جامعة جنوب الوادي

كلية التربية بالغردقة

المجلة التربوية

المتطلباتُ التربويَّةُ لتعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة مخاطر التواصل الاجتماعي

إعداد

هنية جاد عبد الغالي عيد

أستاذ أصول التربية المساعد

كلية التربية– جامعة أسوان

١٤٤٥هـ - ٢٠٢٤م

تاريخ استلام البحث: ٢٠٢٤/٤/٣١ تاريخ قبول النشر: ٢٠٢٤/٥/١

مستخلص البحث

المتطلبات التربوية لتعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة مخاطر التواصل الاجتماعي.

استهدف البحث معرفة درجة توافر المتطلبات التربوية لتعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة مخاطر التوصل الاجتماعي؛ بالإضافة إلى وضع تصور مقترح لمتطلبات تعزيز الأمن الرقمي، واعتمد البحث المنهج الوصفي .

وتكونت عينة الدراسة الميدانية من مجموعة من طلاب جامعة أسوان للعام الدراسي ٢٠٢٣ – ٢٠٢٤م، وعددهم (١٣١١) طالباً وطالبة، ومما أشارت اليه نتائج الدراسة إلى وجود قصور فى توافر المتطلبات التربوية: (الشخصية والاجتماعية والتكنولوجية) لدى طلاب جامعة أسوان.

وخلصت الدراسة إلى وضع تصور مقترح للمتطلبات التربوية لتعزيز الأمن الرقمي لدى طلاب جامعة أسوان لمواجهة مخاطر مواقع التواصل الاجتماعي.

الكلمات المفتاحية: متطلبات تعزيز– الأمن الرقمي – مخاطر مواقع التواصل الاجتماعي.

Research title:

Educational requirements for enhancing digital security among university students to confront the dangers of social media.

Abstract:

The research aimed to determine the degree of availability of educational requirements to enhance digital security among university students to confront the risks of social networking. In addition to developing a proposed vision for the requirements for enhancing digital security، the research adopted the descriptive approach.

The field study sample consisted of a group of Aswan University students for the academic year 2023-2024 AD، and they numbered (1311) male and female students. The results of the study indicated that there was a deficiency in the availability of educational requirements (personal، social، and technological) among Aswan University students.

The study concluded by developing a proposed vision for the educational requirements for enhancing digital security among Aswan University students to confront the dangers of social networking sites.

Keywords: Educational requirements - digital security - risks of social communication.

Print: (ISSN: 2535-2334) Online: (ISSN: 2682-4809)

الإطار العام للبحث

مقدمة:

لقد شهد العالم مؤخراً تطورًا هائلاً في تكنولوجيا الاتصالات والمعلومات، والتي شملت معظم جوانب الحياة، وكانت أشبه ما تكون بالثورة في حياة البشرية وأسلوبها معتمدة على تكنولوجيا الحواسب الآلية والأجهزة المحمولة وشبكات المعلومات والإنترنت، وقد أحدثت هذه التطورات التكنولوجية ثورة ونقله نوعيه كبيرة في عالم الاتصالات، حيث انتشرت شبكة الإنترنت في كافة أرجاء المعمورة، سيطرت على حياتنا اليومية ودخلت في تفاصيلها، سواءً الحياة العلمية أو العملية. وأصبحت أمور حياتنا متعلقة باستخدام الإنترنت والتكنولوجيا.

وقد أدى تنوع تطبيقات، وبرامج الإنترنت واختلاف مهامها، ووسائل التعامل معها خلال السنوات القليلة الماضية، لتحولها إلى وسيلة لجذب فئات متنوعة من البشر على اختلاف أعمارهم واهتماماتهم، فبعد أن كان استخدام الإنترنت في السابق مقصوراً على الكبار، انتشر في الوقت الراهن ليشمل شريحة كبيرة من الأطفال والمراهقين والشباب، الذين وجدوا فيه وسيلة ممتعة؛ لتحقيق الكثير من رغباتهم وإبراز شخصياتهم. (عبد الواحد، ٢٠٢٠، ٦٧)

ومع حدوث ثورة المعلومات والاتصالات التي حدثت في الآونة الأخيرة، ومن خلال الشبكة العنكبوتية (الإنترنت) ظهرت مواقع التواصل الاجتماعي، وإقبال الشباب وغيرهم لاستخدام هذه المواقع فيما بينهم، فقد تحولت إلى ظاهرة اجتماعية عامة.

إن امتلاك حساب على مواقع التواصل الاجتماعي أصبح أسلوب حياة أكثر منه مشاركة اجتماعية على الإنترنت، خصوصاً لدى فئة الشباب، الذين تبنّوا هذه القفزة التكنولوجية بالكامل، واستطاعوا عبر استحداثهم لعدد من التقنيات تغيير كيفية التواصل وتبادل المعلومات والأفكار فيما بين البشر بشكل لا يمحى(Kaplan،2011)

وتعد فئة الشباب – عمومًا – وطلاب الجامعة منهم بصفة خاصة – أكثر الفئات العمرية استخداما للتقنيات الرقمية وخاصة مواقع التواصل الاجتماعي، والأكثر استيعابًا لها، فهم لا يستطيعون التخلي عنها، حيث أصبحوا يقضون أوقاتًا طويلة أمام شاشات الكمبيوتر، في كتابة الرسائل الإلكترونية، والدخول في حوار عبر غرف الدردشة، وإرسال الرسائل القصيرة والسريعة عبر الهواتف المحمولة، وغيرها من الممارسات، في الوقت الذي يفتقد الكثير منهم للمهارات الرقمية، والقدرات التي تقيس مدى سلامة المحتوى، ومختلف العلاقات التي يتعرضون لها عبر الإنترنت.

ورغم كل الإيجابيات والراحة والتي توفرها لنا التكنولوجيا ومواقع التواصل الاجتماعي، إلا أنه ظهرت مشكلات ومن أهمها جرائم الإنترنت التي تهدد الأمن الشخصي والدولي بكافة أنواعه، كما أدى التقدم الهائل والمتنامى فى استخدام الإنترنت ومواقع التواصل الاجتماعي إلى سرعة الانتشار للأفكار البناءة والهدامة ، بل والتأثير فى مجريات الأحداث على الصعيدين الإقليمي والدولى، ونشر روح الغلو والتعصب والانحرافات الفكرية والأخلاقية والتى تؤدى إلى عزعة أمن واستقرار المجتمع.

وفي ظل تلك الفوضى والإتاحة وصراعات القوى والأنظمة الدائمة مع الحقوق والحريات الإنسانية، وفي ظل معطيات الثورة الرقمية نشأ مفهوم الأمن الرقمي؛ لحماية الأفراد والجماعات والمؤسسات من التهديدات، والمخاطر التي قد يواجهونها عند استخدام شبكة الإنترنت، ويتضمن هذا المفهوم معاني ودلالات من بينها الحماية والمكافحة، ويقوم على إرساء معايير من بينها مواجهة العنف، والتمسك بالقيم والأخلاق، ومحاربة الجريمة، فضلاً عن تفعيله لممارسة القوة من خلال العقاب التشريعي والتدبير التنظيمي في الحماية والمواجهة، والذي من شأنهما تشكيل بنية رقمية، تتسم بالضبط والسيطرة، مما ينعكس إيجابًا على ضبط وأمن وسلامة البنية الواقعية (فوزي، ٢٠١٩، ١٣٢).

وتزداد أهمية الأمن الرقمي باعتباره يشمل جميع جوانب العملية التعليمية والاجتماعية والاقتصادية والإنسانية ، وباعتباره ممثلاً لقدرة الدولة على حماية مصالحها

وشعبها فى مختلف المجالات الحياتيه اليومية ومسيرته نحو التقدم بأمان، ومن كونه يرتبط ارتباطاً وثيقاً بسلامة مصادر الثروة المعلوماتية فى العصر الحالى، والقدرة على الاتصال والتواصل وهى المحور الذي يتكون حوله الإنتاج والإبداع والقدرة على المنافسة.

ويعد تحقيق الأمن الرقمي الحل الأمثل لمتابعة الاستخدام الواسع للإنترنت، وتطبيقاته وأنظمته المختلفة؛ للتقليل من المخاطر التي تنشأ عن سوء الاستخدام، في ظل وجود محتويات غير مشروعة، وغير مرغوب فيها ذات تأثير سلبي على أخلاقيات وقيم المجتمع، وتؤدي إلى تغيرات في شخصية أفراده، وميل بعضهم لسلوكيات منحرفة، وبالتالي كثرة الجرائم الإلكترونية؛ الأمر الذي يفرض ضرورة بناء مجتمع واع، مسئول ومدرك لهذه المخاطر؛ ليستطيع التعامل معها، وفقا لقواعد السلامة، مع إدراكه للعواقب القانونية، للتصرفات غير المسئولة، والتي تعرض الآخرين للخطر (جبور، ٢٠١٦ ، ١٣٠).

وبناء على أن ذلك فقد أصبح الأمن الرقمي أصبح جزءًا أساسيًا وعضويًا في مختلف أنظمة الأمن، سواء الوطني، أو الفردي، أو الاجتماعي، أو التربوي، أو الصحي، أو البيئي، أو الاقتصادي؛ بل أصبح الحلقة الأهم والأخطر والأكثر تعقيدًا وفاعلية من بين حلقات كل من تلك الأنظمة، حتى يمكن القول إنه لا أمن ولا أمان من دون أمن رقمي.

وفى هذ الصدد فقد أجرت **المنتشرى (٢٠٢٠)** دراسة لتعزيز الأمن الرقمي فى المدارس، **وأوضح طوالبية (٢٠١٧، ٦٥)** أن الأمن الرقمي هو واحد من أهم القضايا في العصر الحالي، وسوف تستمر هذه الأهمية في النمو لوجود طلب متزايد على الأجهزة الإلكترونية المختلفة والإنترنت.

وأكدت دراسة **السيد(٢٠٢٠ ، ٢١٠)** أن الأمن الرقمي يعد من أهم المداخل الحديثة لمواجهة ظاهرة التنمر الإلكتروني، من خلال تمكن الفرد من حماية ما لديه من معلومات وبيانات شخصية والسيطرة عليها، **ويرى أحمد (٢٠١٣ ، ١٩٦)** أن الأمن

الرقمي يضمن لمستخدمي الإنترنت أمن البيانات والمعلومات وعدم تسريبها وحماية حقوق الملكية الفكرية، ومراعاة الخصوصية واحترامها واتخاذ كافة التدابير الوقائية لحماية أفراد المجتمع من البيانات والمعلومات الضارة.

كما قدمت دراسة سيبونين Siponen) ،(**2009**تصوراً لبرنامج وعى أمن رقمى فى المؤسسات وذلك لتقليل أخطاء المستخدمين، ولتحسين فعالية سيطرة االمن المطبقة توصلت إلى أن تقنيات أو إجراءات أمن المعلومات تفقد فائدتها الحقيقية إذا تم إساءة استخدامها، أو تم تفسيرها بطريقة خاطئة أو تم تطبيقها بشكل غير صحيح من قبل المستخدمين.

وأكد (الزهراني، وآخرون، ٢٠٢٠ ، ٣٦٥) أنه لابد أن يكون لدى الطلاب الوعي الكافي بالمخاطر التي يمكن أن يتعرضوا لها عبر البيئات الرقمية بكافة أنواعها، ومنها سرقة البيانات الشخصية، والانتحال والابتزاز وترويج الأفكار والمعتقدات الفكرية الهدامة، وهذا من شأنه أن يحميهم من خطر الإصابة بما يهدد أمنهم الرقمي.

وعلى الرغم من أن طلاب القرن الحادي والعشرين المنغمسين في التقنية هم أكثر تمكناً في استخدام التقنية من آبائهم أو معلميهم، إلا أنهم يحتاجون دائماً إلى التوجيه والإرشاد حول الاستخدام الأفضل لتطبيق هذ الأدوات القوية في مهام التعلم المعقدة والمبتكرة. (ترلينج، ٢٠١٣، ٨٢٠).

كما أوضح بيوران وآخرونBeuran et al) ،(2016 أن القدرة العملية على التعرف على رسائل بريد الإلكتروني والمواقع الإلكترونية التصيدية أكثر أهمية من المعرفة المجردة لماهية رسائل البريد الإلكتروني والتصيد الاحتيالي، وهي المعرفة التي يتم تقديمها عادة في دورات التعلم الإلكتروني.

وقد أثبتت دراسة مارتن وآخرينMartin et al) ، (2018 أن التسلط عبر الإنترنت والهوية الرقمية وتأثير البصمات الرقمية واستخدام الوسائط الاجتماعية غير الملائمة من الموضوعات التي تحظى باهتمامها في المؤسسات التعليمية، ومع زيادة

مؤسسات التعليم التي تنفذ المبادرات المتعقلة بإحضار أجهزة إلكترونية للطلاب أصبح الاهتمام بهذا الموضوع يتزايد أهميته.

وهدفت دراسة أحمد فرج (٢٠١٣) إلى التعرف على فعالية البرنامج الإلكتروني المقترح في الأمن التكنولوجي لتعديل بعض السلوكيات الخطأ لدى طلاب الجامعات المصرية أثناء تعاملهم مع مواقع شبكات التواصل الاجتماعي.

إن الجامعات المصرية ليست بمنأى عما يدور محلياً وعالمياً، في استخدام ونشر تكنولوجيا المعلومات والاتصالات، مع الاهتمام بإتاحتها للجميع، لاستخدامها بيسر خاصة لدى طلاب الجامعة، باعتبارهم " الثروة الحقيقية للوطن؛ لأنهم سيتولون قيادة المجتمع في المستقبل، ومن ثم فإن على مؤسسات المجتمع أن تعمل بكل طاقاتها من أجل بناء وتنمية شخصية الطلاب من الناحية العقلية، والانفعالية، والأخلاقية، والاجتماعية، والسياسية، وبالتالي تنمية المجتمع، ولكونها المنوطة بعملية إعداد المواطن الصالح الملم بحقوقه وواجباته؛ فقد تعالت الأصوات بالدور الرئيسي الذي يمكن أن تلعبه الجامعات في تحقيق الأمن الرقمي وأبعاده للحفاظ على الطلاب.

فالجامعة مسئولة عن تربية وحماية الشباب تجاه المخاطر والتهديدات المعاصرة التى تواجههم، وخاصة تلك المرتبطة بالجانب الثقافى والمعلوماتى التى أصبحت السمة السائدة فى هذا العصر، وما يترتب عليها من جرئم أو انحرافات أخلاقية قد تلهم بهم أثناء تعاملهم مع تلك التطبيقات التكنولوجية وهو ما يفرض عليها دوراً مضاعفاً فى توعية الطلاب بثقافة الأمن الرقمي خصوصاً مع التزايد المستمر لمستخدمى تلك الأجهزة الإلكترونية الحديثة، ومع وجود العديد من الأبعاد والأثار العلمية والتكنولوجية والقيمية والسياسية السلبية التى قد تنجم عن الاستعمال السيء للمعلومات.

ونظراً لأن إمداد طلاب الجامعة بالقيم والسلوكيات المرتبطة بالأمن الرقمي لم تعد ترفيها أو تسلية بل ضرورة اجتماعية لتنشئة مواطن رقمي قادر على التواصل الإلكترونى والحصول على الخدمات التعليمية والمعرفية والتكنولوجية، وإدراك حقوقه

وواجباته ومسؤولياته تجاه نفسه ومجتمعه؛ لذا يحاول البحث الحالى وضع تصور مقترح لمتطلبات تعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة مخاطر التواصل الاجتماعي.

مشكلة البحث:

لقد شهدت الألفية الأخيرة من الزمن تطوراً إلكترونياً مذهلاً صاحبه تطور وتبادل للمعلومات والتقنيات العلمية ووسائل الاتصال الفوري وظهور شبكة المعلومات التى أدت إلى فتح أبواب عالمية لتسهيل التعاملات والتبادلات بين الأفراد والتى تحولت من تعاملات تقليدية إلى تعاملات إلكترونية عبر فضاء رقمى.

إن التطور التكنولوجي المذهل الذى يعيشه العالم سلاحاً ذو حدين فبالرغم من الإيجابيات التى حققها إلا أن هذا لا ينفى إنعكاساته السلبية التى تولدت عنه وأثرت بدرجة كبيرة على المجتمع بصفة عامة وعلى طلاب الجامعات بصفة خاصة، وقد ظهرت ملامحها فى استخدام واستغلال مختلف التقنيات التكنولوجية الحديثة بصورة غير مشروعة ؛ مما أدى إلى تنامى وتزايد وانتشار نوع من الجرائم لم تكن معروفة سابقاً ألا وهى الجرائم الرقمية أو ما يطلق عليها الجرائم الإلكترونية التى تهدف إلى إضرار بمصالح الأفراد وكذا الجماعات والدول.

فنتيجة للاستخدام غير اللائق لمختلف وسائل التقنية الحديثة ووسائل التواصل الاجتماعي ظهرت معها الجرائم المعلوماتية التي فرضت نفسها على المؤسسات التعليمية والتى من الجرائم أكثرها شيوعًا بين الطلبة الجامعيين: انتحال شخصية الآخرين أثناء تصفح أو استخدام البريد الإلكتروني، أو الانتهاك والتعدي على الملكية الفكرية، أو أخذ المعلومات الشخصية دون الإذن من أصحابها.

كما أثرت وسائل التواصل الاجتماعي الرقمنة سلبيًا على الشباب الجامعي في جوانب كثيرة منها: زيادة الهجمات الإلكترونية عن طريق الإرهاب الإلكترونى أو التحرش من خلال الصور، والفيديوهات العدوانية المعروضة عبر الإنترنت، كما زادت من حدة

التعصب الديني والعرقي، والتشجيع على العنف الإلكتروني، وإضعاف القيم أو غيابها من خلال تقديم معلومات غير صحيحة، إلى جانب التهديد الأخلاقي، المتمثل في انهيار النظم الأخلاقية التي تشكل دعامة النظم الاجتماعية، خاصة وأن شبكة الإنترنت تعج بالمواقع غير الأخلاقية والإباحية، كما أدت إلى زيادة حجم التهديد والمضايقة والابتزاز؛ نتيجة التعرض لمحتويات مزعجة ومحرجة، أو عدوانية عبر رسائل البريد الالكتروني أو الدردشة، وزيادة نسب التنمر الإلكتروني، وذلك باستغلال تقنيات الاتصالات، للوصول إلى أهداف، إجرامية من خلال إرسال تهديدات ورسائل وصور عدائية، والإفصاح عن معلومات شخصية حساسة، أو المضايقة، أو الإحراج، أو السخرية أو الإهانة وتشويه السمعة، من خلال مواقع التواصل الاجتماعي، أو غرف الدردشة، ومنتديات النقاش أو البريد الإلكتروني، والرسائل الفورية أو الهواتف المحمولة أو صفحات الويب أو المدونات أو غيرها، (عبد الواحد، ٢٠٢٠، ٨٥ – ٨٧).

كما يعاني طلاب الجامعة يوميًا من بعض المخاطر عند تقديمهم طلبات تسجيل على شبكات التواصل الاجتماعي ومن هذه المخاطر اختراق الحسابات وتوزيع الصور المحرجة وصعوبة إزالة أو إلغاء الحسابات وغير ذلك.

وبناءً على ما ذُكِر يمكن للتكنولوجيا أن تحقق الشيء ونقيضه بحسب الأسلوب المتبع في الاستخدام، وقد تكون سلاحًا في يد القوي ضد الضعيف، وسببًا تتسع به الفجوةُ بين مالكها ومفتقدها، فلقد أضافت شبكة الإنترنت الكثيرَ من الإيجابيات إلى حياتنا المعاصرة بمسيرتها العلمية والتعليمية إلا أن النظم الحاسوبية والشبكات جلبا معهما أنواعًا جديدة من الجرائم والتجاوزات .

ومع الانتشار السيئ لمواقع التواصل الاجتماعي تأثرت شخصية طلاب الجامعة، وتكوينهم الأخلاقي والعلمي، في ظل عالم رقمي خالي في أغلب الأحيان من القواعد المرتبطة بالسلوكيات السلبية والإيجابية للمواطن الرقمي.

وفى هذا الصدد فقد كشفت نتائج دراسة الغديان وآخرون(٢٠١٨) عن صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين.

ودراسة(الحمادي، ٢٠١٧) التي أشارت إلى الجوانب الإيجابية والسلبية الناجمة عن استخدام مواقع التواصل الاجتماعي، ومخاطرها على الأمن والاستقرار وتمثلت أبرز نتائج الدراسة في التأكيد على أهمية تعزيز الأمن لمنصات التواصل الاجتماعي وعملية الاستخدام المتزايد لها من قبل كافة فئات المجتمع ، والتأكيد على أن منصات التواصل الاجتماعي تعد من أخطر الأدوات في التأثير على الرأي العام وإحداث الميول في الاتجاهات والانتماءات الفكرية والوطنية، وأهمية استحداث وحدات تنظيمية جديدة بالهياكل التنظيمية الشرطية تحت مسمى(وحدة منصات التواصل الاجتماعي.

ويؤكد أوكيفي وبيرسون O'Keeffe & Pearson،(2011) أن الانخراط في أشكال مختلفة من وسائل التواصل الاجتماعي أصبح نشاطًا روتينيًا أثبتت الأبحاث أنه مفيد للأطفال والمراهقين من خلال تعزيز الاتصال والتواصل الاجتماعي وحتى المهارات الفنية، وفي المقابل نظرًا لقدرتهم المحدودة على التنظيم الذاتي والقابلية للضغط على الأقران، يكون الأطفال والمراهقون في خطر ما؛ لأنهم يتنقلون ويجربون وسائل التواصل الاجتماعية.

واهتمت دراسة ويتمان (Whitman،2011) بحصر التهديدات التي تواجه الأمن الرقمي وهي كالتالي: الخطأ أو الفشل البشري (حوادث، أخطاء المستخدمين)، سرقة الحقوق الذهنية والفكرية (قرصنة، انتهاك حقوق الطبع)، أفعال التجسس المتعمدة (وصول غير مخول)، أفعال متعمدة الابتزاز المعلومات (ابتزاز كشف المعلومات)، أفعال متعمدة للتخريب أو التدمير (دمار االنظمة أو المعلومات)، أفعال متعمدة للسرقة (مصادرة غير شرعية من الأجهزة أو المعلومات)، هجوم متعمد للبرمجيات (فيروسات، نكران الخدمة، حصان طروادة)، كما أوضحت النتائج أن التهديد حقيقي، وخطورته

عالية، وركزت الدراسة على أن الإدارة يجب أن تكون مطلعة أكثر على تهديدات الأمن الرقمي، ويجب أن يزداد وعيها في كل المجالات.

ومن خلال عمل الباحثة في الجامعة وخبرتها في الميدان تم عمل دراسة استطلاعية لمجموعة من الطلاب قوامها (٥٠) طالبا وطالبة، وجدت أن مستوى وعى طلاب جامعة أسوان بمتطلبات الأمن الرقمي به قصور مما يقلل من مواجهتهم لمخاطر مواقع التواصل الاجتماعي، وقد أسفرت نتائج الدراسة الإستطلاعية عن الآتى:

- أن مستوى وعى طلاب جامعة أسوان بالأمن الرقمي قليل.
- تكرار استخدام طلاب الجامعة للوسائل التكنولوجية في مجالات الترفيه، والبحث عن الأخبار الرياضية وأخبار آخر الصيحات الشبابية من ملبوسات وألعاب دون الوعى بمخاطر هذه المواقع.
- أن الطلاب يفتقرون إلى الوعي بقوانين التواصل الرقمية ومهارات وفنيات التعامل الإيجابي مع من يتواصلون معهم عبر مواقع التواصل الاجتماعي.
- تواصل الطلاب مع حسابات وهمية لأشخاص أو منظمات مجهولة مما ينتج عنه مشكلات كثيرة.
- تعامل الطلاب مع مواقع لتسويق منتجات وتجارة إلكترونية مشبوهة، وأخلاقيات وأفكار مظللة؛ مما قد يؤدي بالشباب إلى الإنحراف والتخلق بمثل هذه الأخلاقيات السيئة، أو يعرضهم للإبتزاز.
- وكذلك نظرا لاستخدام الشبكات الإلكترونية ومواقع التواصل الاجتماعي فى جميع المجالات فى حياة الفرد فلابد أن يكون لدى الفرد وعى كامل بالمخاطر التى يمكن أن يتعرض لها عبر البيئات الرقمية بكافة أنواعها ومنها: سرقة البيانات الشخصية والإنتحال والابتزاز وترويج الأفكار والمعتقدت الفكرية الهدامة لذلك لابد أن يكون لدى المستخدمين ممارسات بما يتضمنه المحور الرقمي من إرشادات من شأنها أن تحميهم من خطر الإصابة بما يهدد امنهم الرقمى.

- فإذا لم تتوفر الحماية بطريقة كافية للمعلومات فإن هذه المعلومات تصبح متاحة ويمكن استخدامها من أجل تحقيق أغراض غير مرغوب فيها أو غير قانونية، لذا يجب مراعاة الحيطة والحذر من جانب الطلاب، حتى لا يتعرضون إلى أضرار على الشبكات الاجتماعية ومحاولة السيطرة على سمعتهم الرقمية، فهذه الأخيرة تعتمد بشكل كبير على الطالب نفسه بالنظر إلى أنه هو الذي يقوم بنشر المعلومات والصور الخاصة به، وكذلك مشاركة الروابط على الشبكات الاجتماعية لأن هذه المجموعة تمثل ملفه الشخصي الرقمي (المعداوي، ٢٠١٨، ١٩٦٨).

وفى هذا الصدد فقد اهتمت دراسة صلاح الدين (٢٠١٠) بتحديد طرق الحماية التكنولوجية بأنواعها وأشكالها.

ولذلك لابد من إكساب طلاب الجامعة متطلبات الأمن رقمى للبحث في أساليب ونظريات حماية المعلومات والبيانات ووضع الإجراءات اللازمة لضمان سلامتها وحمايتها، بالإضافة إلى وضع التشريعات القانونية لضبط الاعتداء على المعلومات، ومعاقبة من يفعل ذلك.

لذلك جاء البحث الحالي لطرح تصور مقترح لمتطلبات تعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة مخاطر التواصل الاجتماعي.

أسئلة البحث:

وفى ضوء استقراء ما سبق تتمثل مشكلة البحث الحالي في السؤال الرئيسي التالى: ما المتطلبات التربوية لتعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة مخاطر التواصل الاجتماعي؟ ويتفرع منه الأسئلة الفرعية التالية :

١- ما الإطار المفاهيمي للأمن الرقمي؟
٢- ما أهم مخاطر مواقع التواصل الاجتماعي، وانعكاساتها على طلاب الجامعة؟
٣- ما متطلبات تعزيز الأمن الرقمي فى الأدبيات التربوية؟

٤- ما واقع توافر متطلبات تعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة مخاطر التواصل الاجتماعي؟

٥- ما التصور المقترح للمتطلبات التربوية لتعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة مخاطر التواصل الاجتماعي؟

أهداف البحث:

هدف البحث الحالي بشكل أساسي إلى الكشف عن درجة توافر متطلبات تعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة مخاطر التواصل الاجتماعي: وبناء عليه يتم وضع تصور مقترح لمتطلبات تعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة مخاطر التواصل الاجتماعي.

أهمية البحث: تبرز أهمية البحث الحالي من خلال ما يأتي:

الأهمية النظرية:

١- اهتمام البحث الحالى بطلاب الجامعة، رجال الغد وقادة المستقبل، إذ كلما زاد الاهتمام بهم ستكون النتائج إيجابية عليهم، وعلى المجتمع ككل.

٢- تعرض طلاب الجامعة لمخاطر مواقع التوصل الاجتماعي، وخاصة المنغمسين كليًا في المجتمعات الافتراضية عبر الإنترنت؛ مما استوجب القيام بتحقيق أمن رقمى يساعد في مواجهة تلك المخاطر، والتغلب على ما تخلفه من آثار سلبية.

٣- يوفر معلومات وبيانات يمكن الاستفادة منها في وضع الخطط والبرامج التى تساعد فى مواجهة مخاطر موقع التواصل الاجتماعي وتحقيق الأمن الرقمي لدى طلا لجامعة.

٤- تبصير المسئولين عن التعليم الجامعى ومتخذي القرار بأهمية تحقيق متطلبات تعزيز الأمن الرقمي لدى الطلاب، في ظل عالم متغير بشكل متسارع، ومزدحم بوسائل الاتصال الحديثة والمتاحة لدى الجميع.

٥- تظهر أهمية البحث من خلال تعرف مواقع التواصل الاجتماعي كإحدى وسائل التكنولوجيا الحديثة التي تزايد عدد مستخدميها في الآونة الأخيرة بشكل واضح، واتسع نطاق تأثيراتها المباشرة في ثقافة الأفراد واتجاهاتهم.

الأهمية التطبيقية:

١- يعد البحث الحالى من الأبحاث القليلة في مجال الأمن الرقمي، والتي يُمكن أن تثري الإنتاج الفكري في هذا المجال.

٢- مواكبة التغير المحلي والعالمي في مجال الأمن الرقمي، قد يُساعد الطلاب في مواجهة مخاطر التواصل الاجتماعي.

٣- إيجاد حلول عملية قد تساعد طلاب الجامعة فى الحماية من مخاطر مواقع التواصل الاجتماعي.

٤- يساعد البحث على تنمية قدرت وثقافة طلاب الجامعة فى الأمن لرقمى ومعرفة طرق التعامل الصحيح مع حقوقهم ومسولياتهم الإلكترونة.

٥- التوجه الجاد نحو تضمين مفهوم الأمن الرقمي فى المناهج الدراسية .

حدود البحث: اقتصر البحث الحالي على الحدود التالية:

الحدود الموضوعية: إبراز متطلبات تعزيز الأمن الرقمي لدى طلاب الجامعة، على أن يركز البحث على مفهوم الأمن الرقمي وأهميته، مع التركيز على مخاطر التواصل الاجتماعي وانعكاساتها على طلاب الجامعة.

الحدود البشرية: عينة من طلاب وطالبات بعض الكليات النظرية: (الآداب- التجارة) والعملية(التربية – التربية النوعية) بجامعة أسوان.

الحدود المكانية: طبقت الدراسة الميدانية بجامعة أسوان بكليات: (التربية- التربية النوعية- الآداب- التجارة)

الحدود الزمانية: طبقت الدراسة في الفصل الدراسي الثاني للعام الجامعي٢٠٢٣/ ٢٠٢٤م

منهج البحث:

يسير البحث الحالي في خطواته معتمداً على المنهج الوصفي؛ لكونه المنهج الملائم لطبيعة هذا البحث، وذلك للتعرف على الإطار المفاهيمي للأمن الرقمي، وتَعرف مخاطر مواقع التواصل الاجتماعي على طلاب الجامعة وقوفاً على تحديد درجة توافر متطلبات تعزيز الأمن الرقمي والخروج بتصور مقترح للمتطلبات التربوية لتعزيز الأمن الرقمي لدى طلاب جامعة أسوان لمواجهة مخاطر التواصل الاجتماعي.

مصطلحات البحث: تمثلت فيما يلى :

- **المتطلبات التربوية Educational Requirements**

تعرف بأنها سلوكيات وأساليب تُؤدي في ضوء إمكانات مادية وبشرية لتلبية الحاجات المختلفة للفرد أو المجتمع، وذلك لتنميته خلال فترة من فترات النمو، حيث تتولي هذه التلبية المؤسسات التربوية، لتحقيق الأهداف المنوطةGood)،1973، (529 .

كما أنها الموجهات والمداخل التي يعتمد عليها موجهو التربية في صياغة الأهداف التربوية والمحتويات الدراسية والأنشطة وأساليب التقويم؛ بالإضافة إلي مناخ المؤسسة التعليمية التى تساعد على تحسين أداء الطلاب (جويلي،٢٠٠١، ٤٦).

وتعرف المتطلبات التربوية إجرائياً بأنها: السلوكيات والإجراءات اللازمة لتعزيز الأمن الرقمي لدى طلاب جامعة اسوان فى ضوء الإمكانات المادية والبشرية بالجامعة.

- **الأمن الرقمي: Digital security**

تعرفه (الزهراني، وآخرون، ٢٠٢٠ ، ٣٦٣) بأنه: تأمين البيانات والمعلومات التي يتم تبادلها ، ومشاركتها مع المجتمع الرقمي، واتخاذ الإجراءات اللازمة للحد من المخاطر التي يمكن أن يتعرض لها المستخدم للمواقع والشبكات الإلكترونية، ومواقع التواصل الاجتماعي، وتحقيق الاستخدام الأمن لجميع الفئات في المجتمع ، وخاصة الطلاب في المؤسسات التعليمية.

يعرف الأمن الرقمي إجرائياً بأنه: تأمين البيانات والمعلومات التى يتم تبادلها ومشاركتها مع المجتمع الرقمي وإتخاذ الاجراءات اللازمة للحد من المخاطر التى يمكن أن يتعرض لها المستخدم للمواقع والشبكات الإلكترونية ومواقع التواصل الاجتماعي وتحقيق الاستخدام الأمن لطلاب الجامعة.

- **مواقع التواصل الاجتماعي: Social Communication**

تعرف بأنها: مجموعة من المواقع على شبكة الإنترنت ظهرت مع الجيل الثاني للويب أو ما يعرف بإسم ويب٢.٠، والتي تتيح من خلالها التواصل بين الأفراد في بيئة بداخل مجتمع افتراضي يجمعهم حسب مجموعات اهتمام أو شبكات انتماء (بلد، جامعة، مدرسة، شركة)، ويتم ذلك عن طريق خدمات التواصل المباشر مثل إرسال الرسائل أو الإطلاع على الملفات الشخصية للآخرين ومعرفة أخبارهم ومعلوماتهم التي يجعلونها متاحة للعرض (زموري، خيرة ، ٢٠٠٥، ٦٥).

وتعرف مواقع التواصل الاجتماعي إجرائياً بأنها: مجموعة من شبكات التواصل الاجتماعي المتعارف عليها مثل (الفيس بوك، واتس اب، مدونات، تويتر)، والتي يستخدمها طلاب الجامعة للتواصل والبحث عبر الإنترنت.

المحور الأول: الإطار النظري للبحث :

يتناول الإطار النظري خلفية نظرية عن متغيرات البحث المستقلة والتابعة، حيث يتضمن ثلاثة نقاط

أولاً – ماهية الأمن الرقمي.

ثانياً– مخاطر مواقع التواصل الاجتماعي وأثرها على طلاب الجامعة.

ثالثاً– متطلبات الأمن الرقمي لمواجهة مخاطر شبكات التواصل الاجتماعي.

أولاً- ماهية الأمن الرقمي:

يعد الأمن الرقمي من أهم الموضوعات لكل من يتعامل مع التكنولوجيا وخاصة المرتبطة بشبكة الإنترنت، بسبب الهجمات الرقمية والفيروسات المختلفة التي تهاجم مراكز البيانات والأنظمة الخاصة بالأفراد للسيطرة على بيانات الممتلكات الخاصة والعامة، بهدف إخضاعها لعمليات الابتزاز والسرقة، لذا ظهر ما يسمى بالأمن الرقمي، والذي يهدف إلى الدفاع أو الحماية من المخاطر التكنولوجية.

(١): مفهوم الأمن الرقمي:

لم يعد الاهتمام بالجانب الأمني مقتصراً على مظاهر الحياة الحقيقة، فقد دخل مفهوم الأمن إلى جوانب ذات قيمة معنوية غير ملموسة، فقد ساهمت وسائل الاتصال والتكنولوجيا في توسيع مفهوم الأمن إلى جوانب لم تكن محل الاهتمام من قبل. فالبيانات والمعلومات الخاصة أصبح معرضة إلى السرقة بدون الحاجة إلى مغادرة مكان الإقامة.

ويعرف الأمن الرقمي بانه أمن المعلومات على أجهزة وشبكات الحاسب الآلي، والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدماتّ من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو اختلاف قد يحدث، حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها (الربيعة، ٢٠١٧، ٦).

ويعرفه رايبل وبيلى Ribble،(Bailey & 2017) بأنه اتخاذ الاحتياطات اللازمة لضمان السلامة الشخصية وأمن شبكة الإنترنت.

وتعرف المنتشري(٢٠٢٠) الأمن الرقمي بأنه: مفهوم أمنى خاص بحماية المعلومات وكل ما له صلة بتلك المعلومات من عمليات وخدمات وأجهزة والتقنيات ضد أي شكل من الأشكال غير المسموح به أو بتلك المعلومات

وبذلك فإن الأمن الرقمي مصطلح يصف أمن الأنشطة والمعاملات التي تتم عبر الإنترنت. إنه مكون خاص من الأفكار الأكبر للأمن الإلكتروني وأمن الكمبيوتر، بما في ذلك موضوعات تشمل أمان المتصفح والسلوك عبر الإنترنت وأمن الشبكة، حيث إنه مصطلح يصف الموارد المستخدمة لحماية الهوية والبيانات الشخصية عبر الإنترنت، نظراً لكثرة البيانات وزيادة عدد الأشخاص الذين يعملون ويتواصلون من أي مكان، حيث يقوم المستخدمون السيئون باستخدام أساليب معقدة للوصول إلى مواردك وسرقة البيانات أو تخريب العمل أو ابتزاز الأفراد للحصول على الأموال.

ويعرّف أحمد(٢٠١٣) الأمن الرقمي بأنه: "حالة من الشعور بالطمأنينة والاستقرار والأمان الذييعم المجتمع بجميع مؤسساته ونظمه وأفراد من جراء استخدام المستحدثات التكنولوجية وفق قواعد ووابط والتي من خلالها نحمي المجتمع من الأخطار التي تهدد استقرار، كما يضيف أن الأمن الرقمي يضمن لمستخدمي الإنترنت أمن البيانات والمعلومات وعد تسريبها وحماية الملكية الفكرية ومراعاة الخصوصية واحترامها واتخاذ كافة التدابير الوقائية لحماية أفراد المجتمع وجماعاته من البيانات والمعلومات الضارة.

كما يمكن تعريف الأمن الرقمي من خلال تقسيمه إلى ثلاثة أقسام:(حسن، دت، ١٨)

- **من الناحية الأكاديمية:** هو العلم الذى يبحث فى نظريات واستراتيجيات توفير الحماية للمعلومات من المخاط التى تهددها ومن أنشطة الإعتداء عليها.
- **من الناحية التقنية:** هى الوسائل والأدوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.
- **من الناحية القانونية :** هى محل الدراسات والتدابير اللازمة لضمان سرية وسلامة محتوى المعلومات وتوفرها، ومكافحة أنشطة الإعتداء عليها أو استغلالها فى إرتكاب جرائم الإنترنت.

وبذلك يشير مصطلح الأمن الرقمي إلى مجموعة من العمليات وأفضل الممارسات والحلول التقنية التي تساعد في حماية الأنظمة والشبكات الهامة الخاصة بك من الهجمات الرقمية، يتضمن برنامج الأمان عبر الإنترنت الفعال الأشخاص والعمليات والحلول التقنية التي تعمل معاً على تقليل مخاطر أي هجوم يؤدي إلى اضطراب الأعمال والخسارة المالية والإضرار بالسمعة.

من هنا فإن الأمن الرقمي هو الحفاظ على المعلومات بأسلوب سليم، وإبقاؤها تحت السيطرة المباشرة لمالكها، بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر ليس له أي صلاحية لذلك، وأن يكون الأفراد على علم بالمخاطر المترتبة عند السماح لأشخاص آخرين بالوصول إلى معلوماتهم الخاصة.

وبهذا المعنى يكون الأمن الرقمي هو عدم السماح باستخدام النظام إلا فى ما هو معد لأجله، وفى الإطار المسموح به، وذلك من خلال:

- الرقابة على التكنولوجيا وعلى أسلوب انتقال المعلومات.
- إزالة العوائق أمام انسياب المعلومات ومنع اعتراضها.
- التعرف على هوية مستخدمى النظام.
- مراقبة عمليات الخروج والدخول من وإلى النظام.
- مراقبة الحركة على الشبكة وعلى قواعد البيانات والمواقع.

(٢) أهمية الأمن الرقمي:

يعد الأمن الرقمي من الموضوعات الهامة جدًا في وقتنا الحالي، بسبب الاعتماد المتزايد على الإنترنت، في الحياة الشخصيّة أو المهنيّة، سواء لمتابعة أعماله المصرفيّة، أو التواصل الاجتماعي، أو حتّى ممارسة العمل عبر الإنترنت. ومع ذلك، تصاحب هذا الكم الهائل من الراحة والاستمتاع عبر الإنترنت، بكثيرٍ من المخاطر، حيث ظهر مجرمو الإنترنت، بهدف الاحتيال، أو سرقة المعلومات، أو

بدافع الأذى الشخصي فقط؛ الأمر الذي جعل من وجود الأمن الرقمي هامًا جدًا، لوضع حدٍ لهذه الانتهاكات على شبكة الإنترنت.

وتعود أهمية الأمن الرقمي إلى تزايد استخدام التكنولوجيا والإنترنت في حياتنا اليومية، حيث يعتمد الكثير من الأعمال والمعاملات على الشبكة العنكبوتية، وقد يتعرض الأفراد لمختلف أنواع الهجمات مثل اختراق الحسابات، والبرمجيات الخبيثة، والتصيد الاحتيالي، والتجسس الإلكتروني. تلك الهجمات يمكن أن تسبب أضراراً جسيمة للأفراد والمؤسسات من حيث سرقة المعلومات الحساسة أو تعطيل الأنظمة الحاسوبية.

وترجع أهمية الأمن الرقمي في الوقت الراهن إلى استفادة جميع الأفراد والمؤسسات ببرامج جدار الدفاع الإلكتروني المتقدمة، والذي يُمكن بدونها أن يُسفر عن سرقة بيانات سرية وهويات شخصية ، لذا جاءت برامج جدار الحماية الإلكترونية لصد التهديدات واستراتيجيات الهجوم الرقمي، وكشف الثغرات الأمنية وتثقيف أفراد المجتمع حول أهمية الأمن الرقمي وكيفية التعامل معه والتي تجعل تعامل الأفراد مع شبكة الإنترنت أكثر أمانًا (Goutam، 2021، pp. 26– 35) .

لذلك أصبح الأمن الرقمي أمراً ذا أهمية بالغة في حياة مستخدمي التقنية على اختلاف مستوياتهم وأعمارهم، وفى هذا الصدد فقد أشارت دراسة مارتن وآخرين Martin et al،(2018) إلى أن التسلط عبر الإنترنت والهوية الرقمية وتأثير البصمات الرقمية واستخدام الوسائط الاجتماعية غير الملائمة من الموضوعات التي تحظى باهتمامها في المؤسسات التعليمية.

كما تناولت العديد من الدراسات ذات العلاقة بجوانب الأمن الرقمي للمراهقين والشباب جوانب متعددة لقضايا الأمن الرقمي التي تمثل أهمية عالية لهذ المرحلة العمرية، فقد قام دويل وآخرون(Dowell et al 2009،).(550، بدراسة حول تفاعل الطلاب مع السلوكيات الخطرة عبر الإنترنت، وقد أشارت نتائج الدراسة بأن نشر معلومات وصور شخصية على مواقع الشبكات الاجتماعية، ينتج عنه سلوكيات خطرة

منها التعامل مع أشخاص غير معروفة، والتحرش عبر الإنترنت، وتجاوز مرشحات الإنترنت أو الحجب.

وبذلك فالأمن الرقمي يهتم بحماية سير هذه العمليات وحماية البيانات والتطبيقات وحفظ المعلومات للأفراد، والمحافظة عليها؛ يعني منع أي دخول عليها غير مرخص أو العبث بها بمعنى ان هناك نظام قوي يحمي هذه الخدمات والمعلومات التي توفرها وتزوّدنا بها التكنولوجيا الجميلة عبر الإلكتروني، وبذلك أصبح الأمن الرقمي حديث العالم بأسره، بل وأصبح جزءاً اسياسياً من أساسيات المؤسسات التربوية والتعليمية، حيث أصبح صُناع القرار يضعون مسائل الأمن الرقمي كأولويه في سياستهم.

ولذا فإن طلاب الجامعة بحاجة ماسة إلى مثل هذه التوعيات والتثقيف بأهمية الأمن الرقمي وسلامة البيانات وهذه التوعية والتثقيف يكون بعدة طرق كالدورات والندوات والمحاضرات والورش ونقل الثقافة والمعرفة دخل الجامعة، خصوصاً فى ظل ما يتعرض له العالم من هجوم إلكترونى على المعلومات واختراقات تطول مواقع الإنترنت، وكثيراً ما يمارس الطلاب نشاطاتهم عبر مواقع التواصل الاجتماعي كالفيسبوك والتويتر والإنستجرام وبرامج البريد الإلكترونى، حيث تعتبر هذه البرامج تربة خصبة لمثل هؤلاء القراصنة الذين يستهدفون فئة الطلاب لاستدراجهم ونصب الكمائن لهم للحصول على ما يرريدونه منهم، كإرسال روابط مفبركة لتحميل برامج خبيثة، أو الشراء من مواقع وهمية لا وجود لها.

وفى هذا الصدد فقد سعى (ريبيل، ٢٠١٢) إلى ابتكار نموذج تعليمي لمساعدة الطلاب على البدء في التفكير في كيفية استخدام التكنولوجيا في المدرسة والبيت على النحو الملائم باعتبار أنهم يعيشون في عالم مشبع بالتكنولوجيا الرقمية، ويتضمن هذا النموذج أربع مراحل على النحو التالي:

١- الوعي والإدراك ويركز على مساعدة الطلاب ليصبحوا مثقفين من الناحية التقنية، وتتجاوز مرحلة الوعي المعرفية الأساسية لأجزاء الحاسب الآلي وبرامجه إلى معرفة الاستخدام الملائم لهذ التقنيات الرقمية.

٢- الممارسة الموجهة: بعد اتباع التعليمات في مرحلة الوعي، يقوّم المعلمون الطلاب في نشاطات موجهة تساعدهم على تمييز وممارسة الاستخدام الملائم، بحيث يتم منح الطلاب فرصة لتعلم هذ المبادئ في بيئة تشجع على الاكتشاف.

٣- التمثيل والعرض : يقدم المعلمون للطلاب دروس تمثيل واوحة تركز على استخدام التكنولوجيا بشكل ملائم في الصف، بحيث يقوم المعلمون بممارسة عادات الاستخدام الرقمي الجيد أمام الطلاب.

٤- التغذية الراجعة والتحليل :يتم مناقشة استخدام التكنولوجيا داخل وخارج المدرسة من خلال أنشطة صفية يشارك فيها الطلاب، بحيث يمكن استخدام التكنولوجيا بشكل فعّال وملائم.

كما أشار فرويك (**Froehlich**)، **2012** إلى أهمية تطرق المؤسسات التعليمية المختلفة ولا سيما الجامعات لتعزيز مبادئ الأمن الرقمي لمساعدة الشباب على اتباع منهجية سليمة في التعامل مع التكنولوجيا الرقمية وحماية أنفسهم ومن حولهم من مخاطرها، بجانب الاستفادة من ما تقدمه من خدمات له وللمجتمع، وذلك من خلال التربية والمناهج التعليمية في المدارس والجامعات ؛ حتى نتمكن من حماية مجتمعاتنا من الآثار السلبية للتكنولوجيا وتحفيز الاستفادة المثلى منها للمساهمة في بناء الاقتصاد الرقمي للمجتمع.

وأكد العريشي (٢٠١٨، ٣١٨) على ضرورة نشر المؤسسات التعليمية الوعى والتوعية فى مجال الأمن الرقمي ؛ حتى يعى الطلاب أهمية البينات والمعلومات التى يتم تداولها والحفاظ عليها من السرقة أو التسريب. فالتوعية بالأمن الرقمي لدى الطلاب سوف يكون له الأثر الإيجابي والقعال فى غرس أساسيات الأمن القمى فى عقول الطلبة

والطالبات، خصوصاً وأن هذه المؤسسات تحتوى على جيل الشباب الذي باستطاعته فهم هذه الاساسيات وتطيقها فى حياتهم العملية والمستقبلية.

وبذلك يمكن القول: بإن الأمن الرقمي يهتم بوضع الرؤى والسياسات والإجراءات التي تصمم وتنفذ بهدف تحقيق عناصر الحماية والصيانة المختلفة التي تضمن أن يتحقق للمعلومات السرية والموثوقية؛ أي أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.

من هنا أصبحت قضية الأمن الرقمي تهم كل فرد من أفراد المجتمع أياً كان عمله، بل أصبحت تهم كل من لديه معلومات ويتواصل عبر الإنترنت، كما أصبحت تهم المستفيد العادي والشركات التي تقدم خدمات المعلومات، ومصممي النظم والتطبيقات ومطوري الأجهزة والبرمجيات، وفي الوقت ذاته تهم رجال التشريع والقانون ورجال الأمن، والمدرسين والطلاب، ومسؤولي الرقابة. هذا يعني أنها ذات أهمية للجميع بلا استثناء.

(٣) أهداف الأمن الرقمي

مع التقدم التكنولوجي كان لابد من وجود وسيلة أمنة تحقق الثقة بين الفرد والخدمة مما نادى إلى الاهتمام بما يسمى الأمن الرقمي، سعياً إلى حماية وحفظ المعلومات والبيانات والتطبيقات للفرد ، بحيث يمنع أي دخول غير مرخص لتلك البيانات والتطبيقات ، وتأسيسا على ما سبق ظهر مصطلح الأمن السيبراني.

وتهدف وحدة الأمن الرقمي إلي تقديم الخدمات التوعوية والتعليمية والبحثية من خلال: (البشرى، ٢٠٠٠، ٣٩):

١. إثراء التوعية بدور الأمن وأهميته في الثقافية الأمنية .
٢. تقديم خدمات تدريبية للطلاب وأعضاء هيئة التدريس.
٣. تقديم خدمات استشارية بموضوعات الأمن الرقمي للجامعات والمؤسسات التعليمية.
٤. تنظيم ورش العمل والمؤتمر ات تحت مظلة أمنية محكمة.
٥. وضع حلول أمنة للاختراقات الأمنية والثغرات الرقمية.
٦. تسجيل براءات الاختراع لصاحبها وحفظ حقوق الملكية الفكرية.

ويهدف الأمن الرقمي في الجامعات إلى:(الخضري، ٢٠٢٠، ٢٢٣)

١- تأمين البنى التحتية لأمن المعلومات والبيانات الخاصة بالطلاب وأعضاء هيئة التدريس.
٢- حماية شبكة المعلومات والاتصالات من أي اختراق محتمل، والتي تلعب دورا رئيسيا في تدفق المعلومات والبيانات من مقدم الخدمة إلى مستقبل الخدمة.
٣- حماية شبكة المعلومات من أي هجوم محتمل وذلك بدراسة ومعرفة التقنيات المرتبطة بأمن المعلومات ومن أهمها كشف رسائل العدو والعمل على التصدي لها.
٤- تشفير التعاملات الرقمية بحيث لا يستطيع أي مخترق مهاجمتها أو العبث بمحتوياتها.

وبذلك يهدف الأمن الرقمي إلى تخفيف من مخاطر اختراق المعلومات والهجمات الإلكترونية ، وتعمل عدد من المنظمات الدولية باستمرار لمواكبة التطورات بشأن الأمن الإلكترونى ، (المقصودى، ٢٠١٧، ١٠٦).

مما سبق يتضح أن وضع سياسة لأمن الرقمي تعد من أكثر الأمور صعوبة وحساسية ومن أولويات الاهتمام بتقنية الاتصال لتحقيق هدف الأمن الرقمي وهو الدقة وسلامة وأمان كل العمليات ومصادر نظام المعلومات وكذلك إدارة الأمن الرقمي يمكن أن تقلل الأخطاء والاحتيال والخسائر فى النظام المعلوماتى الذي يربط بين أفراد المجتمع.

(٤) خصائص الأمن الرقمي

بما أن الجريمة الإلكترونية تتم بمنهجية وأساليب جديدة ذات بعد تكنولوجي أعلى من الجرائم التقليدية كان لابد أن يأتي الأمن الرقمي للتغلب على هذه المشكلة مواكباً التطور التكنولوجي، ولذا تميز الأمن الرقمي بعدد من الخصائص منها:

١. **الاكتشاف والتعقب:** وذلك من خلال اكتشاف الجريمة الإلكترونية وتعقب أثرها وبالتالى التغلب عليها.

٢. **السرعة وغياب الدليل:** فصعوبات غثبات الجرائم الإلكترونية نظراً لاستخدام المخترقين وسائل تقنية حديثة أتى الأمن الرقمي 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 الرقمي في تحقيق الأمن الرقمي للمؤسسات والجامعات في حماية البيانات والبنى التحتية لتلك المؤسسات (الصلاحى، ٢٠١٥، ١٢٩).

كما يتميز الأمن الرقمي بمجموعة من الخصائص، منها:

- مساعدة الطلاب على البدء في التفكير في كيفية استخدام التكنولوجيا في الجامعة والمنزل على النحو الملائم.
- تنمية مهارة الوعي والإدراك من خلال مساعدة الطلاب ليصبحوا مثقفين من الناحية التقنية وتتجاوز مرحلة الوعي المعرفية الأساسية لأجزاء الحاسب الآلي وبرامجه إلى معرفة الاستخدام الملائم لهذه التقنيات الرقمية.
- تنمية مهارة الممارسة الموجهة التى تساعدالطلاب على تمييز وممارسة الاستخدام الملائم، بحيث يتم منح الطلاب فرصة لتعلم في بيئة تشجع على الاكتشاف
- يقدم عروض تعليمية واضحة تركز على استخدام التكنولوجيا بشكل ملائم في الصف، بحيث يقوم المعلمون بممارسة عادات الاستخدام الرقمي الجيد أمام الطلاب.

كما يتسم الأمن الرقمي بمجموعة من الخصائص، منها: Mukherjee، 2020، (Yastrebenetsky 203)، 2020، & Kharchenko، (77

١. التعامل مع البرامج ذات ثقة فقط: يسمح جدار الحماية لنظام الأمن بمرور البرامج الموثوقة من المستخدم والمتجر الإلكتروني، ومنع البرامج الخبيثة غير الموثوق بها .

٢. الحماية من التهديدات الداخلية: بسبب قلة ثقافة المستخدم بسياسات الأمان التكنولوجي وتنصيب برامج مجهولة المصدر قد تحتوي على فيروسات سيئة، يساعد جدار الحماية لنظام الأمن الرقمي في تنبيه الفرد بخطورة الفيروس واتخاذ إجراء سريع بحذفه بعد موافقة المستخدم.

٣. الحماية من التهديدات الخارجية: وذلك بتقليل المخاطر الخارجية التي تأتي نتيجة العمل على شبكة الإنترنت، مثل رسائل البريد الإلكتروني أو الروابط التي يستغلها الهاكرز للسيطرة والتحكم في أجهزة الأفراد.

٤. الرؤية الشاملة: يوفر الأمن الرقمي رؤية شاملة للمستخدمين عن أنظمتهم لمعرفة الثغرات واتخاذ إجراءات سريعة لسد تلك الثغرات.

٥. منع أي مصدر خارجي من الاضطلاع على أي بيانات أو ملفات خاصة يتم مشاركتها عبر مواقع التواصل على شبكة الإنترنت.

ثانيا: مخاطر مواقع التواصل الاجتماعي وانعكاسها على طلاب الجامعة

نظرًا لما تشهده المجتمعات الحديثة –وبخاصة مصر– من ظاهرة تنامي استخدام تقنيات الاتصال الإلكتروني، فقد ظهر جيل جديد لم يعد يتفاعل مع الإعلام التقليدي بقدر ما يتفاعل مع الإعلام الإلكتروني ولاسيما مواقع التواصل الاجتماعي.

وكان أول ظهور لموقع التواصل الاجتماعي عام ١٩٩٧ وأول موقع ظهورا هو Six com Degrees،من أجل وضع ملفات شخصية وخاصة لمستخدمي الموقع مع التعليق على الأخبار الموجودة بالموقع، وتبادل الرسائل النصية بين المستخدمين وتبع هذا الموقع في الظهور عام ٢٠٠٣ موقع My Space.com ثم ظهر ما يعرف (فيسبوك– تويتر– الإنستغرام –يوتيوب).

(١): مفهوم مواقع التواصل الاجتماعي:

تعتمد شبكات التواصل الاجتماعي على الاتصال بين مجموعة من الأفراد لهم نفس الميول، والاهتمامات، لذلك تعرف بأنها منظومة من الشبكات الإلكترونية التي تسمح للمشترك فيها بإنشاء موقع خاص به، ومن ثم ربطه خلال نظام اجتماعي إلكتروني مع أعضاء آخرين لديهم نفس الاهتمامات والميول والهوايات، أو جمعه مع أصدقائه.

وهى تطلق على مجموعة من المواقع على شبكة الإنترنت- تتيح التواصل بين الأفراد في بيئة مجتمع افتراضي يجمعهم حسب مجموعات اهتمام أو شبكات انتماء(بلد، جامعة، مدرسة، شركة ...لخ)، كل هذا يتم عن طريق خدمات التواصل المباشر؛ مثل: إرسال الرسائل، أو الإطلاع على الملفات الشخصية للآخرين، ومعرفة أخبارهم ومعلوماتهم التي يتيحونها للعرض.

وتعرف بوي واليسون Nicole) ، 2008 ، (211 بأنها: "الخدمات المستندة على تقنيات web 2 ، 0 والتي تسمح للفرد بإنشاء حساب شخصي- رسمي أو غير رسمي- واختيار أشخاص يتاح لهم التواصل والتعاون وتبادل المعلومات معهم، وتوضح له لائحة المستخدمين الآخرين الذين يشتركون مع أصدقاءه، وتعرض نشاطاته ونشاطاتهم التي قاموا بها داخل تلك الشبكة"، هذا وتختلف طبيعة واستراتيجية عمل تلك الشبكات من شبكة لأخرى).

كما تعد شبكات التواصل الاجتماعي شكلاً من أشكال المجتمعات الإفتراضية المقامة داخل الفضاء السايبري (الرمزي)، والتي تعرّف بأنها": تلك المجتمعات التي تلمّ مجموعة من الأفراد يجمع بينهم قيم مشتركة وشعور بالإنتماء، ويعيشون في بيئة جغرافية مكانية واحدة، تحكمهم قيم وأعراف يجتمعون عليها، ويتفقون فيما بينهم على وسائل الردع وقواعد الضبط الاجتماعي التي تحكم ما يحدث بينهم من علاقات(زكي، ٢٠٠٩).

وتعرّف أيضاً بأنها: الشبكات التي تسمح للمستخدم بالوصول إلى المحتويات والخدمات المختلفة عبر الشبكات من خلال الإنترنت، بحيث يقوم المستخدم من خلال هذه الشبكات بالمشاركة في إنتاج المحتوى وتراسله وإعادة استخدامه مرة أخرى في إطار من التفاعلات الإنسانية بين أفراد ومجموعات متنوعة من المستخدمين Research ، 2008،(Waycott،5) ،2009 ،(5).

إن شبكات التواصل الاجتماعي توفر فرصاً غنية للتبادل الاجتماعي لكافة أنواع المعلومات والوسائط المتعددة عبر اتصالات تزامنية وغير تزامنية تشجع على التفاعل والتشارك في إنتاج المعارف المختلفة(Mills. N. 2011،.(350، وعلى ذلك فالشبكات الاجتماعية خدمات شاملة يتم التفاعل معها عبر الإنترنت مما يتيح للطلاب مشاركة الأنشطة والإهتمامات، وتكوين صداقات، والبحث عن اهتماماتهم وأنشطة لدى أفراد آخرين بالإضافة إلى تقديمها مجموعة من الخدمات الأخرى مثل: المحادثة الفورية والرسائل الخاصة والبريد الإلكتروني والتدوين ومشاركة الملفات وغيرها من الخدمات.

وما ينتج عن ذلك من تغيير إنقلابي للنموذج الاتصالي الموروث بما يسمح للفرد العادي إيصال رسالته إلى من يريد في الوقت الذي يريد، وبطريقة واسعة الاتجاهات وليس من أعلى إلى أسفل وفق النموذج الاتصالي التقليدي، فضلاً عن تبني هذه المواقع تطبيقات الواقع الافتراضي وتحقيقه لميزات الفردية والتخصيص وتجاوزه لمفهوم الدولة الوطنية والحدود الدولية.

(٢): خصائص شبكات التواصل الاجتماعي

اتسمت شبكات التواصل الاجتماعي بالعديد من الخصائص، من أهمها: (خليل، ٢٠١٠، ١٤)

أ- **التفاعلية:** حيث أصبح للمتلقي دور فاعل في عملية الاتصال وصار يتبادل الأدوار والحوار مع المرسل، وتحول مسار ممارسة الاتصال ليصير ثنائي الإتجاه وليس أحادي الاتجاه كما كان الوضع في وسائل الإعلام التقليدية.

ب- **اللاتزامنية:** أي عدم فرض تزامن وجود المستقبِل والمرسِل، وإمكانية تفاعلهما مع العملية الاتصالية في أي وقت يناسبهما.

ج- **المشاركة والانتشار:** يتيح الإعلام الجديد لكل شخص يمتلك أبسط أشكال الأجهزة الإلكترونية أن يكون ناشراً يرسل رسالته إلى الآخرين ومستقبلاً بطبيعة الحال لرسائلهم ورجع صداهم، ومما ساعد على انتشار الإعلام الجديد بهذا الشكل العريض والواسع، هو عدم اقتصاره على نطاق فئوي أو نخبوي، وانخفاض تكاليفه نسبياً.

د- **الحركة والمرونة:** حيث أن الحواسب المحمولة والحواسب اللوحية والهواتف الذكية والأجهزة اللوحية، قابلة للانتقال وقابلة لمصاحبة المتلقي والمرسل أينما حلوا، مع قدرتها على الاستفادة من شبكات الإنترنت اللاسلكية.

هـ- **الكونية:** حيث أصبحت بيئة الاتصال بيئة عالمية، تتخطى حواجز الزمان والمكان والرقابة، وتجعل المعلومة بين يدي المتلقي حال صدورها ، وبالتالي ظهر هناك مساواة وتكافؤ في الفرص بين كل أبناء البشر في حق الحصول على المعلومة في نفس الوقت، مما جعل العالم يعيش في عصر يتصف بالمساواة المعلوماتية.

و- **اندماج الوسائط:** تضمن الأنظمة الاتصالية الجديدة القدرة على التعبير عبر استخدام كل وسائل الاتصال، الصوت، والصور الضوئية، والفيديو، والنصوص، والرسوم البيانية ثنائية وثلاثية الأبعاد، مع قابليتها اليسيرة للتحويل من صيغة إلى أخرى.

ز- **التخزين والحفظ:** يسهل على المتلقي تخزين وحفظ الرسائل الاتصالية واسترجاعها، كجزء من قدرات وخصائص الوسيلة نفسها.

وعلى ذلك فالملمح الأساسي لشبكات التواصل الجتماعي أنها: نموذج اجتماعي لبناء المعرفة، هذا النموذج له خصائص أساسية يمكن وصفها من خلال المحاور التالية: (Research، 2008، 8)

- **التكنولوجيا:** حيث تعتمد الشبكات الاجتماعية على ما يسمى تطبيقات سطح المكتب المصغرة، والتي تسحب المعلومات من المستعرض وتعرضها كاملة على سطح

المكتب دون الحاجة إلى استخدام المعلم للشبكات الاجتماعية من خلال مستعرض الويب.

- **الهيكلية:** حيث يجب أن يتميز التخطيط العام للشبكة الاجتماعية بالمرونة ويسمح للمعلمين بإعادة تخطيط محتوياتهم على ضوء أهدافهم.
- **المعرفة:** الأدوات المختلفة للشبكات الاجتماعية تتيح الوصول إلى محتويات متنوعة يتم الإضافة عليها، والتعديل فيها، والحذف منها؛ مما ينتج عنه الوصول إلى كم وكيف أكبر من المعارف الإبداعية الجديدة.
- **المستخدم:** يُطلق على المستخدم مصطلح "Prosumer" ويعني منتج المحتوى ومستخدمه، حيث أن هذا المصطلح خلاصة كلمتي منتج Producer، ومستهلك Consumer، فالمحتوى يتم استهلاكه ممن أنتجه أو شارك في إنتاجه.
- **الاجتماعية:** فالشبكة الاجتماعية يجب أن تسمح بتكوين الجاليات والصداقات بين أعضائها وتبادل الآراء والمعارف المختلفة.

ولقد كان لهذه الخصائص **تأثير إيجابي** على ثقافة طلاب الجامعة، منها على سبيل المثال مساعدتهم في التقريب بين بعضهم البعض، وفيما بينهم وبين الجامعات الأخرى؛ مما سهّل نقل التطور العلمي في سائر المجالات، وسمح بالتلاقي الفكري ونقل الخبرة بين الأفراد من مختلف البيئات، ويسّر تعلمهم اللغات الأجنبية واللهجات المحلية، ونشر العادات والتقاليد المختلفة.

أما **التأثير السلبي** الذي طبعته هذه الخصائص على الثقافة، ما ظهر لدى المستخدمين من لغة جديدة أو ما يطلق عليها "اللغة العربيزية" أثرت بشكل أو بآخر على لغتهم العربية، وانصراف الكثيرين منهم لاستخدام الشبكات الذي قد يصل إلى حد الإدمان، واتباعهم لعادات استهلاكية سيئة منها سعيهم الدائم لاقتناء أحدث الأجهزة الإلكترونية المتاحة لشبكات التواصل حتى وإن استنزفتهم وأثرت عليهم مادياً.

(٣): أنواع شبكات التواصل الاجتماعي:

من أبرز أنواع شبكات التواصل الاجتماعي، وأوسعها انتشاراً، **هي:**(أبو العطا ، ٢٠١٠، ١٢)

- **فيس بوك Face book:**

شبكة التواصل الاجتماعي **Facebook** عبارة عن مدونة شخصية، أو صفحة على الإنترنت يتبادل فيها الأصدقاء مع بعضهم النقاش والصور ولقطات الفيديو والصوتيات، ويُعد أحد أشهر شبكات التواصل الاجتماعي في الشبكة العنكبوتية.

وترجع نشأة الموقع إلى مارك زوكربرج **(MarkZuckerberg)** وكان وقتها طالباً في جامعة هارفارد، حين أطلقه في فبراير ٢٠٠٤م وأعطاه اسم **Facebook** وذلك لرغبته في جمع دليل معروف لأسماء وصور طلبة الجامعة، وقد كان هدفه إقامة شبكة تضم طلبة الجامعة في مكان واحد، مما سيتيح للطلاب إنشاء نبذة خاصة بهم وإضفاء طابعهم الشخصي عليها وتحديثها. وقد كان الاشتراك في **Face book** يقتصر في البدء على طلبة جامعة هارفارد الأمريكية، لكن حقق الموقع شعبية كبيرة جعلته يتوسع بسرعة إلى بقية الجامعات والمعاهد ثم المدارس الثانوية ثم الشركات ثم إلى العالم أجمع، وتساعد هذه الشبكة مستخدميها على الوصول لصداقاتهم وعلاقاتهم القديمة.

- **تويتر Twitter(x):**

منذ عام تقريباً أُعلن أن شركة تويتر تغير اسمها إلى "X Corp"، قام –إيلون ماسك– مالك تويتر الجديد بنشر تغريدة بأن شركة تويتر تغير اسمها لتتضمن حرفاً واحداً فقط، وهو "**X**" .

تويتر**(X)** هو موقع اجتماعي يقدم خدمة تدوين مصغّر تسمح لمستخدميه بإرسال تحديثات (يطلق عليها تغريدات **Tweets**) عن حالتهم بحد أقصى ١٤٠ حرفا للرسالة الواحدة، وأصبحت حاليا ٢٨٠ حرفا بعد التحديث الأخير، ويمكّن مستخدميه من

نشر أفكارهم وخواطرهم لجميع من يتابعهم، فضلاً عن إمكانية مناقشتهم ومحاورتهم والاستفادة منهم.

- **يوتيوب You Tube:**

تقوم فكرة الموقع على إمكانية إرفاق أي ملفات تتكون من مقاطع الفيديو على شبكة الإنترنت دون أي تكلفة مالية، فبمجرد أن يقوم المستخدم بالتسجيل في الموقع يتمكن من إرفاق أي عدد من هذه الملفات ليراها ملايين الأشخاص حول العالم، كما يمكن للمشاهدين إدارة حوار جماعي حول مقطع الفيديو من خلال إضافة التعليقات المصاحبة، فضلاً عن إمكانية التقييم بالسلب أو بالإيجاب للتعبير عن مدى أهمية ملف الفيديو من وجهة نظر مستخدمي الموقع، إضافة إلى إمكانية الإبلاغ عن المواد المسيئة، أو حذفها وإزالتها نهائياً(أمين، ٢٠٠٩، ٥١١).

(٤): مخاطر مواقع التواصل الاجتماعي وأثرها على طلاب الجامعة:

لقد أثرت الثورة الرقمية سلبيًا على سلوك مستخدميها وعلاقاتهم الاجتماعية، وذلك من خلال انشغال الأفراد بالتواصل الإلكتروني، والانعزال عن الأهل في التصفح عبر الشبكة العنكبوتية، دون التفاعل الحيوي مع أفراد الأسرة والمجتمع المحيط، وكذلك ضعف دور الأسرة في التأثير والسيطرة على سلوك أفرادها الذين انشغلوا بالواقع الافتراضي، مما أعلى من القيم الفردية، على حساب القيم الاجتماعية، وقيم العمل الجماعي المشترك، إضافة إلى اتساع الفجوة بين أفراد الأسرة وتكريس العزلة والتخبط وانعدام الأمن والاستقرار وفقدان المعايير، مما أدى إلى شيوع ظاهرة التفكك الاجتماعي والأسري، وهو ما أوجد حالة من الضعف في قدرة المجتمع على التنظيم والتوحيد والتنسيق الثقافي، وهو ما أدى إلى التشتيت وضعف الانتماء للمجتمع.

كما أثرت الثورة الرقمية سلبيًا على علاقة طلاب الجامعة بوالديهم، حيث أصبحت التكنولوجيا تشغل عقول الطلاب أكثر من أي شيء آخر(الزبيدي، ٢٠٠٩، ٣٩).

لقد بدأت شبكات التواصل الاجتماعي كشبكات للتعارف والتواصل الهادف، ولكن بعد قليل تحولت إلى مواقع لمشاركة كل شيء بدءا من الصور الشخصية والمعلومات الخاصة وانتهاء بالآراء السياسية والاجتماعية والأخبار والمعلومات العامة، ووسط هذا السيل من البيانات ومقاطع الفيديو والصور أصبح من الصعب التحقق من كل ما تقع عليه أعيننا، كذلك أصبح هذا القدر الكبير من المعلومات سببا في الإلهاء عن الأمور النافعة.

مما أدى إلى حدوث تغيراً في أساليب تعامل الناس مع بعضهم، ومفاهيم ومحددات المجتمعات عبر شبكات التواصل الرقمية، وظهرت بموازاة الإيجابيات الكبيرة للمستحدثات والتطبيقات التكنولوجية؛ سلبيات متعددة، وممارسات غريبة، وأخلاقيات وأنماط تفكير دخيلة، على سلوكيات مجتمعاتنا الإسلامية المحافظة؛ مما أدى إلى انتشار أنواع حديثة من أساليب الجريمة التي لم تكن معروفة سابقاً والتى تدار بواسطة أيد خفية خلف شاشات الأجهزة الإلكترونية.

إن مخاطر مواقع التواصل الاجتماعي تعد من الموضوعات والحديثة نسبياً ، وذلك نظراً لاعتماد الطلاب بصورة مستمرة على تكتنولوجيا الاتصالات والمعلومات، هذا الإعتماد المفرط ترافقه مجموعة من المخاطر الناشئة والمحتملة التى تهدد وشكل أساسي الشبكة وامن المعلومات، والمجتمع المعلوماتى وأعضائه، وذلك قد يكون بسبب سوء الاستغلال للشبكات الإلكترونية لأهداف إجرامية؛ مما يؤثر سلباً على سلامة البنية التحتية للمعلومات الشخصية وامن الطلاب.

لقد أصبح الاعتماد عليها أساسيًا كوسيلة اتصال ضرورية في جميع الجوانب والمجالات وهذا الاعتماد الكبير نتج عنه مخاطر جسيمة قد تتسبب بتعطيل الأجهزة المستخدمة أو تلف المعلومات الموجودة فيها أو تغييرها أو كشفها وتسربها لجهات أخرى ، أو حتى تعطيل استخدامها نهائياً.

وفى هذا الصدد يشير ثمبسون (Thompson،2013) إلى أن ما وفرته ثورة الاتصالات الرقمية من تسهيل وسرعة في الحصول على مصادر المعلومات لجميع شرائح المجتمع، ومع ما تحمله هذه الثورة من إيجابيات إذا أحسن استغلالها بطريقة رشيدة، ومن عواقب ومخاطر إذا لم تستغل بالطريقة الرشيدة، فما أوجدته الرقمية من ممارسات سلبية "كالجرائم الإلكترونية" التي انتشرت يؤرق العالم، أضف بين الشباب، وأصبحت هاجسا إلى تلك الممارسات المخدرات الرقمية، والإرهاب الإلكتروني، وغير ذلك من ممارسات نتيجة لاستخدام غير الرشيد للرقمية.

ويشير أوكيفي وبيرسون (O'Keeffe & Pearson،2011) إلى وجود سلوكيات متكررة عبر الإنترنت مثل التسلط، وتشكيل العصابات، والممارسات غير الأخلاقية، التي أدخلت مشكلات مثل التسلط عبر الإنترنت، ومشكلات متعلقة بالخصوصية، وإرسال المحتوى الجنسي، بالإضافة إلى المشاكل الأخرى التي تستحق الاهتمام وتشمل إدمان الإنترنت والحرمان من النوم.

كما يحدد ريبيل(٢٠١٣) قضايا الأمن الرقمي المتعلقة بالطلاب في:حماية أجزاء الحاسوب وأمن الشبكة، وحماية الأمن الشخصي: سرقة الهوية والاحتيال، والتحرش، وحماية أمن المدرسة :المتسللون والفيروسات، وحماية أمن المجتمع من التهديدات الإرهابية.

وسعى ليفينجستون وآخرونLivin gstone et al) ،(2011 إلى التحقق من المخاطر الرئيسة عبر الإنترنت، وحدد أبرز هذ المخاطر بالنسبة للمستخدمين في التعرض للمواد الإباحية، والتسلط، وتلقي الرسائل الجنسية، والاتصال بأشخاص غير معروفين وجهاً لوجه، وعقد اجتماعات بلا اتصال مع جهات الاتصال عبر الإنترنت، وإساءة استخدام المحتوى، وسوء استخدام البيانات الشخصية.

ويرى (يوسف ، ٢٠١٠) أن من أبرز مخاطر الإنترنت المحتملة سرقة المعلومات؛ كاعتراض رسائل البريد الإلكتروني، واختراق أجهزة الغير والاطلاع على المعلومات الموجودة فيها أو تغييرها ، وبث وإرسال رسائل ومواقع إباحية ومنافية للدين.

كما أن هناك مجموعة من المخاطر والتهديدات من أبرزها: الإصابة بالفيروسات المدمرة للبيانات والمعلومات المخزنة على الحاسوب، والاختراق للعبث بملفات المستخدم أو استغلال حاسوبه بقصد الإساءة إلى الآخرين أو سرقة البيانات الشخصية بقصد الانتحال أو الابتزاز وسرقة بطاقات الائتمان (المتجر الإلكتروني ، ٢٠١٥) .

كما أنه بمجرد زيارة الشخص لأي موقع إلكتروني يتمكن الموقع من معرفة وتحديد موقع وعنوان الإنترنت الذي يستخدمه الشخص ونظام تشغيل الحاسوب، ونوعية المتصفح الذي يعمل عليه، بل تقوم مواقع الويب بالحصول على ما هو أكثر من هذه المعلومات؛ إذ تسعى إلى تعقب ما يفعله الزائر أثناء زيارته، ونوعية المعلومات التي يجري الاطلاع عليها ، وأوقات الزيارة، والوقت الذي يقضيه في التصفح، وهذه الأمور قد يترتب عليها مخاطر كثيرة ؛ كسرقة الهوية، ووضع معلومات الفرد الشخصية في قواعد المواقع الإلكترونية، وجمع معلومات عن اهتماماته وحياته، كما أنها تزيد المخاطر عند التسوق من الإنترنت، وقد يقع الشخص ضحية الاحتيال والنصب (بسيوني ، ٢٠٠٣، ١٥).

وهناك مجموعة من المخاطر الناجمة من التعامل مواقع التواصل الاجتماعي، منها:

أولاً: الابتزاز الإلكتروني

تعد جريمة الابتزاز الإلكتروني إفرازاً ونتاجاً لتقنية المعلومات ، فهي ترتبط بها وتقوم عليها، وتعتمد على الحصول على وثائق وصور ومعلومات عن الضحية من خلال الوسائل الإلكترونية أو التهديد بالتشهير بمعلومات ووثائق خاصة عنه عن طريق استعمال الوسائل الإلكترونية .

ويعرف الابتزاز الإلكترونى بأنه استخدام وسائل التقنية الحديثة للحصول على مكاسب مادية أو معنوية عن طريق الإكراه من شخص أو أشخاص أو حتى مؤسسات، ويكون ذلك الإكراه بالتهديد بفضح سر من أسرار المبتز بعد أن ينشب الجاني أنيابه على الضحية ويتمكن من جمع صور قد تكون فاضحة أو حتى مقاطع مصورة يكون مقابل عدم الفضيحة مبلغ مالي ضخم وإلا نشر الصور والفيديوهات.

وتتعاظم خطورة الابتزاز الإلكترونى يوماً بعد يوم كونها تمس الانسان فى سمعته وفكره وحياته الخاصة وماله، كما تمس المؤسسات فى اقتصادها وسمعتها أيضاً، ناهيك عن خطورته على البلدان من النواحى الأمنية والسياسية والاقتصادية كما أن ما يبرز خطورة الابتزاز الإلكترونى هو طبيعة الجانى فى جرائم المعلومات ، إذ قد يكون الجانى فى جرائم الابتزاز الإلكترونى شخصاً طبيعياً يعمل لحسابه، ويسعى إلى تحقيق مصلحة خاصة به من وراء الجريمة التى يرتكبها عن طريق الاستعانة بأحد نظم المعالجة الآلية للبينات والمعلومات ، غير أنه غالباً ما يرتكب الشخص الطبيعي السلوك الإجرامى ليس لحسابه وإنما لحساب الأشخاص كشركة عامة أو خاصة تعمل فى ميدان المعلوماتية أو فى ميدان آخر، لذا فإن تنوع أغراض وغايات جرائم الابتزاز الإلكترونى يبرز من خطورتها.(السعدى، وسلام، ٢٠٢٣، ٤٧)

وتتعدد صور الابتزاز الإلكترونى حسب المحل الذي يرد عليه فقد يكون جنسياً عندما يتعلق بعرض ، وقد يكون اجتماعياً عندما يتعلق بالكيان الأدبي للفرد فى المجتمع، وقد يكون مهنياً عندما يتصل بحياة الإنسان المهنية ، وقد يكون سياسياً عندما يتعلق بالوضع السياسي للفرد.

ثانياً: انتهاك الخصوصية

من أبرز سلبيات مواقع التواصل الاجتماعي على المراهقين وعلى غيرهم من جميع الفئات العمرية قضية الخصوصية وما يرتبط بها من مشكلات كثيرة، فبسبب وجود

قدر كبير من البيانات التي يتم مشاركتها عبر مواقع التواصل الاجتماعي، فإن مقدار الخصوصية يتقلص بشكل مستمر.

ويمثل انتهاك خصوصية الأفراد في العصر الرقمي أحد أبرز تحديات الثورة الرقمية، حيث أصبح التواصل عبر الشبكات والمواقع الاجتماعية الوسيلة المفضلة في التواصل الاجتماعي بالنسبة لجيل الإنترنت، إلا أن أغلب هذه المواقع تواجه مشكلة انعدام الخصوصية؛ مما تسبب في الكثير من الأضرار المعنوية والنفسية عند الشباب، قد تصل في بعض الأحيان إلى الأضرار المادية لمستخدمي هذه المواقع والشبكات، حيث تحتوي على جميع المعلومات الشخصية والتي قد تصل إلى أيدي أشخاص قد يستغلونها بغرض الإساءة والتشهير، حيث ساعد الإنترنت على سرعه وإمكانية اقتحام الخصوصية في أي موقع وأي زمان فأصبحت هناك صعوبة في الإخفاء والعزلة (تريكي، ٢٠١٤، ١٩٨).

فهناك العديد من اتفاقيات استخدام المواقع والمنصات تجبر المستخدمين على الموافقة على استخدام قدر كبير من المعلومات الشخصية لأغراض تجارية، ويمكن للمراهقين التورط في العديد من المشكلات بسبب مشاركة البيانات بشكل غير محسوب، أيضاً ربما يتطور الأمر إلى حدوث بعض الحوادث بسبب هذه الإتاحة العلنية للمعلومات والبيانات.

ولعل الجانب الأكثر إثارة للقلق هنا هو التهديد الذي يشكله الاستغلال والانتهاك الجنسى عبر الإنترنت. إذ أصبح الاتصال بالضحايا المحتملة ومشاركة الصور وتشجيع الآخرين على ارتكاب الجرائم في متناول مرتكبي الجرائم الجنسية اليوم أكثر من أي وقت مضى .

ثالثاً: التنمر الالكتروني

مع التطور التكنولوجي ظهر ما يسمى بالتنمر الإلكتروني والذي يكون عادة عن طريق وسائل التواصل الاجتماعي والذي يهدف للإيذاء من خلال شبكات تكنولوجيا المعلومات بطريقة متكررة ومتعمدة.

فالتنمر الإلكتروني وغيره من أشكال العنف قد يؤثر على طلاب الجامعة الذين يستخدمون وسائل التواصل الاجتماعي ومنصات الرسائل الفورية كلما يسجلون الدخول إليها، وتشير الأرقام أن أكثر من ثلث الشباب عبر ٣٠ دولة قد صرحوا أنهم تعرضوا من قبل للتنمر عبر الإنترنت.

والتنمر الإلكترونى هو إيقاع الأذى الجسمي أو النفسي أو العاطفي أو المضايقة أو الإحراج أو السخرية من قبل إنسان متنمر على إنسان آخر أضعف منه، أو أصغر منه أو لأي سبب من الأسباب وبشكل متكرر والفرد المتنمر هو الذي يضايق، أو يخيف، أو يهدد ، أو يؤذي الآخرين الذين لا يتمتعون بنفس درجة القوة التي يتمتع بها، وهو يخيف غيره من الطلاب في المدرسة، ويجبرهم على فعل ما يريد بنبرته الصوتية العالية واستخدام التهديدJaana،2006 ،(310).

وقد يحدث التنمر الإلكترونى عن طريق إرسال الشائعات عن شخص ما في الإنترنت بقصد تكريه الناس به أو ربما يصل لدرجة انتقاء ضحايا ونشر مواد لتشويه سمعتهم وإهانتهم، يمكن عمل ذلك من خلال الرسائل النصية والصور والرسومات مقاطع الفيديو، المكالمات الهاتفية، البريد الإلكتروني، غرف المحادثة، المحادثة الفورية والمواقع الإلكترونية ومواقع التواصل الاجتماعي.

كذلك يمكن أن ينتج عن التواصل المستمر مع الأقران عبر مواقع التواصل الاجتماعي ضغطاً كبيراً على طلاب الجامعة لمحاولة الظهور والشعور بالقبول، وبالطبع يمكن أن يتعرض أي شخص لهذه الآثار السلبية، ولكن المراهقين هم أكثر الأشخاص عرضة لهذه المشكلة، وأخطر ما في هذا الأمر هو أن الأفعال التي يقوم بها المراهقون

المتنمرون قد تكون أكثر حدة من الأفعال التي يمارسونها في الجامعة أو في أي مكان آخر، حيث يكون لديهم انطباعا بأنهم مجهولي الهوية وبعيدين عن المحاسبة عند التخفي وراء الحسابات الوهمية أو الأسماء المستعارة.

ولذلك فإن هذه المشكلة تؤدي إلى القلق والأعراض الشبيهة بالاكتئاب عند المراهقين، وهو ما يدفع العديد منهم إلى الإقدام على الانتحار أو إيذاء النفس، ولذلك لابد من حث الراشدين من أولياء الأمور والمشرفين التربويين وغيرهم على مراقبة هذه الأمور والحد من مخاطر هذه الآثار السلبية.

رابعا: الجرائم الإلكترونية

إن استخدام التكنولوجيا بشكل عام محفوف بالمخاطر، وتعد وسائل التواصل الاجتماعي من الأبواب الخطيرة التي قد تعرض الشخص لخطر الجريمة الإلكترونية، وفي هذا العصر تطورت الجرائم الإلكترونية بصورة كبيرة اعتمادا على التطور التقني الهائل وسرعة تداول المعلومات والبيانات.

ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات، أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون، والجرائم الإلكترونية هي " المخالفات التي ترتكب ضد الأفراد أو المجموعات بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت مثل غرف الدردشة، والبريد الإلكتروني، والموبايل(البداينة، ٢٠١٤).

وتعرف الجريمة الإلكترونية بأنّها المُمارسات التي تُوقَع ضدّ فرد أو مجموعةٍ مع توفّر باعثٍ إجراميّ بهدفِ التَّسبُّبِ بالأذى لسمعة الضحيّة عمداً، أو إلحاق الضَّرر النفسيّ والبدنيّ به سواءً أكان ذلك بأسلوبٍ مباشر أو غير مباشر بالاستعانة بشبكات الاتصال الحديثة كالإنترنت وما تتبعها من أدوات كالبريد الإلكتروني وغرف المُحادثة، والهواتف المحمولة وما تتبعها من أدوات كرسائل الوسائط المُتعدّدة.

وتشتمل الجرائم الإلكترونية على السلوكات والنشاطات غير المشروعة المرتكبة بالوسائل الإلكترونية، وهي كما ما يلي: cooper)، 2017 ،(10

١- الوصول غير المصرح به لشبكة من أجل سرقة أو تدمير أو تغيير المعلومات أو القيام بتزييف أو الابتزاز أو إتلاف المكونات المادية أو المعنوية).

٢- الحرمان من الوصول إلى الشبكة المعلوماتية من قبل الضحية عامة بشكل يلحق الضرر لدى ممارسته لتلك النشاطات.

وعلى الصعيد العالمي، تظهر أفعال الجريمة الإلكترونية انتشاراً واسعاً عبر أعمال مدفوعة مالياً، وأعمال ذات صلة بمحتوى الكمبيوتر، وكذلك العمل ضد السرية والسلامة والوصول إلى أنظمة الكمبيوتر.

وهناك عدد من الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية، منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي، كما أن أسباب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه (فردي، مجتمعي، كوني)، فجرائم الشباب تختلف عن أسباب جرائم المحترفين، وتختلف وفق هدفها سرقة أو معلومات أو تجارة بالمعلومات أو شخصية، ومن هذه الأسباب:

- **أسباب الجريمة الإلكترونية على المستوى الفردي:**

- **البحث عن التقدير**

هناك بعض الجرائم الإلكترونية التي يرتكبها شباب طائش وصغار سن، وذلك من باب التحدي، وحب الظهور في الإعلام وغالباً ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق بعد سن العشرينيات.

لذلك فإن تكنولوجيا المعلومات والاتصالات والاستخدام المتزايد للإنترنت قد خلق فرص جديدة للمجرمين وسهلت نمو الجريمة أن جرائم الإنترنت تمثل شكلاً جديدة ومميزة للجريمة، وقد خلقت تحديات لتوقع التطورات، والوقاية منها.

- **النشاط الروتيني:**

يمكن تفسير زيادة ضحايا الجريمة الإلكترونية من خلال التغييرات في أنشطة الناس الروتينية في الحياة اليومية فمع ظهور شبكة الإنترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية، والترفيه، والتجارة، كذلك استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك، والايميل والمواقع وغيرها قد خلق فرصة للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة يرى كوهين وفيلسون أنه من المرجح أن تحدث الجريمة عندما تتلاقى ثلاثة عوامل هي: الجاني المتحفز والهدف المناسب وغياب الحراسة (Cohen، 2010، 589)

لذلك لابد من توافر هذه العوامل الثلاثة من أجل أن تحدث الجريمة، وعدم وجود واحد من هذه العوامل هو " كافي لمنع حدوث ناجح لإكمال الاتصال المباشر في جريمة السلب، ويعطي اهتمام إلى التقارب في الزمان والمكان، وإن هذا التلاقي يمكن أن يؤدي إلى زيادة كبيرة في معدلات الجريمة من دون أي تغيير في " الحالة الظرفية" التي تحفز المجرمين، والمبدأ الأساسي هو أن التغييرات الهيكلية في النشاط الروتيني تؤثر على التقارب في العناصر الثلاثة من الناحية النظرية، وبالتالي تؤثر على معدل الجريمة.

- أسباب الجريمة الإلكترونية على المستوى المجتمعي:

١- التحضر

يعد التحضر أحد أسباب الجريمة الإلكترونية عامة، حيث الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة. وعادة ما يهاجر الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية، باهظة التكاليف، والتي تتطلب مهارات عالية أحيانا. مما يجعل شرائح

كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية، مما يجعلهم يعيشون في مدن الصفيح والأحياء الطرفية والهامشية. وكنتيجة يجد الناس أنفسهم في تنافس غير قادرين على مجاراته، مما يجعلهم يلتفتون إلى الاستثمار في الجريمة الإلكترونية حيث لا تتطلب رأس مال كبير والتي تعرف أولاً الياهو" (Yahoo Boys)، وكما يرى ستانلى(Stanley،2012،13) فإن التحضر سبب رئيس للجرائم الإلكترونية في نيجيريا، وأن التحضر بدون الجريمة مستحيل، وكنتيجة فإن الصفوة بينهم قد وجدوا أن الاستثمار في الجريمة الإلكترونية مربح.

٢- البطالة

ترتبط الجريمة الإلكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة، وتتركز البطالة بين قطاعات كبيرة من الشباب. وكما يقول المثل النيجيري "العقل العاطل عن العمل هو ورشة عمل للشيطان" ولذا فان الشباب الذين يملكون المعرفة يستثمرون ذلك في النشاط الإجرامي الإلكتروني.

٣- الضغوط العامة

تعد الضغوط العامة التي يتعرض لها المجتمع من فقر وبطالة وأمية وظروف اقتصادية صعبة عوامل ضاغطة على المجتمع عامة وخاصة على قطاع الشباب، مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف وضد المجتمع مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف منها الإتجار الإلكتروني بالبشر والجنس والجريمة الإلكترونية وغيرها.

٤- البحث عن الثراء

يسعى الإنسان إلى المتعة ويتجنب الألم هكذا تقول النظرية العامة في الجريمة لجتفردسون وهيرشي، ويسعى الناس إلى الوسائل غير المقبولة اجتماعياً لتحقيق أهداف مقبولة اجتماعياً، فالرغبة في الثراء يواجهها صعوبات بالغة في تحقيقه بالطرق المقبولة اجتماعياً وقانونياً، ولذا يلجأ بعض الناس إلى الجرائم الإلكترونية حيث المستهدف مجتمع أكبر وسهولة التنفيذ وقلة الخطورة.

٥- ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية

هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مجاراة التقدم في الجرائم الإلكترونية وأساليبها وهذا لا يتوقف عند التشريعات وإنما يشمل الشرطة والتحقيق والقضاء، وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني، كما هو الحالي على المستوى الدولي، فإن ما يشعل الجريمة الإلكترونية غياب التشريعات الجزائية والجنائية وضعف الممارسات العالية والشرطية والقضائية في محاكمة والتحقيق في الجرائم الإلكترونية، وغالبا ما تجد في دول كثيرة تواضع التقنيات المتوافرة وكذلك الخبراء القادرون على متابعة ورصد وملاحقة الجريمة الإلكترونية داخل المجتمع والعابرة منها للحدود الوطنية (البقلي، ٢٠١٠، ٦٧).

ويمكن القول بأن الجريمة الإلكترونية باعتبارها مظهرًا جديدًا من مظاهر السلوك الإجرامي لا يمكن تصورها إلا من خلال ثلاث مظاهر، إما أن تتجسد في شكل جريمة تقليدية يتم اقترانها بوسائل إلكترونية أو معلوماتية، أو في شكل استهداف للوسائل المعلوماتية ذاتها وعلى رأسها قاعدة المعطيات والبيانات أو البرامج المعلوماتية، أو أن يتم اقتران الجرائم العادية في بيئة إلكترونية كما هو الأمر بالنسبة لجرائم الصحافة (الظاهرى، ٢٠١٩، ٤٨).

وكان لذلك انعكاسه السلبي على طلاب الجامعة، حيث أدت إلى زيادة مستوى القلق والخوف والاضطراب النفسي لديهم نتيجة تعرضهم لحملات وهجمات تسعى إلى تشويه سمعتهم والتشهير بهم من خلال نشر بعض الأقوال الكاذبة أو بعض الصور والملفات الشخصية؛ مما قد يدفعهم في بعض الحالات إلى الانتحار Marion،2010 ،(699).

ومن خلال ما تقدم يمكن القول إنه رغم كل ما قدمته الثورة الرقمية من آثار إيجابية للمجتمع وأفراده ومؤسساته، إلا أنها تسببت في وجود العديد من المخاطر والتحديات التي ترتبط بالمجتمع عموماً وبطلاب الجامعة بصفة خاصة، منها ما يتعلق بتهديد القيم والأخلاق، ومنها ما يتعلق بالمحتوى الذي يحث على الإباحية ويدعو إلى العنف والانحلال، ومنها ما يتعلق بالاتصال، كالاتصال بمؤسسات وأفراد مجهولي الهوية؛ بهدف إقناعهم بأفكار وأيديولوجيات خاطئة معادية للدين والمجتمع والقيم الإنسانية، ومخاطر متعلقة بالسلوك، مثل نشر محتويات نابية وغير أخلاقية

ونشر الشائعات المغرضة، ومنها ما يتعلق بالنفس، مثل الإغتراب وضعف التكيف الاجتماعي وإدمان الإنترنت وعدم السيطرة على النفس، وكان لهذه التحديات والمخاطر انعكاساتها السلبية على طلاب الجامعة.

وبالطبع يؤدي هذا الأمر إلى تقليل المهارات الاجتماعية التي يمكننا استخدامها أو اكتسابها في الحياة الواقعية، وبسبب هذه السلوكيات والآثار السلبية يمكن أن يصبح بعض المراهقين أكثر انطوائية أو أكثر عدائية للمجتمع، كذلك يؤثر هذا الأمر على طريقة تواصلهم مع الأشخاص الآخرين وخاصة في المدرسة أو الجامعة أو عند التخرج والالتحاق بالعمل، وهو ما يؤدي إلى العديد من المشكلات النفسية والعملية.

ثالثاً: متطلبات الأمن الرقمي لمواجهة مخاطر شبكات التواصل الاجتماعي.

لم يكن أحد ليتوقع قبل خمسين عامًا كيف ستدور أنماط الحياة اليوم حول الأجهزة المحمولة والعالم الرقمي، لقد أصبحت التكنولوجيا متكاملة بشكل جذري في الحياة اليومية بحيث لا يمكن أن نتصور الحياة بدون هذه التكنولوجيا، وبالتالي القدرة على التعامل مع هذه الأجهزة والتقنيات الرقمية بشكل مفيد وفعال سيمكن الأفراد من عيش لحظات أكثر متعة، ويعطي إنتاجية وكفاءة وجودة ودقة أكثر، ويساعد على تطوير الأعمال أو تغيير المهن.

لقد غيرت التقنية الرقمية من نمط الحياة، وطريقة التفكير، ومن أسلوب المعيشة، بل حتى من السلوك، ودخلت التطبيقات الرقمية كل تفاصيل الحياة، حتى أضحى معظم الأفراد، مدمنين على شاشة الحاسب، بل نقضي أكثر من نصف اليوم عليها وربما أكثر، وأصبحت الحواسيب الصغيرة (الهواتف الذكية)، لا تفارقنا حتى في النوم، بل وغدا جزء لا يمكن فصله عن أي جزئية في الحياة، محدثة ثورة في كيفية استهلاكنا وإنتاجنا وعملنا.

لقد أصبح استخدام شبكات الإنرتنت عن طريق أجهزة الحاسب الآلي أو الأجهزة الذكية والمحمولة نشاطاً روتينياً للأجيال الجديدة، ومع زيادة هذا الاستخدام بشكل هائل فإن الجانب الوقائي والحمايةً الشخصية والاجتماعية يمثل تحدياً أمام المستخدم على

مختلف مراحله العمرية، وبشكل خاص للأجيال الناشئة؛ مما يزيد من مطالب تنمية مهارات الأمن الشخصي والاجتماعي على شبكة الإنترنت لتلك الأجيال.

ولكي يتحقق الأمن والسرية للمعلومات والبيانات الخاصة والشخصية يجب أن توضع بعض الإجراءات والمتطلبات التى تستوجب لتوفير الحماية الكافية للمعلومات لعدم الاطلاع عليها من قبل الآخرين غير المصرح لهم، ولابد من وضع مستويات متعددة للحماية (يس، ٢٠٠٩، ٣٥٢) والمرور إذا كانت طبيعة المعلومات والموارد الأخرى المخزونة تتطلب هذا النوع من الحماية، أو وضع نظام حماية فعال يقلل إلى أدنى حد ممكن مشكلة كشف سرية المعلومات ذات الأهمية القصوى.

كما أصبح تحقيق متطلبات الأمن الرقمي أمراً ضرورياً في القرن٢١، حتى نستطيع من خلالها فهم كل شيء من حولنا، وبالتالي من الضروري الاجتهاد لزيادة المعرفة الرقمية، والتسلح بالمهارات الرقمية الجديدة .

وتعرف متطلبات الأمن الرقمي: بأنها المعارف والمهارات اللازمة للتمكن من حماية الأجهزة والمعلومات الشخصية على شبكة الإنترنت، بعد المراجعة الشاملة للأدبيات ذات الصلة بمجال الأمن الرقمي والتربية التكنولوجية للناشئة، تم التوصل إلى ثلاثة متطلبات رئيسة، هى: المتطلبات(الشخصية، والاجتماعية، والتكنولوجية) للأمن الرقمي.

١- متطلبات الأمن الرقمي على المستوى الشخصي:

وهي المهارات ذات العلاقة بالمستخدم شخصيا، وترتبط بمعلوماته، وبياناته الشخصية وسلوكه، وأسلوب تعامله أثناء استخدام الأجهزة الإلكترونية وشبكة الإنترنت(Sentse،2016، 665).

ويتعلق الأمن الرقمي على المستوى الشخصي بجميع القضايا ذات الصلة بالأجهزة الحاسوبية أو الأجهزة المحمولة، كما يتضمن قضايا حماية المعلومات

الشخصية، وسرقة الهوية والاستخدام غير السليم للأجهزة التقنية وشبكة الإنترنت، وتتمثل هذه المتطلبات في:(Sentse، 2016، 666 & Piwek، 2016، 359)

أ- حماية المعلومات الشخصية(الخصوصية):

وتتضمن : الوعي بأهمية حفظ المعلومات الشخصية والصور الخاصة أثناء استخدام الإنترنت، والتعرّف على أضرار كشف المعلومات الشخصية على المستخدم، وإدراك أهمية حذف الملفات الشخصية عند التخلص من الجهاز.

ب- الاحتيال وسرقة الهوية:

وتتضمن :إدراك أهمية العناية باختيار اسم المستخدم وكلمة المرور، والتعرف على أنواع الاحتيال التي تتم عبر الإنترنت، والوعي بخطورة نشر المعلومات الخاصة في برامج الألعاب المباشرة، وإدراك إمكانية إبلاغ الجهات المعنية بمحاولات الاحتيال والتصيد الإلكتروني.

ج- مواجهة التسلط عبر الإنترنت:

وتتضمن : فهم مصطلح التسلط الإلكتروني، ومعرفة كيفية مواجهة التسلط الإلكتروني، والوعي بأهمية رفض الرسائل والدعوات المشبوهة عبر الإنترنت، وإدراك مخاطر مقابلة جهات الاتصال التي تم التعرف عليها عن طريق شبكة الإنترنت.

د- إدمان الإنترنت:

وتتضمن :التعرف على تأثير الإنترنت على الحياة اليومية والعمل والعلاقات الاجتماعية، والتعرف على الأورار الصحية والعقلية والنفسية التي يسببها الجلوس الطويل أمام شبكة الإنترنت، وإدراك التأثيرات السلبية لإدمان الألعاب الإلكترونية.

هـ- 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.

كما حدد فودمان ومونرو(٢٠١٢، ٢٠٠)، و(Dowell،2009) و(O'Keeffe & Pearson ،2011 ، و(الخطيب وإبيفانيو) مجموعة من المتطلبات الشخصية لتحقيق الأمن الرقمي ، منها:

أ- المحافظة على اسم المستخدم وكلمة المرور:

أول باب يطرقه المهاجم هو محاولة الحصول على كلمات المرور الضعيفة، ومن أهم طرق المهاجم في الحصول على كلمات مرور هي :كسر حماية كلمات المرور الضعيفة، واستخدام الهندسة الاجتماعية، عن طريق التلاعب على شخصية الضحية، أو معرفة معلومات شخصية والتصنت على المستخدم، خاصة وأن الطلاب لا يدركون مدى ما يمثله اختيار اسم المستخدم في عملية الحكم على الوضع الشخصي للطالب، وكيف يمكن أن تكون دالةً على صفات المستخدم وسماته الشخصية، حيث يمكن للأسماء التي يختارونها أن تؤثر كثيراً في تجاربهم على شبكة الإنترنت.

ولذلك فإن قيمة كلمة المرور بقيمة ما تحميه، فأول باب يطرقه المهاجم هو محاولة الحصول على كلمات المرور الضعيفة، وكلمة المرور هي إحدى الطرق وأ رخصها للتحكم بالدخول للنظام.

ب- حماية الأجهزة من الفيروسات وبرمجيات التجسس:

الفيروسات تعتبر برامج حاسوبية خبيثة مضرة بالحواسيب، وتنتقل بين الحواسيب بعدة طرق، وتتكاثر بالاعتماد على ملفات أخرى أما برمجيات التجسس فيعرّفها معجم تكنولوجيا المعلومات للمعهد الجنائي في جامعة أركنساس بأنها :أي برنامج على الحاسوب يقوم بجمع معلومات المستخدم سراً من خلال اتصال المستخدم بالإنترنت بدون معرفته، وتكون في العادة لأهداف دعائية ، وهذ البرمجيات تقوم بمراقبة نشاط المستخدم على شبكة الإنترنت ونقل تلك المعلومات لشخص آخر لاستخدامها .كما تمتلئ شبكة الإنترنت بالعديد من عمليات التحميل والألعاب ونغمات الرنين ومقاطع الفيديو والبرامج

المجانية، وعلى الرغم من مجانية التحميل إلا أن الثمن قد يكون باهظاً؛ حيث قد تكون المقاطع الفلمية أو البرامج السابقة عبارة عن برامج خبيثة للتجسس على جهاز الحاسب.

ج- الحماية من سرقة الهوية وانتحال الشخصية:

يتعرض كثير من المستخدمين إلى محاولة سرقة الهوية على الشبكة الإلكترونية عن طريق رسائل الاصطياد الإلكتروني ، وهي تعنى :سرقة البيانات الشخصية السرية والحساسة عن طريق رسائل البريد الإلكتروني لغرض انتحال الشخصية، وذلك عن طريق انتحال شخصية أحد المصارف، أو منظمة معينة وإيهام الضحية بجدية الطلب وأهميته، وتحدث عملية سرقة الهوية عندما يسرق أحدٌ ما أو يحصل بطريقة ما على المعلومات الشخصية بالطالب، ويقوم بالادعاء بأن ذلك الطالب على الشبكة الإلكترونية، ويسجل الدخول إلى حساباته الشخصية.

د- مواجهة المضايقات الشخصية على شبكة الإنترنت:

إن من أبرز السلوكيات الخطيرة التي يتعرض لها الطلاب في المضايقات التي يتم تشغيلها عبر الإنترنت، مثل تشغيل النكات أو تقديم تعليقات فظة أو إحراج شخص ما عن قصد عبر الإنترنت، وبعض الأشخاص الذين يحاولون إلحاق الأذى أو التخويف والتضييق بشكل مؤذي للآخرين مثل الإساءة اللفظية مثل الاستحقار أو النعت بألقاب أو التهديد واستخدام لغة التحرش والألفاظ البذيئة .وينبغي التأكيد على الطلاب بأن لديهم القدرة على السيطرة وإيقاف المضايقة فوراً أثناء وجودهم على الشبكة؛ بالإضافة إلى أن معظم البرامج والتطبيقات تحتوي على روابط للإبلاغ عن الإساءة، أو الإشارة إلى وجود محتوى غير ملائم.

هـ- مواجهة التسلط عبر الإنترنت:

يستخدم التسلط عبر الإنترنت وسائل التواصل الرقمية عن عمد لإيصال معلومات خاطئة أو محرجة أو معادية عن شخص آخر، وهو ما يمثل الخطر الأكثر شيوعًا على الإنترنت لجميع الطلاب، وهو أمر شائع جدا، يمكن أن يحدث لأي شاب

على الإنترنت، ويمكن أن يسبب نتائج نفسية اجتماعية عميقة بما في ذلك الاكتئاب والقلق والعزلة الشديدة، والانتحار المأساوي.

و- التعامل مع المحتوى غير الملائم:

مع الانتشار الهائل لكمية المحتوى المتوافر على صفحات الإنترنت تصبح عملية الرقابة أمراً بالغ الصعوبة، فمن المألوف أن يتعرض الطلاب إلى مشاهدة محتوى غير ملائم ومخالف للآداب العامة، ويؤكد دويل وآخرون(Dowell ،2009، (551 أن هناك مخاوف إوافية تتعلق بالسلوكيات الخطرة عبر الإنترنت بدأت للتو في نشرها في الأدبيات وترتبط ارتباطًا مباشرًا بالصور غير اللائقة التي يتم العثور عليها عبر الإنترنت، وفي وسائل الإعلام هناك تقارير متزايدة عن مراهقين يتبادلون الصور غير اللائقة أو الجنسية على هواتفهم المحمولة والبريد الإلكتروني.

ز- أمن شبكات الحاسب:

يندفع الكثير إلى تركيب شبكات لاسلكية سواء في محيط منازلهم أو عملهم، دون أن يكون لهم أدنى دراية بكيفية عمل الشبكات، والطريقة الصحيحة لتهيئتها وهذا يقود حتماً إلى إنشاء شبكات غير آمنة، ويظهر أبرز نقاط ضعف الشبكات اللاسلكية في عدم وجود المعرفة الكافية بأمن المعلومات لمن يقوم بتركيب الشبكات اللاسلكية وإنشاء الكلمات السرية للشبكات، ووضع نقاط الدخول في أماكن مفتوحة كالممرات والقاعات، مما يعرض الشبكات للتنصت بشكل كبير.

٢- المتطلبات الاجتماعية للأمن الرقمي:

إن الحماية الأمنية لا تقتصر فيما يتعلق بالحاسب الآلي وشبكة الإنترنت على محيط الشخص الواحد، بل تتجاوز ذلك المحيط إلى المجال الأوسع على مستوى الأسرة والمجتمع والوطن بشكل عام .تتصل قضايا الأمن الرقمي على المستوى الاجتماعي والوطني بالجوانب ذات العلاقة باتصال المستخدم مع أفراد المجتمع الآخرين، والعلاقة

المنظمة لاستخدام محتويات شبكة الإنترنت بين المستخدمين، بالإضافة إلى قضايا التحريض على العنف والإرهاب.

ويقصد بها مجموعة من المتطلبات ذات العلاقة بتأثير الأجهزة الإلكترونية وشبكة الإنترنت على المجتمع ، وعلاقة المستخدم بالمجتمع الرقمي المحيط به، وتتمثل هذه المتطلبات في:

أ- التعامل الجيد مع مواقع التواصل الاجتماعي:

أحدثت انطلاقة الشبكات الاجتماعية على الشبكة الإلكترونية ثورة في أنماط التواصل بين الشباب، وقد أسهمت هجرة المراهقين الصغار إلى مواقع التواصل الاجتماعي ثورةً تسويقية ومكاسب مادية غير متوقعة لكل من المواقع والمعلنين فيها، ومع إتاحة الفرصة للصغار في الانضمام إلى التواصل الاجتماعي فإنهم مستهدفون من قبل عمليات نصب وتحرش تغريهم لإنفاق المال وتعريض أنفسهم للبرامج الضارة(Ryabov، 2012)&(Whitmer ، 2012 ، 18).

ويعد التعامل الغير صحيح مع مواقع التواصل الاجتماعي أبرز مخاطر استخدام الشباب لوسائل التواصل الاجتماعي، حيث يصبح استخدام وسائل التواصل الاجتماعي خطرًا على المراهقين أكثر مما يدرك معظم البالغين، وبسبب صغر سنهم، قد يواجه المراهقون عدم دقة أثناء عمليات البحث هذ ويتطلبون مشاركة الوالدين للتأكد من أنهم يستخدمون موارد موثوقة عبر الإنترنت، ويتلقون المعلومات بشكل صحيح، ولا يتأثرون بالمعلومات التي يقرؤونها.

ب- الحماية من إدمان الإنترنت والعزلة الاجتماعية:

قد يضر الإنسان نفسه بدون أن يشعر وخاصة عند استخدامه للحاسب الآلي، فمن أبرز الأضرار لاستخدام الحاسب الآلي الجلوس لفترات طويلة أمام الحاسب الآلي، وهو ما يعرف بالإدمان على الحاسب .

ويؤكد أوكيفي وبيرسون(O'Keeffe ،Pearson، (2011 أنه كما هو الحال مع الاكتئاب في ووع عدم الاتصال، فإن الأطفال والمراهقين الذين يعانون من الاكتئاب على فيسبوك معروون لخطر العزلة الاجتماعية ويتحولون أحيانًا إلى مواقع الإنترنت المحفوفة بالمخاطر والمدونات من أجل" المساعدة "التي قد تشجع إساءة استخدام المواد أو الممارسات الجنسية غير الأمنة أو السلوكيات العدوانية أو المدمرة للذات.

ج- الحماية من الجماعات التي تدعو إلى العنف والإرهاب:

ينطلق الإرهاب بجميع أشكاله وشتى صنوفه من دوافع متعددة، ويستهدف غايات معينة، ويتميز الإرهاب الإلكتروني عن غير من أنواع الإرهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات.

وتتضمن فهم مصطلح الإرهاب والتطرف على الإنترنت، والوعي بأساليب الجهات المشبوهة في شبكة الإنترنت لجذب الشباب نحو ارتكاب أعمال غير قانونية، وتنمية الوعي بطرق التصدي لتأثيرات الجماعات الإرهابية(الهويمل،٢٠٢٠، ٥٣).

كما يشير (عبدالصادق، ٢٠١٤، ٢٠٠) فإن الإرهاب الإلكتروني من أبرز التأث يرات السلبية التي يمكن أن يتركها مستخدمو الحاسب الآلي على المجتمع، والذي يعني العدوان أو التخويف أو التهديد ماديًّا أو معنويًّا، وذلك باستخدام الحاسب الآلي ووسائله الإلكترونية لدولة ما أو جماعة من الأفراد.

د- الالتزام بالسلوك الاجتماعي والأخلاقي الرقمي:

يستخدم العديد من الشباب الرسائل والمحادثات الإلكترونية كوسيلة رئيسة للاتصال، ومع وجود إمكانية الوصول إلى ملايين الأشخاص تغير مفهوم كلمة" صديق"، فالأصدقاء على شبكة الإنترنت في العادة أشخاصاً لا يعرفهم الطالب شخصياً في واقع الحياة، حيث إن لدى الطلاب حالياً العديد من الأصدقاء الافتراويين الذين لم يلتقوا بهم شخصياً على الإطلاق، وقد يجد بعض الطلاب أن بعض التصرفات تميل إلى الإساءة

بسبب الافتقار إلى المعرفة الحقيقية بهؤلاء الأصدقاء الافتراويين (فودمان ومونرو، ٢٠١٢ ، ١٩٥).

ويتضمن ذلك المحافظة على آداب التعامل والنشر على الإنترنت، وتجنب الكتابة بما يسيء للآخرين عبر الإنترنت، وتقديم الخدمات للمجتمع عبر الحاسب الآلي. (الهويمل،٢٠٢٠، ٥٣)

إن شبكة الإنترنت قد مكنت الناس من التواصل الاجتماعي وتبادل المعلومات الشخصية عبر الإنترنت بدرجة عالية من عدم الكشف عن هويتهم .إلى جانب غياب الإشراف، شجع ذلك على أشكال مختلفة من السلوك المعادي للمجتمع ود الأفراد الضعفاء بما في ذلك الشباب.

هـ- احترام وحماية حقوق الملكية الفكرية:

تتطلب جميع الأنشطة في مجالاتها المختلفة اليوم استخدام الوسائط الرقمية بشكل واسع، ومن أبرز ميزات الشبكة الإلكترونية أنها سهلت بشكل كبير وضع وتحديد وتنزيل المواد، ومع ذلك في أغلب الأحيان لا يأخذ المستخدمون في اعتبارهم ما هو ملائم أو غير ملائم أو غير قانوني عند وضع المعلومات على الشبكة أو تنزيلها على أجهزتهم الخاصة.

وتتضمن احترام وحماية حقوق الملكية الفكرية فهم مصطلح حقوق النشر والتأليف، والتمييز بين المحتوى المجاني والمحتوى الذي يحمل حقوق التأليف والنشر، والتعرف إلى الآثار السلبية لتحميل المحتوى بشكل غير مشروع، وتنمية احترام حقوق الملكية الفكرية للآخرين(الهويمل،٢٠٢٠، ٥٣).

ووحسب رأى (المنيع، ٢٠١٦، ١٨٩٥) فقد أصبح نسخ وتصوير وتبادل الوسائط الإلكترونية من المتطلبات التي ترفضها طبيعة الحياة اليومية، ولكن هذا النسخ والتصوير باختلاف وسائله يبرز قضية الملكية الفكرية وحمايتها، وعلى الرغم من تطور التشريعات المتعلقة بها إلا أن العالم يعاني من صعوبة في اعتماد إجراءات ثابتة ومقبولة

تقنيًّا لتثبيت حماية حقوق الملكية الفكرية؛ وذلك لوجود وجهات نظر مناقضة حول تلك الحقوق إضافة إلى ذلك فقد وفرت مميزات تقنية الحاسبات سهولة انتهاك حقوق الملكية الفكرية، فمثلاً عملية نسخ كتاب كبير في الحاسب الألى لا يحتاج إلا بضع ثوان وبسهولة من دون تكلفة مالية لعملية النسخ.

و- الوعي بالمخاطر المحتملة لاستخدام مواقع التواصل الاجتماعي:

وتتضمن :التعرف على مميزات مواقع التواصل الاجتماعي، والتعرف على الآثار السلبية لاستخدام مواقع التواصل الاجتماعي، والوعي بالآثار المترتبة على نشر المعلومات والرسائل عبر المنصات الاجتماعية وتأثيرها على سمعة المستخدم (الهويمل،٢٠٢٠، ٥٤).

٣- المتطلبات التكنولوجية للأمن الرقمي

يقصد بالمتطلبات التكنولوجية للأمن الرقمي : المهارات ذات العلاقة بالحماية المادية للأجهزة والبيانات، والتي ترتبط بالإجراءات التقنية في تعامل المستخدم مع الأجهزة الإلكترونية والشبكات، ومنها:(Valentine،2016) ،179-189، Dahlstrom ، 2014)

٤- إكساب المفاهيم الأساسية للأمن الرقمي:

وتتضمن: فهم مصطلحات الأمن الرقمي مثل البيانات والمعلومات، أمن المعلومات، حماية الأجهزة، جرائم الإنترنت، والتعرف على التهديدات التي تتعرض لها الأجهزة والبيانات، وإدراك أهمية أمن المعلومات في الحياة المعاصرة.

٥- الحماية من الفيروسات:

وتتضمن : إدراك مفهوم الفيروسات، وأسباب إصابة أجهزة الحاسب بها، والتعرف على طرق حماية الأجهزة من الفيروسات، والتعرف على الأسلوب الأمثل لاستخدام برامج مكافحة الفيروسات.

٦- الحماية من البرمجيات الخبيثة:

وتتضمن: فهم مصطلح البرمجيات الخبيثة، والتعرف على أنواعها، والتعرف على دوافع تطوير، واستخدام البرمجيات الخبيثة، وإدراك طرق الحماية من البرمجيات الخبيثة، والقدرة على التعامل مع ملفات تعريف الارتباط، والإعلانات المنبثقة، والبريد الإلكتروني المزعج.

٧- الاستخدام الأمن للشبكات:

وتتضمن التعرف على أنواع الشبكات الشائعة، وإدراك المزايا والمخاطر المرتبطة باستخدام شبكات الحاسب الآلي، والقدرة على التعامل مع الشبكات اللاسلكية بطريقة آمنة، والتعرف على طرق منع الوصول غير المصرح به إلى الجهاز والبيانات..

٨- حماية الأجهزة، والنسخ الاحتياطي للبيانات:

وتتضمن التعرف على تأثير البيئة المحيطة على الأجهزة الإلكترونية، وإدراك أهمية نسخ البيانات الاحتياطي، وإدراك أهمية إزالة البيانات غير المرغوب فيها.

مما سبق تتضح أهمية تحديد مجموعة من المتطلبات لتعزيز الأمن الرقمي للطلاب، ومواجهة مخاطر التواصل الاجتماعي، منها:

١. تعزيز قدرة الطالب على حماية الأجهزة حماية معلوماته الشخصية على شبكة الإنترنت.
٢. تنمية مهارات الطالب في استخدام برامج حماية الأجهزة.
٣. تنمية قدرة الطالب في التعامل مع المحتوى الإلكتروني في شبكة الإنترنت بالأسلوب المناسب وإنشاء محتوى رقمي مميز ونشره وإدارته.
٤. القدرة على إنشاء خدمة رقمية فعالة والتحكم بها وإدارتها.
٥. تدريب الطلاب على تسويق الخدمات الرقمية بشكل مبدع ومفيد.
٦. تنمية القدرة على استخدام الأجهزة والتقنيات الرقمية بشكل كفؤ وصيانتها.
٧. تنمية مهارات الطالب في استخدام جهاز الحاسب الآلي بطريقة آمنة.
٨. تنمية مهارات الطالب في مواجهة محاولات الاحتيال وسرقة الهوية.

٩. تعزيز قدرة الطالب على التصدي لمحاولات التسلط عبر الإنترنت.
١٠. تعزيز سبل وقاية الطالب من مخاطر الجماعات المتطرفة على شبكة الإنترنت.
١١. التزام الطالب بالآداب العامة للنشر على شبكة الإنترنت وحماية حقوق النشر والتأليف على شبكة الإنترنت.

من هنا يتضح أن الوقاية والحماية الشخصية والاجتماعية لشبكة الإنترنت وتطبيقاتها المختلفة يعد تحدياً أمام المستخدم على مختلف مراحله العمرية، وبشكل خاص طلاب الجامعة؛ مما يزيد من تحديد متطلبات لتعزيز الأمن الرقمي (الشخصي والاجتماعي والتكنولوجى) على شبكة الإنترنت لهؤلاء الطلاب.

المحور الثاني: الإطار الميداني للدراسة

الهدف من الإطار الميداني:

الكشف عن درجة توافر متطلبات تعزيز الأمن الرقمي لدى طلاب جامعة أسوان لمواجهة مخاطر مواقع التواصل الاجتماعي.

أداة الدراسة الميدانية:

تم اعتماد أداة الاستبانة كاداة لجمع بيانات الدراسة ، وقد تم تصميمها بالاستفادة من الإطار النظرى والدراسات السابقة المشابهة ، واشتملت الاستبانة فى صورتها الأولية على ثلاثة محاور :

المحور الأول: المتطلبات الشخصية ؛ حيث تضمن (١٤) عبارة، تهدف لقياس درجة توفر المتطلبات الشخصية لتعزيز الأمن الرقمي لدى طلاب جامعة أسوان.

المحور الثانى: المتطلبات الاجتماعية ؛ حيث تضمن (١٥) عبارة، تهدف لقياس درجة توفر المتطلبات الاجتماعية لتعزيز الأمن الرقمي لدى طلاب جامعة أسوان.

المحور الثالث: المتطلبات التكنولوجية ؛ حيث تضمن (١٤) عبارة، تهدف لقياس درجة توفر المتطلبات التكنولوجية لتعزيز الأمن الرقمي لدى طلاب جامعة أسوان.

وبعد تصميمها تم اتباع الخطوات التالية للتحقق من صلاحيتها للتطبيق الميدانى:

صدق أداة الدراسة الميدانية (الاستبانة):

أ- الصدق الظاهرى للأداة:

تم التأكد من صدق الاستبانة الخارجي من خلال عرضها على مجموعة من المحكمين من ذوي الاختصاص والخبرة في مجال الدراسة؛ وذلك بغرض تحكيمها بعد اطلاعهم على عنوان الدراسة، وتساؤلاتها، وأهدافها، فيبدون آراءهم وملاحظاتهم حول عبارات الاستبانة من حيث مدى ملاءمتها لموضوع الدراسة، وصدقها في الكشف عن المعلومات المرغوبة للدراسة، وكذلك من حيث ترابط كل عبارة بالمحور الذي تندرج تحته ومدى ،وضوحها، وسلامة صياغتها واقتراح طرق تحسينها سواء بالحذف أو الإبقاء، أو التعديل للعبارات، والنظر في تدرج المقياس ومدى ملاءمته وغير ذلك مما يرونه مناسبًا؛ وبناءً على آرائهم وملاحظاتهم تم التعديل لبعض العبارات، وكذلك تم إضافة وحذف بعض العبارات بحيث أصبحت الاستبانة صالحة للتطبيق في الصورة النهائية.

وبعد إجراء التعديلات التي أوصى بها المحكمون تم تعديل وصياغة بعض العبارات، وكذلك إضافة وحذف بعض العبارات، قد بلغ عدد عبارات الاستبانة بعد صياغتها النهائية (٢٩) عبارة موزعة على ثلاثة محاور، معتمدة على نظام ليكرت الثلاثى (موافق) بشدة، موافق محايد غير موافق، غير موافق بشدة)، بحيث أصبحت صالحة للتطبيق في الصورة النهائية.

ب- صدق الاتساق الداخلى

تم التعرف على مدى اتساق أداة الدراسة من خلال حساب معاملات الارتباط بين العبارات والمحور الذي تنتمي إليه كل عبارة باستخدام معامل ارتباط بيرسون (Person Correlation).

حيث جرى التحقق من صدق الاتساق الداخلي للاستبانة بتطبيق الاستبانة على عينة استطلاعية مكونة من (٥٧) طالبا وطالبة بجامعة أسوان، وذلك عن طريق نماذج جوجل (Google form) وتم حساب معامل ارتباط بيرسون بين كل عبارة من عبارات الاستبانة والدرجة الكلية للمحور الذي تنتمي إليه، وكذلك تم حساب معامل ارتباط بيرسون بين درجات كل محور من محاور الاستبانة والدرجة الكلية للاستبانة ، وذلك باستخدام البرنامج الإحصائي (SPSS)، إصدار (٢٣) كما توضح ذلك الجداول التالية:

جدول (١)

معاملات ارتباط بيرسون لعبارات كل محور بالمحور الذى تندرج تحته

المحور الاول: المتطلبات الشخصية		المحور الثانى: المتطلبات الاجتماعية		المحور الثالث: المتطلبات التكنولوجية	
العبارة	معامل ارتباط العبارة بالمحور	العبارة	معامل ارتباط العبارة بالمحور	العبارة	معامل ارتباط العبارة بالمحور
١	٠،٦٥٩**	١	٠،٣٧٩**	١	٠،٤٣٨**
٢	٠،٦٦٠**	٢	٠،٤٥٢**	٢	٠،٧٠٩**
٣	٠،٧٧٧**	٣	٠،٣٧٩**	٣	٠،٤٣٠**
٤	٠،٦٠٤**	٤	٠،٦٠٩**	٤	٠،٥٧١**
٥	٠،٥٦٣**	٥	٠،٣٨٧**	٥	٠،٤٩٤**
٦	٠،٥٤٩**	٦	٠،٣٧٩**	٦	٠،٥٣٤**
٧	٠،٩١٠**	٧	٠،٥٧٤**	٧	٠،٦٤٦**
٨	٠،٩١٠**	٨	٠،٤٨١**	٨	٠،٤٠١**
٩	٠،٨٥٩**	٩	٠،٥٠٨**	٩	٠،٥٢٨**
١٠	٠،٢٩٥*	١٠	٠،٥٠٤**	١٠	٠،٥٧١**
١١	٠،٦٧٠**	١١	٠،٨٨٦**	١١	٠،٦٩٤**
١٢	٠،٢٩٥*	١٢	٠،٥٠٨**	١٢	٠،٨٠٩**
١٣	٠،٧٤٢**	١٣	٠،٥٥٣**	١٣	٠،٦٣٨**
١٤	٠،٨٨٧**	١٤	٠،٦٥٥**	١٤	٠،٧٥٩**
		١٥	٠،٨٨٠**		

** دال عند مستوى ٠،٠١ * دال عند مستوى ٠،٠٥

يتضح من الجدول (١) أن قيم معامل ارتباط كل عبارة من العبارات مع محورها موجبة ودالة إحصائياً عند مستوى الدلالة(٠،٠٠١، ٠،٠٥) ؛ مما يدل على قوة ارتباط

العبارات بالمحاور ، وهو ما يؤكد صدق الاستبانة مما يدل على صدق اتساقها مع محاورها.

جدول (٢)

مصفوفة معاملات ارتباط بيرسون لكل محور والاستبانه ككل

العبارة	المحور الأول	المحور الثانى	المحور الثانى	الإستبانة ككل
المحور الأول	١	٠،٥٦٧**	٠،٤٢٣**	٠،٦٣٤**
المحور الثانى		١	٠،٦٥٧**	٠،٨٤٨**
المحور الثالث			١	٠،٥٦٦**
الاستبانة ككل				١

يتضح من الجدول (٢) أن قيم معامل ارتباط كل عبارة من العبارات مع محورها موجبة ودالة إحصائياً عند مستوى الدلالة(٠،٠٠١، ٠،٠٥) ؛ مما يدل على قوة ارتباط المحاور ببعضها البعض وبالإستبانة ككل، وهو ما يؤكد صدق الاستبانة؛ مما يدل على صدق اتساقها مع محاورها.

ثبات أداة الدراسة (الاستبانة):

أجرت الباحثة خطوات التأكد من ثبات الاستبانة وذلك بعد تطبيقها على أفراد العينة الاستطلاعية حيث تم استخدام (معادلة ألفا كرونباخ) للتأكد من ثبات أداة الدراسة وجدول (٣) يوضح معاملات ثبات أداة الدراسة

جدول (٣)

معامل ثبات الاستبانة باستخدام معادلة ألفا كرونباخ

محاورالاستبانة	عدد العبارات	ثبات المحور
المتطلبات الشخصية لتعزيز الأمن الرقمي لدى الطلاب	١٤	٠،٨٢٠
المتطلبات الاجتماعية لتعزيز الأمن الرقمي لدى الطلاب	١٥	٠،٧٠٦
المتطلبات التكنولوجية لتعزيز الأمن الرقمي لدى الطلاب	١٤	٠،٨٠٦
الثبات العام	٤٣	٠،٧٧٧

يتضح من الجدول ان معامل ثبات الاستبانة عال حيث بلغ (٠،٧٧٧) ؛ وهذا يدل على ان الاستبانة تتمتع بدرجة ثبات مرتفعة يمكن الاعتماد عليها فى التطبيق الميدانى للدراسة.

ويتضح من جدول (٣) أن قيم معاملات الثبات مرتفعة؛ مما يدل على أن الاستبيان يتمتع بدرجة عالية من الثبات.

مجتمع الدراسة:

تكون مجتمع الدراسة من جميع طلاب جامعة أسوان خلال فترة إجراء الدراسة للعام الجامعى(٢٠٢٣-٢٠٢٤) وعددهم (٢٤٥٧١)، بواقع (٩٩٧٧) طالبا، و(١٤٥٩٤)[١] طالبة، ونظرًا لكبر حجم مجتمع الدراسة وصعوبة الوصول إلى جميع مفرداته، فإنه تم اعتماد أسلوب العينات لتجميع البيانات الخاصة بالدراسة، وذلك من خلال أخذ عينة ممثلة من بعض الكليات العملية والنظرية بالجامعة.

عينة الدراسة:

يعتبر اختيار عينة الدراسة من الخطوات المهمة لإتمام الدراسة، لما لها من تأثير علي دقة النتائج التي تحدد فاعلية الدراسة، ولكي يتم اختيار العينة بطريقة صحيحة فإن ذلك يتوقف علي أهداف الدراسة والإجراءات المستخدمة ومجتمع الدراسة الأصلي، وقد اعتمدت الدراسة الحالية علي عينة من طلاب الجامعة بأسوان بكليات(التربية- التربية النوعية- الآداب- التجارة) للكشف عن درجة توافر متطلبات تعزيز الأمن الرقمي لديهم.

ونظراً لكبر حجم مجتمع الدراسة تم أخذ عينة ممثلة من بعض الكليات العملية والنظرية بجامعة اسوان.

حيث قامت الباحثة بالتطبيق إلكترونياً من خلال إرسال الرابط على موقع الفيسبوك واليوتيوب للطلاب كما تم توزيع توزيع بعض الاستبانات ورقياً على بعض

(١) **الخطة الإستراتيجية لجامعة أسوان: إحصائية الجامعة للطلاب المقيدين (٢٠٢٣- ٢٠٢٤).**

طـلاب كليـة التربيـة (محـل عمـل الباحثـة) ، واسترجاعهاوأصـبحت فـى النهايـة عـدد الاستبانات المكتمل الإجابة عليها (١٣١١) استبانة صالحة للتحليل، وهم اللذين شكلوا عينة الدراسة.

جدول (٤)

مجتمع وعينة الدراسة

الكلية	ذكور	إناث	مجتمع الدراسة	العينة	النسبة ٪	عينة الذكور	عينة الإناث
التربية	١٠١٣	٣٤٦٣	٤٤٧٦	٦٠٠	١٣،٤٠	٢١٥	٣٨٥
التربية النوعية	٧٩٩	١٣٤٨	٢١٤٧	٣٩٠	١٨،١٦	١٢٠	٢٧٠
الاداب	٦٤٩	١٤١٥	٢٠٦٤	٢٠٦	٩،٩٨	١٤١	٦٥
تجارة	١٥٢٧	٢١٥٢	٣٦٧٩	١١٥	٣،١٣	٣٠	٨٥
المجموع	٣٩٨٨	٨٣٧٨	١٢٣٦٦	١٣١١	١٠،٦٠	٥٠٦	٨٠٥

تمثلت عينة الدراسة فى مجموعة من طلاب بعض كليات الجامعة قوامها(١٣١١) بنسبة (١٠،٦٠)، حيث شملت (٦٠٠) طالب وطالبة من كلية التربية بنسبة (١٣،٤٠)، و (٣٩٠) طالبا وطالبة من كلية التربية النوعية بنسبة (١٨،١٦%)، و(٢٠٦) طالبا وطالبة من كلية الآداب بنسبة (٩،٩٨%)، و(١١٥) طالبا وطالبة من كلية التجارة بنسبة (٣،١٣%).

تصحيح أداة الدراسة (الاستبانة)

لتسهيل تفسير النتائج استخدمت الباحثة الأسلوب التالي؛ لتحديد مستوى الإجابة على بنود الأداة(الإستبانة)، حيث تم إعطاء وزن للبدائل: (نعم= ٣، إلى حد ما= = ٢، لا= ١)، وبضرب هذه الإستجابات فى التكرار المقابل لكل استجابة وجمعها وقسمتها على عدد عينة الدراسة يعطى ما يسمى بالمتوسط الحسابي الذي يعبر عن الوزن النسبي لكل عبارة على حدة كما يلي:

وقد تحددت درجة التوافر لدى عينة الدراسة (تقدير طول الفترة التى يمكن من خلالها الحكم على التوافر من حيث كونه (مرتفع- متوسط – منخفض)، من خلال المعادلة التالية

طول الفئة = (أكبر قيمة – أقل قيمة) ÷ عدد بدائل الأداة = (ن – ١) ÷ ن) = (٣-١) ÷ ٣ = ٠،٦٦ حيث تشير (ن) إلى عدد الاستجابات وتساوي (٣)، لنحصل على التصنيف التالي:

جدول (٥)

توزيع للفئات وفق التدرج المستخدم في أداة البحث

الاستجابة	المتوسط الحسابي
منخفضة	من ١ إلى ١.٦٦
متوسطة	من ١.٦٧ إلى ٢.٣٣
مرتفعة	من ٢.٣٤ إلى ٣

إجراءات تطبيق أداة الدراسة (الاستبانة)

بعد التأكد من صدق وثبات الاستبانة ودى صلاحيتها للتطبيق تم اتباع الإجراءات التالية

- طلب الموافقة على التطبيق من الجهة المعنية (جامعة أسوان)
- توزيع الاستبانة على أفراد عينة البحث (١٣١١) طالبا وطالبة .
- بعد الانتهاء من تطبيق الاستبانة تم جمعها من جميع أفراد عينة البحث.

قامت الباحثة بتصميم الاستبانة على نموذج جوجل (**Google form**)، وتم إرسال رابط الاستبانة إلى طلاب جامعة اسوان (الكليات المحددة)، وكان عدد الاستجابات الكاملة على الاستبانة(١٣١١) وشكلت أفراد الدراسة أي ما نسبته (١١،٣٠%) من مجتمع الدراسة الأصلي.

أساليب التحليل الإحصائي:

استخدمت الباحثة في تحليل بيانات الدراسة مجموعة من أساليب التحليل الإحصائي التالية:

أولاً : الإحصاء الوصفي، وتمثل في:

- حساب التكرارات والنسب المئوية لوصف خصائص أفراد مجتمع الدراسة وتحديد استجاباتهم.
- المتوسط الحسابي لحساب القيمة التي يُعطيها أفراد مجتمع الدراسة لكل عبارة من عبارات المحور، وعلى المحور بشكل عام، ولترتيب أوزان استجابات أفراد مجتمع الدراسة.
- الانحراف المعياري: لمعرفة مدى تشتت البيانات الاستجابات عن وسطها الحسابي، كما أنه يُفيد في ترتيب المتوسطات عند تساوي بعضها حيث تُعطى الرتبة الأفضل للعبارة التي انحرافها المعياري أقل.
- اختبار التاء للعينات المستقلة لمعرفة الفروق فى الستجابات بين الذكور والإناث حول درجة توافر متطلبات الأمن الرقمي لديهم.

ثانياً: الإحصاء التحليلي، وتمثل في:

- معامل ارتباط بيرسون Pearson Correlation Coefficient) لحساب الصدق البنائي(الاتساق الداخلي) لأداة الدارسة.
- معامل ثبات (ألفا كرونباخ Alpha Cronbach) لتحديد معامل ثبات أداة الدراسة.
- وتم تحليل نتائج الدراسة باستخدام البرنامج الإحصائي ((Statistical Package for Social Sciences) SPSS) الإصدار الثامن عشر.

نتائج الدراسة ومناقشتها:

يتضمن هذا الجزء عرض نتائج الدراسة التي هدفت إلى التعرف على درجة توافر متطلبات تعزيز الأمن الرقمي لدى طلاب جامعة أسوان.

حيث تم حساب المتوسطات الحسابية والانحرافات المعيارية لتقديرات أفراد العينة لدرجة توافر متطلبات تعزيز الأمن الرقمي لدى طلاب جامعة أسوان ، حيث كانت كما هي موضحة في الجدول:

أولاً: النتائج الخاصة بترتيب محاور الاستبانة الخاصة بمتطلبات تعزيز الأمن الرقمي لدى جامعة أسوان لمواجهة مخاطر مواقع التواصل الاجتماعي من حيث المتوسط الحسابي لكل محور ودرجة التوفر عليه، والجدول التالي يوضح استجابات أفراد العينة من الطلاب على توفر محاور الاستبانة إجمالاً:

جدول (٦)

ترتيب محاور الاستبانة

المحور	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة التوفر
المحور الأول: المتطلبات الشخصية لتعزيز الأمن الرقمي	٢،٠٣	٠،٤١	٣	متوسطة
المحور الثاني: المتطلبات الاجتماعية لتعزيز الأمن الرقمي	٢،٣٢	٠،٤٧	١	متوسطة
المحور الثالث: المتطلبات التكنولوجية لتعزيز الأمن الرقمي	٢،٢٢	٠،٥٠	٢	متوسطة
المتوسط العام للاستبانة	٢،١٩	٠،٤٦	متوسطة	

يتضح من الجدول السابق: جاء المتوسط العام للاستبانة ككل بمتوسط حسابي (٢،١٩) بدرجة توافر متوسطة ، وجء ترتيب المحاور كالتالى: المحور الثانى (**المتطلبات الاجتماعية لتعزيز الأمن الرقمي**) في المرتبة الأولى بمتوسط حسابى (٢،٣٢).

المحور الثالث (**المتطلبات التكنولوجية لتعزيز الأمن الرقمي**) في المرتبة الثانية بمتوسط حسابى (٢،٢٢).

المحور الأول (**المتطلبات االشخصية لتعزيز الأمن الرقمي**) في المرتبة الثالثة بمتوسط حسابى (٢،٠٣).

وربما يعزي ذلك إلى قصور الوعي لدى طلاب جامعة أسوان بمتطلبات الأمن الرقمي الشخصية والتكنولوجية والاجتماعية اللازمة لهم في ظل التأثير السلبي للثورة الرقمية عليهم وعلى النسق القيمى لديهم؛ الأمر الذي أدى إلى ضعف القدرة على مواجهة مخاطر مواقع التواصل الاجتماعي.

ثانيا: النتائج الخاصة بكل محور من محاور الاستبانة:

المحور الأول: المتطلبات الشخصية لتعزيز الأمن الرقمي لدى طلاب الجامعة.

جدول (٧)

المتوسطات الحسابية وترتيبها تنازليا لإجابات عينة الدراسة على العبارات التي تقيس درجة توافر (المتطلبات الشخصية) لتعزيز الأمن الرقمي

م	العبارة	نعم		إلي حد ما		لا		المتوسط الحسابي	ت	انحراف معياري	درجة التوافر
		ك٣	%	ك٢	%	ك١	%				
١	اختار كلمة مرور قوية واهتم بتغييرها كل فترة.	٤٣١	٣٢.٨٨	٨٧٣	٦٦.٥٩	٧	٠.٥٣	٢.٣٢	٦	٠.٤٨	متوسطة
٢	اتجنب ارسال معلوماتى الشخصية عبر الرسائل النصية أو البريد الإكترونى.	٤٩٨	٣٧.٩٩	٧٩٢	٦٠.٤١	٢١	١.٦٠	٢.٣٦	٥	٠.٥١	مرتفعة
٣	اتجنب فتح أي رابط مرفق فى رسالة مجهولة المصدر.	٢٢٠	١٦.٧٨	١٠٤٧	٧٩.٨٦	٤٤	٣.٣٦	٢.١٣	١٢	٠.٤٣	متوسطة

م	العبارة	نعم		إلي حد ما		لا		المتوسط الحسابي	ت	انحراف معياري	درجة التوافر
		ك٣	%	ك٢	%	ك١	%				
٤	افحص المحتوى الذي اقوم بنشره على الإنترنت	٣٠٦	٢٣.٣٤	٩٨٧	٧٥.٢٩	١٨	١.٣٧	٢.٢٢	٨	٠.٤٥	متوسطة
٥	استطيع مواجهة المضايقات التى اتعرض لها عبر مواقع التواصل الاجتماعي.	٧٠٧	٥٣.٩٣	٦٠٤	٤٦.٠٧	٠	٠.٠٠	٢.٥٤	١	٠.٥٠	مرتفعة
٦	أهتم بحضور دورات تدريبية عن التوعية بالأمن الرقمي بشكل دورى	٢٩٤	٢٢.٤٣	١٠١٧	٧٧.٥٧	٠	٠.٠٠	٢.٢٢	٧	٠.٤٢	متوسطة
٧	اتحكم فى التعبير براى واتجاهاتى عبر مواقع التواصل الاجتماعي	٢٦٠	١٩.٨٣	١٠٢٢	٧٧.٩٦	٢٩	٢.٢١	٢.١٨	١١	٠.٤٤	متوسطة
٨	اعرف حقوقى وواجباتى عند استخدام مواقع التواصل الاجتماعي	٢٧١	٢٠.٦٧	١٠٠٩	٧٦.٩٦	٣١	٢.٣٦	٢.١٨	١١	٠.٤٤	متوسطة
٩	اتحري الصدق والأمانة فى كل ما اقوم بنشره عبر مواقع التواصل الاجتماعي.	٢٩٣	٢٢.٣٥	١٠١٨	٧٧.٦٥	٠	٠.٠٠	٢.٢٢	٧	٠.٤٢	متوسطة
١٠	اتجنب اختراق أجهزة الاخرين والتعدى على حقوقهم الفكرية.	٥٧٩	٤٤.١٦	٧٣٢	٥٥.٨٤	٠	٠.٠٠	٢.٤٤	٣	٠.٥٠	مرتفعة

م	العبارة	نعم		إلي حد ما		لا		المتوسط الحسابي	ت	انحراف معياري	درجة التوافر
		ك٣	%	ك٢	%	ك١	%				
١١	لدى دراية بمخاطر مواقع التواصل الاجتماعي مثل التنمر والابتزاز والاحتيال والتصيد الالكترونى واتجنبها.	٢٨٧	٢١.٨٩	١٠١١	٧٧.١٢	١٣	٠.٩٩	٢.٢١	٩	٠.٤٣	متوسطة
١٢	اشغل أوقات فراغى بالمشاركة فى الأندية العلمية وثقافية واجتماعية وتطوعية لاكتساب ثقافة الأمن الرقمي.	٤٩٠	٣٧.٣٨	٨٢١	٦٢.٦٢	٠	٠.٠٠	٢.٣٧	٤	٠.٤٨	مرتفعة
١٣	اتفهم خطورة فتح الرسائل مجهولة المصدر التى ترسل لى عبر مواقع التواصل الاجتماعي	٣٣٢	٢٥.٣٢	٩٠٠	٦٨.٦٥	٧٩	٦.٠٣	٢.١٩	١٠	٠.٥٣	متوسطة
١٤	ألتزم بحقوق النشر والتأليف على شبكة الإنترنت.	٦٨٦	٥٢.٣٣	٦١١	٤٦.٦١	١٤	١.٠٧	٢.٥١	٢	٠.٥٢	مرتفعة

المتوسط الحسابي العام للمحور الأول = (٢،٠٣) ، الانحراف المعياري = (٠،٤١)

يتضح من الجدول(٧) حسب استجابات أفراد العينة من الطلاب على واقع توفر المتطلبات الشخصية لتعزيز الأمن الرقمي أن درجة توفر عبارات المحور جاءت متوسطة حيث بلغ المتوسط العام للمحور (٠٣،٢) ، بانحراف معياري (٤١،٠) ، وهو المتوسط الذي يقع في الفئة الثانية من فئات المقياس الثلاثى من (٦٧،١ – ٣٣،٢).؛

وهو ما يشير إلى قصور وعى طلاب جامعة أسوان بمتطلبات تعزيز الأمن الرقمي، وجاء ترتيب العبارات للمحور كما يلي:

أولاً: تبين أن بعض أفراد عينة الدراسة يتوفر لديهم درجة (مرتفعة) من المتطلبات الشخصية لتعزيز الأمن الرقمي على نحو (٥) عبارات تشير إلى توافر تلك المتطلبات لدى طلاب جامعة اسوان، وذلك على النحو التالي:

- جاءت العبارة (٥) وتنص على: "استطيع مواجهة المضايقات التى اتعرض لها عبر مواقع التواصل الاجتماعي" فى المرتبة الأولى بمتوسط حسابي (٥٤،٢) وانحراف معياري (٥٠،٠) ، مما يشير إلى وعى طلاب جامعة اسوان بطرق مواجهة المضايقات لتى يتم التعرض لها من خلال مواقع التواصل الاجتماعي.
- جاءت العبارة (١٤) وتنص على: "ألتزم بحقوق النشر والتأليف على شبكة الإنترنت" فى المرتبة الثانية بمتوسط حسابي (٥١،٢) وانحراف معياري (٥٢،٠)، ويشير ذلك إلى اهتمام طلاب الجامعة بالإلتزام بحقوق النشر والتأليف على شبكة الإنترنت ومعرفة واجباتهم ومسئوليتهم ومرعاة الأمانة العلمية.
- وحول اهتمام طلاب الجامعة بتجنب اختراق أجهزة الاخرين والتعدى على حقوقهم الفكرية جاءت العبارة (١٠) فى المرتبة الثالثة بمتوسط حسابي (٤٤،٢) وانحراف معياري (٥٠،٠)، ويشير ذلك إلى الإلتزام الاخلاقى لطلاب الجامعة بالإلتزام بحقوق النشر والتأليف على شبكة الإنترنت ومعرفة واجبات وحقوق الأخرين.
- جاءت العبارة (١٢) وتنص على: "اشغل أوقات فراغى بالمشاركة فى الأندية العلمية وثقافية واجتماعية وتطوعية لاكتساب ثقافة الأمن الرقمي" فى المرتبة الرابعة بمتوسط حسابي (٣٧،٢) وانحراف معياري (٤٨،٠).
- جاءت العبارة (٢) وتنص على: "اتجنب ارسال معلوماتى الشخصية عبر الرسائل النصية أو البريد الإكترونى" فى المرتبة الخامسة بمتوسط حسابي (٣٦،٢) وانحراف معياري (٥١،٠)، ويشير ذلك إلى وعو طلاب الجامعة بخطورة ارسال معلوماتهم الشخصية عبر الرسائل النصية أو البريد الإكترونى؛ وما ينتج عنه من إبتزاز

الأخرين لهم.، وفى هذا الصدد فقد أشارت **دراسة بيوران وآخرين(Beuran et al)، (2016** بأن القدرة العملية على التعرف على رسائل بريد الإلكتروني والمواقع الإلكترونية التصيدية أكثر أهمية من المعرفة المجردة لماهية رسائل البريد الإلكتروني والتصيد الاحتيالي، وهي المعرفة التي يتم تقديمها عادة في دورات التعلم الإلكتروني.

ثانياً: تبين أن بعض أفراد عينة الدراسة يملكون درجة (متوسطة) نحو (٩) عبارات من المتطلبات الشخصية لتعزيز الأمن الرقمي لتشير إلى قصور توافر تلك المتطلبات لدى طلاب جامعة اسوان، وذلك على النحو التالي:

- جاءت العبارة الأولى فى المرتبة السادسة اختار كلمة مرور قوية واهتم بتغييرها كل فترة فى المرتبة السادسة بمتوسط حسابي (٣٢،٢) وانحراف معياري (٤٨،٠).
- وهذا يُشير إلى قصور وعي طلاب جامعة أسوان بأهمية اختيار كلمة مرور قوية وتغييرها كل فترة؛ مما يؤكد ضرورة أن يهتم أفراد مجتمع الدراسة بذلك ، وألا يكون سرعة الوصول إلى بياناتهم الذي يجعلهم يختارون كلمة مرور سهلة ولا يغيرونها إلا إذا الدائم.
- وحول اهتمام الطلاب بحضور دورات تدريبية عن التوعية بالأمن الرقمي بشكل دورى ، جاءت العبارة (٦) فى المرتبة السابعة بمتوسط حسابي (٢٢،٢) وانحراف معياري (٤٢،٠)، وهذا يُشير إلى قصور وعي طلاب جامعة أسوان بأهمية التسجيل في الدورات التدريبية في مجال الأمن الرقمي لتنمية مهاراتهم الشخصية الرقمية، وقلة وعيهم بقدرة المهارات التي تقدم لهم في الدورات التدريبية في الأمن الرقمي على حمايتهم – بعون الله– من الاختراقات الخطيرة لمواقع التواصل الاجتماعي.
- جاءت العبارة (٩) وتنص على اتحري الصدق والأمانة فى كل ما اقوم بنشره عبر مواقع التواصل الاجتماعي فى المرتبة السابعة بمتوسط حسابي (٢٢،٢) وانحراف معياري (٤٢،٠).

- جاءت العبارة (٤) وتنص على "افحص المحتوى الذي اقوم بنشره على الإنترنت" فى المرتبة الثامنة بمتوسط حسابي (٢٢،٢) وانحراف معياري (٤٥،٠)، ويعزي ذلك إلىقصور اهتمام الطلاب بفحص المحتوى الذي يقومون بنشره على الإنترنت وهو ما انعكس بشكل كبير على ضعف قيامهم بالرجوع إلى المصادر الأصيلة للتأكد من مصداقية المحتوى المنشور على الإنترنت؛ كما قد تعزي تلك النتائج إلى يسر وسهولة التعدي على حقوق الملكية الفكرية للآخرين في ظل ضعف تنفيذ القوانين الرادعة التي تحمي الملكية الفكرية بشكل حقيقي وملموس، وفي ظل استخدام البعض للمعلومات وتداولها بشكل غير قانوني.
- جاءت العبارة (١١) وتنص على: "لدى دراية بمخاطر مواقع التواصل الاجتماعي مثل التنمر والابتزاز والاحتيال والتصيد الالكترونى واتجنبها) فى المرتبة التاسعة بمتوسط حسابي (٢١،٢) وانحراف معياري (٤٣،٠)، وهذا يُشير إلى أن طلاب الجامعة لا يعون بشكل كبير خطورة القيام بذلك، وأن هناك من يستغل بياناتهم للسرقة أو الابتزاز، وفى هذا الصدد فقد أشارت دراسة (الزهراني، وآخرون، ٢٠٢٠ ، ٣٦٥) أنه لابد أن يكون لدى الطلاب الوعي الكافي بالمخاطر التي يمكن أن يتعرضوا لها عبر البيئات الرقمية بكافة أنواعها، ومنها سرقة البيانات الشخصية، والانتحال والابتزاز وترويج الأفكار والمعتقدات الفكرية الهدامة، وهذا من شأنه أن يحميهم من خطر الإصابة بما يهدد أمنهم الرقمي، وأكدت دراسة السيد(٢٠٢٠ ، ٢١٠) أن الأمن الرقمي يعد من أهم المداخل الحديثة لمواجهة ظاهرة التنمر الإلكتروني، من خلال تمكن الفرد من حماية ما لديه من معلومات وبيانات شخصية والسيطرة عليها
- ومن ناحية تفهم طلاب الجامعة لخطورة فتح الرسائل مجهولة المصدر التى ترسل لى عبر مواقع التواصل الاجتماعي جاءت العبارة (١٣) فى المرتبة العاشرة بمتوسط حسابي (١٩،٢) وانحراف معياري (٥٣،٠).

- وأشارت نتائج الدراسة بأن هناك قصور لدى طلاب الجامعة فى التحكم بالتعبير عن آرائهم واتجاهاتهم عبر مواقع التواصل الاجتماعي حيث جاءت العبارة (٧) فى المرتبة الحادية عشر بمتوسط حسابي (١٨،٢) وانحراف معياري (٤٤،٠).
- وحول قصور معرفة طلاب الجامعة بحقوقهم وواجباتهم عند استخدام مواقع التواصل الاجتماعي جاءت العبارة (٨) فى المرتبة الحادية عشر بمتوسط حسابي (١٨،٢) وانحراف معياري (٤٤،٠).
- جاءت العبارة (٣) وتنص على اتجنب فتح أي رابط مرفق فى رسالة مجهولة المصدر فى المرتبة الثانية عشر بمتوسط حسابي (٢،١٣) وانحراف معياري (٠،٤٣)، وهذا يُشير إلى قصور وعي طلا جامعة أسوان بخطورة فتح أي رابط يصل إليهم من مصدر مجهول، مما يعني أنهم لا يعرفون جيداً مدى المفاسد المترتبة على ذلك

مما سبق لقد تراوحت المتوسطات الحسابية الموزونة لجميع عبارات المحور من حيث التوفر ما بين (٢،٥٤-٢،١٣) درجة من أصل (٣) درجات، كما يتضح أن قيم الانحراف المعياري بين (٠.٤٢ – ٠،٥٠) ، وربما يعزي ذلك إلى ضعف وعي طلاب الجامعة بالمتطلبات الشخصية لتعزيز الأمن الرقمي، وأثرها في بناء شخصيتهم وتوجيهها نحو ممارسة السلوك الصحيح في عصر الثورة الرقمية، خاصة في ظل الإفراط الكبير في استخدام التقنيات الحديثة، وفي ظل انتشار المواقع الإباحية وصعوبة السيطرة عليها ، وفي ظل تراجع دور المؤسسات التربوية في المجتمع، مثل الأسرة والجامعة ووسائل الإعلام في نشر الوعي بأهمية تعزيز الأمن الرقمي لدى الطلاب، وفى هذا الصدد **فقد قدمت دراسة Siponen) ،(2009)** تصوراً لبرنامج وعى أمن رقمى فى المؤسسات وذلك لتقليل أخطاء المستخدمين، ولتحسين فعالية سيطرة أألمن المطبقة توصلت إلى أن تقنيات أو إجراءات أمن المعلومات تفقد فائدتها الحقيقية إذا تم إساءة استخدامها، أو تم تفسيرها بطريقة خاطئة أو تم تطبيقها بشكل غير صحيح من قبل المستخدمين.

المحور الثانى: المتطلبات الاجتماعية لتعزيز الأمن الرقمي لدى طلاب الجامعة

جدول (٨)

المتوسطات الحسابية وترتيبها تنازليا لإجابات مجتمع الدراسة على العبارات التي تقيس درجة توافر(المتطلبات الاجتماعية) لتعزيز الأمن الرقمي

م	العبارة	نعم		إلي حد ما		لا		المتوسط الحسابي	ت	انحراف معياري	اتجاه الاستجابة
		ك٣	%	ك٢	%	ك١	%				
١	اتجنب نشر صورى الشخصية والعائلية من خلال تطبيقات التواصل الاجتماعي.	٣٦٧	٢٧.٩٩	٩٤٤	٧٢.٠١	٠	٠.٠٠	٢.٢٨	١٠	٠.٤٥	متوسطة
٢	أستطيع رفع بلاغ عن الإساءات التى قد أتعرض لها فى مواقع التواصل الاجتماعي.	٢٨٩	٢٢.٠٤	٩٨٥	٧٥.١٣	٣٧	٢.٨٢	٢.١٩	١٥	٠.٤٦	متوسطة
٣	أتحدث عبر الإنترنت مع أشخاص موثوق فيهم	٤٩٦	٣٧.٨٣	٨١٥	٦٢.١٧	٠	٠.٠٠	٢.٣٨	٣	٠.٤٩	مرتفعة
٤	أعى خطورة ترويج الشائعات التى تهدد أمن واستقرار المجتمع	٣٠٤	٢٣.١٩	٩٨٣	٧٤.٩٨	٢٤	١.٨٣	٢.٢١	١٤	٠.٤٥	متوسطة
٥	اكون حذر فى تكوين الصدقات الاجتماعية عبر مواقع التواصل	٣٩٤	٣٠.٠٥	٩١٧	٦٩.٩٥	٠	٠.٠٠	٢.٣٠	٩	٠.٤٦	متوسطة

م	العبارة	نعم		إلي حد ما		لا		المتوسط الحسابي	ت	انحراف معياري	اتجاه الاستجابة
		ك٣	%	ك٢	%	ك١	%				
٦	اعبر عن أرائي وأفكارى ومعتقداتى عبر الإنترنت دون الإساءة للاخرين.	٥٢٣	٣٩.٨٩	٧٨٨	٦٠.١١	٠	٠.٠٠	٢.٤٠	٢	٠.٤٩	مرتفعة
٧	التزم بالسلوك الاخلاقى الرقمي فى التعبير عن أفكارى على مواقع التواصل الاجتماعي	٣٦٨	٢٨.٠٧	٩١١	٦٩.٤٩	٣٢	٢.٤٤	٢.٢٦	١٢	٠.٤٩	متوسطة
٨	ادرك مخاطر الكشف عن المعلومات الشخصية للاخرين	٤٩١	٣٧.٤٥	٨٠٩	٦١.٧١	١١	٠.٨٤	٢.٣٧	٤	٠.٥٠	مرتفعة
٩	اعتذر للاخرين عند الخطا فى حقهم عبر منصات التواصل الاجتماعي	٤٤١	٣٣.٦٤	٨٣٦	٦٣.٧٧	٣٤	٢.٥٩	٢.٣١	٨	٠.٥٢	متوسطة
١٠	أحترم حقوق الملكية الفكرية للآخرين.	٤٢٤	٣٢.٣٤	٨٨٧	٦٧.٦٦	٠	٠.٠٠	٢.٣٢	٧	٠.٤٧	متوسطة
١١	إدرك خطورة خداع الاخرين للكشف عن أسرارهم وإفشائها	٤٣٦	٣٣.٢٦	٨٧٥	٦٦.٧٤	٠	٠.٠٠	٢.٣٣	٦	٠.٤٧	متوسطة

Print: (ISSN: 2535-2334) Online: (ISSN: 2682-4809)

م	العبارة	نعم		إلي حد ما		لا		المتوسط الحسابي	ت	انحراف معياري	اتجاه الاستجابة
		ك٣	%	ك٢	%	ك١	%				
١٢	أرفض التشهير بسمعة الآخرين أو تدمير مستقبلهم المهنى من خلال نشر المعلومات عنهم على الانترنت	٧٥٨	٥٧.٨٢	٥٥٣	٤٢.١٨	٠	٠.٠٠	٢.٥٨	١	٠.٤٩	مرتفعة
١٣	أحرص على نشر الوعى الرقمي عند التعرض للمواقف السلبية فى الإنترنت	٣٤٦	٢٦.٣٩	٩٦٥	٧٣.٦١	٠	٠.٠٠	٢.٢٦	١١	٠.٤٤	متوسطة
١٤	أدرك اهمية الالتزام بالأمانه عند الإقتباس من الآخرين او نقل أفكارهم.	٢٦٦	٢٠.٢٩	١٠٤٥	٧٩.٧١	٠	٠.٠٠	٢.٢٠	١٣	٠.٤٠	متوسطة
١٥	أرفض إرسال رسائل ذات محتوى جارح او مهين للأخرين عبر مواقع التواصل الاجتماعي.	٤٤٢	٣٣.٧١	٨٦٩	٦٦.٢٩	٠	٠.٠٠	٢.٣٤	٥	٠.٤٧	مرتفعة
المتوسط الحسابي للمحور الثانى = (٢،٣٢) ، الانحراف المعياري = (٠،٤٧)											

يتضح من الجدول(٨) حسب استجابات أفراد العينة من الطلاب على واقع توفر المتطلبات الاجتماعية لتعزيز الأمن الرقمي أن درجة توفر عبارات المحور جاءت

متوسطة حيث بلغ المتوسط العام للمحور (٣٢،٢) ، بانحراف معياري (٤٧،٠) ، وهو المتوسط الذي يقع في الفئة الثانية من فئات المقياس الثلاثى من (٦٧،١ – ٣٣،٢) ؛ وهو ما يشير إلى قصور وعى طلاب جامعة أسوان بالمتطلبات الاجتماعية لتعزيز الأمن الرقمي، وجاء ترتيب العبارات للمحور كما يلي:

أولاً: تبين أن بعض أفراد عينة الدراسة يملكون درجة (عالية) من المتطلبات الاجتماعية لتعزيز الأمن الرقمي لتشير إلى توافر تلك المتطلبات لدى طلاب جامعة اسوان، وذلك على النحو التالي:

- جاءت العبارة (١٢) وتنص على" أرفض التشهير بسمعة الآخرين أو تدمير مستقبلهم المهنى من خلال نشر المعلومات عنهم على الإنترنت" فى المرتبة الأولى بمتوسط حسابي (٥٨،٢) وانحراف معياري (٤٩،٠)
- وحول توفر متطلب قدرة الطلاب على التعبير عن آرائهم وأفكارهم ومعتقداتهم عبر الإنترنت دون الإساءة للآخرين جاءت العبارة (٦)، فى المرتبة الثانية بمتوسط حسابي (٤٠،٢) وانحراف معياري (٤٩،٠) ليشير إلى اهتمام طلاب الجامعة بهذا المتطلب.
- جاءت العبارة (٣) وتنص على: "اتحدث عبر الإنترنت مع أشخاص موثوق فيهم" فى المرتبة الثالثة بمتوسط حسابي (٣٨،٢) وانحراف معياري (٤٩،٠)، وهذا يُشير إلى أن طلاب الجامعة لا يتحدثون عبر الإنترنت إلا مع من يثقون بهم، لأنهم يُدركون بشكل قاطع الآثار الخطيرة المترتبة على الحديث مع غير الموثوق بهم، والتي قد تؤدي إلى التعدي على خصوصياتهم، أو التحقيق معهم من الجهات الأمنية بسبب هذا التواصل المشبوه.
- أشارت استجابات الطلاب بأن لديهم وعى بإدراك مخاطر الكشف عن المعلومات الشخصية للآخرين ، حيث جاءت العبارة (٨) فى المرتبة الرابعة بمتوسط حسابي (٣٧،٢) وانحراف معياري (٥٠،٠).

- جاءت العبارة (١٥) وتنص على: " أرفض إرسال رسائل ذات محتوى جارح أو مهين للآخرين عبر مواقع التواصل الاجتماعي فى المرتبة الخامسة بمتوسط حسابي (٣٤،٢) وانحراف معياري (٤٧،٠٠) .

ثانياً: تبين أن بعض أفراد عينة الدراسة يملكون درجة (متوسطة) من المتطلبات الاجتماعية لتعزيز الأمن الرقمي لتشير إلى قصور توافر تلك المتطلبات لدى طلاب جامعة اسوان، وذلك على النحو التالي:

- جاءت العبارة (١١) وتنص على: "أدرك خطورة خداع الآخرين للكشف عن أسرارهم وإفشائها " فى المرتبة السادسة بمتوسط حسابي (٣٣،٢) وانحراف معياري (٤٧،٠٠)، وتشير إلى أنه على الغم من وعى فئة من الطلاب بخطورة خداع الاخرين للكشف عن أسرارهم وإفشائها، إلا أن هناك قصور فى هذا المتطلب عند بعضهم.
- جاءت العبارة (١٠) وتنص على: "أحترم حقوق الملكية الفكرية للآخرين" فى المرتبة السابعة بمتوسط حسابي (٣٢،٢) وانحراف معياري (٤٧،٠٠) ، وربما يعزي ذلك إلى قصور وعي طلاب الجامعة بأهمية احترام حقوق الملكية الفكرية الرقمية، ويظهر ذلك جليًا في استجابة عينة الدراسة فيما يتعلق بدرجة إدراكهم لأهمية الالتزام بالأمانة عند الاقتباس من الآخرين.
- جاءت العبارة (٩) لتشير بقصور اهتمام الطلاب بالاعتذر للآخرين عند الخطأ فى حقهم عبر منصات التواصل الاجتماعي فى المرتبة الثامنة بمتوسط حسابي (٣١،٢) وانحراف معياري (٥٢،٠٠).
- جاءت العبارة (٥) وتنص على: "أكون حذر فى تكوين الصداقات الاجتماعية عبر مواقع التواصل" فى المرتبة التاسعة بمتوسط حسابي (٣٠،٢) وانحراف معياري (٤٦،٠٠)، ويشير ذلك إلى قلة توافر ذلك المتطلب لدى طلاب الجامعة.
- جاءت العبارة الأولى وتنص على: "اتجنب نشر صورى الشخصية والعائلية من خلال تطبيقات التواصل الاجتماعي" فى المرتبة العاشرة بمتوسط حسابي (٢٨،٢)

وانحراف معياري (٤٥،٠) ، وهذا يُشير إلى أن طلاب الجامعة يهتمون بدرجة متوسطة بوضع بياناتهم وصورهم الشخصية في مواقع التواصل الاجتماعي؛ لأنهم لا يعون بشكل كبير خطورة القيام بذلك، وأن هناك من يستغل تلك الصور والبيانات للسرقة أو الابتزاز.

- جاءت العبارة (١٣) وتنص على: "أحرص على نشر الوعى الرقمي عند التعرض للمواقف السلبية فى الإنترنت" فى المرتبة الحادية عشر بمتوسط حسابي (٢٦،٢) وانحراف معياري (٤٤،٠)
- جاءت العبارة (٧) وتنص على: "ألتزم بالسلوك الأخلاقى الرقمي فى التعبير عن أفكارى على مواقع التواصل الاجتماعي" فى المرتبة الثانية عشرة بمتوسط حسابي (٢٦،٢) وانحراف معياري (٤٩،٠).
- جاءت العبارة (١٤) وتنص على: "أدرك أهمية الالتزام بالأمانه عند الإقتباس من الآخرين أو نقل أفكارهم" فى المرتبة الثالثة عشر بمتوسط حسابي (٢٠،٢) وانحراف معياري (٤٠،٠) ، ويشير ذلك إلى قلة وعي طلاب الجامعة بأهمية متطلب الالتزام بالأمانة العلمية في العصر الرقمي، وقلة وعيهم بالآثار السلبية الناجمة عن ذلك، قد تتسبب في الكثير من الأضرار المادية والمعنوية والنفسية لهم.
- وحول وعى الطلاب بخطورة ترويج الشائعات التى تهدد أمن واستقرار المجتمع جاءت العبارة (٤) فى المرتبة الربعة عشر بمتوسط حسابي (٢١،٢) وانحراف معياري (٤٥،٠) لتشير إلى قصور توافر ذلك عند الطلاب.
- جاءت العبارة (٢) وتنص على: "أستطيع رفع بلاغ عن الإساءات التى قد أتعرض لها فى مواقع التواصل الاجتماعي فى المرتبة الأخيرة بمتوسط حسابي (١٩،٢) وانحراف معياري (٤٦،٠).

مما سبق يتضح أن هناك قصور فى بعض المتطلبات الاجتماعية لتعزيز الأمن الرقمي لدى طلاب الجامعة، منها قلة خبرة الطلاب الالتزام بالامانة العلمية وقلة وعيهم بخطورة نشر الصور والملفات الشخصية عبر مواقع التواصل الاجتماعي، وقلة وعيهم

بطرق خداع الآخرين للكشف عن أسرارهم وإفشائها ترويج الشائعات التى تهدد أمن واستقرار المجتمع، والقصور فى إحترام حقوق الملكية الفكرية للآخرين وفى هذا الصدد فقد **أكدت دراسة السيد(٢٠٢٠ ، ٢١٠)** أن الأمن الرقمي يعد يمكن الفرد من حماية ما لديه من معلومات وبيانات شخصية والسيطرة عليها، **ويرى أحمد (٢٠١٣ ، ١٩٦)** أن الأمن الرقمي يضمن لمستخدمي الإنترنت أمن البيانات والمعلومات وعدم تسريبها وحماية حقوق الملكية الفكرية، ومراعاة الخصوصية واحترامها واتخاذ كافة التدابير الوقائية لحماية أفراد المجتمع من البيانات والمعلومات الضارة.

المحور الثالث: المتطلبات التكنولوجية لتعزيز الأمن الرقمي لدى طلاب الجامعة.

جدول (٩)

المتوسطات الحسابية وترتيبها تنازليا لإجابات مجتمع الدراسة على العبارات التي تقيس درجة توافر(المتطلبات التكنولوجية) لتعزيز الأمن الرقمي

م	العبارة	نعم		إلي حد ما		لا		المتوسط الحسابي	ت	انحراف معياري	اتجاه الاستجابة
		ك٣	%	ك٢	%	ك١	%				
١	أستخدم في جهازى تقنية التحقق الثنائي (كلمة المرور- البصمة)	٥٧١	٤٣.٥٥	٦٩٦	٥٣.٠٩	٤٤	٣.٣٦	٢.٤٠	١	٠.٥٥	مرتفعة
٢	أعطل خدمات الوصول لموقعى فى التطبيقات المحملة على جهازى.	٤٦٥	٣٥.٤٧	٧٨٦	٥٩.٩٥	٦٠	٤.٥٨	٢.٣١	٤	٠.٥٥	متوسطة
٣	أقوم بإعداد نسخة احتياطية للبيانات المخزنة فى جهازي على الخدمة السحابية.	١٥٨	١٢.٠٥	١١٢١	٨٥.٥١	٣٢	٢.٤٤	٢.١٠	١٣	٠.٣٧	متوسطة
٤	أهتم بتحميل برامج الفيروسات	٣٦٦	٢٧.٩٢	٨٩٣	٦٨.١٢	٥٢	٣.٩٧	٢.٢٤	٧	٠.٥١	متوسطة

م	العبارة	نعم		إلي حد ما		لا		المتوسط الحسابي	ت	انحراف معياري	اتجاه الاستجابة
		ك٣	%	ك٢	%	ك١	%				
	والتجسس وأحافظ على تحديثها بشكل دوري.										
٥	أغير اعدادات جهازي بشكل مستمر حتى لا تخترق شبكة Wi- FI	٢٦٨	٢٠.٤٤	٩٨٣	٧٤.٩٨	٦٠	٤.٥٨	٢.١٦	١٠	٠.٤٧	متوسطة
٦	أهتم بتحديث جهازى بصفة مستمرة حفاظاً عليه.	٢٧٣	٢٠.٨٢	٩٨٩	٧٥.٤٤	٤٩	٣.٧٤	٢.١٧	٩	٠.٤٧	متوسطة
٧	أتبع قواعد الاستخدام الأمن الموضوعة من قبل الشبكات والمواقع الإلكترونية	١٥٠	١١.٤٤	١٠٧٩	٨٢.٣٠	٨٢	٦.٢٥	٢.٠٥	١٤	٠.٤٢	متوسطة
٨	أرفض استخدام برامج القرصنة والبرمجيات الخبيثة	٢٥١	١٩.١٥	١٠٠٨	٧٦.٨٩	٥٢	٣.٩٧	٢.١٥	١١	٠.٤٦	متوسطة
٩	أرفض شراء نسخة غير مرخصة للبرمجيات الحاسوبية	٢٤٠	١٨.٣١	١٠٢١	٧٧.٨٨	٥٠	٣.٨١	٢.١٤	١٢	٠.٤٥	متوسطة
١٠	ألتزم بالقوانين الخاصة حماية مستخدمى الإنترنت من البلطجة الالكترونية	٣٢٨	٢٥.٠٢	٩٢٠	٧٠.١٨	٦٣	٤.٨١	٢.٢٠	٨	٠.٥١	متوسطة
١١	أدرك اهمية الاستخدام الصحى الأمن	٤٥٥	٣٤.٧١	٨١٨	٦٢.٤٠	٣٨	٢.٩٠	٢.٣٢	٣	٠.٥٢	متوسطة

Print: (ISSN: 2535-2334) Online: (ISSN: 2682-4809)

م	العبارة	نعم		إلي حد ما		لا		المتوسط الحسابي	ت	انحراف معياري	اتجاه الاستجابة
		ك٣	%	ك٢	%	ك١	%				
	للأجهزة الإلكترونية مثل وضع الشاشة وارتفاع القدمين والاضاءة										
١٢	استخدم برامج لحفظ محتويات الملفات من التعديل أو الطباعة	٤٣٢	٣٢.٩٥	٧٩١	٦٠.٣٤	٨٨	٦.٧١	٢.٢٦	٦	٠.٥٧	متوسطة
١٣	أحرص على تشفير بياناتى فى مكان آمن خشية سرقتها أو تدميرها	٣٩٠	٢٩.٧٥	٨٧٩	٦٧.٠٥	٤٢	٣.٢٠	٢.٢٧	٥	٠.٥١	متوسطة
١٤	أستخدم ميزات حجب المواقع غير المرغوب فيها.	٥٣٤	٤٠.٧٣	٧٠٨	٥٤.٠٠	٦٩	٥.٢٦	٢.٣٥	٢	٠.٥٨	مرتفعة
المتوسط الحسابي للمحور الثالث = (٢،٢٢) ، الانحراف المعياري = (٠،٥٠)											

يتضح من الجدول السابق:

إن أفراد عينة الدراسة يتوافر لديهم المتطلبات التكنولوجية لتعزيز الأمن الرقمي بدرجة متوسطة، وهو ما يشير إلى قصور وعى طلاب جامعة أسوان بمتطلبات تعزيز الأمن الرقمي حيث بلغ المتوسط الحسابي للمحور الثالث (٢،٢٢)، وانحراف معياري (٠،٥٠).

أولاً: تبين أن بعض أفراد عينة الدراسة يملكون درجة (عالية) نحو عبارتين من المتطلبات التكنولوجية لتعزيز الأمن الرقمي لتشير إلى توافر تلك المتطلبات لدى طلاب جامعة اسوان، وذلك على النحو التالي:

- جاءت العبارة الأولى وتنص على" استخدم فى جهازى تقنية التحقق الثنائي (كلمة المرور– البصمة)" فى المرتبة الأولى بمتوسط حسابي (٢،٤٠) وانحراف معياري

(٠،٥٥)، وتشير إلى اهتمام طلاب الجامعة بتطبيق تقنية التحقق الثنائي (كلمة المرور – البصمة)"

وفى هذا الصدد فقد أشارت دراسة مارتن وآخرون(Martin et al) ، (2018 إلى أن التسلط عبر الإنترنت والهوية الرقمية وتأثير البصمات الرقمية واستخدام الوسائط الاجتماعية غير الملائمة من الموضوعات التي تحظى باهتمامها في المؤسسات التعليمية، ومع زيادة مؤسسات التعليم التي تنفذ المبادرات المتعقلة بإحضار أجهزة إلكترونية للطلاب أصبح الاهتمام بهذا المووضوع يتزايد أهميته.

- جاءت العبارة (١٤) استخدم ميزات حجب المواقع غير المرغوب فيها: "فى المرتبة الثانية بمتوسط حسابي (٢،٣٥) وانحراف معياري (٠،٥٨)، ويرجع ذلك إلى قلة قيام الطلاب بحجب المواقع التي تبث المعتقدات السلبية تجاه المجتمع.

ثانياً: تبين أن بعض أفراد عينة الدراسة يملكون درجة (متوسطة) من المتطلبات التكنولوجية لتعزيز الأمن الرقمي لتشير إلى قصور توافر تلك المتطلبات لدى طلاب جامعة أسوان، وذلك على النحو التالي:

- جاءت العبارة (١١) وتنص على: "أدرك أهمية الاستخدام الصحى الأمن للأجهزة الإلكترونية مثل وضع الشاشة وإرتفاع القدمين والإضاءة"، فى المرتبة الثالثة بمتوسط حسابي (٢،٣٢) وانحراف معياري (٠،٥٢)
- وحول توفر متطلب اهتمام طلاب الجامعة بأعطال خدمات الوصول للمواقع فى التطبيقات المحملة على الجهاز، فقد جاءت العبارة (٢) فى المرتبة الرابعة بمتوسط حسابي (٢،٣١) وانحراف معياري (٠،٥٥)، وهذا يُشير إلى قصور وعي أفراد مجتمع الدراسة المتوسط وغير الكافي بأهمية تحميل البرامج الأمنة المكافحة للفيروسات، مما يؤكد ضرورة أن يهتم أفراد مجتمع الدراسة بذلك ويعون خطورة التفريط فيه.
- جاءت العبارة (١٣) وتنص على: "أحرص على تشفير بياناتى فى مكان آمن خشية سرقتها أو تدميرها" فى المرتبة الخامسة بمتوسط حسابي (٢،٢٧) وانحراف معياري

(٠،٥١)، ويشير ذلك إلى قلة وعى طلاب الجامعة بطرق تشفير البيانات مما يؤدى إلى انتشار مظاهر الاستخدام غير الأخلاقي لشبكة الإنترنت من قِبل الآخرين من إعتداء على الخصوصيات والتجسس المعلوماتي وسرقة الهويات الشخصية.

- جاءت العبارة (١٢) وتنص على" استخدم برامج لحفظ محتويات الملفات من التعديل أو الطباعة فى المرتبة السادسة بمتوسط حسابي (٢،٢٦) وانحراف معياري (٠،٥٧)، وهذا يُشير إلى قلة وعي طلاب جامعة أسوان بطرق المحافظة على بياناتهم وملفاتهم الشخصية؛ مما يشير إلى أهمية تعلم طرق المحافظة على الأمن الرقمي بشكل دقيق وواضح ومستمر، وضعف إدراكهم لخطورة الكشف عن معلوماتهم الشخصية للآخرين، الأمر الذي قد يعرضهم لاختراق الخصوصية، وقد يرجع ذلك لضعف اهتمام الأسرة والجامعة بتنمية وعي الطلاب بأهمية احترام قيمة الخصوصية في العصر الرقمي.
- جاءت العبارة (٤) وهى (أهتم بتحميل برامج الفيروسات والتجسس وأحافظ على تحديثها بشكل دوري) فى المرتبة السابعة من حيث درجة موافقة أفراد عينة الدراسة بمتوسط حسابي (٢،٢٤) وانحراف معياري (٠،٥١)، وهذا يُشير إلى قصور وعي طلاب جامعة أسوان بنوع الحماية التي يمكن أن يقدمها الأمن الرقمي لهم ، وتشير إلى قصور وعيهم بخطورة الهجمات الفيروسية ووعيهم بقدرة الأمن الرقمي على التصدي لهذه الهجمات، وهو ما يتضح في قلة اقتنائهم برامج مكافحة الفيروسات والتجسس.
- جاءت العبارة (١٠) وتنص على "ألتزم بالقوانين الخاصة حماية مستخدمى الإنترنت من البلطجة الالكترونية" فى المرتبة الثامنة بمتوسط حسابي (٢،٢٠) وانحراف معياري (٠،٥١).
- وحول توفر متطلب تحديث الجهاز الإلكترونى بصفة مستمرة حفاظاً عليه جاءت العبارة (٦) المرتبة التاسعة بمتوسط حسابي (٢،١٧) وانحراف معياري (٠،٤٧)، ليشير إلى قصور توفر ذلك عند الطلاب.

- جاءت العبارة (٥) أغير اعدادات جهازي بشكل مستمر حتى لا تخترق شبكة Wi-Fi فى المرتبة العاشرة بمتوسط حسابي (٢،١٦) وانحراف معياري (٠،٤٧)، وهذا يشير إلى أن أغلب أفراد مجتمع الدراسة لا يقومون بتغيير إعدادات أجهزتهم بشكل مستمر مما يجعل شبكة Wi-Fi عرضة للاختراق دائماً، وهذا يعني ضرورة أن يعى أفراد مجتمع الدراسة خطورة هذا التفريط
- وحول توفر المتطلب التالى: "أرفض استخدام برامج القرصنة والبرمجيات الخبيثة"، جاءت العبارة (٨) فى المرتبة الحادية عشر بمتوسط حسابي (٢،١٥) وانحراف معياري (٠،٤٦)تشير بقصور توفر هذا المتطلب.
- جاءت العبارة (٩) وتنص على: "أرفض شراء نسخة غير مرخصة للبرمجيات الحاسوبية" فى المرتبة الثانية عشر بمتوسط حسابي (٢،١٤) وانحراف معياري (٠،٤٥)، وهذا يُشير إلى الأهمية القصوى التي يتبناها أفراد مجتمع الدراسة لعملية الشراء للبرمجيات ، وأن أفراد مجتمع الدراسة يعون بشكل واضح جداً خطورة التفريط بذلك.
- وحول اهتمام طلاب الجامعة بإعداد نسخة احتياطية للبيانات المخزنة فى جهازي على الخدمة السحابية جاءت العبارة (٣) فى المرتبة الثالثة عشر بمتوسط حسابي (٢،١٠) وانحراف معياري (٠،٣٧)، ويعزي ذلك إلى قلة إدراك الطلاب بأهمية الاحتفاظ بنسخ احتياطية من بياناتهم في مكان آمن خشية سرقتها أو تدميرها ، وهذا يُشير إلى وعي طلاب جامعة أسوان المتوسط وغير الكافي بأهمية رفع نسخة البيانات على الخدمات السحابية ، مما يؤكد ضرورة أن من يهتم الطلاب بذلك، وألا يؤدي ضيق الوقت لديهم بالتفريط في إعداد نسخة احتياطية لبياناتهم.
- جاءت العبارة (٧) أتبع قواعد الاستخدام الأمن الموضوعة من قبل الشبكات والمواقع الالكترونية فى المرتبة الرابعة عشر بمتوسط حسابي (٢،٠٥) وانحراف معياري (٠،٤٢)، ويشير ذلك إلى قصور اهتمام طلاب الجامعة بإتباع قواعد الاستخدام الأمن الموضوعة من قبل الشبكات والمواقع الالكترونية، وتأكيداً لذلك فقد

اقترحت **دراسة أحمد فرج (٢٠١٣)** برنامجاً الإلكترونياً في الأمن التكنولوجي لتعديل بعض السلوكيات الخطأ لدى طلاب الجامعات المصرية أثناء تعاملهم مع مواقع شبكات التواصل الاجتماعي.

تشير النتائج السابقة إلى توفر بعض المتطلبات التكنولوجية لتعزيز الأمن الرقمي لدى طلاب الجامعة ومنها: استخدم فى جهازى تقنية التحقق الثنائي (كلمة المرور– البصمة)، واستخدام ميزة حجب المواقع غير المرغوب فيها، ورغم توافر تلك المتطلبات إلا أن هناك قصور فى متطلبات عديدة ، منها : قلة قواعد الاستخدام الأمن الموضوعة من قبل الشبكات والمواقع الإلكترونية، والقصور فى أرفض استخدام برامج القرصنة والبرمجيات الخبيثة، وكذلك قلة الاهتمام بتحديث الجهاز الإلكترونى.

مما سق يتضح أن الثورة الرقمية أسهمت بشكل كبير في تآكل الخصوصية المعلوماتية لمستخدمي الإنترنت نتيجة تدوين المعلومات والبيانات، ونشرها عبر منصات التواصل المختلفة على شبكة الإنترنت، وفى هذا الصدد فقد أشارت **دراسة (الثوابيه الفراهيد،٢٠٢١)** إلى أن من مشكلات الثورة الرقمية والفضاء الرقمي انعدام الخصوصية من خلال مشاركة الشباب الجامعي لأحداثهم اليومية بشكل تفصيلي عبر منصات التواصل المختلفة مما جعل حياتهم كتابا مفتوحا للآخرين.

النتائج الخاصة بالمتغيرات النوعية للدراسة:

النتائج الخاصة بالفروق بين استجابات أفراد العينة المستفتاة من الطلاب لدرجة توفر متطلبات تعزيز الأمن الرقمي (الشخصية– الاجتماعية– التكنولوجية) لمواجهة مخاطر التواصل الرقمي بحسب متغير النوع (ذكور– إناث)، والجدول التالي: لحساب الفروق في آراء العينة حسب النوع (ذكور– اناث) لدرجة توافر متطلبات **تعزيز الأمن الرقمي (الشخصية– الاجتماعية– التكنولوجية) لمواجهة مخاطر التواصل الرقمي، تم** استخدام اختبار(ت) اختبار" T " لمعرفة الفروق ما إذا كانت هناك فروق ذات دلالة إحصائية بين عينتين مستقلتين، وذلك كما يلي:

جدول (١٠)

يوضح نتائج اختبار التاء لعينتين مستقلتين t-test لإظهار دلالة الفروق بين استجابات أفراد العينة المستفتاة من الطلاب نحو التوفر على محاور الاستبانة ومجموعها حسب متغير النوع (ن=١٣١١)

المحور	النوع	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة ت	Sig. (2-tailed)	الدلالة
المتطلبات الشخصية لتعزيز الأمن الرقمي	ذكور	٥٠٦	٣٠،٨٣	٢،٦٢	٢١،٩٩	٠،٠٠٠	دالة
	إناث	٨٠٥	٣٤،١٦	٢،٧٤			
المتطلبات الاجتماعية لتعزيز الأمن الرقمي	ذكور	٥٠٦	٣٦،٣٢	١،٩٧	٤،١٨	٠،٠٠٠	دالة
	إناث	٨٠٥	٣٤،٩٧	٢،٩٣			
المتطلبات التكنولوجية لتعزيز الأمن الرقمي	ذكور	٥٠٦	٢٩،٧١	٢،٧٦	١٧،٦٩	٠،٠٠٠	دالة
	إناث	٨٠٥	٣٢،٠٢	١،٩٤			

(df) درجة الحرية = ١٣٠٩

يتضح من الجدول (١٠) وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة المستفتاة من الطلاب تبعًا لمتغير النوع (ذكور – إناث)، بالنسبة لمحاور الاستبانة ومجموعها، حيث جاءت قيمة (ت) على الترتيب، (٢١،٩٩)، (٤،١٨)، (١٧،٦٩)، وجميعها قيم دالة إحصائيا عند مستوى دلالة (٠.٠١)، وجاءت الفروق جميعها لصالح الفئة الأعلى في المتوسط وهي الإناث فى المتطلبات الثلاث(الشخصية ، والاجتماعية والتكنولوجية) ، ويرجع ذلك إلى أن الإناث أكثر حرصاً والتزاماً من الذكور فى الاهتمام بمتطلبات الأمن الرقمي من خلال الحرص فى التواصل مع الآخرين واحترامهم وعدم التدخل فى خصوصياتهم، كما أنهم أكثر حرصاً على حماية مواقع التواصل الاجتماعي الخاصة بهم.

ويرجع ذلك إلى أن الطالبات كونهن أكثر التزامًا وتمسكا بالقيم نظراً لطبيعة المجتمع المصري وثقافته الدينية التي تغرس في الأنثى منذ الصغر قيم الحياء واحترام الغير، فضلاً عن تمتعهن بالإنضباط السلوكي بشكل أكبر من الذكور، في محاولة منهن للبعد عن المشكلات التي قد تواجهن نتيجة التعامل مع مواقع التواصل الاجتماعي.

ملخص نتائج الدراسة الميدانية :

أولاً: النتائج المتعلقة بالمتطلبات الشخصية لتعزيز الأمن الرقمي لدى طلاب جامعة أسوان:

تبين أن أفراد عينة الدراسة يتوافر لديهم بعض المتطلبات الشخصية نحو (٥) عبارات، وهي العبارة رقم (٢، ٥، ١٠، ١٢، ١٤).

تبين أن أفراد مجتمع الدراسة يتوافر لديهم بدرجة (متوسطة) بعض المتطلبات الشخصية لتعزيز الأمن الرقمي على نحو (٩) عبارات، وذلك على النحو التالي:

كما أشارات نتائج الدراسة الميدانية بأن هناك قصور في توافر بعض المتطلبات الشخصية لتعزيز الأمن الرقمي لدى طلاب جامعة أسوان، ومنها:

١. القصور فى اختيار كلمة مرور قوية والقيام بتغييرها كل فترة.
٢. يقوم بعض الطلاب احياناً بفتح أي رابط مرفق فى رسالة مجهولة المصدر.
٣. قلة فحص المحتوى الذي يقوم الطلاب بنشره على الإنترنت.
٤. قلة اهتمام الطلاب بحضور دورات تدريبية عن التوعية بالأمن الرقمي بشكل دورى.
٥. ضعف قدرة الطلاب على التعبير بحرية عن آرائهم واتجاهاتهم والتحكم فيها عبر مواقع التواصل الاجتماعي.
٦. قلة معرفة الطلاب بحقوقهم وواجباتهم عند استخدام مواقع التواصل الاجتماعي.
٧. القصور فى تحرى الصدق والأمانة فى كل ما يقوم الطلاب بنشره عبر مواقع التواصل الاجتماعي.
٨. قد بلجأ بعض الطلاب باختراق أجهزة الآخرين والتعدى على حقوقهم الفكرية.

٩. قلة معرفة الطلاب بمخاطر مواقع التواصل الاجتماعي مثل التنمر والابتزاز والاحتيال والتصيد الإلكترونى وأتجنبها.

١٠.قلة وعى الطلاب بخطورة فتح الرسائل مجهولة المصدر التى ترسل لى عبر مواقع التواصل الاجتماعي.

ثانياً: النتائج المتعلقة بالمتطلبات الاجتماعية لتعزيز الأمن الرقمي لدى طلاب جامعة أسوان:

أشارات نتائج الدراسة الميدانية بأن هناك قصور في توافر بعض المتطلبات الاجتماعية لتعزيز الأمن الرقمي لدى طلاب جامعة أسوان، ومنها:

١- قيام بعض الطلاب بنشر الصور الشخصية والعائلية من خلال تطبيقات التواصل الاجتماعي.

٢- قلة اهتمام الطلاب برفع بلاغ عن الإساءات التى قد يتعرضون لها فى مواقع التواصل الاجتماعي.

٣- البعد عن ترويج الشائعات التى تهدد أمن واستقرار المجتمع.

٤- قلة تحذير الطلاب من تكوين الصدقات الاجتماعية عبر مواقع التواصل.

٥- القصور فى إلتزام الطلاب بالسلوك الأخلاقى الرقمي فى التعبير عن الأفكار على مواقع التواصل الاجتماعي.

٦- قلة وعى الطلاب بمخاطر الكشف عن المعلومات الشخصية للآخرين.

٧- القصور فى احترام حقوق الملكية الفكرية للآخرين.

٨- قلة وعى الطلاب بخطورة خداع الآخرين للكشف عن أسرارهم وإفشائها.

٩- القصور فى نشر الوعى الرقمي عند التعرض للمواقف السلبية فى الإنترنت.

١٠- قلة وعى الطلاب بأهمية الالتزام بالامانه عند الاقتباس من الآخرين أو نقل أفكارهم.

ثالثاً: النتائج المتعلقة بالمتطلبات التكنولوجية لتعزيز الأمن الرقمي لدى طلاب جامعة أسوان:

أشارات نتائج الدراسة الميدانية بأن هناك قصور في توافر بعض المتطلبات التكنولوجية لتعزيز الأمن الرقمي لدى طلاب جامعة أسوان، ومنها:

١. قلة الدراية بكيفية تعطيل خدمات الوصول للموقع الشخصي فى التطبيقات المحملة على الأجهزة.
٢. قلة الاهتمام بإعداد نسخ احتياطية للبيانات المخزنة فى الجهاز على الخدمة السحابية.
٣. قلة الاهتمام بتحميل برامج الفيروسات والتجسس وأحافظ على تحديثها بشكل دوري.
٤. قلة وعلى الطلاب بتغيير إعدادات الأجهزة الإلكترونية بشكل مستمر حتى لا تخترق شبكة Wi– FI
٥. قلة الاهتمام بتحديث الأجهزة بصفة مستمرة حفاظاً عليها.
٦. القصور فى إتباع قواعد الاستخدام الأمن الموضوعة من قبل الشبكات والمواقع الإلكترونية.
٧. القصور فى تحذير الطلاب من استخدام برامج القرصنة والبرمجيات الخبيثة
٨. القصور فى تحذير الطلاب من شراء نسخة غير مرخصة للبرمجيات الحاسوبية.
٩. قلة الإلتزام بالقوانين الخاصة حماية مستخدمى الإنترنت من البلطجة الإلكترونية.
١٠. القصور فى الاهتمام بمعرفة الاستخدام الصحى الأمن للأجهزة الإلكترونية مثل وضع الشاشة وارتفاع القدمين والإضاءة.
١١. ضعف الاهتمام باستخدام برامج لحفظ محتويات الملفات من التعديل أو الطباعة.
١٢. قلة وعى طلاب الجامعة بطرق تشفير بياناتهم الخاصة فى مكان آمن خشية سرقتها أو تدميرها.

المحور الثالث: التصور المقترح للمتطلبات التربوية لتعزيز الأمن الرقمي لدى طلاب الجامعة لمواجهة مخاطر مواقع التواصل الاجتماعي:

لاشك أن التحولات والمتغيرات العالمية المعاصرة التي يمر بها العالم بشكل سريع ومتلاحق بفضل التطور التكنولوجي والرقمي، مما دفع المؤسسات التربوية والتعليمية ومنها الجامعة إلى إعداد الفرد الرقمي(طالب الجامعة) القادر على التعامل مع التكنولوجيا الرقمية بأمان وفاعلية، ملتزما بأخلاقيات التعامل الرقمي وواجباته تجاه نفسه وتجاه الآخرين ؛ ضمانا لسلامته وتحقيقا لأمنه.

وفي ضوء الإطار النظري للبحث وفى ضوء أهم النتائج التى تم التوصل إليها، يمكن تحديد التصور المقترح للمتطلبات التربوية لتعزيز الأمن الرقمي لدى طلابها لمواجهة مخاطر التواصل الاجتماعي، على النحو التالي:

(١) مبررات التصور المقترح:

يستند التصور المقترح لتعزيز الأمن الرقمي على مجموعة من المبررات التالية:

- ضعف الأمن الرقمي المتطلب لمواجهة مخاطر مواقع التواصل الاجتماعي لدى طلاب الجامعة.
- انتشار أفكار وانحرافات فكرية وثقافية وظهور سلوكيات غير أخلاقية؛ نتيجة الاندماج فى مواقع التواصل الاجتماعي وقضاء أغلب الوقت منشغلاً بها.
- غياب الوعي بمخاطر الثورة التكنولوجية وخاصة مواقع التواصل الاجتماعي.
- ضعف البنية التحتية التكنولوجية داخل الجامعات المصرية التى تمكن طلابها من التدريب على الأمن الرقمي داخلها.
- قصور المناهج التى تهتم بدراسة ثقافة الأمن الرقمي، والتي يمكن من خلالها مواجهة مخاطر مواقع التواصل الاجتماعي.

(٢) فلسفة التصور المقترح ومنطلقاته:

يقوم التصور المقترح للمتطلبات التربوية لتعزيز الأمن الرقمي لدى طلاب الجامعة على مجموعة من المنطلقات على النحو التالي:

- ضرورة مواكبة الثورة التكنولوجية والمعلوماتية التى تجتاح العالم، والتي لا يمكن تجاهلها من قبل أية دولة تسعى إلى مواكبتها؛ تحقيقا للتنمية المستدامة.
- ضرورة الاستفادة من الجامعات الأخرى، والتي تضمنت مناهجها ومقرراتها موضوعات تتعلق بالأمن الرقمي وأبعاده؛ تعزيزاً لقيمه لدى الطلاب؛ وتحقيقا للتوازن بين الحقوق والمسؤوليات الملزم بها الطالب الجامعي.
- العمل على مواكبة الانتشار الرقمي السريع، وانخراط الطلاب في استخدام وسائل التواصل داخل المجتمعات الافتراضية، لضمان الاستخدام الآمن والمسؤول للتقنيات الرقمية، خاصة في ظل وجود مؤسسات جامعية تمتلك بنيه تحتية تكنولوجية ومعلوماتية متطورة ، وكوادر بشرية قادرة على تعزيز الأمن الرقمي لدى الطلاب.
- إن التطور السريع للتقنيات وتكنولوجيا الاتصالات والمعلومات ، والاعتماد المتزايد عليها في السنوات الأخيرة نتج عنها بعض المخاطر التى جعل من الاهتمام بتعزيز الأمن الرقمي لدى الطلاب ضرورة قصوي.

(٣) الأهداف الاستراتيجية للتصور المقترح:

يهدف التصور المقترح للمتطلبات التربوية لتعزيز الأمن الرقمي لدى الطلاب لمواجهة مخاطر مواقع التواصل الاجتماعي إلى ما يلي:

- تبني المفاهيم والأساليب الإدارية الحديثة ومنها الأمن الرقمي داخل جامعة أسوان، والتي تسهم في رفع مستوى الأداء التكنولوجى لدى الطلاب ؛ بهدف رفع مستوى جودة وكفاءة مخرجاتها من الكفاءات الرقمية القادرة على استخدام التقنيات بطريقة آمنه وقانونية ، بل أخلاقية من قبل طالب رقمي.
- الوعي بمخاطر مواقع التواصل الاجتماعي وأخذ الحذر منها.

- تحويل جامعة أسوان إلى أنموذج تطبيقي تتجسد فيه روح التعاون بين أعضاء هيئات التدريس وطلابها، تعزيزاً للأمن الرقمي لدى طلابها.
- يهدف الأمن الرقمي إلى تمكين وحماية الطلاب فى العصر الرقمي؛ مما يعزز السلوك الأخلاقي لديهم من خلال جامعات تعزز مهارات الأمن الرقمي للحماية من مخاطر التقنيات الرقمية، ومواجهة التحديات العالمية المعاصرة.

(٤) آليات وإجراءات تعزيز الأمن الرقمي لدى طلاب جامعة أسوان لمواجهة مخاطر مواقع التوصل الاجتماعي:

من المؤكد أن آليات وإجراءات تعزيز الأمن الرقمي لدى طلاب جامعة أسوان تأخذ أشكالاً ومسميات عديدة لتصل إلى أهدافها، إلا أنها تتفق في نهاية الأمر على المتطلبات التربوية اللازمة لتحقيقها على النحو التالي:

وانطلاقاً من أهداف التصور المقترح، وما توصل إليه البحث الحالي من نتائج توصي بضرورة تعزيز الأمن الرقمي لدى الطلاب لمواجهة مخاطر مواقع التواصل الاجتماعي، ، فإن البحث يحاول تفعيل التصور المقترح من خلال الآليات والإجراءات التالية:

أولاً: الإجراءات والآليات المتعلقة بالمتطلبات الشخصية والتي تلعب دوراً مؤثراً في تعزيز الأمن الرقمي لدى طلاب جامعة أسوان، وذلك من خلال تنفيذ الآليات والإجراءات التالية:

١. اختيار كلمة مرور قوية والقيام بتغييرها كل فترة.
٢. تجنب ارسال المعلومات الشخصية عبر الرسائل النصية أو البريد الإكترونى.
٣. تجنب فتح أي رابط مرفق فى رسالة مجهولة المصدر.
٤. فحص المحتوى الذي يقوم الطلاب بنشره على الإنترنت .
٥. مواجهة المضايقات التى يتم التعرض لها عبر مواقع التواصل الاجتماعي.
٦. عقد دورات تدريبية للطلاب عن التوعية بالأمن الرقمي بشكل دورى

٧. تشجيع الطلاب على التعبير بحرية عن آرائهم واتجاهاتهم والتحكم فيها عبر مواقع التواصل الاجتماعي
٨. تعريف الطلاب بحقوقهم وواجباتهم عند استخدام مواقع التواصل الاجتماعي
٩. تدريب الطلاب على الصدق والأمانة فى كل ما يقومون بنشره عبر مواقع التواصل الاجتماعي.
١٠. تجنب اختراق أجهزة الآخرين والتعدى على حقوقهم الفكرية.
١١. تعريف الطلاب بمخاطر مواقع التواصل الاجتماعي مثل التنمر والابتزاز والاحتيال والتصيد الإلكترونى وأتجنبها.
١٢. شغل أوقات فراغ الطلاب بالمشاركة فى الأندية العلمية وثقافية واجتماعية وتطوعية لاكتساب ثقافة الأمن الرقمي.
١٣. تحذير الطلاب من خطورة فتح الرسائل مجهولة المصدر التى ترسل لى عبر مواقع التواصل الاجتماعي.
١٤. الإلتزام بحقوق النشر والتأليف على شبكة الإنترنت.

ثانياً: الإجراءات والآليات المتعلقة بالمتطلبات الاجتماعية والتي تلعب دوراً فعالاً في تعزيز الأمن الرقمي لدى طلاب جامعة أسوان، وذلك من خلال تنفيذ الآليات والإجراءات التالية:

١. تجنب نشر الصور الشخصية والعائلية من خلال تطبيقات التواصل الاجتماعي.
٢. قيام الطلاب برفع بلاغ عن الإساءات التى قد يتعرضون لها فى مواقع التواصل الاجتماعي.
٣. الحديث عبر الإنترنت مع الموثوق فيهم
٤. البعد ترويج الشائعات التى تهدد أمن واستقرار المجتمع
٥. الحذر فى تكوين الصداقات الاجتماعية عبر مواقع التواصل
٦. التعبير عن الآراء والأفكار والمعتقدات عبر الإنترنت دون الإساءة للآخرين.

٧. الإلتزام بالسلوك الأخلاقى الرقمي فى التعبير عن الأفكار على مواقع التواصل الاجتماعي.
٨. اكتساب ثقافة الإعتذار للآخرين عند الخطأ فى حقهم عبر منصات التواصل الاجتماعي.
٩. إدراك مخاطر الكشف عن المعلومات الشخصية للآخرين.
١٠. إحترام حقوق الملكية الفكرية للآخرين.
١١. إدراك خطورة خداع الآخرين للكشف عن أسرارهم وإفشائها.
١٢. منع التشهير بسمعة الآخرين أو تدمير مستقبلهم المهنى من خلال نشر المعلومات عنهم على الإنترنت .
١٣. الحرص على نشر الوعى الرقمي عند التعرض للمواقف السلبية فى الإنترنت.
١٤. إدراك أهمية الإلتزام بالأمانه عند الإقتباس من الآخرين او نقل أفكارهم.
١٥. منع إرسال رسائل ذات محتوى جارح أو مهين للآخرين عبر مواقع التواصل الاجتماعي.

ثالثاً: الإجراءات والآليات المتعلقة بالمتطلبات التكنولوجية والتي تلعب دوراً فعالاً في تعزيز الأمن الرقمي لدى طلاب جامعة أسوان، وذلك من خلال تنفيذ الآليات والإجراءات التالية:

١. استخدام تقنية التحقق الثنائي (كلمة المرور – البصمة)
٢. القيام بتعطيل خدمات الوصول لموقعى فى التطبيقات المحملة على جهازى.
٣. إعداد نسخ احتياطية للبيانات المخزنة فى جهازي على الخدمة السحابية.
٤. الاهتمام بتحميل برامج الفيروسات والتجسس والمحافظة على تحديثها بشكل دوري.
٥. تغيير إعدادات الأجهزة الإلكترونية بشكل مستمر حتى لا تخترق شبكة Wi– FI
٦. الاهتمام تحديث جهازى بصفة مستمرة حفاظاً عليه.
٧. إتباع قواعد الاستخدام الأمن الموضوعة من قبل الشبكات والمواقع الإلكترونية.
٨. رفض استخدام برامج القرصنة والبرمجيات الخبيثة.

٩. منع شراء نسخة غير مرخصة للبرمجيات الحاسوبية.
١٠. الإلتزام بالقوانين الخاصة حماية مستخدمى الإنترنت من البلطجة الإلكترونية.
١١. إدراك أهمية الاستخدام الصحى الأمن للأجهزة الإلكترونية مثل وضع الشاشة وارتفاع القدمين والإضاءة.
١٢. استخدام برامج لحفظ محتويات الملفات من التعديل أو الطباعة.
١٣. الحرص على تشفير البيانات فى مكان آمن خشية سرقتها أو تدميرها.
١٤. استخدام ميزات حجب المواقع غير المرغوب فيها.

(٥) متطلبات تنفيذ التصور المقترح:

١. توفر البنية التحتية التكنولوجية، والتي تتمثل في الأجهزة والمعدات والبرمجيات الخاصة ومحركات البحث الإلكتروني والحاسوب، والتي تقوم بنقل البيانات والمعلومات وتحزينها ومعالجتها، بالإضافة إلى نظم التشغيل المختلفة والبرمجيات المساندة والمتخصصة .
٢. توفير الكوادر البشرية المؤهلة تكنولوجياً، والتى تتمثل في العنصر البشري الذي يقع على عاتقهم نشر ثقافة الأمن الرقمي بين طلاب الجامعة، من خلال العملية التعليمية والأكاديمية والبحثية .
٣. عقد دورات تدريبية للطلاب حول طرق الاستخدام الأمن لاستخدام مواقع التواصل الاجتماعي.
٤. توافر كوادر وقيادات داعمة لنشر ثقافة الأمن الرقمي عبر شبكات المعلومات الداخلية والخارجية لدى أعضاء هيئة التدريس، وطلاب الجامعة، وكافة العناصر البشرية داخلها.
٥. توفير إستراتيجيات لمراجعة المتطلبات اللازمة لنشر وتنمية ثقافة الأمن الرقمي وأبعادها بين طلاب الجامعة ودورها في تحقيقها، على أن تتسم بالاستمرارية والمرونة.

٦. مراعاة مخاطر مواقع التواصل الاجتماعي من خلال إجراء دراسات وأبحاث مستقبلية تسهم في الحد من مخاطرها وآثارها السلبية على الطلاب.
٧. إعداد مقررات دراسية تتضمن أبعاد الأمن الرقمي.

(٦) المعوقات المحتملة لتنفيذ التصور المقترح:

توجد مجموعة من المعوقات التي يمكن أن تقف حائلا دون تنفيذ التصور المقترح، وتعوق تنفيذه، وتتمثل فيما يلي:

- مقاومة التغيير داخل الجامعة وخارجها.
- ضعف المبادرة من قبل القائمين على الجامعات فى تغيير المناهج وتطبيق سياسة الأمن الرقمي.
- قلة الوعي بأهمية التكنولوجيا الرقمية وتوظيفها في الجامعة.
- نقص الدعم المطلوب ماديًا لتطوير الجامعة إلكترونياً.
- قلة الاهتمام بإعداد برامج تثقيفية وتدريبية للطلاب على استخدام التكنولوجيا الرقمية.

(٧) طرق التغلب على معوقات تحقيق التصور المقترح:

يمكن التغلب عليها من خلال:

- توفير الدعم المادى اللازم لتحقيق متطلبات الأمن الرقمي لدى طلاب الجامعة.
- الاهتمام بعقد دورات تثقيفية للطلاب حول تطبيق الأمن الرقمي لمواجهة مخاطر التواصل الاجتماعي.
- لوضع خطط علاجية التدرج في تطبيق مراحل التصور المقترح.
- توعية الكوادر البشرية (أعضاء هيئات التدريس – الكادر الإداري – الطلاب) بالجامعة بأهمية التكنولوجيا الرقمية وتوظيفها.

المراجـــع

أولاً: المراجع العربية:

١. أبو العطا، مجدي محمد (٢٠١٠): **التواصل الاجتماعي باستخدام فيس بوك،** القاهرة: شركة علوم الحاسب.

٢. أحمد، فرج عبده (٢٠١٣): فعالية برنامج إلكتروني مقترح في الأمن التكنولوجي لتعديل السلوكيات الخطأ لدى طلاب الجامعات المصرية أثناء تعاملهم مع مواقع شبكات التواصل الاجتماعي، **مجلة كلية التربية** ، جامعة بنها ، مجلد (٢٤)، عدد٩٦، ١٨٩-٢٢٤.

٣. أمين، رضا عبد الواحد(٢٠٠٩): استخدامات الشباب الجامعي لموقع يوتيوب ، **دراسة منشورة ضمن وقائع مؤتمر الإعلام الجديد تكنولوجيا جديدة لواقع جديد** ، جامعة البحرين، ٧-٩ أبريل.

٤. البشرى، محمد الأمين (٢٠٠٠): "التحقيق في جرائم الحاسب الآلي"، بحث مقدم إلى **مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة ١-٣ مايو،** كلية الشريعة والقانون، الإمارات.

٥. البقلي، هيثم عبد الرحمن(٢٠١٠): **الجرائم الإلكترونية الواقعة على العرض: بين الشريعة والقانون المقارن،** دار المنهل.

٦. ترلينج، بيرني(٢٠١٣): مهارات القرن الحادي والعشرين: التعلم للحياة في زمننا، **مجلة العلوم التربوية،** مجلد(٢٥)، عدد(٣)، كلية التربية، جامعة الملك سعود.

٧. تريكي، حسان(٢٠١٤): التهديدات الأمنية المرتبطة بالاسنخدامات السيئة لشبكات التواصل الاجتماعي، **مجلة الحقوق والعلوم الإنسانية،** جامعة زيان عاشور بالجلفة.

٨. جبور، منى الأشقر(٢٠١٦): **السيبرانية: هاجس العصر**، لبنان: جامعة الدول العربية، المركز العربى للبحوث القانونية والقضائية.

٩. جويلي، مها عبد الباقي(٢٠٠١): **دراسات تربوية في القرن الحادي والعشرين**، الإسكندرية، دار الوفاء لدنيا الطباعة والنشر.

١٠. حسن، فاروق فؤاد(دت): مدخل إلى امن المعلومات وتعريف الجرائم الإلكترونية وكيفية الحماية.

١١. الحمادي، خالد حمد(٢٠١٧): إسهامات منصات التواصل الاجتماعي في المجال الأمني، **مجلة الفكر الشرطي**، مجلد (٢٤) ،العدد (١٠٠)، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات.

١٢. الخضري، جيهان سعد محمد(٢٠٢٠): الأمن السيبرانى والذكاء الإصطناعى فى الجامعات السعودية: دراسة مقارنة، **مجلة تطوير الأداء الجامعى**، مجلد (١٢)، العدد(١)، أكتوبر ٢٠٢٠، ٢٠٣- ٢٨٢.

١٣. خليل، محمود(٢٠١٠): **الإعلام العربي – مظاهر النمو ومخاطر التفكك**، القاهرة: العربي للنشر.

١٤. الربيعة، صالح بن على بن عبد الرحمن(٢٠١٧): **الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت**، المملكة العربية السعودية.

١٥. ريبيل، مايكل(٢٠١٣): **تنشئة الطفل الرقمي: دليل المواطنة الرقمية لأولياء الأمور**، الرياض : مكتب التربية العربي لدول الخليج (مترجم وناشر).

١٦. الزبيدى، عبد القوى سالم (٢٠٠٩): المراهق وتحديات الثورة الرقمية والمعلوماتية: دراسة اجرائية على عينة من التربويين، **مجلة رسالة التربية**، سلطنة عمان.

١٧. زكي ، وليد رشاد(٢٠٠٩): **المجتمع الافتراضي ..... نحو مقاربة للمفهوم، القاهرة:** صحيفة الأهرام الرقمي، مقالات وكتاب.

١٨. زمورى، زينب ، وخيرة، بغدادى(٢٠٠٥):العلاقة العاطفية بين الجنسين باستخدام الوسائل الإلكترونية بين المجتمع الافتراضى والمجتمع الحقيقى، **مجلة الباحث فى العلوم الانسانية والاجتماعية**، مجلد(٣)، عدد(٥)، عدد

خاص الملتقى الدولي الأول حول الهوية والمجالات الاجتماعية في ظل التحولات السوسيوثقافية في المجتمع الجزائري ، ١٨٩-٢٣٠.

١٩. الزهرانى، جميلةعبدالله، والغامدى، جوهرة بجاد(٢٠٢٠): درجة ممارسة طالبات المرحلة الثانوية بمحافظة جدة لمفهوم الأمن الرقمي والحقوق والمسئوليات الإلكترونية، **المجلة الدولية للعلوم التربوية والنفسية،** المؤسسة العربية للبحث العلمي والتنمية البشرية، مجلد(٢١)، عدد(٤٠)، ٣٥٦-٣٩٠.

٢٠. السعدى، نور على وسلام، شعيبث(٢٠٢٣): الحماية الجنائية للمرأة من ظاهرة الابتزاز الإلكترونى، مجلة العلوم الإنسانية والاجتماعية، **مجلة جامعة دهوك،** المجلد (٢٦)، العدد(١)، ٤٤-٥٦.

٢١. السيد، سماح السيد محمد(٢٠٢٠): مداخل مواجهة ظاهرة التنمر لإلكترونى لدى طلاب الجامعة من وجهة نظر بعض خبراء التربية، **مجلة كلية التربية،** جامعة بنها، مجلد(٣١)، عدد(١٢١)، ١٧٩- ٢٥٤.

٢٢. صلاح الدين، أشرف (٢٠١٠): طرق الحماية التكنولوجية بأنواعها وأشكالها ، **ندوة " مكافحة الجريمة عبر الإنترنت" ورشة عمل أمن المعلومات والتوقيع الإلكترونى،** المنظمة العربية للتنمية الإدارية ، القاهرة ، ٢٠٣-٢١٥.

٢٣. طوالبية ، محمد(٢٠١٧): الأمن فى العالم الإفتراضي:دراسة في سيكولوجية الإرهاب الإلكترونى، **مجلة الأكاديمية للدراسات الاجتماعية والإنسانية،** العدد (١٨)، الجزائر، ٥٥-٦٧.

٢٤. عبد الواحد، إيمان عبد الحكيم رفاعى(٢٠٢٠): دور الأسرة فى تحقيق الأمن الرقمي لطفل الروضة فى ضوء تحديات الثورة الرقمية ، **مجلة دراسات فى الطفولة والتربية،** أسيوط، كلية التربية للطفولة المبكرة ، عدد (١٤)، ٦٤-١١٨.

٢٥. عبد الصادق، عادل (٢٠١٤): الإرهاب الإلكتروني :نمط جديد وتحديات مختلفة، **مجلة الديمقراطية:** مؤسسة الأهرام، مجلد(١٤)، عدد(٥٣) ، ص١٩٢-١٩٣.

٢٦. العريشي ، جبريل حسن (٢٠١٨): دور مؤسسات التعليم العالى فى تعزيز ثقافة أمن المعلومات فى المجتمع، **مجلة مكتبة الملك فهد الوطنية**، مكتبة الملك فهد الوطنية، مجلد(٢٤)، عدد(٢)، ص ص ٣٠٢-٣٧٣.

٢٧. علوان،عماد عبده محمد(٢٠١٦): أشكال التنمر فى ضوء بعض المتغيرات الديموغرافية بين الطلاب المراهقين بمدينة أبها، **مجلة كلية التربية**، جامعة الأزهر، عدد ١٦٨، الجزء الأول، ص٤٣٩- ٤٧٣

٢٨. الغديان، سليمان بن عبد الرازق والنعيمى، عزالدين عبدالله عواد، خطاطية، يحى بن مبارك(٢٠١٨): صور جرائم الابتزاز الإلكترونى ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين ، مجلة البحوث الأمنية، كلية الملك فهد الأمنية، مركز البحوث والدراسات، مجلد (٢٧) ، عدد(٦٩)، ص ١٥٧- ٢٢٦.

٢٩. الصلاحي، فؤاد (٢٠١٥): "الأمن السيبرانى"، **مجلة الدوحة**، وزارة الإعلام، مجلد(٩٦)، عدد(٨)،٥٢-٥٥.

٣٠. فودمان، دوغ؛ ومونرو، مارجي(٢٠١٣): **الممارسات الأمنة عبر شبكة الإنترنت : دليل للمدارس المتوسطة والثانوية**، الرياض: مكتب التربية العربي لدول الخليج(مترجم وناشر).

٣١. فوزى، إسلام(٢٠١٩): الأمن السيبرانى: الأبعاد الاجتماعية والقانونية- تحليل سوسيولوجى، **المجلة الاجتماعية القومية**، المركز القومى للبحوث الاجتماعية والجنائية، مجلد٥٦ ، العدد٢، ٩٩- ١٣٩.

٣٢. الظاهرى، عبد الفتاح(٢٠١٩) :الجريمة المعلوماتية بين ثبات النص وتطور الجريمة، **سلسلة ندوات محكمو الاستئناف بالرباط** ، مجلة القانون

والأعمال، جامعة الحسن الأول – كلية العلوم القانونية والاقتصادية والاجتماعية – مختبر البحث قانون الأعمال ، عدد(٤١)، ٤٢-٦٩.

٣٣. المعداوى، محمد أحمد(٢٠١٨): حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي: دراسة مقارنة، **مجلة كلية الشريعة ولقانون بطنطا**، جامعة الأزهر، عدد (٣٣)، جزء(٤)، ١٩٢٧-٢٠٥٠.

٣٤. المقصودى، محمد أحمد على(٢٠١٧): الأمن السيبرانى والجهود الدولية لمكافحة الجرائم عابرة القارات ، **مجلة الأمن والحياة**، جامعة نايف العربية للعلوم الأمنية، مجلد ٣٧، عدد(٤٢٧)، ص ١٠٢- ١٠٧.

٣٥. المنتشرى ، فاطمة يوسف(٢٠٢٠): دور القيادة المدرسية فى تعزيز الأمن السيبرانى فى المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، **المجلة العربية للعلوم التربوية والنفسية**، المؤسسة العربية للتربية والعلوم والاداب، عدد (١٧)، ٣٥٧- ٣٨٤.

٣٦. المنيع، عثمان محمد(٢٠١٦): أدوار معلمي الحاسب الآلي في تعزيز أخلاقيات الحاسب الآلي والسلوكيات التربوية المرتبطة بها في المرحلة الثانوية من وجهة نظر المشرفين التربويين، **مجلة دراسات**، العلوم التربوية، الجامعة الأردنية- عمادة البحث العلمى، مجلد(٤٣)، عدد(٣)، ١٨٩١-١٩٠٧.

٣٧. الهويمل، سعد عبد العزيز(٢٠٢٠): أثر التكيف بناء على أسلوب تعلم الطالب على تنمية مهارات الأمن الرقمي لطلاب الصف الثالث المتوسط، **المجلة الدولية للعلوم التربوية والنفسية**، الأكاديمية العربية للعلوم الإنسانية والتطبيقية، مصر عدد(٥٤)، ص ١١-١٠٦.

٣٨. البداينة، ذياب موسي(٢٠١٤): الجرائم الإلكترونية المفهوم والاسباب، **ورقة عمل مقدمة إلى الملتقي العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية خلال الفترة ٢-٤/٩ لعام** ٢٠١٤، عمان المملكة الاردنية الهاشمية، ١-٣٢.

٣٩. يس، سعد غالب(٢٠٠٩): نظم المعلومات الإدارية، عمان، دار اليازورى العلمية للنشر والتوزيع.

ثانياً:المراجع الأجنبية:

40. Al-Khateeb، H. M، & Epiphaniou، G. (2016). How technology can mitigate and counteract cyber-stalking and online grooming. Computer Fraud & Security، Vol (1)، p14-18، Doi:10.1016/S1361-3723(16)30008-2

41. Al-Khateeb، H. M.، & Epiphaniou، G (2016): How technology can mitigate and counteract cyber-stalking and online grooming. Computer Fraud & Security، 2016(1)، 14-18، (16).

42. Beuran، R.، Chinen، K. I.، Tan، Y.، & Shinoda، Y:(2016): Towards effective cybersecurity، education and training. Available at: https://www.jaist.ac.jp/~razvan/publications/effective_cybersecurity.pdf

43. Cohen، Lawrence E.، and Marcus Felson(2015): routine activity theory، **International Encyclopedia of the Social & Behavioral Sciences** ،Second Edition.

44. Dahlstrom، D. E.، Brooks، C.، & Bichsel، J. (2014): The current ecosystem of learning management systems in higher education: Student، faculty، and IT perspectives، **Research report. Louisville**، CO: ECAR.

45. Dowell، E. B.، Burgess، A. W.، & Cavanaugh، D. J. (2009). Clustering of internet risk behaviors in a middle school student population. The Journal of School Health، Vol (79)، No(11)، p547-553.

46. Dowell، E. B.، Burgess، A. W.، & Cavanaugh، D. J. (2009): Clustering of internet risk behaviors in a middle school

student population. The Journal of School Health، 79(11)، 547-553.

47. Froehlich، D. (2012):NCTA Web 2.0: "Passport to Digital Citizenship. Participant Manual". North Caroli na Teacher Academy. https://translate.google.com.sa/translate?hl=ar
48. Good ،Carter v(1973): **Dictionary of Education**، 3rd ed، New York، McGraw-hill، Book Company.
49. Goutam، R. Rajesh (2021): Cybersecurity Fundamentals: Understand the Role of Cybersecurity، Its Importance and Modern Techniques Used by Cybersecurity Professionals. BPB Publications.
50. Jaana، J; Cornell، D; Sheras، G. (2006): Identification of School Bullies by Survery Methods، **Professional School Counseling**، Vol(9)،No(4)، 305 - 313.
51. Kaplan ،Rabbi Robert (2011) : Fostering Inter- Generational Leadership Dialogue - YouthBridge-NY، **A paper presented to The 9th Doha Conference of Interfaith Dialogue(Social Media and Inter-Religious Dialogue: A New Relationship)، (24-26 October)**، Doha. Qatar، Available at:http://www.qatarconferences.org /interfaith2011/speech18.pp
52. Livingstone، Sonia and Haddon، Leslie and Görzig، Anke and Ólafsson، Kjartan (2011):Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. EU Kids Online، Deliverable D4. EU Kids Online Network، London، UK
53. Martin، F. & Whitmer، J.C. (2016): Applying Learning Analytics to Investigate Timed Release in Online Learning. Technology، **Knowledge and Learning**، April 2016، Vol(21)، No(1)، pp 59-74.

54. Martin، F.، Chuang، W.، Petty، T.، Weichao، W.، & Wilkins، P. (2018). Middle School Students'، Social Media Use. Journal Of Educational Technology & Society، 21(1)، 213-224

55. Mills. N: (2011): Situated Learning through Social Networking Communities: The Development of Joint Enterprise، Mutual Engagement، and a Shared Repertoire. **Computer-Assisted Language Instruction Consortium Journal (CALICO)**،28(2)، 345-368.

56. Mukherjee، A Aditya. (2020):Network Security Strategies: Protect your network and enterprise against advanced cybersecurity attacks and threats. Packt Publishing Ltd، p197-223

57. Nicole، Boyd، danah m; Ellison،(2008):" Social Network SitesDefinition، History، and Scholarship**"Journal of Computer-Mediated Communication**.

58. O'Keeffe، Gwenn Schurgin & Clarke-Pearson ،Kathleen (2011):The Impact of social media on children، adolescents، and families. Council on Communications and Media ،Vol(127) No(4) April 01، Doi: 10.1542/peds،2011-0054، available at: https://publications.aap.org/pediatrics/article

59. Piwek، L.، & Joinson، A. (2016): "**What do they snapchat about?" Patterns of use in time-limited instant messaging service**، Computers in Human Behavior، 54، p358-367.

60. Ribble، M.، & Bailey، G. (2017):Digital citizenship in schools.; **International Society for Technology in Education (ISTE)**، USA. Washington، D.C.

61. Ryabov، I. (2012):The effect of time online on grades in online sociology courses، **MERLOT Journal of Online Learning and Teaching**، vol(8)،no(1)، 13-23.

62. Research، Juniper (2008): **Share، Collaborate، Exploit Defining Mobile Web 2.0، Juniper Research ، Tiis whitepaper extracted from: Mobile Web 2.0 Leveraging 'Location.** IM، Social Web & Search' 2008-2013،1-10 Available at: http://www0.cs.ucl.ac.uk/staff/d.quercia/others/mobile2.pdf

63. Sentse، M.، Kretschmer، T.، & Salmivalli، C. (2016): **The Longitudinal interplay between bullying، victimization، and social status: Age-related and gender differences**، Social Development، 24، 659-677

64. Stanley ، Meke Eze، N(2012): An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences"،1-16

65. Siponen Mikoo، willison، Ropert(2009): nformation security management standards: Problems and solutions، nformation & Management Vol(46)، No(5):p267-270 DOI:10.1016/j.im.2008.12.007

66. Thompson، P. (2013):"The digital natives as learners: Technology use patterns and approaches to learning". Computers & Education، Vol(65)، No(1)، 12-33.

67. Whitmer، J.، Fernandes، K.، & Allen، W. (2012): **Analytics in progress: Technology use، student characteristics، and student achievement. EDUCAUSE Review**، Available at: http://www.educause. edu/ero/ article/ analytics

68. Waycott.J. & Kennedy.G (2009):Mobile and Web 2.0 technologies in undergraduate science: Situating learning in everyday experience. **In Same places، different spaces. Proceedings ascilite Auckland**،1-12. Available at: http:// www.ascilite. org. au /conferences

69. Whitman، Michael E، Herbert J. Mattord(2011): Principles of Information Security، 6th Edition

70. Valentine، S.، Leyva-McMurtry، at el (2016):The Digital sash: A Sketch-based badge system in a social network for children. In Revolutionizing Education with Digital Ink ، New York City، NY،S**pringer International Publishing**، 179-189.

71. Yastrebenetsky، Michael & Kharchenko، Vyacheslav. (2020): Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems. IGI Global، p57-90.

72. Zack cooper: **a draft paper prepared for the conference on u.s.-china relations: cyber and technology hoover institution national security**، responding to chinese cyber-enabled economic activities، options for u.s. leaders، center for strategic and international studies، technology، and law conference stanford university، march 7، 2017 ،p 10.