعلومات السرية والشخصية للمستخدم.

- ✓ الحصول على الأمان عند استخدام الشبكة العنكبوتية، ومواجهة مستجدات أشكال العنف في شتى المجالات.
- ✓ من أفضل طرق الحماية من الاختراق في الإنترنت.
- ✓ حماية الأفراد والجماعات من الاختراقات.
- ✓ حماية البيانات الحساسة.
- ✓ تتمثل أهميته في أن يكون لدى الطالبة وعي، ولا تتعرض إلى عنف أو اختراق في حسابات مواقع التواصل الاجتماعي.
- ✓ الحفاظ على خصوصية البيانات ضد قراصنة الإنترنت.
- ✓ حماية سمعة الأشخاص وعدم مضايقتهم المتعمدة لمعلوماتهم الشخصية والعلمية.
- ✓ حماية الطالبة ضد عنف الإنترنت، وانتشار معلوماتها، والصور الخاصة بها، والتلاعب عليها.
- ✓ توفير بيئة آمنة لطالبات الجامعة، وحماية المعلومات الشخصية عبر الإنترنت.
- ✓ الحفاظ على الخصوصية والمعلومات الشخصية، وعدم استخدام هذه المعلومات فيما ينافي الآداب العامة.
- ✓ حماية المعلومات الشخصية والعلمية عبر الإنترنت.
- ✓ الحفاظ على المعلومات الخاصة بي.
- ✓ حماية البيانات الحساسة، ومنع الوصول غير المصرح به إلى معلومات شخصية مالية وتجارية.
- ✓ ضمان استمرارية الأعمال، وتقليل خطر انقطاع الخدمات الرقمية بسبب الهجمات الإلكترونية.
- ✓ حماية البيانات الخاصة بكل فرد، وعدم تداول معلوماته الشخصية.
- ✓ الحفاظ على معلوماتي وبياناتي.
- ✓ الحماية الآمنة للبيانات والمعلومات.
- ✓ منع سرقة الهوية والحفاظ على السرية.

- ✓ الحماية من المضايقات والممارسات اللاأخلاقية التي تمارس خلال الإنترنت، ومن ثم الجرائم التي تترتب على هذه الممارسات.
- ✓ تجنب المخاطر والتهديدات عبر الإنترنت.
- ✓ حماية الخصوصية والمعلومات الشخصية، ومنع تعطيل البيانات.
- ✓ حماية معلومات الأفراد من التجسس.
- ✓ الحماية من محاولة اختراق البيانات الشخصية.
- ✓ يوفر تدابير وقائية وتوعية لحماية الطالبات من التهديدات والمضايقات.

- **بالنسبة لاستجابات الطالبات حول السؤال الثالث: ما المهارات التي تمتلكينها في الأمن السيبراني؟**

تباينت آراءهن حول هذا السؤال؛ حيث أجمعت آراء عدد كبير من طالبات كليات (الآداب- التجارة- دار العلوم) حول نقص امتلاكهن لمهارات الأمن السيبراني، في حين أكدت طالبات كلية (الحاسبات والذكاء الاصطناعي) على امتلاكهن لمعظم مهارات الأمن السيبراني ومعرفتهن لها نظرًا لطبيعة دراستهن، في حين أجمعت آراء طالبات كليتي (العلوم والإعلام) وطالبات الدبلوم العامة بكلية الدراسات العليا للتربية على معرفتهن المتوسطة لها، ويمكن إيجاز أبرز آراء الطالبات حول المهارات التي يمتلكنها في الأمن السيبراني، والتي تمحورت فيما يلي:

- تجنب عرض الأشياء والمعلومات المهمة على الأجهزة الإلكترونية التي تدعمها الشبكة العنكبوتية، واستخدامها بحرص حتى تسنح الفرصة للتعلم في مجال الأمن السيبراني.
- عدم مشاركة معلوماتي الشخصية عبر شبكة الإنترنت.
- معرفة كيفية التصرف في حالة الاختراق، والرجوع للأمن السيبراني لتقليل الأضرار.
- عدم نشر بيانات شخصية دقيقة جدًا على مواقع التواصل الاجتماعي حتى لا يتم خرقها.
- عادة أقوم بالدخول إلى المواقع البحثية أو غيرها بمعلومات بسيطة.

- عمل رقم سري لجميع حساباتي.
- تأمين حسابي الخاص بي وحمايته من الهاكرز.
- القيام بعملية التشفير للحماية من الاختراق.
- التعرف على التهديدات والحماية منها.
- التشفير عن طريق تحويل بياناتي لشكل غير قابل للقراءة.
- عمل كلمة مرور قوية بحيث يصعب اختراق الهاتف.

- **بالنسبة لاستجابات الطالبات حول السؤال الرابع: ما التدابير التي يمكنك اتخاذها لحماية معلوماتك الشخصية عبر الإنترنت من وجهة نظرك؟**

يمكن إيجاز أهم آراء الطالبات حول هذا السؤال، والتي تمحورت فيما يلي:

- ✓ تفعيل نظام الحماية للمعلومات الشخصية من خلال تطبيقات التواصل الاجتماعي، مثل: انستجرام، فيسبوك، تويتر، تيك توك، وغيرها من التطبيقات.
- ✓ تجنب استخدام المعلومات الخطيرة الخاصة بي.
- ✓ اللجوء للقانون في إيجاد حلول عند مواجهة عنف ما.
- ✓ التوجه مباشرة والتقدم ببلاغ عند الوقوع في مشكلة من هذا القبيل.
- ✓ عدم استخدام مواقع مجهولة الهوية.
- ✓ عدم الرد على رسائل مجهولة.
- ✓ الاضطلاع على كل ما هو جديد في مجال الأمن السيبراني لمواجهة مخاطر العنف الرقمي.
- ✓ عدم استخدام مواقع إلكترونية غير موثوقة أو غير محمية بنظام **[https//]**.
- ✓ استخدام بطاقة بنكية منفصلة للشراء عبر الإنترنت.
- ✓ لا أعطي الرقم السري الخاص بي لأي شخص.
- ✓ عدم الإفصاح عن معلوماتي الشخصية عبر مواقع التواصل الاجتماعي.

- ✓ استخدام رموز الحماية الخاصة بي.
- ✓ عدم وضع صور أو معلومات شخصية تمثلني على الفيسبوك.
- ✓ عدم الولوج إلى المواقع غير المعروفة إلى حد ما.
- ✓ تحديث البرامج بانتظام، وتفعيل المصادقة الثنائية.
- ✓ استخدام بعض برامج الحماية من الفيروسات.
- ✓ لا أفصح بأي معلومات أو صور شخصية أو فيديوهات مع جهة غير معلومة المصدر.
- ✓ استخدام كلمات مرور قوية للحماية من التجسس والاختراق.
- ✓ تشفير البيانات الخاصة بي.
- ✓ إبلاغ مباحث الإنترنت في حال حدوث أي اختراق لحساباتي أو تهديد لي.
- ✓ استخدام كلمة مرور قوية، وعدم مشاركتها مع الآخرين، وتحديث أجهزتي باستمرار.
- ✓ توخى الحذر عند فتح مرفقات وروابط البريد الإلكتروني.
- ✓ استخدام المواقع الموثوقة وذات السمعة الطيبة عند تصفح الويب أو تنزيل المحتوى.
- ✓ تجنب مشاركة معلوماتي الشخصية علنًا على مواقع التواصل الاجتماعي.
- ✓ عمل نسخة احتياطية لبياناتي.

❖ **تفسير نتائج المحور الثاني: أسئلة تتعلق بالعنف الرقمي**

- **بالنسبة لاستجابات الطالبات حول السؤال الأول: ما أشكال العنف الرقمي التي يمكن أن تتعرض لها الطالبات عبر الإنترنت من وجهة نظرك؟**

يمكن إيجاز أهم آراء الطالبات حول هذا السؤال، والتي تمحورت فيما يلي:

- إيذاء لفظي أو نفسي أو اجتماعي من خلال التهديدات أو المضايقات أو التشويه المتعمد للمعلومات الشخصية.

- الابتزاز والاستغلال والتحرش والمضايقات تصل إلى حد التعرض لأفراد العائلة من خلال التهديد.
- نشر معلومات أو صور شخصية بغير رضا الطرف الآخر على شبكة الإنترنت.
- أن تتعرض إلى اختراق ملف الصور الخاص بها، وفبركة الصور لتشويه صورتها في المجتمع أو لابتزازها بأي شكل من الأشكال بهدف المال أو أمور أخرى.
- التنمر على الطالبات عبر الإنترنت.
- مضايقات نفسية، وتهديدات اجتماعية، وضغط نفسي من خوف وقلق.
- الابتزاز- سرقة صفحة موقع التواصل الاجتماعي "الفيسبوك"- نشر صفح عبر الإنترنت- التحرش.
- أي شكل من أشكال الإيذاء الاجتماعي أو النفسي عبر الإنترنت.
- التهديد لهن باستخدام صورهن أو معلوماتهن الشخصية بصورة مسيئة.
- التحرش الرقمي فيما يتعلق بالمعاكسات والمضايقات.
- محاولة نشر معلومات خاطئة تسيء لسمعتهن.
- سرقة المعلومات الشخصية لهن.
- قد يتعرض بعضهن للهاكر والتهديد، مما قد يؤدي إلى تفكيرهن في الانتحار أو ابتزازهن بالمال، وتهديدهن بالفضيحة.
- انتحال الشخصية والبيانات والهوية لهن.
- العنف الإلكتروني، والتحرش الإلكتروني، والتنمر الإلكتروني عبر الإنترنت والابتزاز.
- إرسال رسائل معاكسات لهن عبر الواتساب والهاتف.

- **بالنسبة لاستجابات الطالبات حول السؤال الثاني: هل تعرضتِ شخصيًا أو تعرفين أحدًا تعرض لأشكال من العنف الرقمي مثل التحرش أو التهديدات عبر الإنترنت؟**

نعم ( ) لا ( )، إذا كانت الإجابة نعم، اذكري أهم هذه المواقف التي تعرضتِ لها أو تعرض لها من تعرفينهم؟

فإن النسبة المئوية للطالبات اللاتي أجبن بـ (نعم) كانت ٦ , ٥٥٪، بينما كانت النسبة المئوية للإجابة بـ (لا) ٤ , ٤٤٪. ويمكن إيجاز أبرز المواقف التي تعرضت لها الطالبات أو تعرض لها من يعرفونهم، كما يلي:

- ✓ ذهبت صديقتي لإصلاح هاتفها، فقام المصلح بتهكير الهاتف، وأخذ المعلومات والصور الشخصية الخاصة بها بطريقة مباشرة أثناء استعمالها للهاتف.
- ✓ تعرضت صديقة لي لموقف لم تدرك جيدًا مخاطره عبر الهاتف، وبالفعل تمكن أحد الأشخاص بالحصول على مبلغ مالي كبير؛ لأنها غير مثقفة حول ما يحدث من سرقات عبر التكنولوجيا ومخاطر استخدامها.
- ✓ قامت صديقتي بإعطاء صور شخصية إلى صديقة لها، فقامت هذه الصديقة بتهديدها بالصور وفضحها عبر مواقع التواصل الاجتماعي إذا لم تسلمها مبلغًا من المال.
- ✓ أعرف فتاة تعرضت للابتزاز من شخص عن طريق عمل Like على صورة على صفحة ما؛ فتم الدخول إلى هاتفها وفتح الكاميرا الخاصة بها، وتصويرها في أوضاع لا تسمح وابتزازها بها، وأنه إذا لم تعطيه المال سوف يتم نشر هذه الصور على جميع صفحات التواصل وإرسال الرقم الخاص بها.
- ✓ تعرضت إحدى زميلاتي لانتحال شخصيتها واستخدام بياناتها وصورها.
- ✓ تم التشهير برخصة القيادة الخاصة بأختي ووضعها على تطبيق الواتساب.
- ✓ تم إرسال رسالة صوتية لي ويوجد بها ألفاظ بذيئة.

- ✓ تعرضت إحدى صديقاتي للتهديد من قبل أحد الأشخاص باختراق بياناتها.
- ✓ تعرضت إحدى صديقاتي لنشر معلومات خاصة ومحرجة لها عبر الإنترنت.
- ✓ تعرضت لإرسال فيروسات إليَ عمدًا عبر رسائل على وسائل التواصل الاجتماعي.
- ✓ تعرضت إحدى صديقاتي لنشر مقاطع الفيديو الخاصة بها عبر الإنترنت دون إذنها.
- ✓ تمت مشاركة صوري عبر الإنترنت دون إذني.
- ✓ تعرضت للتهديد والابتزاز عبر الإنترنت.
- ✓ قام أحد زملائي باستخدام الإنترنت لمعرفة معلومات خاصة عني كعنواني ورقم هاتفي.
- ✓ تعرضت إحدى صديقاتي لنشر محتوى إباحي على صفحتها على الفيسبوك بدون علمها.
- ✓ تعرضت إحدى زميلاتي للسب والشتم والمضايقات عبر الرسائل الخاصة بموقعها على الفيسبوك والواتس آب من إحدى زملائها.
- ✓ تعرضت للتنمر على صورتي المنشورة على صفحتي على الفيسبوك من إحدى زملائي، مما سبب لي حالي من الاكتئاب والعزلة وعدم الثقة بالنفس والإحباط.
- ✓ قمت بالضغط على رابط جائزة هاكر فتم سحب الكثير من أموالي من حسابي الشخصي.
- ✓ تعرضت إحدى صديقاتي لسرقة حسابها الشخصي لصفحة الفيسبوك.
- ✓ تعرضت للابتزاز والتهديد من أحد زملائي بسبب رفضي الرد عليه وتجاهله.

مما سبق عرضه تبين تنوع أشكال العنف الرقمي التي تعرضت له الطالبات أو من يعرفونهم من الابتزاز، والتنمر، والتحرش، والسرقة، والمضايقات، والتهديد، والذي كان له آثاره السلبية على نفسيتهن وتعرضهن للاكتئاب والعزلة والإحباط والقلق والخوف واضطرابات النوم والشهية وعدم الثقة بالنفس، والتأثير على صحتهن النفسية ومستواهن الأكاديمي وتحصيلهن الدراسي.

- **بالنسبة لاستجابات الطالبات حول السؤال الثالث: ما الخطوات التي يمكنك اتخاذها إذا تعرضتِ لتهديدات أو مضايقات عبر الإنترنت من وجهة نظرك؟**

يمكن إيجاز أهم آراء الطالبات حول هذا السؤال، والتي تمحورت فيما يلي:

- إبلاغ الأسرة والأشخاص الناضجين الذين نثق بهم لأخذ مشورتهم ونصائحهم.
- تشفير الرقم السري أو حذف الحساب.
- تغيير بياناتي وتحديثها وعمل كلمة مرور جديدة قوية.

حيث اقتصرت ردود أفعال البعض منهن على التجاهل أو إغلاق حساباتهن على مواقع التواصل الاجتماعي وتنبيه الأصدقاء المشتركون على هذه الصفحات بأنه تم اختراق حساباتهن، وحظر الجناة وحذفهن من قائمة المتابعين، وتفعيل خاصية خصوصية الحساب بإغلاق التعليقات، وإبلاغ إدارة الفيسبوك بالإساءة التي تعرضن لها من قبل أحد الأشخاص. إلا أن من الملاحظ أنه لن تلجأ إحداهن للجوء للقانون والإبلاغ الرسمي نظرًا لنقص معرفتهن بقوانين مكافحة الجرائم الإلكترونية، أو الخوف من الفضيحة ومستقبلهن الدراسي أو سوء الفهم من الآخرين أو لغياب الثقة في الحصول على حقوقهن ومعاقبة الجاني.

- بالنسبة لاستجابات الطالبات حول السؤال الرابع: **هل تعلمين عن أهم قوانين مكافحة الجرائم الإلكترونية؟**

نعم ( ) لا ( )، إذا كانت الإجابة نعم، اذكري أهم هذه القوانين.

فإن النسبة المئوية للطالبات اللاتي أجبن بـ (نعم) كانت ١٥,٣٪، بينما كانت النسبة المئوية للإجابة بـ (لا) ٨٤,٧٪. مما يدل على نقص معرفتهن بقوانين مكافحة الجرائم الإلكترونية، ومن أبرزها:

- ✓ القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.
- ✓ قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣.

- بالنسبة لاستجابات الطالبات حول السؤال الخامس: **هل تعلمين بوجود وحدة لمناهضة العنف ضد المرأة داخل جامعة القاهرة؟**

نعم ( ) لا ( )، إذا كانت الإجابة نعم، اذكري أدوارها.

فإن النسبة المئوية للطالبات اللاتي أجبن بـ (نعم) كانت ٤ , ٢٧٪، بينما كانت النسبة المئوية للإجابة بـ (لا) ٦ , ٧٢٪. مما يدل على نقص معرفتهن بوجود وحدة لمناهضة العنف ضد المرأة داخل جامعة القاهرة، مما يستلزم تفعيل دور الوحدة من خلال قيامها بعقد العديد من الندوات وورش العمل داخل كليات الجامعة للتوعية والتعريف بدورها وتثقيف الطالبات حول مواجهة العنف الرقمي.

- بالنسبة لاستجابات الطالبات حول السؤال السادس: **ما الدور الذي يمكن أن تقوم به الجامعة في مواجهة العنف الرقمي ضد الطالبات من وجهة نظرك؟**

يمكن إيجاز أهم آراء الطالبات حول هذا السؤال، والتي تمحورت فيما يلي:

- ✓ عقد ندوات ودورات تدريبية توعوية عن الأمن السيبراني.
- ✓ التوعية- المساعدة الفعلية- التثقيف من خلال نشرات توعية توضع على الصفحات الرسمية لكليات الجامعة.
- ✓ تكوين وتوفير فريق للأمن السيبراني ليكون مركزًا لدعم الطالبات في حال حدوث أي مشكلة.
- ✓ عمل إيميلات أكاديمية خاصة بالطالبات؛ بحيث لا يتم اختراقها عبر مواقع التواصل الاجتماعي.
- ✓ إعطاء رقم سري لكل طالبة بحيث لا يتم تهكيرها واختراقها.
- ✓ إرساء دعائم الأمان الشبكي؛ من خلال تخصيص وقت قليل أثناء كل محاضرة للحديث عنه.
- ✓ استخدام منصات آمنة للطالبات.

- ✓ عمل وحدة استشارات من السادة المختصين مكونة من رجال ونساء حتى يكون هناك تفاعل من قبل الذكور والإناث.
- ✓ إقامة مؤتمرات داخل كليات الجامعة للتوعية بالمخاطر والتهديدات السيبرانية، والعنف الرقمي.
- ✓ عمل ندوات ومحاضرات لفهم العنف الرقمي من قبل الطالبات لتوعيتهم، والتوجيه الصحيح للطلاب، والاستفادة من خبرات المختصين.
  - سرعة الاستجابة لأفكار الطالبات عن هذا الموضوع ممن تعرضن له.
  - إقامة دورات توعوية بصفة مستمرة لجميع الطالبات حتى يتمكن من التصرف بصورة واضحة في حالات العنف الرقمي، وكيفية تعاملهن معه.
  - أن تقوم الجامعة بتقديم دعم نفسي للطالبات ممكن تعرضن لأي شكل من أشكال عنف الرقمي.
  - أن يكون هناك تعاون مستمر بين الجامعة والأجهزة الأمنية لمكافحة العنف الرقمي ضد الطالبات.
  - إدراج مفاهيم الأمن السيبراني في المقررات الدراسية.
  - عقد ورش عمل تدريبية حول ماهية العنف الرقمي ومخاطره.

مما سبق عرضه يتضح الدور المهم الذي يمكن أن تؤديه الجامعة في تعزيز ثقافة الأمن السيبراني لدى طالباتها، وذلك لمواجهة العنف الرقمي الذي قد يتعرضن له.

ولتحقيق هذا الغرض يمكن وضع تصور مقترح لتعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي، وهذا ما سيتم تناوله في الجزء الثالث للبحث كما يلي:

الجزء الثالث: تصور مقترح لتعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي

فيما يلي عرض تصوُّرٍ مُقترَحٍ لتعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي؛ وذلك في ضوء ما عرضته الدراسة من إطارٍ نظري، وذلك من خلال الحديث عن: منطلقات التصوُّر المُقترَح، وفلسفته، وأهدافه، وآليات تحقيقه، ومعوقات تطبيقه، وسبل التغلُّب على هذه المعوقات.

أولًا: منطلقات التصوُّر المُقترَح

ينطلق التصوُّر المُقترَح من عدة منطلقات منها ما يلي:

١. **اهتمام الدولة الكبير بمجال الأمن السيبراني**، من خلال إطلاق مصر الاستراتيجية الوطنية للأمن السيبراني (٢٠٢٣-٢٠٢٧)، والتي تهدف إلى التصدي للحوادث السيبرانية.

٢. **الحاجة المتزايدة للأمن السيبراني**: مع تزايد الاعتماد على الإنترنت والتكنولوجيا في الحياة اليومية، أصبح من الضروري أن تتسلح طالبات الجامعة بالمعرفة الكافية حول كيفية حماية أنفسهن من المخاطر الإلكترونية، مما يجعل من الضروري تعزيز ثقافة الأمن السيبراني لديهن لحمايتهن من التهديدات الرقمية، كما يعزز قدرة الطالبات على التفاعل بشكل آمن مع التكنولوجيا في بيئات أكاديمية، ويسهم في تطوير مهاراتهن الرقمية.

٣. **مواجهة العنف الرقمي**: يشهد العالم زيادة ملحوظة في مظاهر العنف الرقمي، مثل التحرش الإلكتروني، التنمر، والاستغلال عبر الشبكات الاجتماعية. لذا فإن تعزيز ثقافة الأمن السيبراني سيمكن الطالبات من تعرف هذه المخاطر، والطرق الفعالة للتعامل معها، والوقاية منها.

٤. **مواكبة التوجهات العالمية:** في ظل التحولات الرقمية العالمية، تعزز الجامعات والمجتمعات التعليمية من جهودها لتطوير ثقافة الأمن السيبراني، وهو ما يتماشى مع التوجهات العالمية في تعزيز الأمان الرقمي وحماية الأفراد في الفضاء السيبراني.

٥. **دور الجامعة كمؤسسة تعليمية:** يُعد دور جامعة القاهرة في تطوير وتثقيف جيل الشباب، وخاصة الطالبات، أمرًا حيويًا. حيث تعمل على تحسين ثقافة الأمن السيبراني وتوفير بيئة تعليمية آمنة، سواء في القاعات الدراسية أو على الإنترنت.

٦. **تعزيز الأمن الشخصي والحماية القانونية:** من خلال رفع الوعي حول حقوق الطالبات في حماية بياناتهن الشخصية على الإنترنت وكيفية التعامل مع الهجمات الرقمية من الناحية القانونية، مما يسهم في بناء مجتمع رقمي آمن ومتماسك. حيث أصدرت مصر العديد من القوانين والتشريعات التي تواجه العنف الرقمي، ومكافحة جرائم تقنية المعلومات.

ثانيًا: أهداف التصوَّر المُقترَح

يَتَمَثَّل الهدف العام للتصوُّر المُقترَح في تعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة لمواجهة العنف الرقمي؛ من خلال تأسيس بيئة تعليمية آمنة ضد العنف الرقمي؛ حيث تكون الطالبات مجهزات بالمعرفة والمهارات اللازمة لحماية أنفسهن ومواجهة أي تهديدات قد تطرأ على حياتهن الرقمية. وذلك بهدف:

- تعريف الطالبات بمفاهيم الأمن السيبراني الأساسية، بما في ذلك حماية المعلومات الشخصية، التشفير، وحماية الحسابات الإلكترونية من الهجمات الرقمية.
- زيادة الوعي بمخاطر العنف الرقمي وكيفية التصدي لها من خلال أدوات وتقنيات الأمن السيبراني.
- تعزيز قدرة الطالبات على التعرف على السلوكيات الضارة واتخاذ التدابير الوقائية وتقليل فرص تعرضهن للعنف الرقمي.

- إكساب الطالبات مهارات التعامل مع حالات العنف الرقمي، مثل كيفية الإبلاغ عن حالات التنمر والتحرش، وسبل حماية أنفسهن قانونيًا.
- تشجيع التعاون بين الطالبات والإدارة الجامعية لتطوير سياسات وإجراءات وقائية ضد العنف الرقمي في الحرم الجامعي.

ثالثًا: متطلبات التصوُّر المُقترَح

لتعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة في مواجهة العنف الرقمي، يجب تحديد مجموعة من المتطلبات الأساسية التي تُسهم في تحقيق هذا التصور المقترح. وهذه المتطلبات تشمل: المتطلبات التعليمية والتدريبية، المتطلبات التقنية، المتطلبات التنظيمية والإدارية، متطلبات دعم نفسي واجتماعي، متطلبات تشريعية وقانونية، متطلبات توعوية وإعلامية، متطلبات مالية وموارد، بالإضافة إلى متطلبات تشاركية ومجتمعية. وفيما يلي عرض لهذه المتطلبات:

١. **متطلبات تعليمية وتدريبية**: والتي تتمثل في الآتي:

- **تطوير مقررات دراسية شاملة**: من خلال إدراج موضوعات الأمن السيبراني في المقررات الدراسية، وخاصة في المقررات المتعلقة بالتكنولوجيا والمعلومات. ويجب أن تشمل هذه المقررات أساسيات حماية الخصوصية، التهديدات الرقمية، وكيفية التعامل مع العنف الرقمي.
- **تنظيم ورش عمل ودورات تدريبية**: إقامة ورش عمل ودورات تدريبية عملية للطالبات حول كيفية حماية المعلومات الشخصية، استخدام كلمات مرور قوية، والتصدي للهجمات الإلكترونية. كما يجب توفير تدريبات عملية في كيفية التصرف في حالات العنف الرقمي، مثل التنمر والتحرش الإلكتروني.

- **التثقيف القانوني**: توفير تدريب على القوانين المحلية والدولية المتعلقة بحماية البيانات وحقوق الأفراد في الفضاء الرقمي، بحيث تكون الطالبات على دراية بكيفية حماية حقوقهن القانونية في حال تعرضهن لعنف رقمي.

٢. **متطلبات تقنية**: وتتمثل في الآتي:

- **تطوير منصات تعليمية آمنة**: إنشاء منصات تعليمية رقمية آمنة للمشاركة في التدريبات والأنشطة المتعلقة بالأمن السيبراني، بحيث تكون محمية من أي تهديدات أمنية.
- **أدوات وتقنيات الحماية الشخصية**: توفير أدوات وبرامج للتشفير وحماية البيانات الشخصية على الأجهزة الإلكترونية، مع تدريب الطالبات على كيفية استخدامها.
- **إنشاء نظام مراقبة إلكتروني داخلي**: تطوير آليات لرصد الأنشطة الرقمية المريبة أو غير القانونية على منصات الجامعة الإلكترونية، لضمان بيئة آمنة للطالبات.

٣. **متطلبات تنظيمية وإدارية**: وتتمثل في الآتي:

- **سياسات جامعية لحماية الطلاب من العنف الرقمي**: وضع سياسات واضحة وصارمة لمكافحة العنف الرقمي داخل الجامعة، مع إنشاء آليات للإبلاغ عن أي حالات تعرض للطالبات.
- **تعزيز التعاون بين الأقسام الجامعية**: التنسيق بين إدارات الجامعة المختلفة مثل الإدارة التقنية، والشؤون القانونية، والشؤون الطلابية، لتطوير استراتيجيات شاملة لمكافحة العنف الرقمي وتعزيز الأمن السيبراني.
- **إعداد دليل توجيهي للطالبات**: توفير دليل إرشادي يحتوي على خطوات عملية للتعامل مع حالات العنف الرقمي وكيفية الإبلاغ عنها، بالإضافة إلى الإجراءات الوقائية التي يجب اتخاذها.
- تفعيل وتطوير وحدة مناهضة العنف ضد المرأة داخل جامعة القاهرة.

٤. **متطلبات دعم نفسي واجتماعي**: وتتمثل في الآتي:

- **توفير دعم نفسي للطالبات**: إنشاء قسم متخصص بكل كلية لدعم الطالبات المتضررات من العنف الرقمي، وتقديم استشارات نفسية للمتعرضات لحالات التنمر أو التحرش الإلكتروني.
- **إنشاء خط ساخن للإبلاغ عن العنف الرقمي**: تخصيص خط ساخن أو منصة دعم لاستقبال شكاوى الطالبات بشكل سري، وتقديم المساعدة اللازمة في الحالات التي تتطلب تدخلاً سريعًا.
- **تفعيل "مركز الدعم النفسي وإعادة بناء الذات" بجامعة القاهرة**، وتعريف الطالبات بمهامه، وتوعيتهن بضرورة اللجوء إليه للحصول على الاستشارات والدعم النفسي في حالة تعرضهن لأحد أشكال العنف الرقمي.

٥. **متطلبات تشريعية وقانونية**: وتتمثل في الآتي:

- **إدراج محاضرات قانونية حول حقوق الطالبات في الفضاء الرقمي**: تضمين محاضرات تعريفية في الجامعة حول القوانين المتعلقة بحماية البيانات الشخصية، وحقوق الطالبات في مواجهة العنف الرقمي.
- **التعاون مع الجهات القانونية:** التعاون مع الجهات الأمنية والقضائية لتوفير دورات تدريبية للطالبات حول كيفية التعامل مع الحالات القانونية المتعلقة بالعنف الرقمي وحقوقهن القانونية.

٦. **متطلبات توعوية وإعلامية**: وتتمثل في الآتي:

- **حملات توعية رقمية**: إطلاق حملات توعية عبر الإنترنت وفي الحرم الجامعي، لرفع الوعي بين الطالبات حول أهمية الأمن السيبراني وكيفية حماية أنفسهن من العنف الرقمي.

- **إشراك الطالبات في نشر الثقافة الرقمية**: تشجيع الطالبات على المشاركة في الأنشطة التي تروج للوعي بالأمن السيبراني، مثل إعداد مقاطع فيديو توعوية أو كتابة مقالات.

٧. **متطلبات مالية وموارد**: وتتمثل في الآتي:

- **تخصيص ميزانية كافية لتطوير البرامج التدريبية**، شراء البرمجيات الأمنية، وتقديم الدعم النفسي والتقني للطالبات.
- **تأمين موارد مالية لدعم المبادرات الطويلة الأمد المتعلقة بتعزيز ثقافة الأمن السيبراني ومكافحة العنف الرقمي**، بحيث تكون البرامج متجددة ومتطورة بما يتناسب مع التحديات التقنية الجديدة.

٨. **متطلبات تشاركية ومجتمعية**: وتتمثل في الآتي:

- **التعاون مع منظمات المجتمع المدني**: والتي تعمل على مكافحة العنف الرقمي وحماية حقوق الفتيات في الفضاء الإلكتروني، لتبادل الخبرات والموارد.
- **إنشاء شبكة دعم بين الطالبات**: تعزيز التعاون بين الطالبات في مجال تعزيز الأمن السيبراني من خلال إنشاء مجموعات دعم أو منتديات تعليمية تشجع على تبادل الخبرات والمعرفة.

من خلال تلبية هذه المتطلبات، يمكن تعزيز ثقافة الأمن السيبراني لدى طالبات جامعة القاهرة، والتي تُسهم في توفير بيئة آمنة للدراسة والتفاعل الرقمي، مما يقلل من احتمالات تعرض الطالبات للعنف الرقمي ويوفر لهن الأدوات اللازمة للحفاظ على سلامتهن الشخصية في الفضاء الإلكتروني.

رابعًا: آليات تنفيذ التصوُّر المُقترَح

يتطلب تنفيذ التصور المقترح تحقيق مجموعة من الآليات، منها ما يلي:

- وضع سياسات جامعية تأديبية واضحة وصارمة لمعاقبة الطلاب الذين يتسببون في أعمال عنف رقمي داخل الحرم الجامعي ضد الطالبات، تشمل إجراءات الإبلاغ، التحقيق، وتوفير الدعم للطالبات المتأثرات.

- وضع سياسات تأديبية صارمة لمعاقبة الأفراد الذين يتسببون في أعمال عنف رقمي داخل الحرم الجامعي.
- عقد ندوات ومؤتمرات وورش عمل داخل الجامعة للتوعية بالعنف الرقمي وآثاره السلبية على الطالبات.
- عقد دورات تدريبية لتوعية الطالبات باستخدام التكنولوجيا بالشكل الصحيح لتفادي التعرض لظاهرة العنف الرقمي.
- وضع دليل لمواجهة العنف الرقمي لطالبات جامعة القاهرة، من أجل توعيتهن بكيفية التبليغ عن الجناة والحصول على حقوقهن، وحماية أنفسهن وخصوصيتهن عبر مواقع التواصل الاجتماعي من القرصنة والبرمجيات الخبيثة والصفحات المزيفة، وتقديم الدعم النفسي والاجتماعي لهن.
- توفير برامج تدريبية لأعضاء هيئة التدريس في مركز تنمية قدرات أعضاء هيئة التدريس بجامعة القاهرة على كيفية تدريس مفاهيم الأمن السيبراني، وسبل تقديم المشورة للطالبات حول كيفية التعامل مع التهديدات الرقمية.
- دمج موضوعات الأمن السيبراني في المقررات الدراسية في مختلف الكليات، وخاصة في تخصصات التكنولوجيا والعلوم الإنسانية، مع التركيز على كيفية حماية البيانات الشخصية وكيفية التصدي للعنف الرقمي.
- التنسيق مع الجهات القانونية والأمنية لمساعدة الطالبات في حال تعرضهن لأعمال عنف رقمي تتطلب تدخلًا قانونيًا.
- عقد شراكات مع شركات متخصصة في الأمن السيبراني لتوفير التدريب على أدوات وتقنيات حماية البيانات والمعلومات الشخصية.

- تشجيع التعاون بين الكليات التقنية والعلمية في الجامعة لإعداد برامج مشتركة ودورات تدريبية تركز على تحسين مهارات الطالبات في حماية أنفسهن في الفضاء الرقمي.
- تحديث وتطوير البنية التحتية الرقمية داخل الجامعة لضمان حماية المعلومات وحسابات الطالبات من الهجمات الإلكترونية.

خامسًا: معوقات تنفيذ التصوُّر المُقترَح

قد يواجه تنفيذ التصور المقترح عدة معوقات، منها ما يلي:

١. **المعوقات التقنية**، والتي تشمل ما يلي:

- **نقص البنية التحتية التقنية والأمنية**: قد تواجه الجامعة تحديات في تطوير أو تحديث البنية التحتية التقنية اللازمة لحماية البيانات الشخصية والأنظمة الإلكترونية من الهجمات الرقمية. وكذلك نقص الأنظمة الأمنية المتقدمة مثل التشفير الجيد أو مراقبة الأنشطة المشبوهة قد يعوق تحقيق الأمن السيبراني.
- **صعوبة الوصول إلى أدوات وتقنيات حديثة**: قد تكون تكلفة توفير أدوات وبرامج أمنية مثل مكافحة الفيروسات أو حلول المصادقة الثنائية مرتفعة بالنسبة للجامعة، مما يصعب توفير هذه الأدوات لجميع الطالبات.
- **المشاكل التقنية في المنصات التعليمية الرقمية**: يمكن أن تواجه منصات التعليم الرقمي في الجامعة تحديات في تأمين التفاعل بين الطلاب والمحتوى الرقمي، مثل تعرض المنصات للاختراق أو فشل في تطبيق إجراءات الأمان.

٢. **المعوقات التعليمية والتدريبية**، والتي تشمل ما يلي:

- **قلة الوعي العام حول الأمن السيبراني**: قد تفتقر عدد كبير من الطالبات إلى الوعي الكافي بشأن أهمية الأمن السيبراني، مما يجعل من الصعب تحفيزهن على المشاركة في البرامج التدريبية أو تطبيق أفضل الممارسات لحماية أنفسهن على الإنترنت.

- **نقص البرامج التدريبية المتخصصة**: قد تفتقر بعض البرامج التعليمية الحالية إلى محتوى تعليمي يركز بشكل كافٍ على الأمن السيبراني، مما قد يعيق تقديم التدريب الكافي والمستمر للطالبات.
- **تحديات في تقنيات التدريب عن بُعد**: بسبب الانتقال المتزايد نحو التعليم عن بُعد، قد تطرأ صعوبة في تدريب الطالبات بشكل تفاعلي على أساليب الأمن السيبراني، خاصةً في بيئات تعليمية لا تسمح بالتفاعل الشخصي المباشر.

٣. **المعوقات التنظيمية والإدارية**، والتي تشمل ما يلي:

- **غياب السياسات الجامعية المتكاملة**: قد يكون من الصعب وضع سياسات أمنية فعالة لمواجهة العنف الرقمي داخل الحرم الجامعي، خاصة إذا كانت هناك عدم توافق بين الإدارات المختلفة (مثل إدارة الأمن، الشؤون الطلابية، وتقنية المعلومات) حول الإجراءات المناسبة.
- **نقص التعاون بين الأقسام**: قد تواجه الجامعة صعوبة في التنسيق بين مختلف الأقسام التي يجب أن تعمل معًا مثل الشؤون الطلابية، الكليات التقنية، والأمن الجامعي، مما يعوق تنفيذ التصور المقترح.
- **مقاومة التغيير من قبل بعض الأفراد أو الإدارات:** قد يواجه التصور مقاومة من بعض الموظفين أو الأساتذة الذين قد لا يدركون أهمية الثقافة السيبرانية أو يرفضون تبني تغييرات في طرق العمل المتبعة.

٤. **المعوقات القانونية والاجتماعية**، والتي تشمل ما يلي:

- **نقص القوانين والتشريعات الخاصة بالعنف الرقمي**: قد تكون القوانين الحالية غير متطورة بما يكفي لحماية الطالبات من العنف الرقمي بشكل كامل أو قد تكون غامضة في بعض الحالات، مما يحد من قدرة الجامعة على اتخاذ إجراءات قانونية فعالة.

- **محدودية الدعم القانوني للطالبات**: في حالة تعرض الطالبات للعنف الرقمي، قد يواجهن صعوبة في الحصول على الدعم القانوني الفوري والمناسب، سواء في إطار الجامعة أو من خلال النظام القضائي..
- **المشاكل الثقافية والاجتماعية**: قد تكون بعض الطالبات غير راغبات في الإبلاغ عن العنف الرقمي بسبب الخوف من وصمة العار أو العواقب الاجتماعية، مما قد يجعل من الصعب تطبيق برامج فعالة لمواجهة العنف الرقمي.

٥. **المعوقات المالية والموارد**، والتي تشمل ما يلي:

- **تحديات التمويل**: تخصيص ميزانية كافية لتنفيذ برامج تدريبية وتأمين الأنظمة التقنية وتعزيز التوعية يمكن أن يكون تحديًا ماليًا. وقد لا تكون هناك موارد مالية كافية لتغطية جميع الأنشطة المقررة.
- **عدم توفر موارد بشرية مدربة**: تنفيذ التصور يتطلب وجود متخصصين في مجال الأمن السيبراني والأنظمة التقنية، وقد تواجه الجامعة صعوبة في توفير الكوادر المؤهلة لذلك.
- **ضعف التخصيص المالي للبرامج التوعوية**: قد تفتقر الجامعة إلى التمويل الكافي لتغطية الأنشطة التوعوية والتثقيفية المستمرة حول الأمن السيبراني، مما يقلل من فاعلية البرامج التوعوية.

٦. **المعوقات النفسية والسلوكية**، والتي تشمل ما يلي:

- **ضعف الرغبة في التغيير لدى الطالبات**: قد تجد بعض الطالبات أن التدريب على الأمن السيبراني أو المشاركة في الأنشطة التوعوية ليس ذا أهمية كبرى بالنسبة لهن، مما يقلل من التفاعل مع المبادرات المطروحة.
- **التأثيرات النفسية للعنف الرقمي**: قد تواجه الطالبات المتعرضات للعنف الرقمي صعوبة في التعامل مع آثار هذه التجارب نفسيًا، مما يؤثر على قدرتهن على المشاركة في البرامج التوعوية أو طلب الدعم.

٧. **المعوقات التكنولوجية**، والتي تشمل ما يلي:

- **عدم مواكبة التطورات التقنية السريعة:** قد يصعب على الجامعة متابعة جميع التغيرات السريعة في تكنولوجيا المعلومات ووسائل التواصل الاجتماعي، مما قد يترك فجوة بين البرامج الأمنية الحالية والمستجدات التقنية.
- **الفجوة الرقمية بين الطالبات**: قد تكون هناك فجوة في الوصول إلى التقنيات الحديثة بين الطالبات بسبب تفاوت مستويات الدخل أو البيئة الاجتماعية، مما قد يمنع بعض الطالبات من الاستفادة الكاملة من برامج الأمن السيبراني.

سادسًا: سبل التغلب على معوقات تنفيذ التصوُّر المُقترَح

يمكن التغلب على المعوقات وتعزيز قدرة جامعة القاهرة على تنفيذ التصور المقترح لتعزيز ثقافة الأمن السيبراني لدى الطالبات، مما يُسهم في بناء بيئة تعليمية آمنة وصحية لهن ويحد من العنف الرقمي، كما يلي:

١. **التغلب على المعوقات التقنية**، من خلال ما يلي:

- ✓ **تحسين البنية التحتية للأمن السيبراني**: تخصيص ميزانية لتحديث وتعزيز الأنظمة التقنية والبنية التحتية داخل الجامعة، مثل تأمين الشبكات وتوفير أدوات أمان حديثة. ويمكن التعاون مع شركات تكنولوجيا المعلومات لتوفير حلول أمنية بأسعار معقولة أو من خلال شراكات.
- ✓ **تدريب الفريق الفني**: تحسين مهارات الفريق الفني في الجامعة وتوفير تدريب مستمر في مجال الأمن السيبراني لضمان قدرتهم على مواجهة التهديدات المتطورة.
- ✓ **الاستفادة من المصادر المجانية**: استخدام برامج حماية مجانية أو بأسعار منخفضة للطالبات، مثل برامج مكافحة الفيروسات وحلول الأمان الرقمية المفتوحة المصدر، لضمان توفير الأمان بأقل التكاليف.

- ✓ **زيادة الرقابة على الأنظمة التعليمية الرقمية**: استخدام تقنيات مراقبة الأنشطة الرقمية على منصات الجامعة بشكل دوري للكشف عن أي هجمات أو محاولات اختراق قبل أن تؤثر على النظام.

٢. **التغلب على المعوقات التعليمية والتدريبية**، من خلال ما يلي:

- ✓ **تطوير المقررات الدراسية وتحديثها**: لتشمل وحدات تعليمية تتعلق بالأمن السيبراني وحماية البيانات من خلال أساليب تفاعلية وتطبيقات عملية لتوضيح كيفية حماية المعلومات الشخصية.
- ✓ **استخدام أساليب التعليم عن بُعد الفعالة**: تطوير دورات تدريبية عبر الإنترنت تتضمن تمارين عملية، ومحاكاة لحالات حقيقية من العنف الرقمي لتعريف الطالبات بكيفية التعامل معها.
- ✓ **إشراك الطالبات في تصميم البرامج التدريبية**: دعوة الطالبات لتصميم المحتوى التدريبي والمشاركة في ورش العمل، مما يزيد من التفاعل ويجعل التدريب أكثر جذبًا وفائدة.
- ✓ **تفعيل دور أساتذة الأمن السيبراني**: تعيين أساتذة متخصِّصين في الأمن السيبراني وتطوير البرامج الدراسية التي تركز على هذا المجال.

٣. **التغلب على المعوقات التنظيمية والإدارية**

- ✓ **وضع سياسات واضحة**: العمل على صياغة سياسات وإجراءات واضحة داخل الجامعة تتعلق بحماية الطالبات من العنف الرقمي، مع ضمان توافق جميع الإدارات الجامعية في تنفيذها.
- ✓ **تنظيم ورش عمل بين الإدارات**: تنظيم ورش عمل بين الإدارات المختلفة (الأمن الجامعي، الشؤون الطلابية، وتقنية المعلومات) لضمان التنسيق والتعاون الفعال في مواجهة التحديات.

- ✓ **تشجيع التعاون بين الأقسام**: تأسيس لجنة مشتركة من أقسام مختلفة مثل تكنولوجيا المعلومات، الشؤون القانونية، والشؤون الطلابية، لوضع استراتيجيات متكاملة للتصدي للعنف الرقمي.

٤. التغلب على المعوقات القانونية والاجتماعية

- ✓ **تعزيز الوعي القانوني**: تقديم دورات تدريبية للطالبات حول حقوقهن الرقمية وكيفية التعامل مع المواقف التي تشمل العنف الرقمي. كما يجب تعزيز ثقافة الإبلاغ عن الحالات مع ضمان سرية المعلومات.
- ✓ **تطوير قوانين الجامعة**: العمل مع الجهات القانونية على تطوير قوانين خاصة بالجامعة لحماية الطالبات من العنف الرقمي، وتحديد العقوبات المناسبة للمتورطين في هذا النوع من العنف.
- ✓ **إشراك المجتمع الجامعي في مكافحة العنف الرقمي**: تنظيم حملات توعية داخل الجامعة لتغيير المواقف الثقافية التي قد تُسهم في صمت الطالبات تجاه العنف الرقمي، وتعزيز ثقافة الحوار والاحترام في الفضاء الرقمي.

٥. التغلب على المعوقات الاجتماعية والثقافية

- ✓ **تنظيم فعاليات توعوية في الحرم الجامعي**: تحث على مناقشة القضايا الرقمية المتعلقة بالعنف الرقمي، وتشجيع الطالبات على التعبير عن تجاربهن الشخصية في بيئة آمنة.
- ✓ **تعزيز ثقافة الاحترام المتبادل في الفضاء الرقمي**: من خلال تنظيم ندوات وورش عمل تتعلق بأخلاقيات الإنترنت وحقوق الأفراد في الفضاء الرقمي، يمكن بناء بيئة جامعية أكثر وعيًا بالمسؤولية الرقمية.

٦. التغلب على معوقات التواصل بين الأطراف المعنية

- ✓ **تعزيز التواصل بين إدارات الجامعة والجهات القانونية**: تنظيم اجتماعات دورية بين الإدارات المختلفة لتبادل المعرفة والممارسات الجيدة حول كيفية تعزيز ثقافة الأمن السيبراني بين الطالبات.

٧. التغلب على المعوقات المالية والموارد

- ✓ **الحصول على تمويل إضافي**: البحث عن شراكات مع مؤسسات خارجية أو منظمات غير حكومية لتوفير التمويل اللازم لتنفيذ البرامج التدريبية وتنمية الوعي بالأمن السيبراني.
- ✓ **استثمار الموارد المتاحة**: الاستفادة من الموارد الحالية داخل الجامعة، مثل تعاون الأساتذة المتخصصين في مجال الأمن السيبراني أو التطوير المستمر للأنظمة التي تم توفيرها مسبقًا.
- ✓ **استخدام المنح والتعاون مع القطاع الخاص**: السعي للحصول على منح من الشركات أو منظمات دولية لدعم البرامج التوعوية والتدريبية المتعلقة بالأمن السيبراني.

٨. التغلب على المعوقات النفسية والسلوكية

- ✓ **دعم نفسي مستمر للطالبات**: توفير استشارات نفسية للطالبات المتأثرات بالعنف الرقمي ودعمهن في التعامل مع الآثار النفسية التي قد تترتب على ذلك، مما يساعدهن على التغلب على الخوف من الإبلاغ أو من تبعات الحوادث.
- ✓ **تقديم حوافز مادية أو معنوية**: للطالبات المشاركات في برامج التدريب أو في الحملات التوعوية لتعزيز مشاركتهن وتحفيزهن على المشاركة في التوعية.

٩. التغلب على المعوقات التكنولوجية

- ✓ **مواكبة التطورات التكنولوجية**: يجب على الجامعة الاطلاع الدائم على أحدث التطورات في مجال الأمن السيبراني من خلال المشاركة في مؤتمرات ودورات تدريبية.
- ✓ **التوسع في التعليم التقني**: توفير برامج تعليمية لرفع مستوى المعرفة التقنية للطالبات، لتتمكن من استخدام الأدوات الرقمية بأمان ومعرفة كيفية التعامل مع المخاطر المحتملة.

قائمة المراجع

أولًا: المراجع العربية

أسماء مراد صالح (٢٠٢٤م): "تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية (تصور مقترح)"، **مجلة دراسات تربوية واجتماعية**، كلية التربية، جامعة حلوان، مج٣٠، يوليو. https://journals.ekb.eg/article_384687_d73cf116ac111243ed370ee0e3a03cd9.pdf

بدر الحيمودي (٢٠٢٣): "الأمن السيبراني وحماية الأنظمة المعلوماتية"، **مجلة شمال إفريقيا للنشر العلمي**، مج١، ع٢، أبريل- يونيو. https://najsp.com/index.php/home/article/view/39/28

بدر عدنان أحمد سعد محمد الخبيزي (٢٠٢٣م): "تحديات وتهديدات الأمن السيبراني وكيفية التغلب عليها"، **حوليات آداب عين شمس**، كلية الآداب، جامعة عين شمس، مج٥١، سبتمبر.

https://aafu.journals.ekb.eg/article_322688_56bc7d4c770ac0c54996b18310ee4840.pdf

جمهورية مصر العربية، **القانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات**، المادة ٢/٧٦.

https://elec.eecourts.gov.eg/assets/laws/10-%20%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%B1%D9%82%D9%85%2010%20%D9%84%D8%B3%D9%86%D8%A9%202003%20%D8%A8%D8%B4%D8%A3%D9%86%20%D8%AA%D9%86%D8%B8%D9%8A%D9%85%20%D8%A7%D9%84%D8%A7%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA.pdf

جمهورية مصر العربية، رئاسة مجلس الوزراء، المجلس الأعلى للأمن السيبراني، **الاستراتيجية الوطنية للأمن السيبراني٢٠٢٣-٢٠٢٧.**

https://mcit.gov.eg/Upcont/Documents/Publications_1412024000_ar_National_Cybersecurity_Strategy_2023_2027.pdf

الجهاز المركزي للتعبئة العامة والإحصاء (٢٠٢٤): **الكتاب الاحصائي السنوي، النشرة السنوية، الطلاب المقيدون- أعضاء هيئة التدريس للتعليم العالي**، جمهورية مصر العربية.

https://www.capmas.gov.eg/Pages/Publications.aspx?page_id=5104&YearID=23350

الجوهرة بنت عبد الرحمن إبراهيم المنيع (٢٠٢٢م): "متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠"، **مجلة كلية التربية**، جامعة أسيوط، مج٣٨، ع١، يناير.

https://search.shamaa.org/PDF/Articles/EGJfeau/JfeauVol38No1Y2022/jfeau_2022-v38-n1_156-194.pdf

جيهان سعد محمد الخضري، وآخران (٢٠٢٠م): "الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية- دراسة مقارنة"، **مجلة تطوير الأداء الجامعي**، مج١٢، ع١، أكتوبر.

https://jpud.journals.ekb.eg/article_170391_ac7fb65b42daa75c25cc7e0586fec704.pdf

حسين حسين زيدان، هديل علي قاسم (٢٠٢٣م): "العنف الإلكتروني الموجه نحو المرأة وانعكاساته على صحتها النفسية: دراسة ميدانية"، **مجلة العتبة الحسينية المقدسة**، مركز كربلاء للدراسات والبحوث، العراق، مج٩، ع٣، س٩، يوليو. https://www.iraqoaj.net/iasj/download/6a0460434dd0ab68

حمد بن حمود السواط، وآخرون (٢٠٢٠م): "العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف"، **مجلة البحث العلمي في التربية**، كلية البنات للآداب والعلوم والتربية، جامعة عين شمس، ع٢١، ج٤، أبريل.

https://search.shamaa.org/PDF/Articles/EGBahtht/BahthtNo21P4Y2020/bahtht_2020-n21-p4_278-306.pdf

خالد مخلف الجنفاوي (٢٠٢١م): "التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت"، **المجلة العربية للآداب والدراسات الإنسانية**، مج٥، ع١٩، يوليو. https://journals.ekb.eg/article_323180_5b3091d33981573540137c8c9d77b84b.pdf

دراسة عن العنف الرقمي ضد المرأة في مصر (أبريل ٢٠٢٣م)

https://digitalarabia.network/media/pages/articles/grab-a-coffee-read/089b94cb24-1696929782/cyberviolence_aegypt.pdf

ربيعي حسين، سمر محمود (٢٠٢٢م): "الحروب السيبرانية: المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي"، **المجلة الجزائرية للأمن الإنساني**، مج٧، ع٢، س٧، يوليو.

https://asjp.cerist.dz/en/article/196302

رشا عبد القادر محمد الهندي (٢٠٢١م): "تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول"، **مجلة جامعة الفيوم للعلوم التربوية والنفسية**، مج١٥، ع١١، سبتمبر، ص ص٣٣٨-٣٨٣.

https://jfust.journals.ekb.eg/article_213544_f1d8b90534702e3bd4abcf7eb9a6f91b.pdf

رئاسة الجمهورية (٢٠١٨م): **القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات**، الجريدة الرسمية، ع٣٢ مكرر (ج)، أغسطس، جمهورية مصر العربية.

https://manshurat.org/node/31487

رئاسة الجمهورية: **الدستور المصري ٢٠١٤، الباب الثالث: الحقوق والحريات والواجبات العامة، مادة (٥٧)**، جمهورية مصر العربية.

https://www.presidency.eg/ar/%D9%85%D8%B5%D8%B1/%D8%A7%D9%84%D8%AF%D8%B3%D8%AA%D9%88%D8%B1/

ريهام السيد عبد الجليل إبراهيم (٢٠١٧م): "دور الجامعة في مواجهة مخاطر العنف الإلكتروني عبر شبكات التواصل الاجتماعي- دراسة تحليلية"، **مجلة تطوير الأداء الجامعي**، مركز تطوير الأداء الجامعي، جامعة المنصورة، مج٥، ع٢، أغسطس.
https://jpud.journals.ekb.eg/article_95411_219068dabd0ff834602c999c3876e7bf.pdf

ريهام عصام سيد أحمد حشيش، محمد خيري محمد فتوح نوح (٢٠٢٤م): "تقنيات الذكاء الاصطناعي في الإعلام الرقمي وتأثيرها على آراء الطلاب نحو قضايا الأمن السيبراني داخل الحرم الجامعي"، **مجلة التربية النوعية والتكنولوجيا بحوث علمية وتطبيقية**، مج٣١، ع١، ديسمبر.
https://journals.ekb.eg/article_394263_cea6b78d5503e58698a03da37f7c1312.pdf

زيد نجم عبد الله العبادي (٢٠٢٤م): "العنف السيبراني الموجه ضد المرأة"، **مجلة العلوم النفسية**، المؤتمر العلمي السنوي السادس والعشرون (الأمن المجتمعي... التحديات والمعالجات)، العراق، مج٣٥، ع٢، ج٣.
https://www.iraqoaj.net/iasj/download/9b3eb75ddde8f205

سارة محمد روحي فتحي غزال (٢٠٢٢م): "الأمن السيبراني ودرجة وعي المؤسسات بأهميته"، **المجلة العربية للنشر العلمي**، مركز البحث وتطوير الموارد البشرية- رماح، الأردن، ع٤٧، سبتمبر.
https://search.mandumah.com/Record/1436423

سفيان يوسفي، كلثوم مسعودي (٢٠٢٤م): "الأمن الفكري وتحديات الأمن السيبراني: دراسة نظرية"، **مجلة الباحث**، الجزائر، مج١٦، ع٢. https://asjp.cerist.dz/en/article/254204

شريفة محمد السويدي، زيزيت مصطفى نوفل (٢٠٢٣م): "دور الأسرة في تدعيم الأمن السيبراني لمواجهة الابتزاز الإلكتروني- دراسة كيفية"، **مجلة الآداب**، كلية الآداب، جامعة بغداد، العراق، ع١٤٧، ديسمبر. https://aladabj.uobaghdad.edu.iq/index.php/aladabjournal/article/view/4125/3637

شيماء كمال عبد العليم حسن (٢٠٢٣): "العنف الرقمي وعلاقته بالأفكار الانتحارية وهوية الأنا لدى عينة من المراهقين في ضوء بعض المتغيرات الديموجرافية"، **مجلة قطاع الدراسات الإنسانية**، كلية الدراسات الإنسانية، جامعة الأزهر، ع٣٢، ديسمبر.
https://search.mandumah.com/Record/1458860

صلاح الدين محمد توفيق، شيرين عيد مرسي (٢٠٢٣م): "متطلبات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس (جامعة بنها أنموذجًا)"، **المجلة التربوية**، كلية التربية، جامعة سوهاج، ع١٠٥، ج٢، يناير.
https://edusohag.journals.ekb.eg/article_283004_85504d5b82a4272d8d58c94438d4b252.pdf

عايدة عبد الكريم العيدان، بدور مسعد المسعد (٢٠٢٤م): "درجة الوعي بالأمن السيبراني ودور تكنولوجيا التعليم في تنميته لدى طلبة كلية التربية الأساسية بدولة الكويت"، **مجلة كلية التربية**، جامعة الإسكندرية، مج٣٤، ع٤، ج٢.

https://journals.ekb.eg/article_393474_b990008638a0776a0fb59bcb7b7098fe.pdf

عائشة عبيد الله العازمي (٢٠٢٤م): "واقع الأمن السيبراني في التعليم وعلاقته بالأمن النفسي من وجهة نظر المعلمات بدولة الكويت"، **المجلة الدولية لنشر البحوث والدراسات**، مج٥، ع٥٩، سبتمبر.

https://www.ijrsp.com/pdf/issue-59/2.pdf

عبد الغني محمد إسماعيل العمراني (٢٠١٣م): **أساسيات البحث التربوي**، دار الكتاب الجامعي، صنعاء، اليمن.

https://kolalkotob.com/book4375.html

عبير بنت محمد بن ربيع عاتي (٢٠٢٣م): "الأمن السيبراني والمواطنة الرقمية"، **المؤتمر الدولي الرابع لمستقبل التعليم الرقمي في الوطن العربي**، خلال الفترة ٢٥-٢٧ أغسطس، المملكة العربية السعودية.

https://search.shamaa.org/PDF/Books/Su/BookCh/KECR/FICFDEAW/2023_atia_344860_001-015.pdf

علي آل مداوي (٢٠٢٣م): "الأمن السيبراني: تعريفه- أهميته- أنواعه- استراتيجيات الوقاية من الهجمات السيبرانية"، **مجلة الدراسات الدولية**، وزارة الخارجية- معهد الأمير سعود الفيصل للدراسات الدبلوماسية، ع٣٤.

https://www.ids.gov.sa/ids/wp-content/uploads/intl_studies/%D9%85%D8%AC%D9%84%D8%A9%20%D8%A7%D9%84%D8%AF%D8%B1%D8%A7%D8%B3%D8%A7%D8%AA%20%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9%20%D8%A7%D9%84%D8%B9%D8%AF%D8%AF%2034.pdf

علي بن طراز (٢٠٢٤م): "الأمن السيبراني: المدلول والماهية"، **مجلة البحوث والدراسات المعاصرة**، الجزائر، مج٢، ع١. https://asjp.cerist.dz/en/article/255676

علي صلاح الحديثي، عامر عاشور عبد الله (٢٠١٩): "الحماية القانونية للمرأة من العنف الإلكتروني"، **مجلة الاجتهاد القضائي**، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، مج١٢، ع٢، أكتوبر. http://search.mandumah.com/Record/1031341

علياء عمر كامل فرج (٢٠٢٢م): "دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي- جامعة الأمير سطام بن عبد العزيز نموذجًا"، **المجلة التربوية**، كلية التربية، جامعة سوهاج، عدد فبراير، ج١، مج٩٤.

https://edusohag.journals.ekb.eg/article_212365_d8eb0c9783cebf97a18a4d7a20a2f5e8.pdf

عمار حسن صفر (٢٠٢٤م): "مستوى وعي المعلمين في مدارس التعليم العام بدولة الكويت بالأمن السيبراني من وجهة نظرهم"، **مجلة كلية التربية ببنها**، ع١٣٩، ج١، يوليو.

https://journals.ekb.eg/article_378864_14a7991982a163800fb7c024b08fa3bf.pdf

العنود بنت عبد الله بن محمد الحميد، نورة بنت محمد المطرودي (٢٠٢٤م): "دور المدرسة الثانوية بمنطقة القصيم في تنمية الوعي بالأمن السيبراني لدى طالباتها"، **مجلة كلية التربية**، جامعة طنطا، مج٩٠، ج٢، يوليو.

https://journals.ekb.eg/article_381980_aded4aefb8af45415c8b3cb3b29c68c6.pdf

فاطمة الزهرة قمقاني (٢٠٢٣م): "العنف ضد المرأة: العنف الرقمي ضد المرأة أنموذجًا"، **مجلة الحكمة للدراسات الاجتماعية**، مج١١، ع٣. https://asjp.cerist.dz/en/article/234118

فاطمة يوسف المنتشري (٢٠٢٠م): "دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات"، **المجلة العربية للعلوم التربوية والنفسية**، مج٤، ع١٧، يوليو.

https://search.shamaa.org/PDF/Articles/EGAjeps/AjepsVol4No17Y2020/ajeps_2020-v4-n17_457-484.pdf

قطاف سليمان، بوقرين عبد الحليم (٢٠٢٢م): "الأمن السيبراني والمضامين المفاهيمية المرتبطة به"، **مجلة طبنة للدراسات العلمية الأكاديمية**، الجزائر، مج٥، ع٢.

https://asjp.cerist.dz/en/article/206714

كوكب الزمان بليردوح، وآخران (٢٠٢٢م): "دواعي وتداعيات ظاهرة العنف الرقمي عند الشباب عبر مواقع التواصل الاجتماعي"، **مجلة المعارف للبحوث والدراسات التاريخية**، جامعة الشهيد حمه لخضر الوادي– كلية العلوم الاجتماعية والإنسانية، الجزائر، مج٧، ع٤، مايو.

https://asjp.cerist.dz/en/article/188118

محمد إبراهيم عبده السيد، وليد سعيد أحمد سيد (٢٠٢٢م): "قيم تعزيز الأمن الرقمي لدى طلاب الجامعات في مصر لمواجهة تحديات الثورة الرقمية"، **مجلة جامعة الفيوم للعلوم التربوية والنفسية**، مج١٦، ع٥، يوليو.

https://jfust.journals.ekb.eg/article_255815_1913ebf518c2d469691ad6cd8eb4c57d.pdf

مريم بنت محمد فضل الشهري (٢٠٢١م): "دور إدارة الجامعة في تعزيز الوعي بالأمن السيبراني لدى طلبة كلية التربية بجامعة الإمام محمد بن سعود الإسلامية"، **مجلة العلوم الإنسانية والإدارية**، مركز النشر والترجمة، جامعة المجمعة، المملكة العربية السعودية، ع٢٥، ديسمبر.

https://www.mu.edu.sa/sites/default/files/2022-03/publishing_25_new.pdf

مشاعل بنت شبيب بن مطيران الظويفري (٢٠٢١م): "واقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية"، **المجلة الدولية للدراسات التربوية والنفسية**، مج١٠، ع٣، ديسمبر.

https://search.shamaa.org/PDF/Articles/JOIjeps/IjepsVol10No3Y2021/ijeps_2021-v10-n3_635-655.pdf

مصباح أحمد حامد الصحفي، سناء صالح عسكول (٢٠١٩م): "مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة"، **مجلة البحث العلمي في التربية**، ع٢٠، ج١٠.

https://jsre.journals.ekb.eg/article_56490_f3d9f1fec1531851714069afa219cb0c.pdf

ممدوح الغريب السيد يونس (٢٠٢٣): "العنف الرقمي القائم على النوع الاجتماعي لدى طالبات الجامعات المصرية: دراسة ميدانية في ضوء نظرية بيير بورديو"، **مجلة كلية التربية**، جامعة الأزهر، ع١٩٧، ج٢، يناير. https://journals.ekb.eg/article_289574_e14c7fee15177433d540b23212579c93.pdf

منى عبد الله السمحان (٢٠٢٠م): "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، **مجلة كلية التربية**، جامعة المنصورة، ع١١١، يوليو.

https://maed.journals.ekb.eg/article_140786_92feaa0b360fd79ceb4b6c5d7a95be72.pdf

مؤسسة جنوبية حرة: **السلامة الرقمية**، الجزء الثالث: الوسائل الإجرائية القانونية للتعامل مع العنف الرقمي.

https://ganoubia-hora.com/wp-content/uploads/2023/10/%D8%A7%D9%84%D8%B3%D9%84%D8%A7%D9%85%D8%A9-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A%D8%A9.pdf

نوال وسار (٢٠٢١م): "العنف الرقمي ضد المرأة: امتداد الظاهرة وتمدد الأشكال"، **مجلة الرواق للدراسات الاجتماعية والإنسانية**، المركز الجامعي أحمد زبانة غليزان- مخبر الدراسات الاجتماعية والنفسية والانثروبولوجية، الجزائر، مج٧، ع١. https://asjp.cerist.dz/en/article/156151

نورة عمر الصائغ، وآخرون (٢٠٢٠م): "وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم"، **مجلة كلية التربية**، جامعة أسيوط، مج٣٦، ع٦، يونية.

https://search.shamaa.org/PDF/Articles/EGJfeau/JfeauVol36No6Y2020/jfeau_2020-v36-n6_041-090.pdf

هاني رزق عبد الجواد الألفي (٢٠٢٢م): "القيادات الأكاديمية وأدوارها في تعزيز ممارسات الأمن السيبراني بالجامعات الأمريكية وإمكانية الإفادة منها بالجامعات المصري"، **مجلة كلية التربية**، جامعة المنصورة، ع١١٩، أبريل.

https://maed.journals.ekb.eg/article_269212_78babb976e961a2679a4b0befdedb087.pdf

يوسف بلعباس (٢٠٢٣م): "العنف الرقمي ضد المرأة وتجلياته على العلاقات الاجتماعية في ظل جائحة كورونا في تصور أستاذات التعليم العالي: الفيسبوك أنموذجًا- دراسة ميدانية"، **مجلة المقدمة للدراسات الإنسانية والاجتماعية**، كلية العلوم الإنسانية والاجتماعية، جامعة باتنة١ الحاج لخضر، الجزائر، مج٨، ع٢، ديسمبر. https://asjp.cerist.dz/en/article/238720

ثانيًا: المراجع الأجنبية

ADEJUWON, F. E., & OJEAGBASE, I. O. (2023). Role of Cybersecurity Education in Promoting Ethical and Responsible Use of Technology for Sustainable Development. In **Lead City University Postgraduate Multidisciplinary Conference Proceedings** (Vol. 1, No. 3). https://www.journals.lcu.edu.ng/index.php/LCUPGMCP/article/view/867/641

Amin, M. (2024). The Importance of Cybersecurity and Protecting of Digital Assets and Understanding the Role of Cybersecurity Laws in Safeguarding Digital Assets. **Indian Journal of Public Administration**, 70(3). https://journals.sagepub.com/doi/pdf/10.1177/00195561241271520?casa_token=Q3ydx5NIsUIAAAAA:mRDXa_TdsSyEzLlEJWojA1k6rcgbTRI1dy_sZpYEyqdLjvbMnuXpkcfU-qSkhE0Ahpw5B1bDtfkdoik

Bjelajac, Ž., & Filipović, M.A. (2021). Specific characteristics of digital violence and digital crime**. LAW- theory and practice**, 38(4). https://www.ceeol.com/search/article-detail?id=1014514

Duman, M. Ç. (2023) DIGITAL VIOLENCE AND WOMEN: SYSTEMATIZATION OF RESEARCHS AND SUGGESTIONS FOR FUTURE RESEARCH. **Anadolu University Journal of Economics and Administrative Sciences**, 24(3). https://dergipark.org.tr/en/download/article-file/2700219

European Union's Rights, Equality and Citizenship Programme (2014–2020). **Cyber Violence against Women & Girls REPORT**. https://www.stoponlineviolence.eu/wp-content/uploads/2020/06/Cybersafe_Report_200623_web.pdf

Hassan, F. M.& et.al. (2020). Cyber violence pattern and related factors: online survey of females in Egypt. **Egyptian journal of forensic sciences**, 10. https://link.springer.com/content/pdf/10.1186/s41935-020-0180-0.pdf

Kaphle, P. (2019). Cyber violence against women and girls in Nepal. **Kathmandu School of Law Review (KSLR),** 7(1). https://heinonline.org/HOL/LandingPage?handle=hein.journals/kslr7&div=9&id=&page=

Karanac, R. & et.al. (2016). PREVENTION OF DIGITAL VIOLENCE IN EDUCATIONAL INSTITUTIONS. **Journal Plus Education**, 16(2). https://www.ceeol.com/search/article-detail?id=616264

Mahdi, A. M., & Sheriji, I. L. (2024). Causes and forms of virtual violence against women. **Tamjeed Journal of AI Innovations in E-Learning and Education**, 1(2). https://www.tamjeedpub.com/index.php/TJAI-ELE/article/view/110/41

Malanga, D. F. (2021). Survey of cyber violence against women in Malawi. **Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development**. https://arxiv.org/pdf/2108.09806

Mohammed, M., & Bamasoud, D. M. (2022). The impact of enhancing awareness of cybersecurity on universities students: a survey paper. **Journal of Theoretical and Applied Information Technology**, 100(15).

https://www.jatit.org/volumes/Vol100No15/19Vol100No15.pdf

Odaibat, A. A., & Eyadah, H. T. A. (2024). A Proposed Conception of the Role of the Family in Achieving Digital Security in Light of Achieving Cybersecurity. **International Journal of Latest Research in Humanities and Social Science (IJLRHSS)**, *7* (10).
http://www.ijlrhss.com/paper/volume-7-issue-10/1-HSS-2923.pdf

Oladokun, B. & et.al. (2024). Cybersecurity Risks: A Sine Qua Non for University Libraries in Africa. **Southern African Journal of Security**.
https://unisapressjournals.co.za/index.php/sajs/article/view/15320/7625

Özsungur, F. (2021). Strategic social work management in digital violence against women. **Journal of Society & Social Work,** 32(2).
https://dergipark.org.tr/en/download/article-file/1432249

Polyzoidou, V. (2024). Digital Violence Against Women: Is There a Real Need for Special Criminalization?. **International Journal for the Semiotics of Law-Revue**, 37(6).
https://link.springer.com/content/pdf/10.1007/s11196-024-10179-3.pdf

Sevinch, Q. (2024). CYBERSECURITY, CYBERCRIME, CYBERWARS AND THEIR PROBLEMS IN CYBERETHICS. **International Conference on Developments in Education**, Bursa, Turkey, May 20th.
https://www.econferencezone.org/index.php/ecz/article/view/2846/2691

Un Broadband Commission (2015). Cyber Violence Against Women and Girls. **A Report by the UN Broadband Commission for Digital Development Working Group on Broadband and Gender**.
https://networkedintelligence.com/wp-content/uploads/2019/02/Cyber_violence_Gender-report.pdf

West, J. (2014). **Cyber-violence against women**. Battered Women's Support Services.

http://www.bwss.org/wpcontent/uploads/2014/05/CyberVAWReportJessicaWest.pdf