دور الوالدين في تعزيز الوعي بالأمن السيبراني للطفل

إعداد

أ/ منيفة بنت سعد المطيري
باحثة ماجستير الآداب في تربية الطفولة المبكرة،

د/ غادة بنت صالح السدراني
أستاذ الطفولة المبكرة المساعد

كلية التربية، جامعة الملك سعود

مجلة الدراسات التربوية والانسانية. كلية التربية. جامعة دمنهور
المجلد السادس عشر، العدد الثاني (أبريل) - لسنة 2024

دور الوالدين في تعزيز الوعي بالأمن السيبراني للطفل

أ/ منيفة بنت سعد المطيري

د/ غادة بنت صالح السدراني

المستخلص:

هدفت الدراسة إلى التعرُّف على دور الوالدين في تعزيز الوعي بالأمن السيبراني للطفل، بالإضافة إلى التعرُّف على دور الوالدين في تعزيز الوعي بأمن الشبكات وأمن التطبيقات للطفل، والكشف عن وجود فروق في استجابات الوالدين حول تعزيز الوعي بالأمن السيبراني للطفل تبعًا للمتغيرات: (نوع الوالدين، المستوى التعليمي للوالدين، والمستوى الاقتصادي للوالدين)، واعتمدت الدراسة على المنهج الوصفي المسحي، وذلك لطبيعة الدراسة وتحقيق أهدافها، وطُبِّقَت أداة الاستبانة على عينة عشوائية من الآباء والأمهات السعوديين في مدينة الرياض والبالغ عددهم (450) من الآباء والأمهات الذين لديهم أطفال، في عمر (6–9 سنوات)، وتوصلت الدراسة إلى أن دور الوالدين في تعزيز الوعي بالأمن السيبراني مرتفع، كما أن دور الوالدين في تعزيز الوعي بأمن الشبكات وأمن التطبيقات للطفل كبير.

الكلمات المفتاحية: الأمن السيبراني، أمن الشبكات، أمن التطبيقات، وعي الأطفال، الطفولة المبكرة.

Abstract:

The study aimed to identify the role of parents in enhancing awareness of cybersecurity for the child, in addition to identifying the role of parents in enhancing awareness of network security and application security for the child, and to reveal the presence of differences in parents' responses regarding enhancing awareness of cybersecurity for the child according to the variables: (type of parent, level The educational level of the parents, and the economic level of the parents). The study relied on the descriptive survey method, due to the nature of the study and achieving its objectives. The questionnaire tool was applied to a random sample of Saudi parents in the city of Riyadh, who numbered (450) Saudi parents (Mothers and Fathers) in the city of Riyadh, the study found that the role of parents in promoting awareness of cybersecurity is high, and that the role of parents in enhancing awareness of network security and application security for the child is great.

Keywords: Cybersecurity, network security, application security, children's awareness, early childhood.

مقدمة:

يشهد العالم اليوم تطورًا سريعًا في التكنولوجيا الرقمية، يتميَّز بسهولة الوصول لجميع فئات المجتمع على اختلاف أعمارهم وتنوُّع اهتماماتهم، وقد تؤثِّر التكنولوجيا الرقمية تأثيرًا سلبيًّا أو إيجابيًّا على حياتنا؛ فمن خلالها استطعنا التطور والنمو في شتى المجالات وتسهيل الكثير من أمور حياتنا، وفي المقابل قد يتعرَّض المستخدمون لجرائم الإلكترونية؛ التي قد تؤدي لآثار على المستخدمين تضر بهم صحيًّا أو ماديًّا أو اجتماعيًّا، إذا كان الاستخدام دون رقابة آمنة.

فالجريمة الإلكترونية تشير إلى الأنشطة الإجرامية التي تستخدم أجهزة الحاسوب؛ لغزو البيانات والمعلومات الشخصية بشكل غير قانوني؛ مثل: أعمال التخريب، وانتهاك الخصوصية، والابتزاز، ولهذه الجرائم الإلكترونية العديد من السمات والخصائص؛ فالجرائم الإلكترونية سرية يصعب اكتشافها وملاحظتها إلا بعد وقوعها، ويمكن إخفاء الأدلة في مدّة زمنية قصيرة؛ مما يجعل من الصعب إثبات الجريمة (حمادي، 2017).

ولذا تضامنت الجهود لوضع قوانين للحماية من هذه الجرائم الإلكترونية؛ ومن هذا المنطلق بذلت المملكة العربية السعودية جهودًا لحماية المستخدمين من الجرائم الإلكترونية بمجموعة من التدابير التي تهدف لتعزيز سلامتهم الرقمية؛ ومن بين هذه القوانين والتشريعات التي تنظم استخدام الإنترنت؛ فقد صدر أمر ملكي رقم (6801) في نهاية شهر أكتوبر عام (2017) بتأسيس الهيئة الوطنية للأمن السيبراني، ومجموعة من المؤسسات المعنية بالأمن السيبراني: كالهيئة الوطنية للأمن السيبراني، ومركز التميُّز لأمن المعلومات بجامعة الملك سعود، "أبوثنين، 2019، 231"، وتمَّ تحديد العديد من مهام الهيئة الوطنية للأمن السيبراني لرفع الوعي بالأمن السيبراني، وتقديم الخدمات الاستشارية، وتنظيم برامج التوعية لجميع فئات المجتمع (المركز الوطني للوثائق والمحفوظات، 2023).

وتعاونت هيئة الأمن السيبراني مع عدة مؤسسات، ومنها المؤسسات التعليمية؛ لتقليل الجرائم الإلكترونية؛ فقد أوضحت دراسة (M.Bidgoli, Knijnenburg, 2016) ضرورة رفع مستوى الوعي عند الطلاب فيما يتعلق بأمن المعلومات الإلكتروني؛ فالمعلم يسعى للبحث عن

الاستراتيجيات الحديثة لتوعية الطلاب بالأمن السيبراني والطرق الممكنة لاستخدام الإنترنت في البيئة التعليمة بحذر.

فتأثير الجرائم الإلكترونية لم يكن لفئة معينة بل طال الضرر الأطفال؛ فدراسة حدادي (2020) أكَّدت أن (80%) من الأطفال يتمّ استدراجهم عن طريق طلب صورهم والعبث فيها ونشرها في صور مسيئة ومخلة بالأخلاق، وقد تعاون المهتمون بالطفولة والمربون لتوعية الأطفال بالأمن السيبراني؛ ويكون قادرًا على التعامل مع التقنية الرقمية بحذر وأمن؛ حيث أظهرت نتائج دراسة العوفي (2015) الحاجة إلى توعية الأطفال بالأمن السيبراني وتزويدهم بالاستراتيجيات الممكنة؛ لحماية أنفسهم من الجرائم الإلكترونية.

وبناءً على الجهود السابقة؛ لاحظت الباحثتان أهمية دور الوالدين في توجيه سلوك أطفالهم من التأثيرات السلبية لاستخدام التقنية الرقمية وتأثيرها في جميع جوانب حياتهم (المغربي، 2018)؛ فاستخدام الأطفال للتقنية الرقمية يُعَدُّ تحديًا كبيرًا للوالدين يتطلَّب التثقيف والتوعية؛ لمعرفة الاستراتيجيات الممكن استخدامها؛ للتحقق من إعدادات الخصوصية الآمنة لأجهزة الأطفال، والتأكُّد من كيفية الإبلاغ في حال تعرضوا لأي خطر أو رسائل من مجهولين (الغانمي، 2019)؛ ولذا جاءت هذه الدراسة لتسليط الضوء على موضوع دور الوالدين في تعزيز الوعي بالأمن السيبراني للطفل.

مشكلة الدراسة:

يتيح عصرنا الحالي للأفراد سهولة الوصول إلى معلومات متنوِّعة وهائلة، وتمكِّن من التواصل الفعّال مع العالم من خلال الأجهزة الشخصية، وبما أن الأطفال أحد المستخدمين المعرضين للجرائم الإلكترونية؛ كالابتزاز، واختراق المعلومات الشخصية، والتعرض للمحتوى غير اللائق، فلتقليل هذه المخاطر؛ ينبغي الضبط الجيد لإعدادات الأمان بمواقع الإنترنت التي يستخدمها الأطفال؛ للحفاظ على أمنهم وسلامتهم (Smith, 2023).

كما أكَّدت اليونيسف (2017) في تقرير حالة الأطفال في العالم على أنَّه من المهم تعليم الأطفال في سن مبكرة وتزويدهم بالمهارات اللازمة لحماية أنفسهم من المحتوى الضار، كما يحتاج الأطفال إلى الوعي؛ لتزويدهم بالمهارات الأساسية اللازمة التي تمكِّنهم من مواجهة

المخاطر السيبرانية، والقدرة على اتخاذ القرارات المناسبة، والابتعاد عن المواقف التي تهدِّد أمنهم (عسيري، 2023).

ومن منظور حماية الأطفال في الفضاء السيبراني، وقَّعت الإدارة الوطنية للأمن السيبراني اتفاقية تعاون مع وكالة الأمم المتحدة المتخصصة لتقنية المعلومات والاتصالات والاتحاد الدولي للاتصالات في 17 ديسمبر 2020، تهدف إلى إطلاق خطة عالمية لحماية الطفل، وذلك في إطار تعزيز تحقيق أهداف مبادرة حماية الطفل التي اعتمدها صاحب السمو الأمير محمد بن سلمان آل سعود في المنتدى الدولي للأمن السيبراني بالرياض (الهيئة الوطنية بالأمن السيبراني، 2023).

وسعت الهيئة الوطنية للأمن السيبراني بتكثيف الجهود مع العديد من المجالات بالتعاون مع وزارة التعليم والمركز الوطني الإرشادي للأمن السيبراني، وأطلقت حملة "بأمان نتعلم"، والهدف من ذلك تقليل المخاطر على شبكة الإنترنت عند الممارسة التعليمية، ورفع الوعي بالأمن السيبراني لدى الأطفال، ولإحداث الأثر ينشر المركز بالتعاون مع وزارة التعليم المواد التوعوية للوصول الفعَّال والآمن للفئات المستهدفة المركز الوطني الإرشادي للأمن السيبراني 2022 (عسيري، 2023).

وهذا ما تؤكِّده نتائج البحث (المغربي، 2018) التي توصي بأهمية توعية الوالدين بالآثار السلبية لاستخدام الأطفال للأجهزة الإلكترونية، وفهم الاستراتيجيات الحديثة المستخدمة لحماية أطفالهم، ولاحظت الباحثتان – على حد علمهما– اهتمام الأبحاث السابقة بتعليم الأمن السيبراني للأطفال من خلال ممارسات من قبل عدة جهات الحكومية أو المؤسسات التعليمية، وبناءً على هذه الدراسات اتضح وجود فجوة بحثية في هذا المجال لقلة الدراسات التي توضِّح دور الوالدين في تعزيز مفهوم الوعي بالأمن السيبراني لدى الأطفال الذين تتراوح أعمارهم بين (6–9 سنوات)، وقد أكَّد ذلك إفادة مكتبة الملك فهد الوطنية؛ ولذلك فقد تحدَّدت مشكلة الدراسة في الإجابة عن السؤال التالي: ما دور الوالدين في تعزيز الوعي بالأمن السيبراني للطفل؟

أسئلة الدراسة

1– ما دور الوالدين في تعزيز الوعي بأمن الشبكات للطفل؟

2- ما دور الوالدين في تعزيز الوعي بأمن التطبيقات للطفل؟

أهداف الدراسة:

1- التعرُّف على دور الوالدين في تعزيز الوعي بأمن الشبكات للطفل.

2- التعرُّف على الوالدين في تعزيز الوعي بأمن التطبيقات للطفل.

أهمية الدراسة:

1. تتبع أهمية الدراسة الحالية من خلال ندرة الدراسات التي أجريت في المملكة العربية السعودية، والتي تناولت دور الوالدين في تعزيز الوعي بالأمن السيبراني للطفل.
2. إثراء المكتبة العربية بالبحوث الاجتماعية الداعمة لرؤية المستقبلية للملكة العربية السعودية (2030)، وتوجيه اهتمام المسئولين في مجال رعاية الطفل بأهمية تقديم البرامج التوعية المناسبة لعمر الطفولة المبكرة؛ لتزويدهم بالمعارف حول الأمن السيبراني.
3. تأتي الدراسة الحالية استجابة لتوجُّهات المملكة العربية السعودية في تعزيز وعي الأطفال بالأمن السيبراني.
4. رفع درجة الوعي بالأمن السيبراني لدى الأطفال، وتوضيح كيفية تأثير هذا الوعي على حماية الطفل من أخطار الإنترنت بما سيعود بالنفع على الطفل من خلال تعزيز قدرته على التعامل بشكل سليم مع هذه الأخطار.
5. توجيه اهتمام الوالدين نحو أهمية توعية الأطفال بمفهوم الأمن السيبراني بالتركيز على تعزيز الوعي بأمن الشبكات وأمن التطبيقات للطفل.
6. تساهم الدراسة في تشجيع المؤسسات التربوية ومعلمات الطفولة المبكرة بإضافة أنشطة تعزِّز الوعي بالأمن السيبراني في مرحلة الطفولة المبكرة.

حدود الدراسة: تتمثَّل حدود الدراسة فيما يأتي:

الحدود الموضوعية: اقتصرت هذه الدراسة على معرفة دور الآباء والأمهات للفئة العمرية للطفل (6-9 سنوات) في تعزيز الوعي بالأمن السيبراني للطفل في مجالين؛ هما: مجال أمن الشبكات؛ لأهميته في حماية الشبكات من الوصول غير المصرح به، ومجال أمن التطبيقات؛ لنتمكَّن من

حماية التطبيقات التي يستخدمها الأطفال من الاختراق الضار، وتفعيل حماية الخصوصية؛ لجعل التطبيق آمنًا للطفل.

الحدود المكانية: اقتصرت هذه الدراسة على مدينة الرياض في المملكة العربية السعودية وقد اختارت الباحثتان مدينة الرياض؛ لسهولة الوصول إلى مجتمع الدراسة.

الحدود الزمانية: طُبِّقَت الدراسة خلال الفصل الدراسي الأول في العام الدراسي (1445هـ).

مصطلحات الدراسة:

الأمن السيبراني (Cybersecurity)

يُعرَّف الأمن السيبراني تربويًّا بأنه:"حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدِّمه من خدمات وما تحتويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع" (الهيئة الوطنية للأمن السيبراني، 2023).

ويُعرَّف الأمن السيبراني إجرائيًّا بأنه: تبنَّت الباحثتان تعريف جبور (2016) للأمن السيبراني بأنَّه النشاط الذي يحمي الموارد المالية والبشرية التي ترتبط بالاتصالات، ويخفِّف حدة الأضرار والخسائر التي تحدث في حال وجود قرصنة أو مخاطر أو تهديدات، ويحاول تصليح ما أفسدته هذه الهجمات.

وفي هذا البحث ستركز الباحثتان على مجالات الأمن السيبراني التالية:

أمن الشبكات (Network security)

يُعرَّف أمن الشبكات تربويًّا بأنه: "عملية اتخاذ تدابير وقائية؛ لحماية البنية التحتية للشبكات الأساسية من الوصول غير المصرح به، أو التعطيل، أو التعديل، أو التدمير، فيسمح من تطبيق هذه الإجراءات لأجهزة الحاسوب والمستخدمين والبرامج بأداء وظائفهم الحيوية المسموح بها في بيئة آمنة" (وزارة الاتصالات وتقنية المعلومات، 2023).

ويُعرَّف أمن الشبكات إجرائيًّا بأنه: تأمين شبكة الإنترنت من أي اختراق غير قانوني يضر بالبيانات الخاصة ويؤدي إلى فقدان المعلومات.

أمن التطبيقات (Application security)

يُعرَّف أمن التطبيقات تربويًّا بأنه: "نظام العمليات والإجراءات الأمنية التي تهدف إلى حماية مستخدمي تطبيقات الإنترنت من التهديدات السيبرانية، ويشمل كذلك عملية تطوير ميزات الأمان، وإضافتها، واختبارها، داخل التطبيقات؛ لمنع الثغرات الأمنية ضد التهديدات المختلفة طيلة دورة حياة تطوير التطبيق بأكملها" (Harvard Business Terminology Guide, 2023).

ويُعرَّف أمن التطبيقات إجرائيًّا بأنه: مجموعة من الإجراءات المستخدمة؛ لتأمين التطبيقات من التعرض للهجوم الإلكتروني، وحماية التطبيقات من صفحات الويب غير الملائمة للطفل.

الإطار النظري:

مفهوم الأمن السيبراني:

يُعرَّف الأمن السيبراني بأنه: عبارة عن "مجموعة من التقنيات الحديثة، والعمليات المصممة؛ بغرض حماية أجهزة الكمبيوتر والشبكات والبرامج والبيانات من الهجوم أو التلف أو جميع أشكال الوصول غير المصرح به" (Sarker,2020, 4).

كما يُقْصَد بالأمن السيبراني: "مجموع الأطر القانونية والتنظيمية والهياكل التنظيمية والوسائل التكنولوجية الوطنية والدولية، التي تهدف إلى حماية الفضاء السيبراني الوطني، كما تركِّز على حماية بيانات الأفراد ومؤسسات الدولة من الاستخدام غير المصرح به، أو أي أذى يلحق بشبكة البيانات" (شويرب ومراد، 2023، 164).

وأكَّد (Cheng, 2019) أن الأمن السيبراني يتمثَّل في التدابير التي تهدف إلى حماية أنظمة المعلومات، بما في ذلك التكنولوجيا المتنوعة؛ مثل: الآلات، والأجهزة، والشبكات، والبرامج، والتطبيقات، والبيانات، والمعلومات، والأفراد المرتبطين بها، من مختلف أشكال الهجوم السيبراني.

وممَّا سبق يتضح أن الأمن السيبراني يشير عمومًا إلى العمليات والإجراءات المستخدمة لحماية شبكات الإنترنت من أي محاولة اختراق غير مشروع، وفقًا لمهام محددة ومنظمة؛ للدفاع ضد الهجمات الإلكترونية.

أهمية الأمن السيبراني:

مع التقدم التكنولوجي، اكتسب الأمن السيبراني أهمية كبيرة في مجال البحث والممارسة؛ حيث تتزايد قضايا الأمن السيبراني بشكل كبير عبر مختلف القطاعات العاملة في عالم الأعمال، وتركِّز المؤسسات المختلفة بشكل أكبر على متى سيكون هناك هجوم إلكتروني بدلًا من التركيز على ما إذا كان سيكون هناك هجوم أو لا، وتحث الشركات الحكومات على مكافحة هجمات الأمن السيبراني؛ لأن مشكلات الأمن السيبراني تسبِّب خسائر مالية فادحة؛ فالهجمات الإلكترونية لها تأثير شديد على المؤسسات؛ حيث إن (61%) من المؤسسات الصغيرة والمتوسطة تعرضت لهجمات إلكترونية في وقت من الأوقات (Mahmood, 2022).

ولقد تزايدت أهمية الأمن السيبراني مع تزايد أهمية استخدام التقنية في حياتنا اليومية مهنيًّا وشخصيًّا؛ نظرًا لأن المزيد من الأشياء أصبحت متصلة رقميًّا بالإنترنت، ومع تخزين المزيد من البيانات وتبادلها رقميًّا، يصبح من الصعب بشكل متزايد الحماية من المخاطر السيبرانية (Mijwil, 2023).

وتتمثَّل أهمية الأمن السيبراني بحسب ما يراها السمحان (2020) في الآتي:

- الحفاظ على المعلومات وسلامتها وتجانسها؛ من خلال منع طرق العبث بها.
- حماية الشبكات الإلكترونية والأجهزة من الاختراقات المتنوعة؛ حتى تكون بمثابة درع واقع للبيانات والمعلومات.
- العمل على استكشاف نقاط الضعف والثغرات الموجودة في الشبكات والأنظمة.
- استخدام الأدوات الخاصة بالمصادر المفتوحة؛ ومن ثَمَّ تطويرها من أجل تحقيق مبادئ ومتطلبات الأمن السيبراني.
- العمل على توفير مناخ وبيئة عمل تتسم بالأمان خلال العمل عبر الشبكة العنكبوتية.

وأضاف المنتشري وحريري (2020) أن الأمن السيبراني يساعد في التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة بأنواعها، وسد الثغرات في أنظمة المعلومات، كما يسهم في الحد من التجسس والتخريب الإلكتروني (Corradini et. al., 2020)، ويُعِدّ تعزيز الأمن السيبراني وحماية البنى التحتية الضرورية لتكنولوجيا المعلومات أمرًا ضروريًّا للتنمية الاجتماعية والاقتصادية لأي بلد؛ حيث يمكن أن تؤدي حوادث الأمن السيبراني إلى تعريض توافر وسلامة وسرية المعلومات المرسلة عبر الشبكات للخطر، وتعطيل تشغيل وأداء البنى التحتية الرقمية والمادية الحيوية، وحتى تهديد أمن الأفراد والبلدان بأكملها (فتوح، 2021).

أهداف الأمن السيبراني:

تتمثل أهداف الأمن السيبراني بحسب ما يؤكده السمحان (2020) وعسيري (2023) في الآتي

- تعزيز حماية نظم المعلومات ومكوناتها من أجهزة وبرمجيات، وما تشمله من بيانات.
- التصدي للهجمات السيبرانية التي تستهدف شبكات وأجهزة مؤسسات القطاع العام والخاص.
- توفير بيئة تكنولوجية آمنة لتبادل المعلومات والبيانات.
- حجب الثغرات الأمنية في أنظمة تكنولوجيا المعلومات
- مقاومة البرامج الضارة التي يتمُّ إرسالها من قبل القراصنة على هيئة ملفات مختلفة.
- توفير البنية التحتية اللازمة؛ للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
- صد برامج التجسس والتخريب الإلكتروني، سواء على مستوى الأفراد أو المؤسسات.
- تدريب الأفراد على آليات وإجراءات جديدة؛ لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية؛ بقصد الإضرار بمعلوماتهم الشخصية، سواء بالإتلاف أو السرقة.
- اتخاذ جميع التدابير اللازمة؛ لحماية المواطنين والمستهلكين على حد سواء، من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.

بالإضافة للأهداف السابقة ذكر توفيق ومرسي (2023) النقاط التالية:

- ضمان استمرارية عمل تطبيقات نظم المعلومات.

- حماية خصوصية وسرية المعلومات الشخصية، سواء للأفراد أو المؤسسات العامة أو الخاصة.
- حماية المواطنين من المخاطر المترتبة على دخول شبكة الإنترنت المختلفة.
- حماية مصلحة المؤسسات الحيوية، وأمنها، والبنى التحتية الحساسة فيها.
- حماية الأجهزة التقنية، وكذلك التشغيلية، من أي محاولات للولوج بشكل غير مسموح به؛ لتحقيق أهداف غير مشروعة.
- المحافظة على شبكات المعرفة والمعلومات.

وأضاف المنتشري (2020) أيضًا الأهداف التالية للأمن السيبراني:

- الحماية المالية: حيث يمكن عن طريق الأمن السيبراني معرفة جميع أنواع وطرق الاحتيال الإلكترونية التي تستهدف المعلومات البنكية، والبطاقات الائتمانية، وبطاقات الصرف الآلي الشخصية، والإعلانات والدعايات التجارية المضللة؛ ومن ثَمَّ التغلب عليها والتصدي لها.
- الحماية الوطنية: إن الفضاء السيبراني أصبح مجالًا للحروب الإلكترونية الخفية التي تؤدي إلى تدمير الوطن وتخريب ممتلكاته؛ ولذا فالأمن السيبراني يجعل لهذا المواطن حزام أمان، يستطيع من خلاله الحذر من مثل هذه الحروب، وكذلك التنبؤ بها، والتصدي لها.
- الحماية الدينية والأخلاقية: في الآونة الأخيرة أصبح من الممكن تجاوز القيم والمعايير والضوابط الاجتماعية؛ فهناك مواقع إباحية تعمل على تدمير القيم والأخلاق، وتبعد الإنسان عن دينه وعاداته وتقاليده، وتدفعه لارتكاب الجرائم وفعل المحرمات؛ ولذا فالأمن السيبراني يقدم الحلول التكنولوجية والحماية التامة من مثل هذه المواقع المدمرة.

وفي ضوء ما سبق ترى الباحثتان أن الباحثين أجمعوا على أن أهداف الأمن السيبراني تتمثل في التصدي للهجمات السيبرانية التي تستهدف الشبكات والأجهزة، وتوفير بيئة تكنولوجية آمنة لتبادل المعلومات والبيانات، وحماية خصوصية وسرية المعلومات الشخصية، كما أجمع الباحثون أن الأمن السيبراني لا يقتصر على توفير حماية الخصوصية للأشخاص فقط، بل للمؤسسات المجتمعية الحيوية والشركات المختلفة. وتجدر الإشارة إلى أنَّه من أجل تحقيق هذه الأهداف المرجوة؛ فمن الضروري البدء في زيادة الوعي بالأمن السيبراني منذ سن مبكرة، وتدريب

الأشخاص على اتخاذ التدابير اللازمة لحماية الشبكات عبر الإنترنت والمحتوى الشخصي، وحماية المواطنين والمستهلكين على حد سواء، من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.

مجالات الأمن السيبراني:

ناقشت العديد من الدراسات والبحوث مجالات الأمن السيبراني؛ حيث أشارت دراسة كل من (توفيق ومرسي، 2023، عميرة، 2023، عدلي، 2023، حمادي، 2017، Waldock, 2022، Kotenko, 2022، Zeng, E,2019) إلى عدد من المجالات الخاصة بالأمن السيبراني والمتمثلة في الآتي:

أمن الشبكات (Security Network)

أمن الشبكات؛ حيث تكون أجهزة الكمبيوتر محمية من الهجمات التي قد تواجهها داخل وخارج الشبكة، ويُعَدّ جدار الحماية أحد أهم تقنيات ضمان أمان الشبكة، والذي يعمل كحماية بين جهازك الشخصي والأجهزة الأخرى على الشبكة.

أمن المعلومات (Security Information)

عبارة عن مجموعة من الإجراءات الفنية التي يتمُّ مراعاتها؛ من أجل منع الأشخاص غير المسموح، وغير مصرح لهم الدخول إلى الشبكات وتغيير معلوماتها؛ وذلك تجنبًا لسرقتها أو إحداث تدمير نظم المعلومات.

أمن التطبيقات (Application Security)

وفيه تتمّ حماية المعلومات التي تتعلق بتطبيق معين على جهاز الحاسب الآلي؛ مثل: إجراءات كلمات المرور، وعمليات المصادقة الثنائية، وكذلك أسئلة الأمان التي تتضمن هوية المستخدم.

الأمن السحابي (Cloud Security)

وتُعَرَّف هذه البرامج بأنها: برامج التخزين السحابية التي يتمّ حفظها على الإنترنت، ويلجأ إليها الكثير من الأشخاص؛ لحفظ بياناتهم بدلًا من برامج التخزين المحلي؛ ممَّا أدى إلى ظهور الحاجة لحماية تلك البيانات.

أمن إنترنت الأشياء (Internet of things security)

وهو عبارة عن ثورة تكنولوجية قائمة بذاتها، وذلك وفقًا لتقرير صادر عن شركة (Bain and company)، وقد ذكر التقرير أن حجم السوق الخاص بأمن إنترنت الأشياء سوف يتوسّع بمقدار (520) مليار دولار أمريكي خلال العام (2021)، ومن خلال شبكة الأمان الخاصة سوف يقوم أمن إنترنت الأشياء بتوفير أجهزة مهمة للمستخدم؛ مثل: أجهزة الاستشعار، والطابعات (عميرة، 2023).

أمن العمليات (Operations security)

أحد العناصر المهمة في أي استراتيجية شاملة للأمن السيبراني هو عملية تحديد الإجراءات المصرح بها، والإجراءات الأخرى ذات الصلة التي يصل من خلالها المتسللون إلى البيانات الحساسة، ويحاول الأمن التشغيلي (OPSEC) القضاء على الوصول غير المصرح به أو على الأقل تقليله؛ ولهذا السبب يُعَدّ أمن المعلومات مهمًّا في جميع جوانب الحياة الإلكترونية على الإنترنت (عدلي، 2023).

أمن إدارة الهوية والوصول (Identity and access management security)

باختصار، تُعَدّ إدارة الهوية والوصول (IAM) مجالًا مهمًّا لأمن الشبكة؛ حيث تتعامل مع مشكلات الأذونات، ومن يمكنه الوصول إلى البيانات الموجودة على شبكة مشتركة؛ ولذلك فهو يحل العديد من القضايا الأمنية والهجمات السيبرانية؛ لأنه عبارة عن مجموعة من القواعد والممارسات؛ كما يضمن حصول الشخص المناسب على المعلومات الصحيحة في الوقت المناسب للسبب الصحيح، ويتداخل هذا المجال مع العديد من المجالات الأخرى؛ مثل: أمن التطبيقات والأمن السيبراني، كما أنه يُعَدّ مجالًا له طلب كبير في سوق العمل.

أمن المستخدم النهائي (End user security)

التقنيات والسياسات والإجراءات التي تعمل على حماية المستخدم النهائي للشبكة، وتوفر له وصول آمن عن بُعد إلى جميع البرامج التي يستخدمها من أجل إتمام مهامه اليومية، وهناك العديد من المؤسسات والشركات التي تعتمد على ما يُسَمَّى حوسبة المستخدم النهائي (EUC) ؛ حتى يستطيع موظفو الشركة إنجاز أعمالهم من أي مكان خارج نطاق المؤسسة.

أمن الأجهزة المحمولة (Mobile device security)

مجموعة من السياسات والإجراءات والتقنيات المستحدثة؛ من أجل حماية جميع الأجهزة المحمولة بكافة أشكالها وأنواعها من أي تهديدات أو اختراقات؛ بهدف حماية بيانات الأفراد من الهجمات السيبرانية.

وفي هذا الإطار يمكن تطبيق بعض الممارسات الجيدة التي يجب على مستعمل الفضاء السيبراني أخذها بعين الاعتبار؛ ومنها:

- السيطرة على ردود أفعالنا العاطفية (الأمن السيبراني للعقل البشري).
- كن حذرًا على الإنترنت.
- كن حذرًا مع هاتفك الذكي أو جهازك اللوحي.
- كن حذرًا عند استخدام نظام المراسلة الخاص بك.
- كلمات المرور يجب أن تكون معقدة وقوية، وأن تُغيَّر بانتظام، ولكل تطبيق كلمة مرور خاصة به.
- أن تكون لديك استراتيجية حفظ بيانات منتظمة، ومخطط لها بشكل صحيح ودقيق.
- فصل الاستخدامات الشخصية عن الاستخدامات المهنية.
- عدم تثبيت برامج أو تطبيقات من مواقع غير رسمية.
- استخدام الحلول الأمنية المثبتة(جدار الحماية والبرامج المضادة للفيروسات).
- فحص وتحليل وسائط التخزين المحمولة؛ مثل: اليواس بي قبل استخدامها.
- قم بتنظيف محفوظات التصفح بانتظام، سواء على الهاتف المحمول، أو الجهاز اللوحي، أو جهاز الكمبيوتر الخاص بك، بعد كل استخدام للإنترنت.
- في حالة عدم استعمال كاميرا الويب الخاصة بجهاز الكمبيوتر؛ يُستحسَن إيقاف تشغيلها؛ حتى لا يستطيع مجرم سيبراني استغلالها عن بعد لأغراض دنيئة.
- عند نهاية استعمال البريد الإلكتروني أو تصفح الإنترنيت باستعمال كمبيوتر مشترك يجب قطع الاتصال بالموقع أو البريد الإلكتروني، ومسح سجل التصفح، ثمَّ إغلاق البريد الإلكتروني أو موقع الويب.

- قبل الدخول في موقع ويب وأخذ معلومات منه؛ يجب محاولة تقييم موثوقيته بالإجابة على الأسئلة؛ مثل:(مَنْ ؟ – ماذا؟ – أين؟ – متى؟ – لماذا ؟ وكيف؟)
- قم بإيقاف تشغيل الكمبيوتر، أو الهاتف المحمول، أو الجهاز اللوحي، أثناء فترات عدم النشاط (العتيبي، 2022).

وتأسيسًا على ما سبق؛ فقد ركَّزت هذه الدراسة على المجالات الأكثر شيوعًا للأمن السيبراني، وهذا ما أكده السمحان (2020)؛ حيث إن أمن الشبكات وأمن التطبيقات هما الفئتان الأكثر شيوعًا في مجالات الأمن السيبراني، وإلى أي مدى يساهم هذان المجالان في تحسين حياة الأطفال، فمن خلال حماية الشبكات التي يستخدمها الطفل يقل تعرض الأطفال للشبكات الخطرة، ويتم الحد من الوصول إلى التطبيقات غير المناسبة لهم؛ وبالتالي تقليل تعرضهم للتهديدات السيبرانية، وهذا يجعل الأمر أكثر أهمية؛ لجعل الطفل على دراية بأمان التطبيق من خلال اتخاذ تدابير مختلفة لحماية استخدامه الشخصي.

توعية الطفل بالأمن السيبراني:

إن نشر الوعي بخطورة الهجمات السيبرانية وطرق الوقاية منها هام جدًّا لحماية المجتمع؛ فمهما كانت قوه التجهيزات التقنية الأمنية في الشبكات فإنه يسهل اختراقها بدون الوعي لدى الأفراد، وخصوصًا الأطفال؛ لأن العنصر البشري أكثر تعرض لثغرات تتمّ من خلاله الهجمات السيبرانية (جاب لله، 2022).

واستخدام الطفل في مرحلة الروضة للتكنولوجيا والإنترنت دون توجيه ومتابعة؛ يعرضه للعديد من المخاطر النفسية، والاجتماعية، والخلقية، والصحية، وقد أوصت الدارسات السابقة بضرورة إعداد الطفل؛ لمواجهة تحديات العصر الرقمي الجديد؛ من خلال إكسابه مفاهيم الحماية من مخاطر الإنترنت (الدهشان، 2018).

وتوجد العديد من آليات الترويج والتوعية بأهمية الأمن السيبراني لحماية الطفل؛ حيث وضعت الجمعية العامة للأمم المتحدة بعض المقترحات والسياسات التي من شأنها إرساء ثقافة عالمية وتوعية بأهمية الأمن السيبراني تتمثَّل في الجوانب التالية Assembly (2015):

- الترويج لثقافة وطنية تتعلق بأهمية الأمن السيبراني؛ ليس فقط لدور الحكومة في تأمين تشغيل واستخدام البنية التحتية للمعلومات، ولكن أيضًا يجب توعية القطاع الخاص، والمجتمع المدني، وكذلك الأفراد؛ وبالتالي يجب تدريب العنصر البشري وكذلك مستخدمي الأنظمة الحكومية والخاصة؛ وذلك بغرض إكسابهم تحسينات في المستقبل على النواحي الأمنية، وفيما يتعلق بقضايا الخصوصية، والرسائل الاقتحامية، والهجمات السيبرانية، والبرمجيات الضارة.
- تنفيذ تطبيقات وخدمات الحكومة الإلكترونية؛ فعلى الإدارات الوطنية تنفيذ تطبيقات وخدمات الحكومة الإلكترونية؛ من أجل تحسين عملياتها الداخلية، وتوفير الخدمات الأفضل للقطاع الخاص والمواطنين، كما ينبغي أن يشمل هذا الإطار التوعية بالمخاطر الخاصة بالأمن السيبراني، وتوعية المستخدمين، ومن ثَمَّ يجب تعزيز ثقافة الأمن السيبراني لدى المواطنين.
- الاهتمام بمبادرات استثارة الوعي والتوعية بالأمن السيبراني، وخاصة في الدول النامية.
- التعاون الدولي نحو نشر الوعي بأهمية الأمن السيبراني، وتعزيز ثقافة الأمن السيبراني؛ من خلال اشتراك المنظمات الإقليمية والمؤسسات المختلفة.

ولعل أهم سبل التوعية؛ للحد من مخاطر الأمن السيبراني ما ذكره التيماني (2019) والمتمثلة فيما يأتي:

- الموثوقيّة؛ فعند الدخول إلى موقع إنترنت يتضمن (https)، فهذا يعني أنه موقع آمن، أمّا إذا كان عنوان (URL) يحتوي على(http) بدون (s)؛ فتجنّب إدخال أيّ معلومات حساسة؛ مثل: بطاقة الائتمان، أو رقم التأمين الاجتماعي؛ حيث إنَّ الموقع الخاص بتقنية (HTTPS) يقوم بعملية نقل البيانات محمية ومشفرة.
- الرسائل الإلكترونية المشبوهة؛ حيث يجب التوعية بتجنب فتح مرفقات البريد الإلكتروني غير المعروفة؛ كونها إحدى الطرق الأكثر شيوعًا التي يتعرض فيها الأشخاص للسرقة أو الاختراق.

- النسخ الاحتياطي؛ عن طريق التوعية بضرورة عمل نسخ احتياطية من الملفات بانتظام وفق جدول زمني محدد ومستمر؛ بحيث يتسنى للفرد في حالة التعرض لهجمات إلكترونية أو إتلاف الملفات الهامة استعادتها، وتقليل خسائره بنسبة كبيرة جدًا.

وفيما يتعلق بتوجيه الأطفال؛ فقد وجَّه المركز الوطني الإرشادي للأمن السيبراني بالمملكة العربية السعودية باتباع بعض آليات حماية الأطفال من جرائم الامن السيبراني؛ حيث أكد المركز من خلال دراسته الإحصائية أنه يوجد طفل تحت عمر (18) عامًا من بين كل ثلاثة أفراد يستخدمون شبكة الإنترنت العالمية، وأن ما يقرب من (50%) من الأطفال حول العالم تعرضوا للعنف، كما يوجد أكثر من (13%) من الأطفال يعانون من التنمر الإلكتروني (المركز الوطني الإرشادي للأمن السيبراني بالمملكة العربية السعودية، 2020).

وترى الباحثتان أن إبلاغ الجهات المعنية بحدوث جرائم سيبرانية مع الطفل يعد قرارًا فعالًا في الحد من تكرار هذه الحوادث الأمنية، والتقليل من تبعاتها وآثارها على شخصية الطفل وخصوصية، كما أن التغيير المستمر كلمات المرور الخاصة بالمنصات التي يستخدمها الطفل يمنع الفرص أمام المتسللين لاختراق حسابات الأطفال داخل هذه المنصات. كما ترى الباحثتان أنه لكي يتم تفعيل هذه الآليات مع الأطفال عند حدوث جرائم سيبرانية لهم، يجب أولًا تدريب الطفل على كيفية إبلاغ الجهات المعنية بالحوادث الأمنية، وتدريبه على تذكر أرقام الطوارئ والإبلاغ الخاصة بالجهات المعنية في المواقف التي تمثل جرائم سيبرانية. كما يجب تدريب الطفل على القيام بنفسه بتغيير كلمات المرور الخاصة بالمنصات التي يستخدمها.

دور الوالدين في تعزيز الوعي بالأمن السيبراني للطفل:

يقع على عاتق الآباء والأمهات دور كبير في حماية أطفالهم، وتوعيتهم أمنيًّا، وحمايتهم من التهديدات الإلكترونية، وإكسابهم مهارات المواطنة الرقمية، وتتمثل تلك المهام في الآتي (الشريف، 2020):

- إجراء محادثة مفتوحة مع الأطفال حول التعريف بالإنترنت، ومخاطره، وما هو مسموح مشاركته، وما لا يجب مشاركته.

- محاولة تقليل الوقت المتاح للأطفال على الإنترنت تقلل من احتمال تعرضهم لشيء غير مناسب، وتحديد مدة زمنية يومية لاستخدام وسائل التواصل الاجتماعي والألعاب، والعمل على حظر استخدام الأجهزة الرقمية في غرفة النوم.
- استخدم برامج وتطبيقات الرقابة الأبوية؛ لأنها تُعَدّ وسيلة فعَّالة للحد من وقت استخدام الأجهزة ومراقبة السلوك عبر الإنترنت، وتتمثل تلك التطبيقات في الآتي Clean Router، Content Watch Net Nanny، Qustodio Parental Control.
- التعرُّف على المواقع التي يزورونها، ومع مَنْ يتفاعلون، ومَنْ يتابعون عبر منصات التواصل الاجتماعي والإنترنت.
- تعليم الأطفال احترام سمعتهم عبر الإنترنت؛ فالمواطنة الرقمية هي تعليم الأطفال التعامل مع الآخرين، وكذلك التأكد من الطريقة التي يمثلون بها أنفسهم عبر الإنترنت بالالتزام بقيمنا الإسلامية وأخلاقنا الدينية وتقاليدنا العائلية، ويجب تعليمهم أن سلوكهم عبر الإنترنت أيضًا انعكاس لتربيتهم وتعليمهم.

وقد وجه المركز الوطني الإرشادي للأمن السيبراني بالسعودية الآباء والأمهات لاتباع بعض السياسات التي من شأنها توعية الأطفال؛ وتتمثل في الرقابة الأبوية عن طريق التحكم في إعدادات التطبيقات، وتثبيت برامج الحماية من أجل تقليل مخاطر الاختراق، وتوعية الطفل بعدم الضغط على الروابط الغريبة، وتحديد أوقات معينة لاستخدام الأجهزة الإلكترونية (المركز الارشادي للأمن السيبراني بالمملكة العربية السعودية، 2020)

فضلًا عمَّا أوضحته دراسة (التيماني، 2019) من التركيز على تناول الوعي السيبراني لدى المجتمع السعودي؛ حيث هدفت الدراسة إلى التعرُّف على واقع الأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بأمن المعلومات، وترجع أهمية هذا البحث لتفاقم المهددات، وكثرة الاختراقات وتواترها على كل الأصعدة، وعلى كافة المستويات من الفرد إلى المؤسسات والوزارات والشركات، فقد بدأت الحكومات والشركات تعي تدريجيًّا أخطار الجرائم السيبرانية، وأهمية الأمن المعلوماتي على الأمن الاقتصادي والسياسي للبلد؛ وذلك بالاعتماد على المنهج الوصفي، وأداة المقابلة المطبقة على عينة من الخبراء المختصين بالأمن السيبراني

في مدينة الرياض، وقد تكوَّنت العينة من الأفراد العاملين في القطاع المصرفي المختصين في إدارة أمن المعلومات في العمل المصرفي في البنوك السعودية المحلية في مدينة الرياض، والأفراد العاملين المختصين في إدارة أمن المعلومات في القطاع التعليمي المتمثل في الجامعات الحكومية في مدينة الرياض، فضلًا عن إجراء المقابلة مع مجموعة من الخبراء المتخصصين في الأمن السيبراني والبالغ عددهم (5) خبراء، وتوصلت النتائج إلى أن الاهتمام الحكومي بموضوع الأمن السيبراني بدأ بشكل مبكر قبل أن يدرك الأفراد في المجتمع هذا المفهوم، وأن أكثر أنماط الجرائم السيبرانية انتشارًا بين الأفراد في المجتمع السعودي هي جريمة الاحتيال الإلكتروني، كما توصلت الدراسة إلى أن أكثر العوامل التي تزيد من فرصة حدوث الجرائم السيبرانية ضعف الوعي لدى الأفراد، ومشاركتهم المعلومات الشخصية مع الآخرين دون دراية ومعرفة بطبيعة عمل هؤلاء الأشخاص.

وتأسيسًا على ما تقدم؛ نستنتج أن رفع الوعي بالأمن السيبراني عند الطفل يتطلب تبني إستراتيجيات نظرية وعملية تتوافق مع قدرات الطفل في هذا العصر الرقمي؛ لذلك ينبغي للوالدين معرفة طرق حماية الطفل في هذا العصر، وتقليل تعرضهم للمخاطر السيبرانية؛ حيث كشفت دراسة عبد المجيد (2018) عن دور الآباء والأمهات في حماية أبنائهم من خطر الاختراق؛ فقد وجدت الدراسة أن هناك دورًا مهمًّا جدًّا للوالدين في حماية أطفالهم من التهديدات الإلكترونية، بما في ذلك الحالات التي يكون فيها لدى الأبناء المستوى التعليم الكافي للتعامل مع هذه التكنولوجيا الجديدة؛ ولذا فسعت الدراسة للمساهمة في رفع الثقافة الأمنية لدى الوالدين؛ لحماية الأطفال من الأخطار المحدقة بها.

لذا ترى الباحثتان ضرورة الاهتمام بتنمية الوعي بالأمن السيبراني للأطفال في المملكة العربية السعودية؛ وذلك من خلال تبني العديد من الإستراتيجيات، والأسس التي تعزز قدرات الأطفال في استخدام شبكة الإنترنت؛ وذلك بتقديم العديد من الدورات وورش العمل التي تُتاح إلكترونيًّا، أو من خلال قنوات على اليوتيوب تقدم برامج توعية باستخدام الإنترنت، والتعريف بالأمن السيبراني، ومخاطره، وكيفية تجنبها، فضلًا عن دور المدرسة من خلال ما تقدمه المعلمة من طرح المفاهيم المرتبطة بالأمن السيبراني، والتعريف به وكيفية حماية الخصوصية لدى

الأطفال، بالإضافة إلى دور الأسرة في تعزيز وعي الأطفال بالأمن السيبراني، وكيفية التعامل مع شبكة الإنترنت، وحماية بياناتهم من الاختراق، ومتابعة المواقع التي يستخدمها الأطفال، والعمل على توجيههم وقت ظهور أي مشكلة.

الإجراءات المنهجية للدراسة:

منهج الدراسة: اعتمدت هذه الدراسة على المنهج الوصفي المسحي؛ للتعرف على دور الوالدين في تعزيز الوعي بالأمن السيبراني للطفل، ويناسب هذا المنهج طبيعية مشكلة الدراسة، كما أنه مناسب من حيث انسجامه مع أهدافها، وطبيعة الأسئلة التي تسعى الدراسة للإجابة عنها.

مجتمع الدراسة:

يتكوَّن مجتمع الدراسة من جميع الآباء والأمهات السعوديين في مدينة الرياض، ممَّن لديهم أطفال في عمر (6–9سنوات)، وتم اختيار الوالدين كمجتمع دراسة دون غيرهم لأن الوالدين هم أساس النشأة وتقع على عاتقهم الدور الاكبر في تربية الأبناء، وتم اختيار منطقة الرياض تحديدا وذلك لسهولة الوصول إلى عينة الدراسة، والحصول على المعلومات. فقد بلغ حجم مجتمع الدراسة (805803) نسمة تبعًا لنتائج الهيئة العامة للإحصاء (الهيئة العامة للإحصاء،2017).

عينة الدراسة:

تم اختيار عينة الدراسة بالطريقة العشوائية البسيطة من مجتمع الدراسة الأصلي والذي يميز هذا الأسلوب بأعطاء جميع أفراد المجتمع فرصة متساوية فى الأختيار؛ وحيث قامت الباحثتان بتطبيق معادلة ستفين تامسون التالية؛ لتقدير حجم العينة:

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

حيث إن:

d : نسبة الخطأ المسموح به في التقدير (0.05).

Z : الدرجة المعيارية المقابلة لمستوى الثقة (95%) = (1.96).

P : نسبة توفر الخاصية وتساوي (0.50).

N : مجتمع الدراسة وبلغ عددهم (805803) نسمة.

وبالتطبيق على المعادلة السابقة، نجد أن حجم العينة المطلوب سحبها (94.383)، وبالتقريب يصبح (384)، وهي عينة ممثلة للمجتمع الأصلي من الآباء والأمهات السعوديين في مدينة الرياض، وتمَّ الاقتصار عليها؛ بسبب صعوبة الوصول لكامل المجتمع، ولكن تمَّ زيادة عينة الدراسة ليصبح (450)؛ لزيادة الدقة في نتائج الدراسة.

أداة الدراسة: وفقًا للمنهج الذي تمَّ اتباعه؛ استخدمت الدراسة الحالية الاستبانة أداةً لجمع البيانات التي تجيب عن أسئلة الدراسة.

صدق أداة الدراسة: تحققت الباحثتان من صدق أداة الدراسة المتمثلة في الاستبانة من خلال استخدام نوعين من الصدق؛ وهما:

1- الصدق الظاهري (صدق المحكمين) بعد بناء الأداة وبغرض التأكد من الصدق الظاهري لها؛ تمَّ عرضها على ستة محكمين ذوي الاختصاص من أعضاء هيئة التدريس في مجال الطفولة المبكرة، وبعد تحكيم الاستبانة تمَّ التعديل على عباراتها؛ بحذف بعض العبارات التي أجمع المحكمون على حذفها، وإضافة وتعديل بناءً على إجماع (80%) من المحكمين على إضافتها، إلى أن بلغت عبارات الاستبانة في صورتها النهائية (28) عبارة، تمَّ تقسيمها إلى محورين؛ هما: المحور الأول: دور الوالدين في تعزيز الوعي بأمن الشبكات للطفل، وبلغ عدد العبارات (14) عبارة، والمحور الثاني: دور الوالدين في تعزيز الوعي بأمن التطبيق للطفل، وبلغ عدد العبارات (14) عبارة، وتمَّ إرسال الأداة إلى لجنة أخلاقيات البحث العلمي بجامعة الملك سعود؛ للحصول على الموافقة على تطبيقها، وتحتوي الاستبانة على جزأين رئيسيين (ملحق5).

2- الاتساق الداخلي: للتأكد من صدق الاتساق الداخلي لأداة الدراسة، وتماسك العبارات بالدرجة الكلية للمحور الذي تنتمي إليه؛ فقد تمَّ قياس صدق الاتساق الداخلي للأداة من خلال حساب معاملات الارتباط لسبيرمان؛ لقياس العلاقة بين كل عبارة من عبارات المحور والدرجة الكلية للمحور الذي تنتمي إليه، وكانت النتائج كالتالي:

جدول(1) معاملات ارتباط كل عبارة من عبارات المحور الأول بالدرجة الكلية للمحور

م	العبارة	معامل الارتباط	درجة المعنوية
1	أحرص على استخدام تقنية التحقق بأكثر من طريقة؛ مثل: بصمة الإصبع، والرقم السري لتأمين شبكة الاتصال بالإنترنت.	0.581**	0.000
2	أحرص على الاطلاع على تعليمات الهيئة الوطنية للأمن السيبراني والتوجيهات الخاصة باستخدام تأمين شبكة الاتصال بالإنترنت.	0.771**	0.000
3	أحرص على وضع إجراءات لحماية شبكة الاتصال بالإنترنت وفق ضوابط الهيئة الوطنية للأمن السيبراني بواسطة مراجعة إعدادات الخصوصية في التطبيقات الجديدة.	0.716**	0.000
4	أحرص على التواصل مع خبراء ومختصين بشكل متواصل؛ لفحص التطبيقات الإلكترونية لأجهزة طفلي.	0.693**	0.000
5	أنبه طفلي بعدم القيام بأي تعديلات في سياسة الخصوصية دون استشارة أحد الوالدين.	0.656**	0.000
6	أدرب طفلي على استخدام كلمة مرور قوية في شبكة الاتصال بالإنترنت.	0.734**	0.000
7	أحرص على تقديم البلاغ للجهات الخاصة عند التعرض للاختراق أو تعطيل في شبكة الإنترنت.	0.740**	0.000
8	أحرص على تأمين متصفح الإنترنت في أجهز طفلي.	0.747**	0.000
9	أشارك طفلي المواد المسموعة والمرئية حول طرق حماية الخصوصية في شبكة الإنترنت.	0.783**	0.000
10	أغلق شبكة الاتصال بالإنترنت لطفلي عند الضرورة بواسطة تفعيل خاصية المراقبة الأبوية.	0.751**	0.000
11	أذكر طفلي بعدم نشر كلمة المرور الخاصة بشبكة الاتصال بالإنترنت.	0.687**	0.000
12	أتحدث مع طفلي حول التهديدات الأمنية على شبكة الإنترنت؛ حتى يتعرفوا عليها في حال حدوث اختراق.	0.724**	0.000
13	أحذر طفلي من التواصل عن طريق الفيديو أو صوت مع المجهولين؛ لتجنب الابتزاز.	0.622**	0.000
14	أشجع طفلي على التواصل معي عند حدوث أي تهديد عن طريق الإنترنت.	0.621**	0.000

ملاحظة: تشير إلى معنوية معامل الارتباط عند (0.01%)

أكدت نتائج الجدول (1) على صلاحية جميع عبارات المحور الأول؛ حيث تراوحت قيم معاملات الارتباط بين (0.581) و (0.783)؛ حيث جاءت عبارات الاستبانة دالة إحصائيًّا عند مستوى (0.01)؛ ممَّا يشير إلى الاتساق الداخلي بين فقرات المحور، وأن أداة الدراسة صادقة ومتسقة داخليًّا، وتقيس الجوانب التي تمَّ إعدادها من أجل قياسها.

جدول(2) معاملات ارتباط كل عبارة من عبارات المحور الثاني بالدرجة الكلية للمحور

م	العبارة	معامل الارتباط	درجة المعنوية
15	أتحدث مع طفلي حول إجراءات المحافظة على أمن التطبيق؛ مثل إلغاء الإعلانات في التطبيق.	0.732**	0.000
16	أحرص على تعطيل خدمات الوصول إلى الموقع في أثناء استخدام طفلي للتطبيق.	0.736**	0.000
17	أحرص على تحميل برامج مكافحة الفيروسات على أجهزة طفلي.	0.661**	0.000
18	أدرب طفلي على التعامل الصحيح عند التعرض لتهديدات من مجهولين عن طريق إبلاغ أحد الوالدين.	0.715**	0.000
19	أنبه طفلي حول استخدام التطبيقات التعليمية من مصادر غير رسمية وغير موثوقة.	0.790**	0.000
20	أحذر طفلي من نشر أي معلومات شخصية في الإنترنت.	0.713**	0.000
21	أحذر طفلي من استخدام تطبيقات مجهولة المصدر.	0.764**	0.000
22	أحرص على تفعيل التنبيهات في التطبيقات التي يستخدمها طفلي؛ ليصلني كل تعديل في سياسية الخصوصية.	0.760**	0.000
23	أحرص على ربط تطبيقات طفلي بجوالي الشخصي؛ لأتمكن من متابعة التطبيق.	0.786**	0.000
24	أوعي طفلي بعدم فتح روابط غير رسمية.	0.765**	0.000
25	أوعي طفلي بتأثير الاستخدام السيئ للإنترنت دون وجود برامج الحماية.	0.786**	0.000
26	أقدم نصائح لتوعية طفلي من اختراق الأجهزة بما يتناسب مع عمره.	0.759**	0.000
27	أحدد وقت استخدام طفلي لتطبيقات الإنترنت.	0.752**	0.000
28	أحرص على اختيار متصفح موثوق؛ ليتمكن طفلي من التصفح بأمن.	0.777**	0.000

ملاحظة: تشير إلى معنوية معامل الارتباط عند (0.01%).

أكدت نتائج الجدول (2) على صلاحية جميع عبارات المحور الثاني؛ حيث تراوحت قيم معاملات الارتباط بين (0.715) و (0.790)؛ حيث جاءت عبارات الاستبانة دالة إحصائيًّا عند مستوى (0.01)؛ ممَّا يشير إلى الاتساق الداخلي بين فقرات المحور، وأن أداة الدراسة صادقة ومتسقة داخليًّا، وتقيس الجوانب التي تمَّ إعدادها من أجل قياسها.

ثبات أداة الدراسة: تمَّ حساب ثبات الأداة باستخدام معامل ثبات كرونباخ ألفا، ويوضح الجدول (3) قيمة معامل الثبات لكل محور من محاور الاستبانة والاستبانة ككل.

جدول (3) قيمة معامل ثبات كرونباخ ألفا

محاور الاستبانة	عدد العبارات	معامل الثبات
المحور الأول: دور الوالدين في تعزيز الوعي بأمن الشبكات للطفل.	14	0.919
المحور الثاني: دور الوالدين في تعزيز الوعي بأمن التطبيق للطفل.	14	0.938
الاستبانة ككل	28	0.957

من خلال الجدول (3)، تظهر النتائج أن معامل ثبات محاور الاستبانة عال؛ حيث تراوحت بين (0.919) للمحور الأول؛ و (0.938) للمحور الثاني، كما بلغ معامل الثبات الكلي للاستبانة (0.957)؛ مما يدل على تمتعها بمعامل ثبات جيد جدًّا.

نتائج الدراسة ومناقشتها وتفسيرها:

عرض نتائج السؤال الأول ومناقشتها

لقد نص السؤال الأول على: ما دور الوالدين في تعزيز الوعي بأمن الشبكات للطفل؟ وللإجابة عن هذا السؤال تمَّ حساب المتوسط الحسابي والانحراف المعياري للمحور الأول: (دور الوالدين في تعزيز الوعي بأمن الشبكات للطفل)، وكل عبارة من عبارات المحور؛ ويمكن الاطلاع على تلك النتائج من خلال الجدول رقم (4)، التالي:

جدول (4) رأي عينة الدراسة حول المحور الأول: دور الوالدين في تعزيز الوعي بأمن الشبكات للطفل.

م	العبارة	المتوسط	الانحراف المعياري	الترتيب	درجة الممارسة
1	أحرص على استخدام تقنية التحقق بأكثر من طريقة؛ مثل: بصمة الإصبع، والرقم السري لتأمين شبكة الاتصال بالإنترنت.	2.76	0.503	7	دائمًا
2	أحرص على الاطلاع على تعليمات الهيئة الوطنية للأمن السيبراني والتوجيهات الخاصة باستخدام تأمين شبكة الاتصال بالإنترنت.	2.65	0.602	11	دائمًا
3	أحرص على وضع إجراءات لحماية شبكة الاتصال بالإنترنت وفق ضوابط الهيئة الوطنية للأمن السيبراني بواسطة مراجعة إعدادات الخصوصية في التطبيقات الجديدة.	2.71	0.582	10	دائمًا
4	أحرص على التواصل مع خبراء ومختصين بشكل متواصل؛ لفحص التطبيقات الإلكترونية لأجهزة طفلي.	2.47	0.749	14	دائمًا
5	أنبه طفلي بعدم القيام بأي تعديلات في سياسة الخصوصية دون استشارة	2.79	0.498	4	دائمًا

م	العبارة	المتوسط	الانحراف المعياري	الترتيب	درجة الممارسة
	أحد الوالدين.				
6	أدرب طفلي على استخدام كلمة مرور قوية في شبكة الاتصال بالإنترنت.	2.58	0.696	13	دائمًا
7	أحرص على تقديم البلاغ للجهات الخاصة عند التعرض للاختراق أو تعطيل في شبكة الإنترنت.	2.73	0.565	8	دائمًا
8	أحرص على تأمين متصفح الإنترنت في أجهز طفلي.	2.77	0.494	6	دائمًا
9	أشارك طفلي المواد المسموعة والمرئية حول طرق حماية الخصوصية في شبكة الإنترنت.	2.62	0.636	12	دائمًا
10	أغلق شبكة الاتصال بالإنترنت لطفلي عند الضرورة بواسطة تفعيل خاصية المراقبة الأبوية.	2.73	0.549	9	دائمًا
11	أذكر طفلي بعدم نشر كلمة المرور الخاصة بشبكة الاتصال بالإنترنت.	2.81	0.469	3	دائمًا
12	أتحدث مع طفلي حول التهديدات الأمنية على شبكة الإنترنت؛ حتى يتعرفوا عليها في حال حدوث اختراق.	2.78	0.494	5	دائمًا
13	أحذر طفلي من التواصل عن طريق الفيديو أو صوت مع المجهولين؛ لتجنب الابتزاز.	2.86	0.424	1	دائمًا
14	أشجع طفلي على التواصل معي عند حدوث أي تهديد عن طريق الإنترنت.	2.85	0.416	2	دائمًا
	المتوسط الكلي للمحور الأول	**2.72**	**0.388**		دائمًا

يتضح من الجدول رقم (4) أن العبارة رقم (13) والتي تنص على: "أحذر طفلي من التواصل عن طريق الفيديو أو صوت مع المجهولين؛ لتجنب الابتزاز" جاءت في المرتبة الأولى بمتوسط حسابي (2.86) وانحراف معياري (0.424) وبدرجة (دائمًا)، واتفقت هذه النتيجة مع دراسة عسيري (2023)؛ حيث جاءت في المرتبة الأولى أيضًا من درجة ممارسة معلمة الروضة لحماية الأطفال من التحرش الإلكتروني، وجاءت بدرجة مرتفعة جدًّا عبارة" أحذر الأطفال بعدم التواصل مع مجهولين عبر الإنترنت"، وترى الباحثتان خطورة مشاركة الأطفال لمعلوماتهم الشخصية مع مجهولين، وضرورة توعية الوالدين أطفالهم لذلك؛ لأنَّ التعامل مع الأشخاص المجهولين قد يعرضهم للابتزاز.

تليها عبارة رقم (14) والتي تنص على: "أشجع طفلي على التواصل معي عند حدوث أي تهديد عن طريق الإنترنت" بمتوسط حسابي (2.85) وانحراف معياري (0.416) وبدرجة (دائمًا)، واتفقت هذه النتيجة مع دراسة عسيري (2023) أيضًا؛ حيث جاءت في المرتبة الثانية

وبدرجة موافق بشدة على عبارات "أجيب على جميع أسئلة الطفل؛ حتى لا يبحث عن الإجابة لدى الآخرين على الإنترنت" من ممارسة معلمة الروضة لحماية الأطفال من التحرش الإلكتروني، وترى الباحثتان أهمية هذه العبارة؛ حيث إنه من الضروري أن يكون الطفل متواصلًا مع أحد والديه؛ حتى لا يتعرض للأشخاص المجهولين عبر الإنترنت، فالتواصل مع الأشخاص المجهولين قد يكون مدخلًا للتأثير غير السوي على الطفل. وقد أكدت ذلك دراسة التيماني (2019) التي أكدت على أن تواصل الأطفال مع الأشخاص الآخرين المجهولين عبر الإنترنت قد يعرضهم لجرائم الاحتيال والاستغلال الإلكتروني، فعندما يتواصل الأطفال مع مجهولين عبر الإنترنت، قد يُطلب منهم أن يشاركوا معلوماتهم الشخصية معهم، دون أن يكون لدى الأطفال أي علم أو دراية بطبيعة عمل هؤلاء الأشخاص، ونواياهم وأهدافهم.

وجاءت في المرتبة الثالثة عبارة رقم (11) والتي تنص على: "أذكر طفلي بعدم نشر كلمة المرور الخاصة بشبكة الاتصال بالإنترنت" بمتوسط حسابي (2.81) وانحراف معياري (0.469) وبدرجة (دائمًا)، واتفقت هذه النتيجة مع دراسة الصانع وآخرون (2020) التي تنص على: "أتجنب الكشف عن أي بيانات شخصية أو عائلية أثناء تصفحي للإنترنت"؛ حيث حصلت على أعلى متوسطات وبدرجة ممارسة عالية جدًّا؛ حيث جاءت أيضًا في المرتبة الثالثة من درجة وعي المعلمين بمدينة الطائف بالأمن السيبراني من وجهة نظرهم، وترى الباحثتان من وجهة نظرهما حصول هذه العبارة على أعلى المتوسطات ودرجات الموافقة إلى أهمية حماية الأطفال لأنفسهم وأجهزتهم؛ سواء من قبل الوالدين أو المعلمين. وذلك عن طريق تعزيز دور الوالدين في رفع درجة هذا الوعي بتذكرهم دائمًا بعدم نشر كلمة المرور الخاصة بشبكة الاتصال بالإنترنت، وعدم نشر أي معلومات شخصية أو عائلية؛ حتى تتوافر لهم درجة حماية كافية لأجهزتهم؛ ليتعرضوا لمخاطر الاختراق الإلكتروني والهجمات السيبرانية.

في حين جاءت العبارة رقم (9) والتي تنص على: "أشارك طفلي المواد المسموعة والمرئية حول طرق حماية الخصوصية في شبكة الإنترنت" بمتوسط حسابي (2.62) وانحراف معياري (0.636) وبدرجة (دائمًا)، وقد اتفقت هذه النتيجة مع دراسة عسيري (2023) التي أشارت إلى أن الأبناء يتم الإجابة عن جميع أسئلتهم وتوعيتهم بكل شيء؛ حتى لا يبحثوا على الإنترنت عن

إجابات لتساؤلاتهم؛ ممَّا قد يتسبب في حصولهم على معلومات مغلوطة أو غير صحيحة، وتفسر الباحثتان هذا الاتفاق في ضوء وعي وحرص عينة الدراسة على عدم اللجوء إلى الآخرين على الإنترنت للحصول على معلومات كافية، خاصة مع الأطفال؛ لأن ذلك قد يشعرهم بعدم وعي الوالدين بكافة الأمور، وقد انعكس هذا الوعي لدى الوالدين في استجاباتهم على العبارة رقم (9) والتي جاء متوسط الاستجابات عليها أقل من بقية العبارات.

كما جاءت العبارة رقم (6) في الرتبة قبل الأخيرة والتي تنص على: "أدرب طفلي على استخدام كلمة مرور قوية في شبكة الاتصال بالإنترنت" بمتوسط حسابي (2.58) وانحراف معياري (0.696) وبدرجة (دائمًا)، وقد اتفقت هذه النتيجة مع دراسة عسران (2020) التي توصلت إلى أن تدريب التلاميذ على استخدام كلمات مرور قوية في شبكات الاتصال بالإنترنت من أهم عناصر حماية الأجهزة؛ حيث حصلت هذه العبارة على أعلى متوسط، ويدل ذلك على ارتفاع درجة الوعي بالأمن السيبراني لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف، ويرجع ذلك إلى تدريبهم على الوعي بالأمن السيبراني في مرحلة الطفولة المبكرة، وترى الباحثتان ضرورة توعية الوالدين لأبنائهم في مرحلة الطفولة بأساسيات أمن الشبكات وخصوصًا تدريبهم على استخدام كلمة مرور قوية. وهنا يجب أن يكون كلمات المرور قوية أو معقدة، حتى لا يتثنى لأحد تخمين كلمات المرور الخاصة بالطفل، كما يجب أن يتم تغيير كلمات المرور الخاصة بانتظام، حتى يتم منع استمرار أي محاولة للاختراق السيبراني، فبمجرد تغيير كلمات المرور بشكل مستمر، يتم تسجيل الخروج من الحسابات الشخصية لمسجلة في الأجهزة الأخرى (العتيبي، 2022).

كما جاءت العبارة رقم (4) أقل عبارة من حيث المتوسط، والتي تنص على: "أحرص على التواصل مع خبراء ومختصين بشكل متواصل؛ لفحص التطبيقات الإلكترونية لأجهزة طفلي" بمتوسط حسابي (2.47) وانحراف معياري (0.749) وبدرجة (دائمًا)، وقد اتفقت هذه النتيجة مع دراسة عسيري (2023) التي أكدت على أن الأطفال يتم تدريبهم على تحميل التطبيقات الآمنة والمناسبة، كما أشارت إلى أنه يتم استخدام برامج التحكم ومراقبة التصفح التي تقوم بحظر المواد والإعلانات المسيئة، كما أشارت إلى أنه يتم تحذير الأطفال من الاستجابة لأي طلب أو

رسائل أو إعلانات تظهر لهم أثناء استخدام الإنترنت؛ ومن ثمَّ قد يرى الوالدان أنه لا حاجة أو ضرورة للتواصل مع الخبراء والمختصين؛ لفحص التطبيقات الإلكترونية لأجهزة الأطفال؛ ونتيجة لذلك فإن متوسط استجابات عينة الدراسة الحالية على العبارة رقم (4) جاء أقل من بقية العبارات الأخرى؛ حيث حرص الآباء والأمهات في الدراسة الحالية بدرجة كبيرة على الاطلاع على تعليمات الهيئة الوطنية للأمن السيبراني والتوجيهات الخاصة باستخدام تأمين شبكة الاتصال بالإنترنت، وكذلك تنبيه الأطفال بعدم القيام بأي تعديلات في سياسة الخصوصية دون استشارة. وقد يرجع ذلك إلى مستوى تعليم الوالدين، الذي يؤثر بدوره في درجة وعيهم بكيفية فحص التطبيقات الإلكترونية على أجهزة أطفالهم بأنفسهم (الشريف، 2020). وهذا يتفق مع ما أشارت إليه الدراسة الحالية بشكل عام، حيث تم التأكيد على أن دور الوالدين في تعزيز الوعي بالأمن السيبراني كان مرتفعًا، وأن دور الوالدين في تعزيز الوعي بأمن الشبكات وأمن التطبيقات للطفل كان كبيرًا واوضحًا.

وترى الباحثتان أنه يمكن تفسير ذلك بأن دور الوالدين في تعزيز الوعي بأمن الشبكات للطفل كبير وأن أهم الخطوات التي يجب أن يتبعها الوالدين لتعزيز وعي الطفل بأمن الشبكات للطفل هي تحذير الطفل من التواصل عن طريق الفيديو أو صوت مع المجهولين؛ لتجنب الابتزاز؛ وتشجيع الطفل للتواصل مع أحد الوالدين عند حدوث أي تهديد عن طريق الإنترنت، فضلًا على تذكير الطفل بعدم نشر كلمة المرور الخاصة بشبكة الاتصال بالإنترنت؛ وبالتالي توفير بيئة آمنة عند تعامل الطفل مع الشبكات. وفي هذا السياق، أوضح المركز الوطني الإرشادي للأمن السيبراني بالمملكة العربية السعودية عدد من الآليات والإجراءات المهمة للتعامل بشكل آمن ومفيد عند حدوث جرائم سيبرانية للطفل، حيث أوضح أهمية الوالدين في ذلك الأمر، وأوصى بتدريب الوالدين على أن يقوموا بتعليم وتعويد الأطفال على إبلاغ الجهات المعنية بالأمر عند حدوث تهديد، وتدريبهم على ضرورة تغيير جميع كلمات المرور الخاصة بالمنصات التي يستخدمها الطفل، ووقف البطاقات الائتمانية بشكل عاجل؛ لمنع تسريب بياناتها عند التعرض لأي هجمات إلكترونية (عبد العاطي وآخرون، 2018).

عرض نتائج السؤال الثاني ومناقشتها:

لقد نص السؤال الثاني على: ما دور الوالدين في تعزيز الوعي بأمن التطبيقات للطفل؟ وللإجابة عن هذا السؤال تمَّ حساب المتوسط الحسابي والانحراف المعياري للمحور الثاني: (دور الوالدين في تعزيز الوعي بأمن التطبيقات للطفل)، وكل عبارة من عبارات المحور؛ ويمكن الاطلاع على تلك النتائج من خلال الجدول (5)، التالي:

جدول (5) رأي عينة الدراسة حول المحور الثاني : دور الوالدين في تعزيز الوعي بأمن التطبيق للطفل

م	العبارة	المتوسط	الانحراف المعياري	الترتيب	درجة الممارسة
15	أتحدث مع طفلي حول إجراءات المحافظة على أمن التطبيق؛ مثل إلغاء الإعلانات في التطبيق.	2.74	0.525	12	دائمًا
16	أحرص على تعطيل خدمات الوصول إلى الموقع في أثناء استخدام طفلي للتطبيق.	2.70	0.558	14	دائمًا
17	أحرص على تحميل برامج مكافحة الفيروسات على أجهزة طفلي.	2.71	0.566	13	دائمًا
18	أدرب طفلي على التعامل الصحيح عند التعرض لتهديدات من مجهولين عن طريق إبلاغ أحد الوالدين.	2.82	0.449	5	دائمًا
19	أنبه طفلي حول استخدام التطبيقات التعليمية من مصادر غير رسمية وغير موثوقة.	2.78	0.495	8	دائمًا
20	أحذر طفلي من نشر أي معلومات شخصية في الإنترنت.	2.86	0.401	1	دائمًا
21	أحذر طفلي من استخدام تطبيقات مجهولة المصدر.	2.85	0.414	2	دائمًا
22	أحرص على تفعيل التنبيهات في التطبيقات التي يستخدمها طفلي؛ ليصلني كل تعديل في سياسية الخصوصية.	2.77	0.517	10	دائمًا
23	أحرص على ربط تطبيقات طفلي بجوالي الشخصي؛ لأتمكن من متابعة التطبيق.	2.76	0.530	11	دائمًا
24	أوعي طفلي بعدم فتح روابط غير رسمية.	2.85	0.409	3	دائمًا
25	أوعي طفلي بتأثير الاستخدام السيئ للإنترنت دون وجود برامج الحماية.	2.81	0.471	7	دائمًا
26	أقدم نصائح لتوعية طفلي من اختراق الأجهزة بما يتناسب مع عمره.	2.82	0.452	6	دائمًا
27	أحدد وقت استخدام طفلي لتطبيقات الإنترنت.	2.78	0.481	9	دائمًا
28	أحرص على اختيار متصفح موثوق؛ ليتمكن طفلي من التصفح بأمن.	2.83	0.437	4	دائمًا

يتضح من جدول (5) أن المتوسط العام للمحور الثاني: "دور الوالدين في تعزيز الوعي بأمن التطبيق للطفل" هو (2.79)، وتراوح المتوسط الحسابي لعبارات هذا المحور بين (2.70)

و(2.85)؛ ممَّا يعنى أن الاتجاه العام لاستجابات عينة الدراسة على المحور طبقًا لمقياس ليكرت الثلاثي هو (دائمًا) أي أن رأي عينة الدراسة حول دور الوالدين في تعزيز الوعي بأمن التطبيق للطفل كبير.

جاءت عبارة رقم (20) والتي تنص على: "أحذر طفلي من نشر أي معلومات شخصية في الإنترنت" في المرتبة الأولى بمتوسط حسابي (2.86) وانحراف معياري (0.401) وبدرجة (دائمًا)، وتتفق هذه النتيجة مع دراسة السواط وآخرون (2020) التي توصلت إلى أن تحذير الأطفال من نشر معلوماتهم الشخصية عبر الإنترنت من أهم عناصر أمن خدمات تصفح الإنترنت؛ حيث حصلت هذه العبارة على أعلى متوسط؛ ممَّا يدل على ارتفاع الوعي بالأمن السيبراني في مجال التعامل مع أمن خدمات تصفح الإنترنت لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف حيث كان كبير جدًّا.

وترى الباحثتان أن تحذير الطفل من نشر معلوماته الشخصية عبر الإنترنت شيء في غاية الأهمية من قبل الوالدين، فالأطفال عند استخدامهم للإنترنت قد يُطلب منهم معلومات شخصية خاصة بهم، أو طلب صور ومقاطع خاصة بهم أو بأفراد أسرهم، مما قد يتسبب في استخدام هذه المعلومات الشخصية بشكل مسيء يتنافى مع الأخلاق والدين. وقد أكد ذلك حدادي (2020) الذي أشار إلى أن (80%) من الأطفال الذين يستخدمون البريد الإلكتروني ويتصفَّحون الإنترنت دون علم أهاليهم يتمّ استدراجهم عن طريق طلب صورهم والعبث فيها ونشرها في صور مسيئة ومخلة بالأخلاق.

ثم تلتها العبارة رقم (21) التي تنص على "أحذر طفلي من استخدام تطبيقات مجهولة المصدر" بمتوسط حسابي (2.85) وانحراف معياري (0.414) وبدرجة دائمًا. وقد اتفقت هذه النتيجة مع دراسة القحطاني (2022) حيث جاءت درجة الوعي بأهمية عدم فتح روابط مجهولة المصدر بدرجة مرتفعة وفي المرتبة الثانية من حيث الوعي بأمن تطبيقات الأمن السيبراني لذوي الإعاقة البصرية بالمملكة العربية السعودية، مما يدل على الاتفاق على ضرورة تجنب الروابط غير الرسمية ومجهولة المصدر مما يعزز الوعي بأمن التطبيقات.

ثم جاءت العبارة رقم (24) في المرتبة الثانية، والتي تنص على: "أوعي طفلي بعدم فتح روابط غير رسمية" بمتوسط حسابي (2.85) وانحراف معياري (0.409) وبدرجة (دائمًا)، ثم تلتها عبارة رقم (21) التي تنص على: "أحذر طفلي من استخدام تطبيقات مجهولة المصدر" بمتوسط حسابي (2.85) وانحراف معياري (0.414) وبدرجة (دائمًا). واتفقت هذه النتيجة مع دراسة القحطاني (2022)؛ حيث جاءت درجة الوعي بأهمية عدم فتح روابط مجهولة المصدر بدرجة مرتفعة، وفى المرتبة الثانية من حيث الوعي بأمن تطبيقات الأمن السيبراني لذوي الإعاقة البصرية بالمملكة العربية السعودية؛ ممَّا يدل على الاتفاق على ضرورة تجنب الروابط غير الرسمية ومجهولة المصدر؛ ممَّا يعزز الوعي بأمن التطبيقات. ولأهمية وعي الطفل بضرورة تجنب فتح الروابط الغريبة والمجهولة، حث المركز الوطني الإرشادي للأمن السيبراني بالسعودية الآباء والأمهات لاتباع بعض الإجراءات التي تحقق هذه الوعي لدى الأطفال؛ ومن أهم هذه الإجراءات قيام الوالدين بضبط إعدادات التطبيقات بحيث لا تسمح بمشاركة أي معلومات على الهاتف أو الجهاز الذكي، أو عدم التحويل التلقائي للروابط الغريبة بمجرد الضغط عليها لفتحها (المركز الارشادي للأمن السيبراني بالمملكة العربية السعودية، 2020). وترى الباحثتان أن ذلك يعمل على تقليل أخطار حدوث الهجمات السيبرانية وتوعية الطفل بعدم الضغط على الروابط الغريبة.

وقد جاءت العبارة رقم (15)، والتي تنص على: "أتحدث مع طفلي حول إجراءات المحافظة على أمن التطبيق؛ مثل إلغاء الإعلانات في التطبيق" بمتوسط حسابي (2.74) وانحراف معياري (0.525) وبدرجة (دائمًا)، وقد اتفقت هذه النتيجة مع دراسة عسيري (2023) التي أكدت على أن الأبناء يتمُّ توعيتهم وتدريبهم بشكل كافٍ داخل رياض الأطفال على طريقة تحميل التطبيقات الآمنة والمناسبة لهم، وترى الباحثتان أن استجابات عينة الدراسة الحالية على عبارة "أحذر طفلي من استخدام تطبيقات مجهولة المصدر" جاءت بدرجة عالية، وكانت هذه العبارة في الترتيب الثالث؛ مما يشير إلى اطمئنان الوالدين إلى أن أبناءهم لن يتضرروا من إعلانات التطبيقات؛ لأنهم بالفعل يحذرونهم من تثبيت التطبيقات غير الآمنة؛ فيتوقعون أن جميع تطبيقات أطفالهم آمنة.

وترى الباحثتان أهمية ذلك بأن دور الوالدين في تعزيز الوعي بأمن التطبيقات للطفل كبير، وأن أهم الخطوات التي يجب أن يتبعها الوالدان؛ لتعزيز وعي الطفل بأمن التطبيق للطفل؛ تحذير الطفل من نشر أي معلومات شخصية في الإنترنت؛ وتوعية الطفل بعدم فتح روابط غير رسمية، فضلًا عن تحذير الطفل من استخدام تطبيقات مجهولة المصدر.

وجاءت بالمرتبة قبل الأخيرة عبارة رقم (17)، والتي تنص على: "أحرص على تحميل برامج مكافحة الفيروسات على أجهزة طفلي" بمتوسط حسابي (2.71) وانحراف معياري (0.566) وبدرجة (دائمًا)، واختلفت هذه النتيجة مع دراسة القحطاني (2022)؛ حيث حصلت هذه العبارة على درجة متوسطة لدرجة الوعي بأمن تطبيقات الأمن السيبراني، وترى الباحثتان أن الاختلاف يرجع إلى وعي الوالدين بأهمية تحميل برامج مكافحة الفيروسات؛ لتعزيز الوعي بأمن تطبيقات الطفل؛ ومن ثمَّ الوعي بالأمن السيبراني. حيث ترى الباحثتان أن برامج مكافحة الفيروسات تعمل على حماية جهاز المحمول أو الحاسب الآلي من جميع أنواع الفيروسات، وبالتالي حفظ كافة البيانات الخاصة والمهمة من أي أخطار ممكنة قد تؤدي الى تلفها أو الاستيلاء عليها أو استغلالها. كما تحمي برامج مكافحة الفيروسات الأجهزة من الاختراق من قبل المجهولين، وتوفر إمكانية التحكم الكامل في البرامج الموجودة بالجهاز وتوقع الثغرات بها أو الكشف عنها، والكشف عن البرامج والتطبيقات الضارة والمثبتة على الجهاز، والتي يستخدمها الصغار أو الكبار دون علم بضرر هذه التطبيقات عن غيرها، كما ترى الباحثتان أن برامج مكافحة الفيروسات توفر إمكانية التحكم الكامل بكل مكونات الجهاز ووسائل الإدخال، كما توفر إمكانية التحكم في فتح وغلق مواقع الإنترنت، وجمع سجلات الحماية لتحليلها ومعرفة مدى أمان المواقع التي يتم التعامل معها أو تصفحها. وفي هذا السياق أوصى المركز الوطني الإرشادي للأمن السيبراني بالسعودية بضرورة قيام الوالدين بتثبيت برامج الحماية من الفيروسات على أجهزتهم وأجهزة أطفالهم؛ لتقليل أخطار الاختراق والأضرار الناتجة عن وجود برامج وتطبيقات ضارة على الأجهزة (المركز الارشادي للأمن السيبراني بالمملكة العربية السعودية، 2020).

في حين كانت أقل عبارة من حيث المتوسط هي العبارة رقم (16) التي تنص على: "أحرص على تعطيل خدمات الوصول إلى الموقع في أثناء استخدام طفلي للتطبيق" بمتوسط

حسابي (2.70) وانحراف معياري (0.558) وبدرجة (دائمًا)، ويتفق ذلك مع دراسة عسيري (2023) التي أكدت على تقديم الوعي الكافي للأبناء حول كيفية حماية أنفسهم على الإنترنت، على الرغم من أن هذه العبارة حصلت على أقل متوسط حسابي، إلا أن درجة توافرها أو الموافقة عليها كانت دائمة وكبيرة، وترى الباحثتان أن هذه النتيجة تتماشى مع طبيعة عمل نظام GPS (نظام تحديد المواقع) على الأجهزة، فهي تقنية أصبحت أساسية وضرورية لمعظم التطبيقات المتاحة على المتاجر الإلكترونية، كما ترى الباحثتان أن نظام الـ GPS يعد واحدًا من أبرز المميزات الموجودة في الهواتف الذكية الحديثة، حيث يقوم بمساعدة المستخدمين على معرفة موقعهم الجغرافي، وتوفير القدرة على مشاركة هذا الموقع مع الآخرين أو إلى الأجهزة الأخرى، كما يمكن أن تعزى هذه النتيجة إلى وعي الوالدين بأهمية نظام GPS الكبيرة عند فقدان الهاتف أو سرقته، حيث يساعد نظام GPS بشكل كبير في استعادة الجهاز المفقود أو المسروق من خلال تحديد المكان الذي يتواجد فه.

توصيات الدراسة: في ضوء النتائج التي أسفرت عنها الدراسة الحالية تقترح الباحثتان بعض التوصيات التي قد تساعد في تعزيز دور الوالدين في التوعية بالأمن السيبراني للطفل؛ وذلك على النحو التالي:

- بناءً على نتيجة السؤال الأول الذي يدور حول دور الوالدين في تعزيز الوعي بأمن الشبكات للطفل، توصي الباحثتان بضرورة تدريب الوالدين على حماية شبكاتهم الخاصة لهم ولأطفالهم بكلمات مرور قوية، وتحميل برامج مكافحة الفيروسات على الأجهزة الخاصة لهم وللأطفال.
- بناءً على نتيجة السؤال الثاني المتعلق بدور الوالدين في تعزيز الوعي بأمن التطبيقات للطفل، توصي الباحثتان بضرورة تواصل الوالدين مع الخبراء والمتخصصين؛ لفحص التطبيقات الإلكترونية لأجهزة الطفل.
- توصلت الدراسة إلى وجود تفاوت في الاهتمام بأمن الشبكات وأمن التطبيق؛ نتيجة لعدم إدراك تأثير مجالات الأمن السيبراني في الحد من أضرار الإنترنت على الأطفال؛ لذلك توصي الدراسة بالتوازن والتركيز على جميع مجالات الأمن السيبراني باعتبار أن عملية

التوعية الناجحة تتطلب التثقيف العالي وفق أسس محددة تراعي كافة عناصر الأمن في استخدام الإنترنت.

- وبشكل عام توصي الدراسة بضرورة دمج مفاهيم الأمن السيبراني في المناهج الدراسية في المراحل التعليمية المختلفة، مع مراعاة التسلسل والتكامل بينها. وتضمين مناهج رياض الأطفال أنشطة متنوعة؛ لتوعية الأطفال بالاستخدام الآمن للإنترنت، والتعرُّف على مجالات الأمن السيبراني التي يمكن أن تساعدهم في تحقيق الأمن.
- ضرورة نشر الوعي الأمني السيبراني لكافة فئات المجتمع، والمساهمة في الحد من الجرائم الإلكترونية، وحماية أسرهم من أخطار الإنترنت. وتعزيز التعاون بين أولياء الأمور والجهات الحكومية ذات العلاقة بالأمن السيبراني؛ لمواكبة التطورات في مجال مكافحة الجرائم الإلكترونية.

مقترحات الدراسة:

تأمل الباحثتان أن تكون الدراسة الحالية مقدمة لدراسات أخرى في مجال توعية الطفل بالأمن السيبراني؛ ذلك تقترح الدراسة عددًا من الدراسات المستقبلية؛ وذلك على النحو التالي:

- توسيع مجتمع الدراسة؛ ليشمل مدنًا مختلفة في المملكة العربية السعودية.
- إجراء دراسة نوعية حول واقع توعية الأطفال بالأمن السيبراني.
- فاعلية تنفيذ الأنشطة الصفية في زيادة وعي الأطفال في مرحلة الطفولة المبكرة بمفاهيم الأمن السيبراني.
- دراسة مقارنة؛ لمعرفة أثر الوعي بالأمن السيبراني لدى الأطفال في مرحلة رياض الأطفال والمرحلة الابتدائية.
- إجراء دراسة؛ للتعرُّف على التحديات التي تواجه أولياء الأمور في التوعية بالأمن السيبراني للطفل.

المراجع:

1.البياتي، راجي يوسف محمود (2022). الإرهاب السيبراني: نماذج من الجهود الدولية للحد منه .مجلة تكريت للعلوم السياسية، (28)، 87– 121.

2.توفيق، صلاح الدين محمد، ومرسي، شرين عيد (2023). متطلبات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمية من وجهة نظر أعضاء هيئة التدريس: جامعة بنها أنموذجًا. المجلة التربوية، (105)، 737 – 861.

3.التيماني، مداخل زيد عبد الرحيم (2019). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني. جامعة الملك سعود. السعودية. 1 –23.

4.جاب الله، عادل موسى (2022). وسائل حماية الأمن السيبراني دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة. المجلة العلمية .34 (3).

5.جبور، منى (2016). السيبرانية هاجس العصر. المركز العربي للبحوث القانونية.

6.حدادي، وليدة (2020). مرتكزات التربية الإعلامية للطفل في ظل تهديدات الجريمة الرقمية عبر الإنترنت، مجلة الأحياء، 20 (27).

7.حمادي، آلاء محمد رحيم (2017). الجريمة السيبرانية ومخاطرها على الأطفال: الإشكاليات والحلول: دراسة تحليلية في ضوء الإحصائيات الدولية والعربية والوطنية، مجلة كلية التربية للبنات، 28(4)، 1104 – 1119.

8.الدهشان، جمال (2018). تربية الطفل المصري في العصر الرقمي بين تحديات الواقع وطموحات المستقبل.

9.السمحان، منى عبد الله صالح (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية بالمنصورة، 1 (111)، 2 – 29.

10.الشريف، هيثم عبد الله (2020). أطفالنا والسيبرانية وأمنهم على الإنترنت. العطاء الرقمي. تمَّ الاطلاع بتاريخ 25 سبتمبر 2023 في https://attaa.sa/library/view/536

11.شويرب، جيلالي، ومراد، فائزة (2023). مفهوم الحروب السيبرانية والأمن السيبراني. مجلة الحقوق والحريات، 11 (1)، 157 - 178.

12.عبد العاطي، محمد لطفي محمد جاد، ومحمد، وهدان أحمد محمد، والدجدج، عائشة عبد الفتاح مغاوري (2018). تنمية مهارات فهم المقروء لدى الدارسين بفصول مواصلة التعليم باستخدام نظرية التعلم ذي المعنى لأوزوبل .العلوم التربوية، 2 (3)، 378 – 402.

13.عدلي، هدى (2023). واقع وتحديات الأمن السيبراني وإجراءاته. مجلة قانونك، (16)، 185 - 218.

14.عسيري، ذكرى (2023). دور معلمات الروضة في تعزيز وعي الأطفال السعوديين بالأمن السيبراني في مدينة الرياض. مجلة دراسات الطفولة، 26 (99)، 115– 126.

15.عميرة، محمد زين العابدين علي حنفي (2023). الأمن السيبراني ومنظومة التعليم الدولية . مجلة القراءة والمعرفة، (260)، 55– 96.

16.فتوح، وسام حسن (2021). الأمن السيبراني في المنطقة العربية: توعية المصارف والمؤسسات المالية لاتباع المعايير العالمية .مجلة اتحاد المصارف العربية، 490، 1– 5.

17.القحطاني، عبدالله (2022). درجة الوعي بالأمن السيبراني لدى الأشخاص ذوي الإعاقة البصرية بالمملكة العربية السعودية من وجهة نظرهم. مجلة التربية الخاصة والتأهيل. 14 (50)، الجزء الثاني ص 1–31.

18.المركز الوطني للوثائق والمحفوظات (2023). تنظيم الهيئة الوطنية للأمن السيبراني. المركز الوطني للوثائق والمحفوظات(ncar.gov.sa) .

19.المغربي، راندا محمد (2018). أثر استخدام التكنولوجيا على سلوك الأطفال في مرحلة ما قبل المدرسة من وجهة نظر الوالدين. مجلة بحوث التربية النوعية. جامعة المنصورة، 18(52).

20.المنتشري، فاطمة يوسف (2020). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للعلوم التربوية والنفسية، (17)، 457 – 484.

21.المنتشري، فاطمة يوسف، وحريري، رندة (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية: المؤسسة العربية للتربية والعلوم والآداب، (14)، 95 – 140.

22.الهيئة الوطنية للأمن السيبراني (2023). الضوابط الأساسية للأمن السيبراني.

23.اليونيسيف (2017). حالة أطفال العالم في عالم رقمي. شعبة الاتصال التابع لليونيسيف.

24.Assembly, G. (2015). Resolution adopted by the General Assemby on 11 September 2015. A/RES/69/315 15 September 2015. New York: United Nations.

25.Cheng, L., Pei, J., & Danesi, M. (2019). A sociosemiotic interpretation of cybersecurity in US legislative discourse. Social Semiotics, 29(3), 286-302.

26.Harvard Business Terminology Guide. (2023).

27.ITU (2023). Committed to connecting the world. Definition of cybersecurity. Retrieve at 23/9/2023. From: https://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx

28.Kotenko, I., Izrailov, K., & Buinevich, M. (2022). Static analysis of information systems for IoT cyber security: a survey of machine learning approaches. Sensors, 22(4), 1335.

29.Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity challenges in blockchain technology: A scoping review. Human Behavior and Emerging Technologies, 2022, 1-11.

30.Mijwil, M., Aljanabi, M., & Ali, A. H. (2023). Chatgpt: Exploring the role of cybersecurity in the protection of medical information. Mesopotamian journal of cybersecurity, 2023, 18-21.

31.Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 7 (1), 1-29.

32.Smith, A. (2023). The Impact of Technological Advancements on Society.

33.Waldock, K. E., Miller, V., Li, S., & Franqueira, V. N. (2022, February). Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people. Global Forum on Cyber Expertise.

34.Zeng, E., & Roesner, F. (2019). Understanding and improving security and privacy in {multi-user} smart homes: A design exploration and {in-home} user study. In 28th USENIX Security Symposium (USENIX Security 19) (pp. 159-176).

35.Bidgoli, M., Knijnenburg, B. P., & Grossklags, J. (2016, June). When cybercrimes strike undergraduates. In 2016 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-10). IEEE.