دور الأمن السيبراني في الحد من التنمر الإلكتروني من وجهة نظر أولياء الامور

أ/هدى أحمد العيسى
قسم رياض الأطفال
كلية التربية – جامعة الملك فيصل
hf_7748@hotmail.com

أ/أنوار خلف العتيبي
قسم رياض الأطفال
كلية التربية –جامعة الملك فيصل
Anwarr_@outlook.sa:

د/نيرة عز السعيد عبد الفتاح
أستاذ مساعد تخصص دراسات طفولة
(صحة نفسية قسم رياض الأطفال -كلية التربية
طفولة)جامعة الملك فيصل
nabdelfattah@kfu

المستخلص:

- هدف البحث إلى الحد من التنمر الإلكتروني عن طريق الأمن السيبراني من وجهة نظر أولياء الامور حيث استخدمت الباحثة المنهج الوصفي وتكون مجتمع الدراسة من أولياء الامور وعددهم (٣١٧١).واستخدمت الاستبانة كأداة مناسبة للبحث حيث كانت النتائج أن لدرجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني جاءت بدرجة كبيرة بمتوسط حسابي (٣,١٨) وبانحراف معياري (٠,٤٨٦) وتراوحت المتوسطات الحسابية على فقرات درجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني بين (٢,٩٦ – ٣,٣٣)،وأوصت الباحثة بإتاحة التقنيات الرقمية التي توفر فرصاً للتعلم والتعليم للأطفال ولاسيما في المناطق النائية وأثناء الأزمات الإنسانية وعمل برامج وقائية تحول دون انغماس الأطفال على الشاشات الرقمية بما يكرس الاعتماد على الإنترنت، ويسهم في الإصابة بالسمنة.

مقدمة البحث:

أصبحت شبكة الأنترنت أحد أهم الدعامات في المجتمعات والتي تقوم عليها، بسبب ما تتيح من الحرية والاستخدامات المختلفة وصور التفاعل الجديدة لمستخدميها كما هو ظاهر على مواقع التواصل الاجتماعي وما تقدمة من مميزات مثل مشاركة الصور والفيديو والمراسلات والبحث عن الأصدقاء وإمكانية عرض. المعلومات المحددة والغير محددة، وإمكانية المستخدم من إخفاء هويته وعلى الرغم م الاهمية المتزايدة والإيجابيات التي تؤثر مواقع التواصل الاجتماعي في حياة الافراد بشكل عام والشباب بشكل خاص في العديد من المجالات الاجتماعية والثقافية والاقتصادية والعلمية كونها تمثل البيئة الحديثة للتواصل وتكوين العلاقات الاجتماعية، الا انها افرزت بعض المضامين الغير مرغوبة والتي انتجت العديد من الاثار السلبية ومن أبرزها ظاهرة التنمر الالكتروني

فالمجتمع يعاني من ظاهرة التنمر بين الشباب على ارض الواقع ومع تطور التكنولوجيا وظهور مواقع التواصل الاجتماعي وقوة تأثيرها على القضايا الاجتماعية ظهر نوع التنمر الالكتروني بشكل أكثر حدة، فأصبح مشكلة عصرية ذات اثار سلبية كبيرة سواء على مستوى المتنمرين او انواعه الضحايا، فقد أصبح التنمر الالكتروني مشكلة خطيرة تستدعي معرفه اشكاله وتفسيرها ورصد اثارها باعتباره مظهر حديث للسلوك العدائي المنتشر في المجتمع.

ويتمثل التنمر الإلكتروني في إرسال التعليقات والصور والرسائل المخجلة والمهينة والغير أخلاقية إلى فرد بشكل متعمد ومتكرر وعبر الوسائل الإلكترونية بهدف إيذاءه؛ مما يؤدي إلى شعور ذلك الفرد بالألم المادي والمعنوي والقلق المستمر، فالتنمر الإلكتروني يؤثر في البناء النفسي والأمني والاجتماعي، والمجتمع المدرسي بشكل خاص، فهو يجعل الطالب ضحية التنمر غير مرغوب فيه ومرفوض من بقية الطلبة الآخرين، وكذلك يؤثر في بناء المجتمع بشكل عام (يوسف ٢٠١٨) (العمار، ٢٠١٧).

ويحث التنمر الإلكتروني عندما يتعرض فر ما بشكل متكرر إلى سلوك تنمري يسبب له مزيداً من الألم، ويكون التنمر الإلكتروني ناتج عن عدم التكافؤ بين القوى لدى المتنمر والضحية، وقد يكون التنمر على شكل ألفاظ أو صور أو مقاطع خادشه بقصد إيذاء أو إحراج شخص آخر عن طريق استخدام وسائل الاتصال بالإنترنت لدعم هذا السلوك العدواني، فالتنمر

الإلكتروني عبارة عن شكل من أشكال العدوان، حيث يقوم المتنمر بإشباع رغباته وسلوكياته المضطربة على حساب الضحية دون مراعاة لمشاعره (حسين، ٢٠١٦) (أبو غزالة، ٢٠٠٩). ويلاحظ أن التنمر الإلكتروني يشبه التنمر المدرسي التقليدي ولكنه يختلف من حيث انتشاره على نطاق واسع وتأثيراته الأكثر خطورة، ويعود ذلك لعدة أسباب منها: قدرة المتنمر على التخفي، وسهوله نشر محتوى التنمر، وضعف التعاطف الوجداني الذي ينبثق من أن المتنمر لا يرى آثار أفعاله على الضحية، ونقص الرقابة على وسائل التواصل الاجتماعي. الأمر الذي جعل المتنمر يستطيع تتبع ضحيته خارج نطاق المدرسة؛ فأصبح التنمر لا يتقيد بالتواجد بالمدرسة حيث يمكن الوصول إلى ضحية من خلال الهاتف النقال، أو البريد الإلكتروني أو برامج المراسلات في أي وقت من اليوم، ومع سرعة وصوله إلى أكبر عدد من الجمهور مع القدرة السريعة على الانتشار، وتجاوز حدود الوقت والمكان وهذا ما يجعله أكثر حدة مقارنة بالتنمر العادي.

لذا يعرف التنمر الإلكتروني بأنه تعمد إيذاء الآخرين بطريقة متكررة وعدائية عن طريق استخدام الإنترنت (البريد الإلكتروني و/أو الألعاب الإلكترونية، و/أو الرسائل النصية، و/أو شبكات التواصل الاجتماعي مثل يوتيوب، استجرام، تويتر وغيرها). وتصف الدراسات السابقة نمطين مختلفين من التنمر الإلكتروني في ضوء الوسيلة التي يتم استخدامها وهما: التنمر المباشر؛ ويتم عن طريق استخدام الإنترنت/الهاتف الخلوي للتهديد أو الإهانة؛ أو إرسال ملفات تحمل فيروسات عن عمد؛ أو إرسال صور أو رسوم توضيحية فاحشة أو مهددة. وهناك التنمر غير المباشر؛ وهو التنمر الذي يحدث دون أن يلاحظ الضحية ذلك مباشرة ويتم عند يقوم المتنمر بتصفح بريد إلكتروني لشخص ما، التنكر وخداع شخص ما والتظاهر بأنه شخص أخر؛ أو نشر ما يسئ إلى الآخر عبر الهاتف النقال والبريد الإلكتروني، وبرامج الدردشة (الشناوي، ٢٠١٤).

وفي ظل التحول الرقمي الكبير الذي يشهده العالم في وقتنا الحالي، أصبح الأمن السيبراني ضرورة ملحة تتطلب الاهتمام الفوري كما يتوجب التعامل مع التهديدات والتحديات الجديدة بشكل سريع وفي حالة فقدان الأمن السيبراني تقع الجرائم الإلكترونية(جبور،٢٠٢٤).

مشكلة البحث واسئلته:

يتعرض الكثير من الأطفال لخطر التنمر الإلكتروني بشكل يومي، إذ أن ٢٠-٤٠٪ من الطلبة يمكن تصنيفهم على أنهم ضحايا التنمر الإلكتروني ورغم تزايد معدلات التنمر الإلكتروني، فإن الدراسات السابقة المتعلقة بالتنمر الإلكتروني والبرامج الوقائية وبرامج التدخل العلاجي لضحايا التنمر تعد محدودة للغاية، وخاصة في البيئة العربية. ودور الامن السيبراني في الحد من هذه الظاهرة لذلك، تقدم الدراسة الحالية مراجعة شاملة لآخر الدراسات الحديثة المنشورة حول الموضوع بما في ذلك معدلات انتشاره، وتأثيراته السلبية، والعوامل المتنبئة به، والتدخلات الوقائية له، كما سيتم مراعاة اراء أولياء الأمور حول ومعرفة ما تم ملاحظته حول هذه الظاهرة.

السؤال الرئيسي:

ما دور الأمن السيبراني في الحد من التنمر الإلكتروني من وجهة نظر أولياء الأمور؟

وتتفرع عنه الأسئلة التالية:

الأسئلة الفرعية:

ما درجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت؟

ما درجة انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي؟

ما درجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني؟

اهداف البحث:

يسعي البحث لتحقيق الاهداف التالية:

١. الكشف على دور الأمن السيبراني في الحد من التنمر الإلكتروني من خلال وجهة نظر أولياء الأمور؟

٢. تحديد درجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت؟

٣. تحديد درجة انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي؟

٤. تحديد درجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني؟

أهمية البحث:

تتمثل أهمية الدراسة في الآتي:

أولاً: الأهمية النظرية:

• الكشف عن معدلات انتشار التنمر الإلكتروني بين الأطفال من وجهة نظر أولياء الامور، ومناقشة العوامل المرتبطة بها.

• الكشف عن دور الامن السيبراني في الحد من ظاهرة التنمر الالكتروني من وجهت نظر أولياء الامور

• توضيح عوامل الوقاية من التنمر الإلكتروني من خلال الامن السيبراني.

ثانياً: الأهمية التطبيقية:

• يفيد البحث في سد النقص في الدراسات حول التنمر الإلكتروني.

• تفيد نتائج البحث في التوعية فئات المجتمع للحد من ظاهرة التنمر خاصة في مرحلة الطفولة المبكرة.

• يفيد البحث شريحة حساسة ومهمة من المجتمع، وهم فئة الأطفال والمراهقين الذين هم في طور التكوين والتطبيع الاجتماعي، ليكونوا سواعد بنائه في التنمية الاقتصادية والاجتماعية للمجتمع.

• يستفيد من نتائج الدراسة الحالية، الإخصائيين الاجتماعيين والنفسيين العاملين في المدارس، من حيث التعريف بطرق تشخيص مشكلة التنمر الإلكتروني لدى فئة الأطفال، وتحديد طرق الوقاية منه.

• سلطت البحث الضوء على أهمية التعاون بين أولياء الامور في علاج مشكلة التنمر الإلكتروني وتحديد دور الامن السيبراني، وهذا التعاون لن يأخذ مساره الحقيقي إلا إذا وعت كل مؤسسة دورها في عملية التنشئة الاجتماعية.

مصطلحات البحث:

عرف بدر الحيمودي. (٢٠٢٣) الأمن السيبراني: الأمن الذي يعني بتطبيق التقنيات، والعمليات والضوابط بهدف حماية الأنظمة وشبكات الحواسيب والبرامج والأجهزة والبيانات من التعرض للهجمات الالكترونية.

وتعرفه الباحثات الأمن السيبراني بأنه: نظام يتضمن ضوابط تحمي الأجهزة وبيانات الأشخاص من التعرض للهكر من أي جهة.

تعريف التنمر الإلكتروني:

وتعرفه عز،نيرة(٢٠٢٢) ظاهرة عدائية يمارسها طفل أو مجموعة أطفال على طفل آخر أضعف منهم وتمارس على منصات التعلم متعمدا مضايقته لإهانته نفسيا واجتماعيا.

وتعرفه الباحثات: بأنه الإيذاء المتكرر والمتعمد من قبل الأشخاص نتيجة استخدام الأجهزة الالكترونية.

حدود البحث:

يقتصر البحث على الحدود التالية:

الحد الموضوعي: الأمن السيبراني في الحد من التنمر الالكتروني من وجهة نظر أولياء الأمور

الحد المكاني: محافظة الاحساء في المنطقة الشرقية بالمملكة العربية السعودية.

الحد الزماني: الفصل الدراسي الاول للعام الجامعي ٢٠٢٤-٢٠٢٥م.

الحد البشري: أطفال الروضة- أولياء الأمور.

- الإطار النظري للبحث والدراسات السابقة:

يتناول محورين، المحور الأول: الأمن السيبراني، والمحور الثاني: التنمر الإلكتروني

أولًا: الأمن السيبراني:

١- تعريف الأمن السيبراني:

تعددت تعاريف الأمن السيبراني:

يعرفه آل مداوي، علي. (٢٠٢٣) على أنه: عبارة عن مجموع من الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع: الاستخدام غير المصرح به، وسوء الاستغلال، واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر

واستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء المعلوماتي.

ويعرف الظويفري (٢٠٢١) الأمن السيبراني بأنه: النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة.

ويعرف (Niekerkan & Ch&arman،٢٠١٧) الأمن السيبراني بأنه: مجموعة المعارف والمهارات والسلوك الفعلي والعلاقات المتبادلة بينها التي تساعد في حماية الأجهزة ووسائل التخزين المعلومات والتعامل الآمن مع خدمات الإنترنت والبرمجيات.

لاشك أن مصطلح الأمن السيبراني أو الحروب السيبرانية مرتبطة بخدمة الإنترنت؛ لكون العالم يشهد في الفترة الراهنة نوعًا جديداً من سباق التسلح، لكنه ليس بالشكل المعروف التقليدي، بل سباق يقوم على استحداث أو تطوير برامج إلكترونية معدة لأغراض عسكريه، تعرف اختصارًا بالسايبر .

٢- أهمية الأمن السيبراني:

أ- للأمن السيبراني أهمية كبيرة في حماية البيانات وخصوصية المؤسسات والأفراد، والكثير من المجالات المختلفة التي يختص بها، ويمثل الأمن السيبراني أهمية كبيرة للكثير من المنظمات الحكومية وغير الحكومية، مثل: الشركات والمؤسسات العامة والخاصة، فهو بمثابة جدار الحماية الأساسي لكافة المعلومات السرية لكل جهة مستفيدة. ولا شك أن بانهياره أو اختراقه سوف تكون المؤسسة أو الشركة هدفًا سهلًا للجهات الإجرامية والهاكرز بكل سهولة.

ب- كما يحمي الأمن السيبراني كذلك مختلف أنواع البيانات الحساسة والمهمة – سواء للحكومات أو الشركات، أو حتى الأفراد العاديين – من تعرضها للسرقة أو التدمير أو التلف. إن تعرض الأمن السيبراني للاختراق من شأنه أن يُحدث الكثير من الأضرار التي تلحق بسمعة الشركة أو المؤسسة، وبالتالي تؤثر على مستوى التعاملات التي تقوم بها في الأسواق التجارية.

ج- يؤدي اختراق الأمن السيبراني لأي جهة إلى تهديدًا كبيرًا ومباشرًا للكثير من البيانات الشخصية للعملاء، وهي عملية من شأنها أن تفسد علاقة العميل مع هذه الجهة وبالتالي تعرض الشركة لخطر الانهيار إذا ما قرر العملاء وقف التعاون معها بسبب هذا الخرق أو الانتهاك.

د-ويُساعد كذلك الشركات والمؤسسات على حماية نفسها، والدفاع عنها ضد هجمات خرق البيانات إذ تُعد المؤسسات والشركات هدفا سهلا لمجرمي الإنترنت بسبب استخدامها للخدمات السحابية ولتخزين معلوماتها الشخصية والحساسة فيها، وتُعد أغلب الخدمات السحابية وخاصة ذات التكوين السبئ هدفًا لهجمات الكثير من المجرمين الإلكترونيين المتطورين. (آل داوي، على ،٢٠٢٣)

٤- أنواع الأمن السيبراني:

أ- أمن البنية التحتية الحيوية: يعتمد على البنية التحتية الفيزيائية الإلكترونية للشبكة.

ب-تطبيقات الأمن: وهو الاختيار السليم للبرامج التي تحمي الأجهزة والشبكات من عمليات الاختراق الإلكتروني،

ج-أمن الشبكة: يهتم بالاختراقات الخارجية التي تهدد المنظومة الإلكترونية والمواقع التكنولوجية.

د-سحابة الأمان: وهي نظام مراقبة وحماية لكل مصادر المعلومات والبيانات التابعة للمستخدم عبر المواقع والمنصات الإلكترونية.

هـ-إنترنت الأشياء: يشمل عدة منظومات أساسية مثل أجهزة التلفاز وأجهزة الاستشعارات والطابعات. (آل داوي، على ،٢٠٢٣)

٥-جهود المملكة العربية السعودية في مجال الأمن السيبراني:

إن الأمر الملكي القاضي بإنشاء الهيئة الوطنية للأمن السيبراني وارتباطها بمقام مولاي خادم الحرمين الشريفين الملك سلمان بن عبد العزيز آل سعود – تعد بمثابة قفزة نوعية رائدة للمحافظة على أمن وسلامة المجتمع السعودي واستقراره وتأمين سلامة عمل كل قطاعات الدولة المختلفة، جاءت رؤية المملكة ٢٠٣٠م منسجمة ومتناغمة مع تعزيز الأمن السيبراني؛ لدورها الحيوي في حفظ، ودعم استخدام تقنيات المعلومات وتعزيز البنية التحتية الرقمية؛ لكي تكون مركزاً أساسياً لبناء أنشطة صناعية متطورة، وتحقيق مراكز متقدمة عالمياً في مؤشر

الأمم المتحدة للحكومة الإلكترونية؛ فقد حققت المرتبة الثانية عالمياً في محور التحسن المستمر في مؤشر الأمن السيبراني من بين ١٩٣ دولة ضمن تقرير الكتاب السنوي للتنافسية العالمية لعام ٢٠٢٢م. (آل داوي، على ،٢٠٢٣)

٦-عناصر الأمن السيبراني:

توجد ثلاث ركائز للأمن السيبراني وهي المستخدمون والنظم، وقابلية الاستخدام، وتوجد علاقة متبادلة بين الركائز الثلاثة، كما يوجد نوعان من المستخدمين وهما (الخبراء وغير الخبراء) الذين لديهم خصائص مختلفة تؤثر في استخدامهم لأنظمة الأمن السيبراني. (Ashdown & Sharpies,2020)

كذلك توجد ثلاثة عناصر أساسية، يعتمد عليها الأمن السيبراني، وتتمثل فيما يلي:

السرية:

يقصد بسرية المعلومات، الحفاظ عليها من خلال منح الإذن للمخول لهم فقط للوصول لتلك المعلومات والبيانات، مع منع الأشخاص غير المخول لهم الوصول إليها، وضرورة التأكد من عدم الإفصاح عنها أو تسريبها لأشخاص غير متخصصين أو مخول لهم ذلك.

تكامل المعلومات وسلامتها:

وتعنى الحفاظ على المحتوي من التعديل أو التغيير، أو الحذف، أو الإضافة بواسطة الأشخاص المؤهلين والمتخصصين بالإشراف على هذا المحتوى.

توافر المعلومات وإتاحته:

ويقصد بها توافر المعلومات من قبل المتخصصين والمشرفين على تقديمها وإتاحتها في الوقت المناسب (المنيع،٢٠٢٢).

٧-فئات الأمن السيبراني:

يمكن تقسيم الأمن السيبراني إلى عدة فئات مشتركة:

أمان الشبكة: ويتمثل في ممارسة تأمين شبكة الكمبيوتر من المتطفلين، سواء أكانوا مهاجمين ومستهدفين أم برامج ضارة.

أمان التطبيقات: وهو نظام العمليات والأدوات والإجراءات الأمنية والذي يعمل على حماية تطبيقات الحاسوب، كما يركز على إبقاء البرامج والأجهزة خالية من التهديدات.

أمن المعلومات: ويشمل سلامة البيانات وخصوصيتها، سواء في التخزين أو أثناء النقل.

الأمن التشغيلي: الذي يشمل العمليات والقرارات الخاصة بمعالجة أصول البيانات وحمايتها والأذونات التي يمتلكها المستخدمون عند الوصول إلى الشبكة، والإجراءات التي تحدد كيف وأين يمكن تخزين البيانات أو مشاركتها كلها وهي ما تندرج تحت هذه المظلة

–التعافي من الكوارث واستمرارية الأعمال: وهو يحدد كيفية استجابة المنظمة لحادث الأمن السيبراني، أو أي حدث آخر يتسبب في فقدان العمليات أو البيانات، وتملي سياسات التعافي من الكوارث كيفية استعادة المؤسسة لعملياتها ومعلوماتها للعودة إلى القدرة التشغيلية نفسها كما كانت قبل الحدث، وهي الخطة التي تعمل بها المنظمة أثناء محاولتها العمل من موارد معينة.

تعليم المستخدم النهائي: التعامل مع أكثر من عامل من عوامل الأمن السيبراني التي لا يمكن التنبؤ بها.

٨–الدوافع النفسية الكامنة وراء القيام بالتهديدات السيبرانية:

جذبت الدوافع النفسية الكامنة وراء التهديدات السيبرانية اهتمام الباحثين؛ لمعرفة الدوافع النفسية للمشاركة في سلوك القرصنة وقد كشف هذا الاهتمام البحثي عن عدد من العوامل كما يلي: السعي للانتقام والمرح والإثارة والشهرة والترويح والربح، تحقيق المكاسب الشخصية من اختراق أنظمة الكمبيوتر" بشكل غير قانوني، الاستعداد الشخصي لدى الفرد، ليكون من صناع الأذى الاجتماعي والممثل في إثارة الهجوم أو الانتقام أو السعي إلى الشهرة، دوافع أيديولوجية تترجم إلى هجمات قرصنة ضد خصم موقف سياسي، الدافع الاقتصادي، إذ يمكن أن تؤثر هذه الهجمات سلبًا في العمليات التجارية، وحساسية التسوية ومعلومات العميل، حرية التعبير والتوجه المناهض للبيروقراطية وانعدام الثقة.

المحور الثاني : التنمر الالكتروني:

١– مفهوم التنمر الإلكتروني:

عرفه (Sheryl ،٢٠١٥) :بأنه سلوك عدواني، عادة ما يتضمن تباينات في القوة بين المتنمر والضحية، ويتكرر مع مرور الوقت.

٢-أسباب انتشار التنمر:

أ-الألعاب الالكترونية العنيفة.

ب-أفلام الكارتون العنيفة.

ج-الخلل التربوي في بعض الأسر.

د-انتشار قنوات المصارعة. (أمل يوسف العمار ،٢٠١٧، ص ٣٣٨)

لوحظ في الفترة الأخيرة تزايد كبير في قنوات المصارعة الحرة العنيفة جدا التي تستخدم فيها كل الوسائل الغير عادية في الصراع، والتي غالبا ما تنتهي بسيلان دماء أحد المتصارعين أو كليهما في منظر شديد التخلف والعدوانية. والغريب أن جمهوراً كبيراً من المتابعين لهذه القنوات من الفتيات في ملاحظة غريبة حول هذه الرياضة التي ظلت فترة كبيرة هواية خاصة من هوايات الذكور لا الاناث، مما أثر كثيراً على السلوك العام للفتيات المتابعات والذي أدى لظهور ظاهرة سميت "بالبويات" ، وهن الفتيات المتشابهات بالرجال في سلوكهن وتعاملهن وبالتالي تكونت بذرة لنمو التنمر داخل الأوساط الطلابية للفتيات في المدارس

٥-العنف الأسري والمجتمعي:

يطبع كل انسان وخاصة في مطلع حياته على ما شاهده من تصرفات داخل بيئته الصغيرة كالأسرة وكذلك على ما يشاهده يومياً من تصرفات مجتمعية، فمن شاهد أفعالاً أو ردود أفعال تتسم بالعنف بين والديه، أو من عاش بنفسه عنفاً يمارسه أحد أفراد الأسرة عليه هو شخصياً أو

على أي أحد من المتعاملين مع الأسرة كالخدم والمربيات والسائقين، أو شاهد عنفاً مجتمعياً وخاصة في البلاد التي ضعفت فيها القبضة الأمنية نتيجة الثورات وغيرها فانتشرت البلطجة كوسيلة مضمونة لنيل الحقوق أو للاعتداء على الحقوق دون خشية عقاب رادع أو محاسبة فاعلة، فلابد عليه أن يتأثر بما شاهده، وربما يمارسه فعلياً إذا سنحت له الفرصة ذلك، وأيضاً هكذا يساهم الأبوان في إفساد سلوك أبنائهما بدفعهم بصورة عملية في إتباع ذات النهج الذي شاهدوه

مما سبق يمكن القول أن العنف الأسري من أهم أسباب التنمر فالطفل الذي ينشأ في جو أسري يسوده العنف سواء بين الأبوين أو تجاه الأبناء لابد أن يتأثر بما شاهده أو مورس عليه، فبالتالي يميل إلى ممارسة العنف والتنمر مع أقرانه (Bulach،٢٠١٢,١١)

٣-أسباب خطورة التنمر الالكتروني:

ويعد التنمر الإلكتروني أكثر خطورة من أشكال التنمر التقليدية الأخرى وذلك للأسباب التالية: ثناء هاشم محمد(٢٠١٩): يعتمد التنمر الإلكتروني على درجة معينة من الخبرة التكنولوجية، فيتطلب المزيد من المهارات والكفاءة لإرسال رسائل البريد الإلكتروني والرسائل النصية والتخفي لتنفي الهجمات، مثل أن يتظاهر بأنه شخص أخر ويقوم بتشويه سمعة الضحية والنشر عبر الإنترنت، يصعب الهروب من التنمر الإلكتروني حيث لا تجد ضحية التنمر الإلكتروني مكان للاختباء فيتم التنمر عليها أينما كانت من خلال الرسائل لهواتفهم المحمولة أو الكمبيوتر أو التعليقات المسيئة عبر مواقع الإنترنت على عكس التنمر التقليدي فبمجرد ذهاب الضحية للمنزل يكون بعيداً عن التنمر، من السمات المتفردة أيضاً للتنمر الإلكتروني؛ قدرة مرتكب التنمر على أن يكون غير معروف، وأن يقوم بالتنمر بعدد كبير من الأقران، وذلك بأقل مجهود وفي أي مكان وزمان خلال اليوم، يتميز التنمر الإلكتروني عن التنمر التقليدي بأنه يسمح للمتنمر بمضايقة الضحية في أي وقت ويقلل من مستوى المسؤولية والمحاسبة للمتنمر عما هو عليه في التنمر التقليدي، عدم المواجهة كما في حالات التنمر التقليدي، حيث لا يكون المتنمر الإلكتروني وجهاً لوجه مع الضحية ولذا فلديه فرصة أكبر لعدم الكشف عن هويته والتقليل من المخاطر التي قد يتعرض لها إذا تم القبض عليه أو تعرف عليه عدم وجود فرد أو جماعة بعينها تنظم السلوك المنحرف وإتاحة الهدف وقدرة المتنمر على تتبعه خارج نطاق المدرسة، مما يجعل التنمر الإلكتروني أكثر انتشارا في حياة الضحية ولا يتقيد بالتواجد بالمدرسة حيث يمكن الوصول إلى الضحية من خلال الهاتف الخلوي، أو البريد الإلكتروني أو برامج المراسلات في أي وقت من اليوم، ومع سرعة وصوله إلى أكبر عدد من الجمهور مع القدرة السريعة على الانتشار وتجاوز حدود الوقت والمكان وهذا ما يجعله أكثر حدة مقارنة مع التنمر التقليدي.

مما سبق يتضح خطورة التنمر الالكتروني بسبب الغموض وعدم القدرة على كشف هوية المتنمر وبالتالي لا يتعرض لأية مسائلة قانونية ويهرب بجريمته.

٤-أشكال التنمر الإلكتروني:

أ – المضايقة: وذلك عن طريق إرسال رسائل مسيئة ومهينة للشخص عبر البريد الإلكتروني.

ب – تشويه السمعة: وتشير إلى إرسال أو نشر الشائعات حول شخص معين بهدف تشويه سمعته.

ت – انتحال الشخصية: وتشير إلى تظاهر المتنمر بأنه شخص أخر ويقوم بإرسال أو نشر المواد الإلكترونية لجعل شخص ما في خطر يهدد سمعته.

ث – إفشاء الأسرار: وتشير إلى تقاسم أسرار شخص ما أو معلومات محرجة أو الصور على الإنترنت

ج – المخادع: ويقصد به تحدث المتنمر الإلكتروني مع شخص ما في الكشف عن أسرار أو معلومات محرجة، ثم يقوم المتنمر الإلكتروني بإعادة توجيه الرسائل إلى العديد من الأصدقاء ومن ثم تقاسمها على الإنترنت.

د – الاستبعاد: ويشير إلى قيام شخص ما باستثناء شخص أخر من جماعة على الإنترنت وذلك عن عمد وبقصد.

هـ – المضايقة الإلكترونية: ويشير إلى المضايقات المتكررة والتشويه الذي يتضمن تهديدات أو يخلق خوف كبير، مثل أن يقوم المتنمر الإلكتروني باختراق الحساب الشخصي لشخص ما، ويقوم بإرسال الشائعات السيئة إلى أصدقاء ذلك الشخص.

٥-الآثار الناجمة عن التنمر الإلكتروني:

بينت دراسة ثناء هاشم (٢٠١٩) ودراسة منصور العسيري (٢٠١٨) العديد من الآثار للتنمر الإلكتروني والتي تشمل الضحايا، والمتنمرين أنفسهم، وهي كالآتي:

أولا: آثار التنمر على الضحايا :

من هذه الآثار: تصبح الضحية مرفوضة وغير مرغوب فيها، يؤدي التنمر إلى مشاكل نفسية وعاطفية وسلوكية على المدى الطويل كالاكتئاب والشعور بالوحدة والانطوائية والقلق والإدمان وإيذاء النفس، بالإضافة إلى سوء العلاقات الاجتماعية وسوء الظن، تلجأ الضحية للسلوك العدواني نتيجة للتنمر، وقد تتحول مع مرور الوقت إلى متنمر أو إلى إنسان عنيف، قد يستمر

التنمر ويزداد انسحاب الضحية من الأنشطة الاجتماعية الحاصلة في العائلة أو المدرسة، حتى يصبح إنسانا صامتا ومنعزلا، الانتحار، حيث أثبتت الدراسات أن ضحايا الانتحار بسبب التنمر في ازدياد مستمر، اضطرابات النوم، كما يعاني من يتعرض للتنمر إلى الصداع وآلام المعدة وحالات من الخوف والذعر، تدني التحصيل الدراسي، بسبب ترك الدراسة أو كثرة التغيب، مع كثرة الهروب من المدرسة خوفا من المتنمرين.

ثانياً: آثار التنمر على المتنمرين منها: الحرمان والطرد من المدرسة، وبالتالي يواجهون قصورا في الاستفادة من البرامج التعليمية المقدمة لهم الإدمان على الخمور والمخدرات، مع التورط في أعمال إجرامية ومخالفات قانونية، الدخول في عراك دائم، وتخريب الممتلكات، وترك الدراسة ممارسة نشاطات جنسية مبكرة (الانحراف الجنسي).

مما سبق يمكن القول ان هذه الآثار السلبية المدمرة تحتم على الأسرة القيام بدورها لمواجهة تلك الظاهرة الخطيرة والتقليل بل الحد من أثارها السلبية.

٦-العلاقة بين المشكلات الأسرية والتنمر الإلكتروني:

أ-الخلافات الزوجية والتفكك الأسري:

يحتاج الأبناء لجو أسري هادئ ومريح يشعرون فيه بالأمن والأمان، ولكن الخلافات الزوجية تشعر الأبناء بالقلق والتوتر، كما أن التفكك الأسري وحالات الطلاق وما يصاحبها من تشرد وضياع واضطراب علاقات الأخوة مع بعضهم البعض، أو علاقة الأسرة بغيرها من الأسر له علاقة كبيرة بانحراف الأبناء وقد يتبنون أفكارًا متطرفة معادية لمجتمعهم(كلير فهيم ،٢٠٠٧،ص٢٠) .؛ لذا ينبغي على الوالدين تجنب الخلافات بين أبنائهما أو إخفاؤها حتى لا تؤثر عليهم، وأن يعملوا على تقوية علاقة الإخوة ببعضهم، وحل أي خلاف ينشب بينهم، ليعيش الأبناء حياتهم في جو أسري مليء بالحنان والعطف والحب؛ الأمر الذي ينعكس أثره على الأبناء، فيشعرون بالاستقرار النفسي والثقة والأمن.

ب-غياب أحد الوالدين أو كليهما:

قد ينحرف الطفل أو المراهق نتيجة لغياب أحد والديه أو وفاته، فعدم تواجد أحد الوالدين في الأسرة قد يدفع الأبناء إلى ارتكاب السلوك المنحرف، فقد تتغيب الأم عن الأسرة نتيجة عملها أو لطلاقها

فتبتعد عن الطفل في المراحل التي يكون بحاجة إليها ، وهذا قد يؤثر على حالته النفسية، وقد يلجأ إلى مصادر أخرى يغطي بها ذلك النقص وقد تؤدي به إلى الانحراف، كما أن لغياب الأب أو وفاته تأثيرًا كبيرًا على الطفل أو المراهق ، حيث يمثل مصدر السلطة والحماية فبغياب الأب سيفتقد الطفل أو المراهق تلك السلطة الأبوية، ونتيجة لذلك سيواجه أكبر عقبة تعترض توافقه الاجتماعي بشكل طبيعي، كما قد يتغيب الوالدان معا وهذا له تأثير كبير وخطير على حياة الطفل، إذ يعيش في جو متوتر، وبالتالي سيفقد الشعور بالأمن والطمأنينة (زراقة فيروز ، ٢٠٠٥، ص١٣٧) .

ج-ترك الأبناء للأجهزة الإلكترونية بدون متابعة:

ربما لانشغال الآباء أو لعدم معرفتهم بخطورة هذه الأجهزة على أبنائهم أو لعدم امتلاكهم الخبرة في التعامل معها، أو لكونهم جاهلين بمساوئها المتعددة، ربما لذلك كله تتاح الفرصة للأبناء الذين لديهم الاستعداد لاستغلال هذه الأجهزة لإشباع حاجاتهم النفسية وفرصة لتعلم السلوك الإجرامي مجانا من خلال ما يُعرض عليهم من إعلانات أو ألعاب إلكترونية تحرض على العنف والعدوان. (فاطمة الزهراء خموين ٢٠١٩ ص١٨٢).

٧- كيفية التعامل مع التنمر والحد منه: ترسيخ مفاهيم التربية الرقمية والوعي المعلوماتي والهوية الافتراضية لدى الأطفال والمراهقين وأسرهم، للأسرة دور مهم في الحد من التنمر فلا بُدَّ من شرح مفهوم التنمر الإلكتروني والتنمر عموما بكل أشكاله للطفل، وتشجيعه على التحدث مع والديه إذا تعرضوا إلى أي نوع من أنواع التنمر في أي وقت والتأكد أيضًا أن الطفل نفسه لا يقوم بالتنمر على الآخرين، وأن يوضح لهم تأثير ذلك عليهم وعلى الضحية، تكون الأسرة على دراية بكل الأنشطة التي يمارسها الأطفال بعد المدرسة وعلى معرفة جيدة بأصدقائهم، فمن المهم أن يمتد إشراف الوالدين إلى أنشطتهم على وسائل التواصل الاجتماعي، إذا كان الطفل من المتنمرين عبر الإنترنت، فيجب على الأسرة وضع قواعد صارمة بشأن السلوك الملائم لاستخدام الإنترنت، يمكن الحصول على دعم قانوني معين؛ خاصة إذا كان شخص بالغ طرفًا في المشكلة، حيث في مستوى جريمة المطاردة أو التحرش الإلكتروني، لا بد وأن تكون المدرسة مهتمة بقضية التنمر، وتقوم بتوعية التلاميذ حول هذه الظاهرة الخطيرة

الدراسات السابقة:

سوف يتم عرض الدراسات السابقة من الأقدم إلى الأحدث:

دراسة نورة القحطاني (٢٠١٩) هدفت إلى: معرفة مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية، وقد استخدمت الدراسة منهج المسح الاجتماعي بأسلوب العينة، وبلغت عينة الدراسة (٤٨٦) طالب وطالبة، واعتمدت الدراسة على الاستمارة الإلكترونية لتجميع البيانات، وكشفت نتائج الدراسة بأن أقرب مفهوم للأمن السيبراني من وجهة نظر عينة الدراسة هو استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعاملات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها.

دراسة (PotgieterK, ٢٠١٩) هدفت إلى: الكشف عن السلوك المتعلق بالوعي بالأمن السيبراني لدى الطلاب في الجامعة المركزية للتكنولوجيا بجنوب أفريقيا، حيث كان منهج الدراسة المنهج التجريبي واشتملت العينة على (٤٣) طالبًا، منهم (٣٣) من الذكور ، و (١٠) من الإناث، واعتمدت الدراسة علة الاستبانة الإلكترونية وقد توصلت الدراسة إلى عديد من النتائج، منها وجود قصور لدى الطلاب فيما يتعلق بالمشاركة في المبادرات المتعلقة بالوعي بالأمن السيبراني المتوفرة عبر منصات التواصل الاجتماعي، كما كشفت الدراسة أن الطلاب يستخدمون البريد والمواقع الإلكترونية؛ للحصول على المواد المتعلقة بالوعي بالأمن السيبراني.

دراسة الصفحي وسناء عسقول (٢٠١٩) هدفت إلى: الكشف عن مستوى الوعي الأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينه جدة، وتم استخدام المنهج الوصفي وتكونت عينة الدراسة من (٣٥٢) معلمة من إدارة تعليم جدة، وكان من أهم نتائجها وجود ضعف لدى معلمات الحاسب الآلي في الوعي وقصور بمفاهيم الأمن السيبراني. كذلك عدم وجود فروق ذات دلالة

إحصائية بين متوسطات استجابات أفراد عينة الدراسة عند مستوى الدلالة (٠٠٠٥) في درجة وعي معلمات الحاسب بالأمن السيبراني، تعزى لسنوات الخبرة (المؤهل العلمي) والدورات التدريبية.

دراسة القحطاني (٢٠٢٠) هدفت إلى: مستوى الوعي بالأمن السيبراني في مدارس بوابة المستقبل الثانوية في المملكة العربية السعودية، وكانت الدراسة مستخدمة المنهج التجريبي

وتكونت عينة الدراسة، من (١٠٠) مشارك من كل قسم مما جعل إجمالي حجم العينة (٣٠٠) مشارك، طبق عليهم استبانة لقياس الوعي بالأمن
السيبراني، وكشفت الدراسة عن فعالية نموذج نظرية الألعاب لزيادة الوعي بالأمن السيبراني بين طلاب مدارس بوابة المستقبل الثانوية في المملكة العربية السعودية.

دراسة (Elgharnah & Ozdamli, 2020) هدفت إلى :تحديد مستوى وعي الوالدين بالاستخدام الآمن للإنترنت والتعرف على مدى وعي الوالدين بطرق الاستخدام الآمن للإنترنت ومستوى الوعي بمخاطر الإنترنت وخصوصية المعلومات والبيانات الشخصية، وكان المنهج الوصفي الذي تم استخدامه واعتمدت الدراسة على استبيان تم تطبيقه على عينة مكونة من (٢٥٢) بمتوسط أعمار (٢٧) عاما، وتوصلت الدراسة إلى أن مستوى وعي الوالدين تُجاه الاستخدام الآمن للإنترنت يمثل مستوى متوسطا، كما توصلت إلى عدم وجود فروق ذات دلالة إحصائية في وعى الوالدين بالاستخدام الآمن للإنترنت وفقًا للمتغيرات الديموغرافية.

دراسة مداخل التيمانى (٢٠٢١) هدفت إلى: معرفة واقع الأمن السيبراني لدى الأفراد في المجتمع السعودي، كما يدركها الخبراء المختصون بأمن المعلومات، وقد استخدمت الباحثة في هذه الدراسة المنهج الوصفي، وأداة المقابلة المطبقة على عينة من الخبراء المختصين بالأمن السيبراني في مدينة الرياض، وقد كانت أهم النتائج التي توصلت إليها هذه الدراسة أن الاهتمام الحكومي بموضوع الأمن السيبراني، بدأ بشكل مبكر قبل أن يدرك الأفراد في المجتمع هذا المفهوم.

دراسة (Bada et al .٢٠١٩) هدفت إلى: إلى الكشف عن حملات الوعي بالأمن السيبراني والتعرف على العوامل الأساسية التي تؤدي إلى إخفاق هذه الحملات في تغيير سلوكيات الأمن لدى الأشخاص، واعتمدت على المنهج الوثائقي القائم على مراجعة أدبيات الحالة، بناءً على النظريات النفسية المتعلقة بالوعي والسلوك في مجال الأمن السيبراني، وقد توصلت الدراسة إلى عديد من النتائج كان أهمها تعد المعرفة والوعي شرطين أساسيين في تغيير السلوك؛ لذا يساعد دمج السلوكيات الإيجابية للأمن السيبراني على تعزيز الممارسات المتعلقة بالتفكير والثقافة المرتبطة بالأمن السيبراني.

دراسة أفاد (Agatston et al, 2007) كانت النتيجة أن الطلاب الجامعيين الذكور يبدو أنهم أقل عرضه للهجوم من ضحايا أكثر التنمر الالكتروني في الإناث الجامعيات، وتتعرض الطالبات للتنمر الإلكتروني من الذكور؛ في الواقع، الذكور إما متنمرون، أو ضحايا متنمرون، بينما يتم الإبلاغ إلى حد كبير عن معظم الإناث كضحايا. وهذا يعني أن الطالبات من ضحايا للتنمر على وسائل التواصل الاجتماعي أكثر من نظرائهن الذكور الذين انغمسوا في معظم الأحيان في سلوكيات التنمر عبر الإنترنت)، ولا سيما الطلاب الجامعيين

دراسة (Balakrishnan, ٢٠١٥) إلى أنه نظرا للحداثة النسبية للتنمر على وسائل التواصل الاجتماعي، قد لا يتم تحديد الجنس الذي يتأثر في الغالب بالتنمر عبر الإنترنت بسهولة لأن كلا الجنسين يبدو متأثرًا بالتساوي في معظم الحالات ويعاني العديد من طلاب الجامعات في صمت بسبب الآثار السلبية للاعتداءات عبر الإنترنت. بينما يمكن للبعض التخلي عن ذلك، غالبًا ما يلجأ الكثيرون إلى أفعال مثل: الميول الانتحارية بسبب التحديات النفسية

إجراءات البحث:

١-منهج البحث:

من أجل التعرف على دور الامن السيبراني في الحد من التنمر الالكتروني من خلال وجهة نظر أولياء الامور، ولتحقيق أهداف الدراسة الحالية اعتمدت الباحثة المنهج الوصفي لجمع البيانات وذلك الملائمة لطبيعة الدراسة الحالية

٢- مجتمع وعينة البحث:

مجتمع البحث:

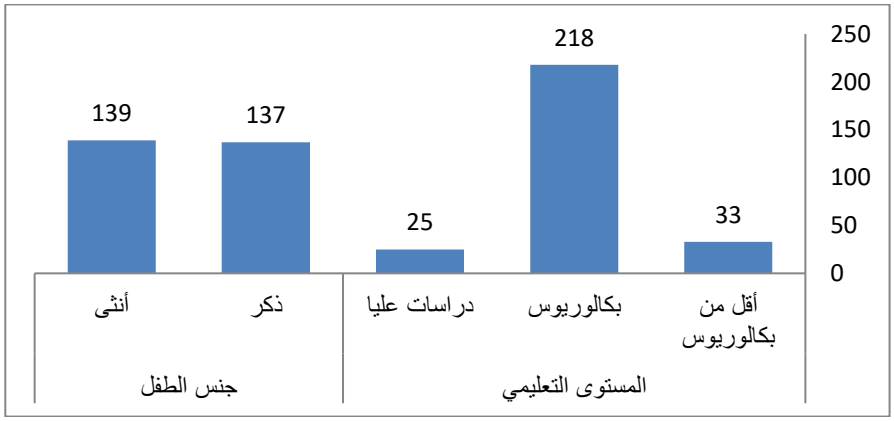
يتكون مجتمع الدراسة من أولياء الامور وعددهم (٣١٧١).

٣-العينة:

- العينة الاستطلاعية: تكونت العينة الاستطلاعية من (٢٠) ولي أمر وذلك للتأكد من صدق أداة الدراسة وثباتها.
- العينة الأساسية: استخدمت الباحثة أسلوب العينة (المتاحة) حيث تم عمل رابط الكتروني وتعميمه على الفئة المستهدفة وبعد تحديد مدة الاستجابات المتمثلة (اسبوعين لاستقبال الردود وبلغ عددهم (٢٧٦) ولي أمر وبنسبة (٨,٧%) من مجتمع الدراسة، والجدول (١) يبين توزيع أفراد عينة الدراسة وفقًا لمتغير المستوى التعليمي لولي الامر، جنس الطفل

جدول (١): التكرارات والنسب المئوية لتوزيع افراد عينة الدراسة وفقًا لمتغير المستوى التعليمي لولي الامر، جنس الطفل

المتغير	الفئة	العدد	النسبة%
المستوى التعليمي	أقل من بكالوريوس	33	12.0
	بكالوريوس	218	79.0
	دراسات عليا	25	9.1
جنس الطفل	ذكر	137	49.6
	أنثى	139	50.4
الإجمالي		276	100



شكل (١): توزيع أفراد عينة الدراسة حسب المتغيرات

٣-٣- أداة الدراسة:

استخدمت الباحثة في الدراسة الحالية الاستبيان كأداة لجمع البيانات حيث تم بناء الاستبيان لقياس دور الامن السيبراني في الحد من التنمر الالكتروني من خلال وجهة نظر أولياء الامور، وتكون الاستبيان في صورته النهائية من ثلاثة أقسام:

١. القسم الأول: يحتوي على مقدمة تعريفية بعنوان الدراسة والهدف من الاستبيان، ونوع البيانات والمعلومات التي يراد جمعها من أفراد عينة الدراسة، وتعليمات الاستجابة والغرض من جمع البيانات.

٢. القسم الثاني: يحتوي على البيانات الأولية الخاصة ، والمتمثلة في (جنس الطفل، المستوى التعليمي للوالدين).

٣. القسم الثالث: فقرات الاستبانة والمكونة من (٤٠) فقرة، موزعة على (٣) محاور وفق سلم التقدير الرباعي (موافق بشدة – موافق – غير موافق–غير موافق بشدة) وتأخذ القيم على التوالي (٤، ٣، ٢، ١)، والجدول (٢) يوضح عدد فقرات الاستبيان، وكيفية توزيعها على المحاور.

جدول (٢) استبيان دور الامن السيبراني في الحد من التنمر الالكتروني من خلال وجهة نظر أولياء الامور

م	المحور	عدد العبارات
١	المحور الأول: درجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني	13
٢	المحور الثاني: درجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت.	14
٣	المحور الثالث: مدى انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي من خلال وجهة نظر أولياء	13
	المجموع	40

صدق الأداة (الاستبيان):

تم التحقق من صدق أداة الدراسة (الاستبيان) من خلال:

أ – الصدق الظاهري (المحكمين):

تم التحقق من صدق الاستبانة من خلال عرضها على عدد من المحكمين من أصحاب الخبرة والاختصاص وبلغ عددهم (١١) من محكما (ملحق) وتم الأخذ بتوجيهاتهم ومقترحاتهم حول الفقرات من تعديل الفقرات غير المناسبة، ووضع الفقرات في المحور الذي تنتمي إليه، ووضوح الصياغة وسلامة اللغة.

ب – صدق الاتساق:

تم تطبيق أداة الدراسة على عينة استطلاعية من خارج عينة الدراسة مكونة (٢٠) ولي أمر وتم احتساب معامل ارتباط بيرسون بين فقرات دور الامن السيبراني في الحد من التنمر الالكتروني من خلال وجهة نظر أولياء الامور والدرجة الكلية للمحور المنتمية له، وكذلك بين الفقرات والمحاور مع الدرجة الكلية للأداة، والجدول (٣) يبين ذلك:

جدول (٣) معامل ارتباط بيرسون بين فقرات دور الامن السيبراني في الحد من التنمر الالكتروني من خلال وجهة نظر أولياء الامور والدرجة الكلية للمحور المنتمية له، وكذلك بين الفقرات والمحاور مع الدرجة الكلية للأداة

م	المحور – الفقرات	معامل الارتباط مع المحور	معامل الارتباط مع الأداة
	المحور الأول: درجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني	1	.969**
١	اختار كلمة مرور قوية تحتوي على الاحرف والأرقام والرموز.	.798**	.701**
٢	اتجنب فتح الروابط من أي مصدر غير معروفين.	.876**	.811**
٣	احرص ان لا أرسل بياناتي الشخصية لأشخاص لا اعرفهم	.919**	.865**
٤	اتخذ الحذر عند الاتصال بالشبكات العامة.	.881**	.847**
٥	الغي أي اشتراك لي في الإعلانات المستهدفة وذلك لحماية بياناتي الشخصية والمالية.	.596**	.523*
٦	استخدم تقنية التحقق الثنائي (كلمة المرور– البصمة).	.671**	.709**
٧	احرص على تحميل برامج الحماية ضد المواقع الضارة.	.738**	.742**
٨	افحص الروابط التي تبدو لي انها ضارة.	.763**	.742**
٩	ادعم البيانات المخزنة على جهازي بإعداد نسخة احتياطية على الخدمة السحابية.	.752**	.684**
١٠	احرص على تعطيل خدمات الوصول لموقعي في التطبيقات المحملة على جهازي.	.853**	.855**
١١	احرص على عدم وصول التطبيقات التي على جهازي للكاميرا وألبوم الصور المخزنة.	.672**	.683**

١٢	اغير اعدادات جهازي بشكل مستمر حفاظاً من اختراق شبكة الانترنت.	.795**	.835**
١٣	احرص على الإبلاغ عن المواقع المشكوك فيها للجهات المختصة.	.829**	.842**
	المحور الثاني: درجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت.	1	.948**
١٤	احدد المصادر الموثوقة للحصول على المعلومات والبيانات المفيدة.	.755**	.739**
١٥	اتحدث معهم حول أهمية حماية الملفات الخاصة بهم.	.740**	.731**
١٦	أطبق مهارات معالجة المعلومات الالكترونية والتأكد من صحتها.	.783**	.735**
١٧	اعزز الوعي لديهم بمخاطر الروابط الضارة عند تصفح الانترنت.	.657**	.758**
١٨	ادربهم على التصفح الامن واستخدام التطبيقات الأمنه.	.699**	.658**
١٩	اثقفهم حول بعض المشكلات الناتجة عن استخدام الانترنت لفترات طويلة.	.763**	.729**
٢٠	اوعيهم بأهمية استخدام المحتوى المرخص من قبل الناشر او المؤلف.	.523*	.487*
٢١	اثقفهم بالقوانين التي تفرضها الدولة عند استخدام الانترنت.	.657**	.758**
٢٢	اوعيهم بتجنب تبادل الصور والملفات غير اللائقة.	.520*	.459*
٢٣	اشراكهم عند اختيار برامج الحماية والأمن من المواقع والالعاب الضارة.	.628**	.614**
٢٤	احرص على تحديث برامج الحماية بشكل دوري.	.538*	.442
٢٥	الحرص عليهم بعدم الإفصاح عن بياناتهم الشخصية مع افراد غير معروفين.	.753**	.672**
٢٦	أشجعهم بالإفصاح المستمر عندما يتعرضون لأي تهديد من خلال الانترنت.	.626**	.633**
٢٧	التأكيد على أهمية الاحترام المتبادل عند استخدام المواقع الالكترونية مع الغرباء.	.661**	.577**
	المحور الثالث: مدى انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي من خلال وجهة نظر أولياء	1	.974**
٢٨	تهديد الطفل عبر مواقع التواصل الاجتماعي.	.559*	.548*
٢٩	تلقي الطفل للرسائل القصيرة بذيئة.	.459*	.486*
٣٠	تعرض الطفل للسخرية والاستهزاء عبر مواقع التواصل الاجتماعي.	.735**	.682**
٣١	ينشر اشاعات واكاذيب عن الطفل عبر مواقع التواصل الاجتماعي	.735**	.705**

٣٢	يطلق أسماء غير لائقة على الأطفال ويتداولها.	.711**	.691**
٣٣	يتعمد تشويه صور الطفل من قبل المتنمرين	.683**	.711**
٣٤	انتحال شخصية الطفل عبر مواقع التواصل الاجتماعي.	.884**	.846**
٣٥	اقصاءه من الألعاب الجماعية عبر الانترنت عن عمد.	.741**	.730**
٣٦	السخرية من مظهرة عبر مواقع التواصل الاجتماعي.	.896**	.875**
٣٧	تشر صور او مقاطع فيديو تسيء للطفل.	.884**	.863**
٣٨	نشر محادثات خاصة بين زملاءه بهدف أحراجه.	.872**	.824**
٣٩	نشر اسراره الشخصية عبر الانترنت.	.884**	.863**
٤٠	بعث رسائل تشوية واحتقار للضحية.	.872**	.824**

** دالة احصائيا عند (٠,٠١)، * دالة احصائيا عند (٠,٠٥)

بين الجدول (٣) ان معاملات بيرسون بين فقرات دور الامن السيبراني في الحد من التنمر الالكتروني من خلال وجهة نظر أولياء الامور والدرجة الكلية للمحور المنتمية له دالة احصائيا عند مستوى دلالة (٠,٠١)، (٠,٠٥)، وتراوحت معاملات ارتباط بيرسون بين الفقرات مع الدرجة الكلية للمحور بين (٠,٤٥٩* – – ٠,٩١٩**)، كما تراوحت معاملات ارتباط بيرسون بين الدرجة الكلية للمحور مع الدرجة الكلية للأداة بين (٠,٩٤٨** – ٠,٩٧٤**)، وجميعها دالة عند (٠,٠١)، وبذلك تحققت الباحثة من صدق أداة الدراسة.

ثبات أداة الدراسة:

تم حساب معاملات الثبات على محاور دور الامن السيبراني في الحد من التنمر الالكتروني من خلال وجهة نظر أولياء الامور والدرجة الكلية من خلال معادلة الفا كرونباخ، حيث تم تطبيق اداة الدراسة على عينة استطلاعية مكونة من (٢٠) ولي أمر والجدول (٤) يبين معاملات الثبات.

جدول (٤): معاملات ثبات الفا كرونباخ لمحاور دور الامن السيبراني في الحد من التنمر الالكتروني من خلال وجهة نظر أولياء الامور وعلى الدرجة الكلية

م	المحور	عدد الفقرات	معامل الثبات
١	المحور الأول: درجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني	13	0.94
٢	المحور الثاني: درجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت.	14	0.85
٣	المحور الثالث: مدى انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي	13	0.93
٤	الدرجة الكلية	40	0.96

يبين الجدول (٤) ان معامل الثبات الفا كرونباخ على الدرجة الكلية لدور الامن السيبراني في الحد من التنمر الالكتروني بلغ (٠,٩٦)، كما تراوحت معاملات الثبات على المحاور بين (٠,٨٥ –٠,٩٤)، وهي معاملات ثبات مرتفعة ومناسبة لغايات الدراسة وبذلك تحققت الباحثة من الثبات.

٣-٤- إجراءات البحث :استخدمت الباحثة المنهج الوصفي المسحي في دراستها دور الامن السيبراني في الحد من التنمر الالكتروني، وذلك تم اتباع الإجراءات التالية: الاطلاع على الدراسات السابقة المتعلقة بمشكلة الدراسة، وتحديد مشكلة وأسئلة الدراسة الاطلاع على الدراسات السابقة المرتبطة بموضوع الدراس، اختيار المنهج الملائم للدراسة وصياغة إجراءات الدراسة – المنهج الوصفي المسحي، اختيار مجتمع الدراسة وعينتها، إعداد استبيان الدراسة بالصورة الأولية وعرضه على مجموعة من المحكمين، ومن ثم إخراجها بصورتها النهائية، إجراء دراسة استطلاعية هدفت إلى التأكد من صلاحية أداة الدراسة وصدقها وثباتها، وتكونت العينة الاستطلاعية من (٢٠) ولي امر، تم توزيع الاستبيان إلكترونيا على أفراد عينة الدراسة، وبعد فترة تم استرجاع الاستبيانات بعد استجابة جميع أفراد عينة الدراسة، القيام بتفريغ الاستبيانات وإدخالها حاسوبيا باستخدام برنامج (SPSS) لمعالجتها إحصائياً، وإجراء التحليلات الإحصائية المناسبة للوصول إلى نتائج الدراسة وتفسيرها ثم وقديم التوصيات والمقترحات.

-أساليب المعالجة الإحصائية:

اعتمدت البرمجية الإحصائية (SPSS) نسخة (٢٣) في تحليل نتائج الدراسة والإجابة عن أسئلتها حيث تم استخدام: معامل ارتباط بيرسون للتحقق من صدق الاتساق ، الفا كرونباخ للتحقق من ثبات أداة الدراسة

– المتوسطات الحسابية والانحرافات المعيارية والرتبة للإجابة عن السؤال الرئيس "ما دور الامن السيبراني في الحد من التنمر الالكتروني؟

نتائج البحث:

جدول (٥) معايير تفسير قيم المتوسطات الحسابية وفقا لسلم ليكرت الرباعي

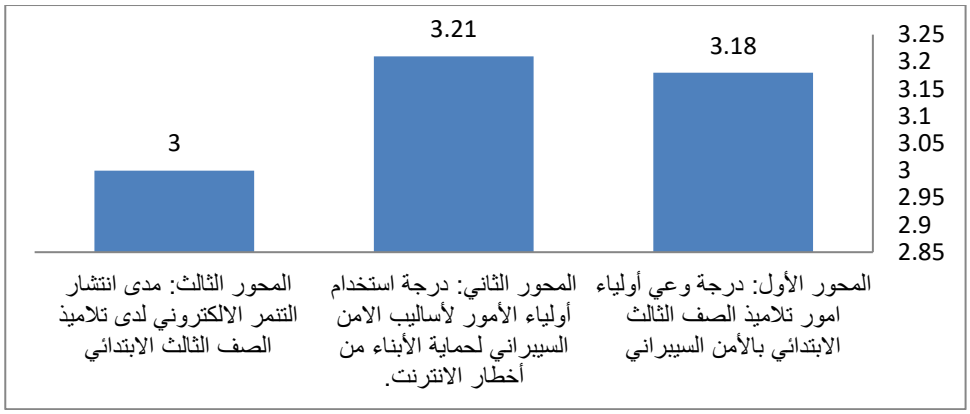
درجة الموافقة	قليلة	متوسطة	كبيرة
الوسط الحسابي	من ١ إلى ٢,٠	اكبر من ٢,٠ إلى ٣,٠٠	اكبر من ٣,٠ إلى ٤,٠٠

نتائج السؤال الرئيس: "ما دور الامن السيبراني في الحد من التنمر الالكتروني؟

قامت الباحثات بحساب المتوسطات الحسابية والانحرافات المعيارية والرتبة لاستجابات أفراد عينة الدراسة لدور الامن السيبراني في الحد من التنمر الالكتروني، والجدول (٦) يبين ذلك:

جدول (٦): المتوسطات الحسابية والانحرافات المعيارية لدور الامن السيبراني في الحد من التنمر الالكتروني

م	الرتبة	المحور	المتوسطات الحسابية	الانحرافات المعيارية	الدرجة
١	2	المحور الأول: درجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني	3.18	.486	كبيرة
٢	1	المحور الثاني: درجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت.	3.21	.542	كبيرة
٣	3	المحور الثالث: مدى انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي	3.00	.637	متوسطة



شكل (٢): الرسم البياني دور الامن السيبراني في الحد من التنمر الالكتروني

يبين الجدول (٦) ان درجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني جاءت بدرجة كبيرة بمتوسط حسابي (٣,١٨) وبانحراف معياري (٠,٤٨٦) جاء بالمرتبة الثانية، وجاء المحور الثاني: درجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت بالمرتبة الأولى بمتوسط حسابي (٣,٢١) وبانحراف معياري (٠,٥٤٢)، وجاء المحور الثالث: مدى انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي بالمرتبة الثالثة بمتوسط حسابي (٣,٠٠) وبانحراف معياري (٠,٦٣٧) وبدرجة متوسطة.

نتائج السؤال الاول: ما درجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني؟

قامت الباحثة بحساب المتوسطات الحسابية والانحرافات المعيارية والرتبة لاستجابات أفراد عينة الدراسة لدرجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني ، والجدول (٧) يبين ذلك:

جدول (٧): المتوسطات الحسابية والانحرافات المعيارية لدرجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني

م	الرتبة	الفقرات	المتوسطات الحسابية	الانحرافات المعيارية	الدرجة
١	3	اختار كلمة مرور قوية تحتوي على الاحرف والأرقام والرموز.	3.29	.588	كبيرة

٢	5	اتجنب فتح الروابط من أي مصدر غير معروفين.	3.28	.625	كبيرة
٣	2	احرص ان لا أرسل بياناتي الشخصية لأشخاص لا اعرفهم	3.31	.599	كبيرة
٤	6	اتخذ الحذر عند الاتصال بالشبكات العامة.	3.24	.602	كبيرة
٥	7	الغي أي اشتراك لي في الإعلانات المستهدفة وذلك لحماية بياناتي الشخصية والمالية.	3.23	.641	كبيرة
٦	1	استخدم تقنية التحقق الثنائي (كلمة المرور– البصمة).	3.33	.625	كبيرة
٧	11	احرص على تحميل برامج الحماية ضد المواقع الضارة.	3.05	.678	كبيرة
٨	12	افحص الروابط التي تبدو لي انها ضارة.	3.01	.729	كبيرة
٩	13	ادعم البيانات المخزنة على جهازي بإعداد نسخة احتياطية على الخدمة السحابية.	2.96	.750	متوسطة
١٠	9	احرص على تعطيل خدمات الوصول لموقعي في التطبيقات المحملة على جهازي.	3.14	.635	كبيرة
١١	8	احرص على عدم وصول التطبيقات التي على جهازي للكاميرا وألبوم الصور المخزنة.	3.21	.590	كبيرة
١٢	10	اغير اعدادات جهازي بشكل مستمر حفاظاً من اختراق شبكة الانترنت.	3.08	.631	كبيرة
١٣	4	احرص على الإبلاغ عن المواقع المشكوك فيها للجهات المختصة.	3.28	.618	كبيرة
		درجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني	3.18	.486	كبيرة

يبين الجدول (٧) أن لدرجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني جاءت بدرجة كبيرة بمتوسط حسابي (٣,١٨) وبانحراف معياري (٠,٤٨٦) وتراوحت المتوسطات الحسابية على فقرات درجة وعي أولياء امور تلاميذ الصف الثالث الابتدائي بالأمن السيبراني بين (٢,٩٦ – ٣,٣٣)، وجاءت الفقرة (٦) استخدم تقنية التحقق الثنائي (كلمة

المرور– البصمة) بالمرتبة الاولى بمتوسط حسابي (٣,٣٣) وبانحراف معياري (٠,٦٢٥) وبدرجة كبيرة. تلتها الفقرة (٣) احرص ان لا أرسل بياناتي الشخصية لأشخاص لا اعرفهم بمتوسط حسابي (٣,٣١) وبانحراف معياري (٠,٥٩٩) وبدرجة كبيرة، بينما جاءت الفقرة (٩) ادعم البيانات المخزنة على جهازي بإعداد نسخة احتياطية على الخدمة السحابية" بالمرتبة الاخيرة بمتوسط حسابي (٢,٩٦) وبانحراف معياري (٠,٧٥٠) وبدرجة متوسطة.

نتائج السؤال الثاني: ما درجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت؟

قامت الباحثة بحساب المتوسطات الحسابية والانحرافات المعيارية والرتبة لاستجابات أفراد عينة الدراسة لدرجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت ، والجدول (٨) يبين ذلك:

جدول (٨): المتوسطات الحسابية والانحرافات المعيارية لدرجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت

م	الرتبة	الفقرات	المتوسطات الحسابية	الانحرافات المعيارية	الدرجة
١	4	احدد المصادر الموثوقة للحصول على المعلومات والبيانات المفيدة.	3.28	.600	كبيرة
٢	5	اتحدث معهم حول أهمية حماية الملفات الخاصة بهم.	3.26	.581	كبيرة
٣	14	أطبق مهارات معالجة المعلومات الالكترونية والتأكد من صحتها.	2.99	.782	متوسطة
٤	8	اعزز الوعي لديهم بمخاطر الروابط الضارة عند تصفح الانترنت.	3.21	.640	كبيرة
٥	13	ادربهم على التصفح الامن واستخدام التطبيقات الأمنه.	3.10	.711	كبيرة
٦	7	اثقفهم حول بعض المشكلات الناتجة عن استخدام الانترنت لفترات طويلة.	3.23	.594	كبيرة
٧	9	اوعيهم بأهمية استخدام المحتوى المرخص من قبل الناشر او المؤلف.	3.16	.645	كبيرة
٨	10	اثقفهم بالقوانين التي تفرضها الدولة عند استخدام الانترنت.	3.16	.661	كبيرة

٩	6	اوعيهم بتجنب تبادل الصور والملفات غير اللائقة.	3.26	.629	كبيرة
١٠	12	اشراكهم عند اختيار برامج الحماية والأمن من المواقع والالعاب الضارة.	3.14	.709	كبيرة
١١	11	احرص على تحديث برامج الحماية بشكل دوري.	3.16	.648	كبيرة
١٢	3	الحرص عليهم بعدم الإفصاح عن بياناتهم الشخصية مع افراد غير معروفين.	3.30	.620	كبيرة
١٣	2	أشجعهم بالإفصاح المستمر عندما يتعرضون لأي تهديد من خلال الانترنت.	3.31	.634	كبيرة
١٤	1	التأكيد على أهمية الاحترام المتبادل عند استخدام المواقع الالكترونية مع الغرباء.	3.34	.654	كبيرة
		درجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت	3.21	.542	كبيرة

يبين الجدول (٨) أن درجة استخدام أولياء الأمور لأساليب الامن السيبراني لحماية الأبناء من أخطار الانترنت جاءت بدرجة كبيرة بمتوسط حسابي (٣,٢١) وبانحراف معياري (٠,٥٤٢)، وتراوحت المتوسطات الحسابية على الفقرات بين (٢,٩٩ – ٣,٣٤) وجاءت الفقرة (١٤) التأكيد على أهمية الاحترام المتبادل عند استخدام المواقع الالكترونية مع الغرباء بالمرتبة الاولى بمتوسط حسابي (٣,٣٤) وبانحراف معياري (٠,٦٥٤) وبدرجة كبيرة، بينما جاءت الفقرة (٣) أطبق مهارات معالجة المعلومات الالكترونية والتأكد من صحتها" بالمرتبة الاخيرة بمتوسط حسابي (٢,٩٩) وبانحراف معياري (٠,٧٨٢) وبدرجة متوسطة.

نتائج السؤال الثالث: ما مدى انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي؟

قامت الباحثة بحساب المتوسطات الحسابية والانحرافات المعيارية والرتبة لاستجابات أفراد عينة الدراسة لمدى مدى انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي، والجدول (٩) يبين ذلك:

جدول (٩): المتوسطات الحسابية والانحرافات المعيارية لمدى انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي

م	الرتبة	الفقرات	المتوسطات الحسابية	الانحرافات المعيارية	الدرجة
١	5	تهديد الطفل عبر مواقع التواصل الاجتماعي.	3.02	.677	كبيرة
٢	1	تلقي الطفل للرسائل القصيرة بذيئة.	3.06	.664	كبيرة
٣	2	تعرض الطفل للسخرية والاستهزاء عبر مواقع التواصل الاجتماعي.	3.03	.668	كبيرة
٤	4	ينشر اشاعات واكاذيب عن الطفل عبر مواقع التواصل الاجتماعي	3.03	.695	كبيرة
٥	3	يطلق أسماء غير لائقة على الأطفال ويتداولها.	3.03	.684	كبيرة
٦	7	يتعمد تشويه صور الطفل من قبل المتنمرين	3.00	.685	متوسطة
٧	10	انتحال شخصية الطفل عبر مواقع التواصل الاجتماعي.	2.96	.692	متوسطة
٨	6	اقصاءه من الألعاب الجماعية عبر الانترنت عن عمد.	3.02	.682	كبيرة
٩	9	السخرية من مظهرة عبر مواقع التواصل الاجتماعي.	2.98	.721	متوسطة
١٠	12	تشر صور او مقاطع فيديو تسيء للطفل.	2.96	.737	متوسطة
١١	11	نشر محادثات خاصة بين زملاءه بهدف أحراجه.	2.96	.727	متوسطة
١٢	13	نشر اسراره الشخصية عبر الانترنت.	2.95	.727	متوسطة
١٣	8	بعث رسائل تشوية واحتقار للضحية.	2.99	.757	متوسطة
		مدى انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي	3.00	.637	متوسطة

يبين الجدول (٩) أن مدى انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي جاء بدرجة متوسطة بمتوسط حسابي (٣,٠٠) وبانحراف معياري (٠,٦٣٧)، وتراوحت المتوسطات الحسابية على فقرات مدى انتشار التنمر الالكتروني لدى تلاميذ الصف الثالث الابتدائي بين (٢,٩٥ – ٣,٠٦)، وجاءت الفقرة (٢) تلقي الطفل للرسائل القصيرة بذيئة بمتوسط حسابي (٣,٠٦) وبانحراف معياري (٠,٦٦٤) وبدرجة كبيرة، وفي المرتبة الثانية الفقرة (٣) تعرض الطفل للسخرية والاستهزاء عبر مواقع التواصل الاجتماعي بمتوسط حسابي (٣,٠٣) وبانحراف

معياري (٠,٦٦٨) وبدرجة كبيرة، بينما جاءت الفقرة (١٢) نشر اسراره الشخصية عبر الانترنت بالمرتبة الاخيرة بمتوسط حسابي (٢,٩٥) وبانحراف معياري (٠,٧٢٧) وبدرجة متوسطة

التوصيات البحث:

في إطار ما تم عرضه عن التنمر الإلكتروني وعلاقته بقضايا الهوية الرقمية والمواطنة الرقمية ينبغي العمل على توطين التقنيات الرقمية بما يعظم ويؤكد مكامن القوة لها ويعمل على إضعاف سلوكيات التنمر الإلكتروني من خلال:

- إتاحة التقنيات الرقمية التي توفر فرصاً للتعلم والتعليم للأطفال ولاسيما في المناطق النائية وأثناء الأزمات الإنسانية.
- عمل برامج وقائية تحول دون انغماس الأطفال على الشاشات الرقمية بما يكرس الاعتماد على الإنترنت، ويسهم في الإصابة بالسمنة.
- توفر فرص اقتصادية من خلال تزويد الشباب بفرص التدريب على التقنيات الرقمية الحديثة وخدمات البحث عن الوظائف المناسبة وخلق أنواع جديدة من العمل.
- ترشيد وعقلنة قرارات الأطفال والشباب من ناجية الاستخدام المفرط للتقنية الرقمية وتأثيراته السلبية على الفرد والمجتمع بما يزيد من معدلات الإصابة بأمراض الاكتئاب والقلق.

شكر وتقدير:
تشكر الباحثات جامعة الملك فيصل

قائمة المراجع

أولاً: المراجع العربية

أبو غزالة، معاوية محمود. (٢٠٠٩). *التنمر وعلاقته بالشعور بالوحدة والدعم الاجتماعي*. عمان: المجلة الأردنية في العلوم التربوية.

آل مداوى، علي. (٢٠٢٣). الأمن السيبراني: تعريفه – أهميته – أنواعه – استراتيجيات الوقاية من الهجمات السيبرانية. *مجلة الدراسات الدولية*، ع٣٤، ١١٥ – ١٢٤. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1454807

بدر، بثينة بنت محمد بن محمود. (٢٠١١). فعالية التدريس باستراتيجية مقترحة للتعلم النشط على تنمية مهارات التفكير العليا في الهندسة لدى التلميذات منخفضي التحصيل بالمرحلة المتوسطة. *دراسات عربية في التربية وعلم النفس*، مج ٥، ع ٣، ١١٥ – ١٤٣. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/104792

التيماني، مداخل زيد عبد الرحيم. (٢٠٢١). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني. *مجلة الخدمة الاجتماعية*، ع٦٧ج، ١ – ٢٣. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1195996

جبور، منى الأشقر. (٢٠١٦). السيبرانية: هاجس العصر. *مجلة المكتبات والمعلومات والتوثيق في العالم العربي*، ع٥، ٢٦٢ – ٢٦٣. مسترجع من http://search.mandumah.com/Record/854700

حسين، رمضان عاشور. (٢٠١٦). *البنية العاملية لمقياس التنمر الإلكتروني كما تدركها الضحية لدى عينة من المراهقين*، القاهرة: المجلة العربية للبحوث والدراسات التربوية والإنسانية.

الحيمودي، بدر. (٢٠٢٣). الأمن السيبراني وحماية الأنظمة المعلوماتية. *مجلة شمال إفريقيا للنشر العلمي*، مج١، ع٢، ١٧٤ – ١٨٩. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1378486

خموين، فاطمة الزهراء. (٢٠١٩). الأسرة والجريمة. *مجلة الاجتهاد للدراسات القانونية والاقتصادية*، مج٨، ع٢، ١٧٦ – ١٨٦. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/944312

زرارقة، فيروز مامي. (٢٠١٢). الأسرة وعلاقتها بانحراف الحدث المراهق. *مجلة الآداب والعلوم الاجتماعية*، ع١٦، ٢٩٠ – ٣١٣. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/836727

الزميتي، أماني كمال حسن، ندا، ندا الحسيني، والطحاوي، خلف حسن محمد. (٢٠١٣). استخدام القصة المصورة فى تدريس القواعد اللغوية وأثرها فى تنمية التحصيل لدي تلاميذ الصف الرابع الابتدائي. *مجلة كلية التربية*، ع١٤، ٨١٤ – ٨٣٨. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1005827

السالم، بندر (November, 2019). "الأمن السيبراني – صوت المواطن"، *جريدة عكاظ الإلكترونية*، مسترجع من: https://www.okaz.com.sa/citizenvoice/na/1754249

سلامي، نادية. (٢٠١٧). التجسس الإلكتروني كأثر للاستخدام غير المشروع للفضاء الإلكتروني على أمن الدولة الخارجي. *دراسات*، ع٥٦، ٢٣٦ – ٢٤٩. مسترجع من

http://search.mandumah.com.sdl.idm.oclc.org/Record/833693

السواط، حمد بن حمود بن حميد، عسران، عواطف سعد الدين، الصانع، نورة عمر أحمد، منصور، إيناس محمد سليمان علي، وأبو عيشة، زاهدة جميل نمر. (٢٠٢٠). العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف. *مجلة البحث العلمي في التربية*، ع٢١، ج٤ ، ٢٧٨ – ٣٠٦. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1071575

الشايع، خالد بن سعد. (٢٠١٩). *الأمن السيبراني*، الدار العالمية.

الشريف، بندر بن عبد الله، وأحمد، عبد العاطي عبد الكريم محمد. (٢٠٢٠). دليل إرشادي للحد من ظاهرة التنمر السيبراني. *دراسات عربية في التربية وعلم النفس*، ع١٢٧، ٢٣ – ٩٢. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1091027

الشناوي، أمينة إبراهيم. (٢٠١٤). الكفاءة السايكومترية لمقياس التنمر الإلكتروني (المتنمر/الضحية)، *مجلة مركز الخدمة الاستشارية البحثية*، كلية الآداب، جامعة المنوفية، مصر.

الصحفي، مصباح أحمد حامد، وعسكول، سناء بنت صالح. (٢٠١٩). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. *مجلة البحث العلمي في التربية*، ع٢٠، ج١٠، ٤٩٣ – ٥٣٤. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1029923

صحيفة سبق. (٢٠١٩). *السعودية تحقق المركز ١٣ عالمياً في مؤشر الأمم المتحدة للأمن السيبراني*، نشرت في ٢٧/٣/٢٠١٩، مسترجع من: https://sabq.org/saudia/sr5xkt

الظويفري، مشاعل بنت شبيب بن مطيران. (٢٠٢١). واقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بالمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية. *المجلة الدولية للدراسات التربوية والنفسية*، مج١٠، ع٣، ٦٣٥ – ٦٥٥. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1224807

عبد الفتاح، نيرة، عز، رمضان، رباب رفعت. (٢٠٢٢) التنمر الإلكتروني كمقدمة للعدوان في الطفولة المبكرة. *المجلة الأكاديمية العالمية في العلوم التربوية والنفسية*. مج. ٣، ع. ٢، ٢٠٢٢. مسترجع من: https://search.shamaa.org/FullRecord?ID=361739

عبد الله، سيف النصر خوجلي. (٢٠٢١). أحكام التوقيع الإلكتروني وحجيته في القانون. *مجلة القلزم للدراسات السياسية والقانونية*، ع٣، ٢٠٧ – ٢٢٨. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1105324

العمار، أمل يوسف عبد الله. (٢٠١٦). التنمر الإلكتروني وعلاقته بإدمان الإنترنت في ضوء بعض المتغيرات الديموغرافية لدى طلاب وطالبات التعليم التطبيقي بدولة الكويت. *مجلة البحث العلمي في التربية*، ع١٧، ج٣، ٢٢٣ – ٢٤٩. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/846842

العمال، أمل يوسف عبد الله. (٢٠١٧). *علم النفس الاجتماعي*، رؤية معاصرة، القاهرة: مركز الإسكندرية للكتاب.

العنيزى، منصور عمر. (٢٠١٨) التنمر المدرسي لدى بعض تلاميذ مرحلة التعليم الاساسي، *مجلة كلية الآداب*، جامعة الزاوية، ليبيا، ع ٢٦، ج١، ص ٢٢١.

فهيم، كلير. (٢٠٠٧). *الصحة النفسية في مراحل العمر المختلفة*، القاهرة: مكتبة الأنجلو المصرية.

فوزي، أماني. (٢٠١٧). مفهوم القرصنة الإلكترونية من منظور اقتصادي. *المجلة الجنائية القومية*، مج٦٠، ع٣، ١٤١ – ١٥٣. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1043708

القحطاني، ناصر بن موسى. (٢٠٢٠) *مستوى الوعي بالأمن السيبراني في مدارس بوابة المستقبل الثانوية في المملكة العربية السعودية*، [رسالة ماجستير]، جامعة نايف العربية للعلوم الأمنية–كلية أمن الحاسب والمعلومات. مسترجع من https://repository.nauss.edu.sa/handle/123456789/66726

القحطاني، نورة بنت ناصر. (٢٠١٩). مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. *شؤون اجتماعية*، مج٣٦، ع١٤٤، ٨٥ – ١٢٠. مسترجع من http://search.mandumah.com/Record/1024050

كريم، أوراغ. (٢٠٢١). الاختراق الإلكتروني في الفضاء السيبراني وأفضل الطرق للحماية منه. *مجلة التطوير العلمي للدراسات والبحوث*، ع٤، ٢٩ – ٤٢. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1191645

محمد، ثناء هاشم محمد. (٢٠١٩). واقع ظاهرة التنمر الإلكتروني لدى طلاب المرحلة الثانوية في محافظة الفيوم وسبل مواجهتها: دراسة ميدانية. *مجلة جامعة الفيوم للعلوم التربوية والنفسية*، ع١٢، ج٢، ١٨١ – ٢٤٧. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1040530

المنيع، الجوهرة بنت عبد الرحمن إبراهيم. (٢٠٢٢). متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠. *مجلة كلية التربية*، مج٣٨، ع١، ١٥٥ – ١٩٤. مسترجع من http://search.mandumah.com.sdl.idm.oclc.org/Record/1251585

يوسف، ريهام سامي. (٢٠١٨). *التنمر الإلكتروني وعلاقته بإدمان مواقع التواصل الاجتماعي*، مصر: جامعة الأهرام الكندية.

ثانياً: المراجع الأجنبية

Agatston, P. W., Kowalski, R., & Limber, S. (2007). Students' perspectives on cyber bullying. *Journal of Adolescent Health*, 41(6), S59-S60.

Ashdown, I., & Sharpies, S. (2020). Virtual and Real World 3D Representations for Task-Based Problem Solving. *In Contemporary Ergonomics 2006* (pp. 285-289). Taylor & Francis.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Balakrishnan, V. (2015). Cyberbullying among young adults in Malaysia: The roles of gender, age and Internet frequency. *Computers in Human Behavior*, 46, 149-157.

Bulach, C. R. (2002). Implementing a Character Education Curriculum and Assessing Its Impact on Student Behavior. The Clearing House, 76(2), 79–83. http://www.jstor.org/stable/30189797.

Elgharnah, K. G. E., & Ozdamli, F. (2020). Determining Parents' Level of Awareness about Safe Internet Use. *World Journal on Educational Technology*: Current Issues, 12(4), 290-300.

Hemphill, S. A., Tollit, M., Kotevski, A., & Heerde, J. A. (2015). Predictors of Traditional and Cyber-Bullying Victimization: A Longitudinal Study of Australian Secondary School Students. *Journal of interpersonal violence*, 30(15), 2567–2590. https://doi.org/10.1177/0886260514553636.

Potgieter, P. (2019, October). The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. *In ICICIS* (pp. 272-280).

Sheryl A. Hemphill, PhD, and others, Predictors of Traditional and Cyber-Bullying Victimization: A Longitudinal Study of

Australian Secondary School Students, *Journal of Interpersonal Violence*, Vol. 30 (15), 2015, p. 2568.

van Niekerka, J., & von Solmsb, R. (2017). *ORGANISATIONAL LEARNING MODELS FOR INFORMATION SECURITY*.

Abstract:
* The aim of the research is to reduce cyberbullying through cybersecurity from the perspective of parents, where the descriptive user interface is used to identify the study community of parents, numbering (3171). The questionnaire was used as a tool to search for the goal, where it was found that the awareness of parents of third-grade primary school students about cybersecurity exploded, reaching a large extent with an arithmetic mean (3.18) and a standard deviation (0.486), and a large arithmetic deviation on the paragraphs of the awareness of parents of third-grade primary school students about cybersecurity reached between (2.96 - 3.33), and the researcher recommended providing digital capabilities that provide opportunities for learning and education for children, especially in remote areas of humanitarian light, and anti-terrorism programs without children's immersion in digital screens, including reliance on the Internet, and contributes to the month. Obesit