فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني لدى عينة من المراهقين مستخدمي الإنترنت بمدينة جدة.

د. أحمد مصطفى محمد أحمد القوصي

أستاذ علم النفس الكلينيكي المساعد

بجامعة الملك عبدالعزيز

ملخص: هدفت الدراسة إلى معرفة مدى فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني لدى عينة المراهقين من طلاب المرحلة الثانوية بمدينة جدة، واشتملت عينة الدراسة على عينة استطلاعية قوامها(١٠٩) طالباً، متوسط أعمارهم (١٨,٥) وعينة أخرى وهى عينة التدخل الإرشادي مكونة من (٣٠) طالباً، قسمت إلى مجموعتين(١٥) طالبًا تمثل المجموعة التجريبية، وعدد(١٥) طالبًا تمثل أفراد المجموعة الضابطة من طلاب المدارس الثانوية الصف الثالث الثانوي بمدينة جدة، واستخدم الباحث اختبار الوعي بالأمن السيبراني: من إعداد نورة الصانع وآخرين(٢٠٢٠). وبرنامج إرشادي لتنمية الوعي بالأمن السيبراني من إعداد الباحث، وقد توصلت الدراسة إلى عديد من النتائج أهمها أن وعى أفراد العينة بالأمن السيبرانى كان ضعيفًا، كما كشفت الدراسة عن وجود فروقاً دالة إحصائيًا عند مستوى دلالة (٠,٠٠١) بين درجات القياسين البعدي والقبلي في اختبار الوعي بالأمن السيبراني بعد تطبيق البرنامج الإرشادي في اتجاه القياس البعدي، كما كشفت الدراسة عن وجود فروقاً دالة إحصائيًا عند مستوى دلالة (٠,٠٠١) بين درجات المجموعتين التجريبية والضابطة في اختبار الوعي بالأمن السيبراني بعد تطبيق البرنامج الإرشادي في اتجاه المجموعة التجريبية، كما كشفت الدراسة عن عدم وجود فروق ذات دلالة إحصائية بين القياس البعدي والتتبعي في الوعي بالأمن السيبراني بأبعاده المختلفة.

فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني لدى عينة من المراهقين مستخدمي الإنترنت بمدينة جدة.

د. أحمد مصطفى محمد أحمد القوصي
أستاذ علم النفس الكلينيكي المساعد
بجامعة الملك عبدالعزيز

مقدمة

ثمة اعتقاد أن الأمن لن يخرج عن نطاق مفهومه التقليدي المعروف، بيد أن الدائرة اتسعت مؤخرًا، وظهر أنواع أخر من أنواع الأمن أتي في مقدمتها الأمن السيبراني والذي يعني في أبسط تعريف له: أنه يمثل حماية المعلومات الموجودة على أجهزة الحاسب الآلي وشبكاته، في مواجهة أي تدخل غير مصرح به قد يستهدف إحداث تغيير في المعلومات أو إتلافها، أو الحرمان من الوصول إليها (Hadlington & Parsons, 2017).

ففي خلال العشر سنوات الماضية أحدثت تكنولوجيا المعلومات تغييرًا في استخدام التطبيقات الرقمية بأجهزة الاتصال في حياتنا اليومية، مما جعل الحياة أيسر في مختلف مجالات الحياة: مثل قراءة الصحف الرقمية والعملية التعليمية والسياحة والسلوك الاستهلاكي، وتقديم الدعم والتوصية لمتخذي القرار (Sabillon et al., 2021).

ومع تدفق الوسائل المعلوماتية الحديثة وازدهارها، وانتشار التقنيات الرقمية واستعمالها في مختلف مجالات الحياة في المجتمعات كافة، ظهرت التهديدات الأمنية السيبرانية التي أصبح لها تأثير كبير وضخم في أمن المعلومات، وأصبحت عملية حصر أنواع التهديد أمرًا بالغ الصعوبة (Alzubaidi, 2021).

وهذه التهديدات في أبسط صورها يقوم بها عن غير قصد أفراد من ذوي المهارات التكنولوجية، بيد أن خطورة هذه التهديدات تزيد إذا تم من قبل مجموعات ذات نوايا سيئة من المتسللين والإرهابيين ممن لديهم مهارات تكنولوجيا لمهاجمة المعلومات على نظم الكمبيوتر، وغالبًا ما تسبب هذه التهديدات خسائرًا اجتماعية واقتصادية للمجتمعات المستهدفة، ومع تزايد نسبة مستخدمي الإنترنت تتزايد خطورة التهديدات السبيرانية، لذلك أصبح تحقيق الأمن السيبرانى من الأهمية بمكان (Bordoff et al.,2017).

وعلى الرغم من تخصص العديد من الشركات التكنولوجيا في مجال مكافحة التهديدات الأمنية السيبرانية، بيد أن عملية إحصاء هذه التهديدات أصبحت شبه مستحيلة؛ لأنها لا تتوقف بل تظهر أشكال جديدة وليدة اللحظة، مع الزيادة المضطردة في التهديدات الأمنية السيبرانية، واستخدام التقنيات التكنولوجية للمواجهة، وقد نبه هذا المتخصصين إلى أن العامل البشري هو الحلقة الأضعف في تحقيق الأمن السيبرانى عبر منظور نفسي لمعالجة تلك القضية من خلال رؤيته للطبيعة البشرية؛ إذ يؤدى علم النفس دورًا حاسمًا في التخفيف من خطر التهديدات السبيرانية، وأن تحقيق الأمن السيبرانى لا يتطلب التركيز على التكنولوجيا وحدها بل يستلزم ذلك التركيز على البشر وطبيعتهم النفسية، وخاصة أن أنظمة الأمان الأكثر تعقيدًا تظل غير قادرة على منع الأشخاص من الوقوع بوصفهم ضحايا للهجمات السيبرانية وللجرائم الإلكترونية (Wiederhold,et al.,2014).

ومن هذا المنطلق، يمكن أن يساعد علماء النفس في تحقيق الأمن السيبرانى بطرق مختلفة اعتمادًا على الجوانب النفسية لمستخدمى الإنترنت، ووفقًا لتباين قدرتهم على تقييم مخاطر التهديدات، فقد أظهرت دراسة (Hadlington & Parsons, 2017) أن نسبة ٢٣٪ فقط يتعاملون بشكل صحيح مع سيناريوهات الأمن السيبراني؛ وأن نسبة ٤٪ فقط يمكنهم التعامل مع أكثر من ٩٠٪ من سيناريوهات الأمن السيبراني.

يضاف إلى ما سبق أن نمو الإنترنت قد ارتبط بنمو إمكان وصول المراهقين إليه، فالمراهقون هم الفئة الأكثر استخدامًا للإنترنت، ومن ثم يتم تعزيز خطورة وقوعهم ضحية لتهديد إلكتروني.

ومن الطريف هنا أن نذكر ظهور جيل عادة ما يشار إليه باسم الجيل Z، وهم الذين ولدوا بين عامي ٢٠٠١ و ٢٠١٣، حيث نشئوا حول الإنترنت؛ فهذا الجيل أكثر الأجيال ذكاءًا واستقلالية على الويب. ورغم ذلك يواجه هذا الجيل كثيرًا من الانتقادات؛ بسبب انفصاله عن المجتمع وبسبب إهداره للوقت؛ نظرًا لاستخدامه التكنولوجيا، إذ يقضي هذا الجيل ما يقرب من ثلاث ساعات يوميًا على الأقل من الوقت على الإنترنت، وفي عصر هذا الجيل ولدت مواقع ووسائل التواصل الاجتماعي مثل MySpace و Facebook و Twitter (Cash et al.,2013).

في ضوء ما تقدم، تتجلى الحاجة إلى تنمية الوعي بالأمن السيبراني، والتخفيف من وطأة التهديدات لأمن المعلومات، لدى المستخدمين للإنترنت، وبخاصة المراهقين عبر برامج تدريبية وإرشادية، وعلى الرغم من تدخلات علم النفس السيبراني فإنه لايزال في المهد والبدايات، بيد أن البرامج التدريبية لتنمية الوعي بالأمن السيبرانى قد ظهرت معتمدة على تحديد العوامل النفسية الرئيسة المتعلقة بتحقيق الأمن السيبراني أو فشله (Bordoff et al.,2017).

وهذا ما حدا بالباحث إلى الاهتمام بضرورة تحقيق الأمن السيبرانى اعتمادًا على العنصر البشري؛ لخفض حدة التهديدات السيبرانية من خلال فنيات الإرشاد النفسي، ودوره الفعال في تنمية وعى المستخدمين للإنترنت، وبخاصة المراهقين تجاه مختلف مخاطر الهجمات السيبرانية.

مشكلة الدراسة:

يشهد العالم اليوم تطورًا سريعًا في تقنيات الاتصال واستخدام الإنترنت في جميع أنحاء العالم، فضلا عن التبادل المعلوماتي وصاحب هذا التزايد –أيضًا– تزايد الحروب السيبرانية التي لا تقل شراسة وخطورة عن الحروب التقليدية التي تصنعها الأسلحة، وأصبحت الهجمات الإلكترونية شائعة مثل الإنترنت نفسه، بل إنها تتزايد كل عام وتشير التقارير الإخبارية، ومقالات أكاديمية إلى تزايد حجم المخاطر والهجمات الإلكترونية وتنوعهما، واللتان تقترنان بشكل كبير بعدم فهم المستخدمين وإدراكهم لمخاطر الإنترنت وطرق التعامل معها (Raineri,& & Resig,2020).

وتجدر الإشارة في هذا السياق إلى أن بيئة الدراسة الحالية، والتي تتمثل في المملكة العربية السعودية والتي سببت الهجمات الإلكترونية فيها ضررًا كبيرًا على البنية التحتية، وتمثلت أبرز الحوادث الرئيسة في الهجمات التي استهدفت شركة أرامكو السعودية، وعطلت نشاطها لمدة شهر، ويعد هذا الأختراق الأكبر في التاريخ، وتسببت هذه البرمجيات الخبيثة في حدوث خلل مرة أخرى بالشركة نفسها في نوفمبر 2016، ويناير 2017 (إبراهيم،٢٠٢١).

وقد تبنت المملكة العربية السعودية منهجًا متكاملًا للأمن السيبرانى والعمل على تحقيق رؤية المملكة ٢٠٣٠ والأهداف الاستراتيجية الوطنية، وهو ما سيعزز من حماية فضائها السيبراني ومصالحها الحيوية، ويمكن من تحقيق رؤية المملكة ٢٠٣٠، كما أن تطوير مبادئ الأمن السيبرانى والعمل عليها في جميع الجهات الحكومية، والقطاع الخاص

والمجتمع؛ سيعزز من إدراك الجهات والأفراد ويزيد من مسئولياتهم في الحفاظ على أصولهم وخدماتهم الحيوية، ويعد التعاون أساسًا لهذه المنظومة (الهيئة الوطنية للأمن السيبراني، ٢٠٢١).

وعلى المستوى العالمي تُبذل جهودًا كبيرة لمواجهة مخاطر الإنترنت للمحافظة على المعلومات وسريتها وسلامتها وتوافرها، ضد الهجمات والتهديدات التي تمثل تحديًا في هذا العصر الرقمي، إذ قامت المنظمات في جميع أنحاء العالم باستثمارات ضخمة في التدابير المضادة التكنولوجية لأمن المعلومات، ومع ذلك فقد أخفقت كثيرٌ من هذه المؤسسات في حماية أصول المعلومات الخاصة بها، فقد يرجع ذلك إلى اعتمادها بشكل أساسي على الحلول التقنية فقط، والتي غالبًا تكون غير كافية (Raineri,& & Resig,2020).

وإنصافًا للواقع فإن عددًا كبيرًا من حوادث أمن المعلومات يرجع إلى استغلال العناصر البشرية التي تتسبب بشكل مباشر، أو غير مباشر في معظم الحوادث السيبرانية، لذا يصبح وعي الأفراد بأمن المعلومات (ISA) أحد الجوانب الحاسمة للحماية ضد السلوكيات غير المرغوب فيها (Khando et al.,2021).

ونود أن نوضح في هذا السياق، أن الجانب الإنساني للأمن السيبراني مازال يمثل أكبر التحديات أمام الباحثين والممارسين في جميع أنحاء العالم أثناء اتخاذ التدابير لتحسين أمن المعلومات، إذ تُعزى الغالبية العظمى من الحوادث السيبرانية إلى سلوك المستخدم نفسه، بل إن المهاجمين يعتمدون على استغلال العامل البشري؛ مما يشير إلى أن أساليب التقنية التكنولوجية لحماية المعلومات الحالية ليست كافية (Raineri,& & Resig,2020).

ومن الجدير بالذكر أن الدراسات النفسية التي تناولت الهجمات السيبرانية ومنها: دراسات (Bada, & Nurse,2020,Halevi et al.,2016,Odemis et al.,2022,) Seigfried-Spellar,et al.,2015 والتى أشارت إلى أن من أهم العوامل المؤدية إلى نجاح استهداف الهجمات السيبرانية هي أن كثيرًا من مستخدمي الإنترنت لا يزالون يفتقرون للوعى الكافي بتهديدات الإنترنت المختلفة والتي تُعرف -أيضًا- باسم "المخاطر الإلكترونية" فغالبًا ما يفتقد الأفراد الوعي بمخاطر الإنترنت؛ مما يؤثر سلبًا في استعدادهم لاستخدام تدابير الحماية الأمنية السيبرانية؛ لحفظ المعلومات والسرية على أجهزة الحاسوب لديهم.

وتأسيسًا على ما سبق فقد أصبح التأكيد على تنمية الوعي بالأمن السيبراني من الأهمية بمكان، وظهر ذلك جليًا في اهتمام المنظمات بتعزيز الوعي بالأمن السيبراني، مما يؤدي إلى تغيير المواقف الفردية والتنظيمية لإدراك أهمية الأمن والعواقب السلبية للتهديدات السبيرانية، فالوعي مهم للغاية في مجال أمن تكنولوجيا المعلومات والاتصالات؛ لأن تصرفات المستخدم يمكن أن تؤثر في المؤسسة بأكملها، إذ يتسبب عدم وعي المستخدم، وخاصة إن كان الفرد مسئولًا في مؤسسة ما في التعرض لأضرار جسيمة للمؤسسة (Yunos et al., 2016).

وأصبح الوعي بالأمن السيبراني، ضرورة للحفاظ على المراهقين من الوقوع بوصفهم ضحايا للتهديدات السيبرانية، والجرائم السيبرانية؛ مما يستدعي توعية المراهقين بسبل الأمن السيبرانى، والإجراءات التي تؤمن معلوماتهم الشخصية، والحفاظ على الخصوصية، وحمايتهم من التعرض للاحتيال والابتزاز الإلكتروني وتأمين الأجهزة الإلكترونية أثناء استخدامهم الإنترنت، إذ أضحى الأمن الإلكتروني ضمن مجالات الحاسوب، بل إن مؤسسات خاصة تقوم بإنتاج نظم حماية وتضع الحلول الشاملة لأى تهديد إلكترونى، والإفادة من آراء الخبراء المتخصصين في مجال الأمن السيبرانى، الذين يستخدمون موقع اليوتيوب، للقيام بدور توعوي من خلال نشر أخبار ومعلومات وقوانين تخص طرق الحماية من الجرائم المستحدثة، ورفع مستوى الوعي بالأمن السيبرانى لدى متابعيهم، وكون المراهقين يمثلون شريحة كبيرة من بين مستخدمي الثورة الرقمية بأدواتها المختلفة خاصة الإنترنت؛ وعليه ينبغي أن يكون الفضاء السيبرانى الذي يستخدمونه اليوم مكانًا أمنًا(متولي، ٢٠٢١).

ومن اللافت لانتباه الباحث أن التقارير العلمية أشارت إلى أن أكثر فئة عمرية مستخدمة للإنترنت؛ هم المراهقون من الجنسين، وهم من تمثلهم عينة الدراسة الحالية، إذ أوضحت نتائج الدراسة السعودية التى قام بها (الرويس، ٢٠١٣) أن نسبة استخدام المراهقين السعوديين للإنترنت كانت مرتفعة، إذ يستخدمه المراهقون من الجنسين في أكثر الأحيان دون موعد محدد، ويُعزى ذلك إلى تطور تقنيات تطبيقات مواقع التواصل الاجتماعي وسهولة استخدامها، ووفقًا لما يشهده مجال الهواتف الذكية والحواسيب من تطور تقني عالي المستوى.

وتشير البيانات إلى أن المراهقين من طلاب المدارس الثانوية الأمريكية غالبًا ما يتعرضون للإيذاء الإلكتروني على مواقع الشبكات الاجتماعية بنسبة (٦٠٪) وعبر الرسائل النصية أو منصات المراسلة الأخرى٤٠٪(Waasdorp & Bradshaw 2015) .

ومن هذا المنطلق جاءت الضرورة لبناء برنامج يسهم في زيادة الوعي بالأمن السيبراني؛ نظرًا لصعوبة التهديدات السيبرانية ونواتجها النفسية والاجتماعية.

ومن أجل نجاح فاعلية هذه البرامج فإنه يكون من المهم التفكير في التحديات التي تقف حائلا أمام تحسين سلوكيات أمن المعلومات للمواطنين والمستهلكين والموظفين، وتناول هذه التحديات من منظور علم النفس، إذ إن فهم كيفية إدراك الأفراد للمخاطر السيبرانية أمر بالغ الأهمية ويستدعى حملات فعالة للتوعية، تكون قادرة على بناء الفهم والامتثال لنصائح المتخصصين بالأمن السيبرانى والذى ينمى الرغبة في القيام بتغيير السلوك ونوايا المستخدمين للإنترنت أكثر من مجرد توفير المعلومات عن مخاطر الإنترنت من خلال تقنيات الإقناع، بما في ذلك "نداءات الخوف" المستخدمة على نطاق واسع في دراسات تنمية الوعي بالأمن السيبراني (Tosun et al.,2020)

يضاف إلى ما سبق نتائج بعض الدراسات السابقة وما طرحته من توصيات أبرزت جميعها أهمية الأمن السيبراني، وضرورة توعية المستخدمين للإنترنت به لحماية بياناتهم، والحفاظ على بيئة آمنة من الاختراقات وعمليات التجسس والابتزاز، ومن هذه الدراسات (المنتشري وحريري، ٢٠٢٠، والقيسى، ٢٠٢٠، إبراهيم، ٢٠٢١، و Richardson et,2020 ، وصائغ، ٢٠١٨، والقحطانى، ٢٠١٨).

ومن الأمور المهمة التي استرعت انتباه الباحث في الآونة الأخيرة على المستوى الغربي ازدهار البرامج التدريبة لتنمية الوعي بالأمن السيبراني من خلال تحديد العوامل الرئيسة المتعلقة بتحقيق الأمن السيبرانى أو فشله والتي قد تؤدي في حالة إلى النجاح بتغيير سلوك المستخدمين بشكل مناسب لتحسين ممارسات الأمان، ومن هذه الدراسات Proctor,2016, Banfield, (Alavi, 2016, Chang & Coppel, 2020).

وعلى الرغم مما تزخر به الدوريات العلمية المتخصصة من اهتمام ببرامج التدريب والبرامج الإرشادية؛ لتنمية الوعي بالأمن السيبراني، فإن القدر اليسير من هذا الاهتمام كان من نصيب الدراسات المحلية والعربية في هذا المجال.

وفي سياق الإدراك لمعالم تلك الأهمية تبرز أهمية تنمية الوعي بالأمن السيبراني لدى أكثر الفئات العمرية استخدامًا للإنترنت، وهم المراهقون على نحو خاص، على الرغم من ذلك تندُر الدراسات التي أجريت على عينات من المراهقين في البيئة العربية بوجه عام، والمحلية بصورة

خاصة –في حدود اطلاع الباحث–إذ لم يتسنَّ له الحصول على دراسة واحدة تناولت تنمية الوعي بالأمن السيبراني لدى المراهقين في المملكة العربية السعودية.

وتأسيسًا، على ما تم طرحه من دراسات إمبريقية واتجاهات نظرية للأمن السيبراني، فضلا عن معايشة الباحث لواقع الشباب السعودي –وخاصة المراهقين–وهو ما شجع الباحث نحو بناء برنامج إرشادي يهدف لتنمية الوعي بمفاهيم الأمن وآليات حفظ أمن المعلومات من خلال مجموعة من الخبرات والمهارات المرتبطة، ويمكن تحديد مشكلة الدراسة الحالية في السؤال الرئيس الذي نصه: ما مدى فاعلية برنامج إرشادي لتنمية الوعي بالأمن السيبراني لدى عينة المراهقين من طلبة التعليم الثانوي في مدينة جدة؟ **وينبثق من هذا السؤال الرئيس الأسئلة الفرعية التالية:**

١) ما مستوى الوعي بالأمن السيبراني لدى المراهقين من طلبة التعليم الثانوي في مدينة جدة؟
٢) ما الفروق الدالة إحصائيًا في رتب متوسطات درجات أفراد المجموعة التجريبية على مقياس الوعي بالأمن السيبراني قبل تطبيق البرنامج الإرشادي وبعده؟
٣) ما الفروق الدالة إحصائيًا في رتب متوسطات درجات أفراد المجموعة التجريبية ورتب متوسطات درجات أفراد المجموعة الضابطة على مقياس الوعي بالأمن السيبراني بعد تطبيق البرنامج الإرشادى؟
٤) ما الفروق الدالة إحصائيًا في رتب متوسطات درجات أفراد المجموعة التجريبية وعلى مقياس الوعي بالأمن السيبراني بين التطبيق البعدي والتتبعى للبرنامج الإرشادي (بعد شهر)؟
٥) ما التحديات النفسية التي تعوق فاعلية برامج الوعي بالأمن السيبراني وسيناريوهات المواجهة لهذه التحديات؟

أهداف الدراسة:

تهدف الدراسة الحالية إلى:

١) التعرف على مستوى الوعي بالأمن السيبراني لدى عينة المراهقين من طلبة التعليم الثانوى في مدينة جدة.

٢) التعرف على فاعلية برنامج إرشادي لتنمية مستوى الوعي بالأمن السيبراني لدى عينة المراهقين من طلبة التعليم الثانوي في مدينة جدة.

٣) التأكد من استمرار فاعلية البرنامج الإرشادي المقترح لتنمية مستوى الوعي بالأمن السيبراني لدى عينة المراهقين من طلبة التعليم الثانوي في مدينة جدة بعد شهر من تطبيق البرنامج.

٤) التعرف على التحديات النفسية لبرامج الوعي بالأمن السيبراني وسيناريوهات المواجهة.

أهمية الدراسة:

يمكن إيجاز الأهمية النظرية والتطبيقية للدراسة في النقاط التالية:

أولا الأهمية النظرية:

١- ترجع أهمية هذه الدراسة لتفاقم المهددات وكثرة الاختراقات وتواترها على كل الأصعدة وعلى المستويات كافة من الفرد إلى المؤسسات والوزارات والشركات، فقد بدأت الحكومات والشركات تعي تدريجيًا أخطار الجرائم السيبرانية، وأهمية الأمن المعلوماتي على الأمن الاقتصادي والسياسي للبلد، وعلى المصالح العامة.

٢- حداثة الدراسة ومواكبتها للتغير المحلي والعالمي في مجال الأمن السيبراني؛ إذ تعد الدراسة الأولي على المستوى المحلي والعربي (بحسب اطلاع الباحث) إذ تتناول فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني أي محاولة توظيف الإرشاد الوقائي في معالجة قضايا معاصرة.

٣- تنبع أهمية الدراسة الحالية من موضوعها ومن أهمية العينة التي تجري عليها وهم المراهقون في المجتمع السعودي، إذ إنهم من الفئات العمرية الأكثر استخدمًا للإنترنت ولوسائل التواصل الاجتماعي، وما ترتب عليها من آثار اجتماعية نتج عنها كثير من المشكلات النفسية والاجتماعية نتيجة لعدم الوعي بالأمن السيبراني.

ثانيًا الأهمية التطبيقية:

١- توجيه اهتمام الجهات المعنية مستقبلًا سواء في مجال الأمن والتعليم إلى أهمية إدراج مفاهيم الأمن السيبرانى ضمن البرامج التدريبية والتعليمية للمجتمع.

٢- رفع درجة الوعي لدى أفراد المجتمع السعودي بخصوص الأمن السيبرانى، وأهمية الالتزام بمفاهيم الأمن السيبرانى عند التعامل مع مصادر المعلومات المختلفة.

٣- يمكن الإفادة من نتائج الدراسة الحالية في إعداد برنامج إرشادي للتنمية بالامتثال للمحافظة على أمن المعلومات.

٤- تسليط الضوء على ما هو أبعد من الحاضر، حتى يتوفر لدى صانع القرار بناء برامج تدريبية وإرشادية تسهم في توعية أفراد المجتمع بالأمن السيبراني.

حدود الدراسة:

اقتصرت الدراسة الحالية على مدى فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني لدى المراهقين من مستخدمي الإنترنت وممن لديهم مستوى منخفض من الوعي بالأمن السيبراني من طلبة المدارس الثانوية من مدينة جدة في المملكة العربية السعودية في العام الدراسي ١٤٤٣/١٤٤٤هـ.

مصطلحات الدراسة وتعريفاتها الإجرائية:

البرنامج:

ويتمثل في تخطيط لمجموعة من الخبرات المترابطة والمتكاملة لتحقيق مجموعة من الأهداف من خلال أنشطة متنوعة، ويسعى البرنامج إلى تنمية الفرد الذي أعد من أجله البرنامج في جميع جوانب النمو العقلي والنفسي والجسمي والروحي ويتضمن أسلوب العمل وأسلوب التقييم (فرماوي، ١٩٩٢). ويعرف البرنامج إجرائيًا بأنه تخطيط لمجموعة من الإرشادات والمعلومات والخبرات والمهارات المرتبطة في إطار دقيق ومحدد، بهدف تنمية الوعي بالأمن السيبراني وإكساب الفرد المهارات والخبرات التي تساعده في ذلك.

الفاعلية:

هي القدرة على إحداث أثر حاسم في زمن محدد، وهي القدرة على القيام بعمل معين بنجاح دون تضييع الوقت والجهد أو هي القيام بعمل ما بطريقة جيدة والوصول إلى النتائج المتوقعة (مؤنس، ١٩٩٠).

الأمن السيبراني: (Cyber Security)

عرفه التقرير الصادر عن الاتحاد الدولي للاتصالات (2011): بأنه مجموعة من المهمات مثل: (تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات)يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين.

الوعي بالأمن السيبرانى: (Awareness of Cyber Security)

يعرف (Shaw et al.,2009) الوعي بالأمن السيبرانى على أنه: درجة الفهم من المستخدمين حول أهمية أمن المعلومات ومسؤولياتهم عن ممارسة مستويات كافية من مراقبة أمن المعلومات لحماية البيانات المنظمة والشبكات على نطاق واسع.

ويعرف الباحث الوعي بالأمن السيبراني إجرائيًا أنه: إدراك الطالب بما يدور حوله من جرائم إلكترونية واختراقات للبيانات والحسابات الشخصية؛ وهو السعى لتحقيق الأمن المعلوماتي، واتخاذ الإجراءات الاحترازية كافة؛ للوقاية من اختراق الأجهزة والبيانات وكل ما يتعلق بالتقنية ذات العلاقة ويتم تحديد مستوى الوعي بالأمن السيبراني من خلال المقياس المستخدم في الدراسة الحالية.

الإطار النظري للدراسة والدراسات السابقة

أولا الوعي بالأمن السيبراني:

١-تعريف الوعي بالأمن السيبراني:

للوصول إلى تعريف محدد لمفهوم الوعي بالأمن السيبرانى، يجب تعريف الوعي ثم الأمن ثم السيبراني ثم الأمن السيبرانى وصولاً إلى تعريف لمفهوم" الوعي بالأمن السيبراني على النحو التالي:

يعرف الوعي: بأنه إدراك الفرد لنفسه ولعناصر الموقف أو البيئة أو المجتمع الذي يحيط به، إذ يغيب الوعي أو يضطرب كما يحدث أثناء الغفلة أو النوم أو الإغماء (طه وقنديل، ٢٠٠٣).

أما تعريف الأمن: فهو نقيض الخوف، أي بمعنى السلامة، والأمن مصدر الفعل أَمِن أَمناً وأَماناً: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِن من الشر، أي سلِم منه. أما مصطلح السيبرانية الآن فهو واحد من أكثر المصطلحات تردداً في معجم

الأمن بمعنى الشخص وهي لفظة يونانية الأصل مشتقة من كلمة "cyber" بمعنى الذي يدير دفة السفينة، إذ تستخدم مجازًا للمتحكم "governor". فى التدابير المضادة المطلوبة" (Singer, & Friedman,2014)

أما مفهوم الأمن السيبرانى فيعد من المفاهيم الحديثة نسبيًا التي ظهرت في إطار الثورة الرقمية والتكنولوجية المعاصرة، التي أدت إلى تدفق المعلومات بشكل كبير وغير مسبق، مع تعدد وسائل الاتصال و مصادر المعلومات عبر أجهزة الحاسوب، وغيرها من الأجهزة المحمولة، وفي هذا السياق ظهر مفهوم الأمن السيبراني؛ ليعبر عن الجانب الأمني المرتبط بحماية تلك المعلومات، وشكل هذا المفهوم محل اهتمام العديد من المؤسسات الرسمية البحثية وقد وردت تعريفات عديدة لهذا المفهوم من حيث الناحية اللغوية والناحية الاصطلاحية كما يلى:

ويُعرف الأمن السيبراني وفقًا لتقرير الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام ٢٠١٠-٢٠١١ بأنه: "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات وتقنيات يمكن استخدامها لحماية البيئة السيبرانية".

كما يقصد بالأمن السيبراني "Security Cyber" حماية الأشياء من خلال تكنولوجيا المعلومات وذلك اختصار مثل الأجهزة والبرمجيات ويشار إليها " ICT Communication")

(Shaw et al.,2009)

ويعرف (Pusey& Sadera,2011) الأمن السيبرانى على أنه الإجراءات التقنية الهادفة لحماية البيانات، والهوية الشخصية، والمعدات التقنية من أي شكل من أشكال الوصول غير المسموح به إلى تلك المعلومات أو المعدات.

كما عرف (Amoroso, 2012) الأمن السيبرانى على أنه: وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة.

وعرف (Canongia & M&arino,2014) الأمن السيبراني بأنه: فن وجود مجتمع المعلومات واستمراريته، من خلال ضمان المعلومات وحماية أصولها وبنيتها التحتية في

الفضاء السيبراني.

كذلك يعرف (Craigen et al,2014) الأمن السيبراني على أنه ممارسة الدفاع عن أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة، ويعُرف أيضًا باسم أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكترونية.

ويعرف خليفة (٢٠١٧) الأمن السيبراني على أنه جميع الأدوات والسياسات، ومفاهيم الأمن، والضمانات الأمنية، والمبادئ التوجيهية، ومداخل إدارة المخاصر والإجراءات والتدريب وأفضل الممارسات والتقنيات التي يمكن استخدامها بهدف حماية الفضاء السيبراني، وتنظيم الأصول المعلوماتية للمستخدم.

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.

وعن تعريف الوعي بالأمن السيبرانى فقد تعددت التعريفات حول مفهوم الوعي المعلوماتي بشكل عام بتعدد المهتمين بهذا الموضوع، فقد ورد عدة التعاريف الخاصة بالوعي المعلوماتي الصادرة من منظمات معلوماتية، بيد أنها تنبثق جميعها من تعريف الوارد من اللجنة الرئاسية للوعي المعلوماتي جمعية المكتبات الأمريكية، ولمزيد من التوضيح سوف نركز على تحديد مفهوم الوعي بالأمن السيبراني.

أما عن تعريف الوعي بالأمن السيبرانى، فإننا نود أن نذكر تعريفات تم صياغتها لهذا المفهوم ومنها تعريف (Shaw et al., 2009.) للوعي بالأمن السيبرانى بأنه: درجة الفهم من المستخدمين حول أهمية أمن المعلومات ومسئولياتهم عن ممارسة مستويات كافية من مراقبة أمن المعلومات لحماية البيانات المنظمة والشبكات على نطاق واسع ويتم تحديد مستوى الوعي بالأمن السيبرانى من خلال مقياس الوعي بالأمن السيبرانى المستخدم في الدراسة الحالية

ويعرف (Niekerk Van & Ch&arman,2017) الوعي بالأمن السيبراني بأنه: مجموعة المعارف والمهارات والسلوك الفعلي والعلاقات المتبادلة بينها التي تساعد في حماية الأجهزة ووسائل التخزين المعلومات، والتعامل الآمن مع خدمات الإنترنت والبرمجيات.

وفي السياق نفسه عرف (Aldawood, & Skinner,2018) الوعي بأمن الإنترنت أو الوعي بالأمن السيبراني: إلى مدى معرفة مستخدمي الإنترنت بالتهديدات التي تواجهها شبكاتهم والمخاطر التي يقابلونها وأفضل الممارسات الأمنية لتوجيه سلوكهم.

٢-المفاهيم المرتبطة بالأمن السيبراني:

يوجد العديد من المفاهيم المرتبطة بالأمن السيبراني، ومن أهمها ما يلي:

الفضاء السيبراني:

عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI بأنه: فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية، فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكونة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أم مستعملين.

الهجمات السيبرانية:

وتعرف بأنها "فعل يقوض من قدرات شبكة الكمبيوتر ووظائفها، لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة، تمكن المهاجم من التلاعب بالنظام"

الردع السيبراني:

يعرف الردع السيبراني بأنه: "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية"

الجريمة السيبرانية:

وهي مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياته (السمحان،٢٠٢٠).

أمن المعلومات:

وهو حماية بيانات المؤسسة ويعتمد ذلك علي ثلاثة محاور رئيسة، ويرمز لها "CIA" وهي السرية "Confidentiality" سلامة المعلومة "Integrity" إتاحة المعلومة في أي وقت Availabilityوهو عبارة عن مجموع من الإجراءات التقنية والإدارية التى تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به بالتجسس أو اختراق الاستخدام أو سوء استغلال المعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات، كما تضمن تأمين البيانات الشخصية وحمايتها وسريتها وخصوصيتها

للمواطنين، كما تشمل استمرارية عمل حماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف (عيسى، ٢٠١٩).

٣-عناصرُ الأَمْن 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 (Shappie et al.,2020).

كذلك توجد ثلاثة عناصر أساسية، يعتمد عليها الأَمْن السيبرانيّ، وتتمثل فيما يلي:

السريَّة:

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 لإشخاص 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.

توافرُ المعلومات وإتاحتُه:

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

٣-فئات الأمن السيبرانى:

يمكن تقسيم الأمن السيبرانى إلى عدة فئات مشتركة.

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

٤-تهديدات السيبرانية:

تتعدد أشكال التهديدات السيبرانية بتعدد أهدافها، فهناك هجمات البرمجيات والأكواد الخبيثة التي تشمل هجمات الفيروسات وبرامج الاختراق وبرامج التجسس الإلكتروني، وكسر كلمات المرور، وهجمات تعطيل الخدمة، وهجمات الخداع للتمكن من الوصول إلى الأجهزة بشكل غير شرعي عبر رسائل تحتوي عناوين إنترنت تبدو موثوقة، وهجمات الهندسة الاجتماعية التي يستهدف المهاجم النواحي الاجتماعية والاهتمامات الشخصية للأفراد للسيطرة على ضحاياه بكسب ثقتهم والتقرب منهم؛ بهدف الحصول على معلوماتهم السرية وأموالهم، وهذا النوع من الهجمات من أكثر الهجمات انتشارًا في الأونة الأخيرة (البار والمرحبى، ٢٠١٨). ويمكن حصر التهديدات السيبرانية في الأنماط والأشكال التالية:

- **تهديدات سيبرانية للأجهزة المحمولة:** يركز هذا النوع على إيصال تهديد ما إلى نوع من أنواع الأجهزة المحمولة الإلكترونية المتصلة بشبكة الإنترنت، ويعد هذا النوع من أخطر التهديدات وأكثرها شيوعًا؛ بسبب انتشار الأجهزة المحمولة بكثرة حول العالم،

إذ أصبحت اليوم الجوالات المحمولة مع كل فرد صغير وكبير، ونادرًا ما نجد شخصًا لا يحمل هاتفًا محمولًا.

- **تهديدات التصيد الاحتيالي وهجماته:** يعتمد هذا النوع على الطريقة التي يتم بها، فهو أحد وأخطر أشكال الهندسة الاجتماعية التي تتم عبر البريد الإلكتروني، فمن خلالها يقوم المجرم الإلكترونى بإرسال رسالة نصية عبر البريد الإلكتروني في رابط ملغم من أجل الإيقاع بالضحية، وتكون الرسالة ودودة جميلة لا يوجد بها أي شكوك، بيد أن الأشخاص ضعيفي الخبرة في هذا المجال، يقعون في شراكها على الفور، والأمر الخطير في هذا النوع من التهديدات هو إرسال رسالة لآلاف الضحايا بشكل عشوائي من أجل الإيقاع بهم والحصول على المراد منهم.
- **سرقة المعلومات والهوية والانتحال:** تتم عملية سرقة المعلومات الرقمية وانتحال الهوية عن طرق برامج خاصة وأنظمة متخصصة في هذا المجال، يقوم من خلالها الهاكرز بسرقة البيانات والتجسس عليها من أجل الحصول على معلومات حساسة: مثل البطاقات الائتمانية، والحسابات البنكية، وغيرها من المعلومات المهمة.
- **المخاطر على الأجهزة الطبية الذكية:** حيث يركز هذا النوع من المخاطر على المنشآت الصحية والمستشفيات والمقرات الحكومية، والأمر الخطير في هذه المخاطر أنها، تركز على القطاع الصحي، الأمر الذي قد يهدد حياة الملايين من الأشخاص في غضون ثوانٍ معدودة، فعندما يكون الهجوم يهدف إلى إيقاف أجهزة التنفس التي تعمل بالمستشفيات عن العمل قد يؤدي ذلك الى خسائر بأعداد هائلة في الأرواح.
- **الهجمات على المصارف والبنوك:** وهي أخطر أنواع التهديدات السيبرانية، يتم من خلالها إيقاف أنظمة البنوك والمصارف عن العمل من أجل سرقة الأموال منها، أو بهدف سرقة معلومات مهمة جدًا، تخص المتعاملين مع البنوك.

ويضيف خميس(٢٠١١) أنوعًا أخرى من الهجمات السيبرانية وهي نشر الأفكار المتطرفة والتي تؤسس للأفكار المنحرفة عبر مواقع الإنترنت، وتوزيع المواد الإباحية عبر مواقع الإنترنت المختلفة، وهجمات انتحال الشخصية والتي تهدف لاستغلال المكانة

المجتمعية أو العلمية للشخص في الوصول إلى المعلومات أشخاص آخرين يثقون بتلك الشخصية، وهجمات التشهير وتشويه السمعة إلى الضحية من أجل ابتزازهم.

إلى جانب ذلك ذكر (Willard,2007) أنواعًا أخرى من الهجمات والمخاطر السيبرانية، وهى الإيذاء الإلكتروني وهى مجموعة السلوكيات التي يمكن تصنيفها على أنها عدوان سيبراني، وقد صنفها إلى سبعة أنواع من العدوان السيبراني وهى: (١) الملتهب (وهو الاتصال العدائي عبر الإنترنت)، (2) المضايقات (وهي الرسائل العدوانية المتكررة المرسلة للضحية)، (3)التنزه والخداع (وهو طلب معلومات شخصية من شخص ما ثم مشاركة تلك المعلومات إلكترونيًا مع الآخرين دون موافقة الفرد)، (4) الاستبعاد (وهو منع فرد عبر الإنترنت)، (5) انتحال الهوية (وهو انتحال شخصية الضحية وإبلاغ الآخرين إلكترونيًا بمعلومات سلبية أو غير مناسبة كما لو كانت من الضحية)، (6) المطاردة الإلكترونية (وهي استخدام الاتصالات الإلكترونية لمطاردة شخص آخر عن طريق إرسال رسائل تهديد متكررة)، (٧) إرسال رسائل جنسية (كتوزيع صور عارية لشخص آخر دون موافقة ذلك الشخص).

٥-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 وهي 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.

- ❖ خصائص الثالوث المظلم والتي تشمل على النرجسية والسيكوباتية والميكافيلية والتي تكمن وراء الدافع نحو إساءة استخدام الكمبيوتر وارتكاب الجرائم الإلكترونية (Maasberg et al,2020).
- ❖ البحث عن الإثارة والفضول والاهتمام بالبحث عن التشويق.

٦-بعض العوامل النفسية التي تعوق تحقيق الأمن السيبرانى:

تناولنا في الفقرات التالية العوامل النفسية التي تعوق تحقيق الأمن السيبرانى إذ يشير (Gcaza& von Solms,2017)، إلى أن تحقيق الأمن السيبراني لايقتصر -فقط-على مجرد التحكم التكنولوجي، بل إن الأمر يتعلق بالإنسان فهو النقطة المركزية في تحقيق الأمن السيبرانى، ولذلك تناول العلماء العوامل البشرية بوصفها عوامل ذات تأثير فعال في الأمن السيبرانى.

وقد ذكر (Ahram, &Karwowski,2019) أن العوامل البشرية لها جانب(نفسي وبيئى) ويمكن للمرء أن يتعرف إلى العوامل البشرية التي يمكن أن تسبب خطأ بشريًا، فمن تلك الجوانب النفسية الإرهاق وفقدان اليقظة والتعب والإلهاء في حدوث أخطاء متعمدة..

كذلك نقص معرفة التواصل، والرضا عن النفس والإلهاء ونقص الموارد، والضغط، والافتقار إلى الحزم والتوتر ونقص الوعي وكل هذه العوامل يمكن أن تؤثر سلبيًا على الأمن السيبراني، وهو ما يزيد من الاستهداف للتهديدات السيبرانية.

إضافة إلى ذلك وجود بعض التحيزات المعرفية والتي تتمثل في تضخيم المخاطر البسيطة مع التقليل من المخاطر الأكثر شيوعًا ومنها التقليل من المخاطر التي تقع ضمن تحويلات المالية مع المبالغة في تقدير المخاطر الخارجة عن سيطرتهم؛ من خلال إدراك المخاطر الشخصية على أنها أكبر من المخاطر المجهولة، والاعتقاد بأنهم أقل عرضة للخطر من أقرانهم، وهذه التحيزات تؤثر في سلوكيات الأمن السيبراني، فعلى سبيل المثال يتم إظهار الأفراد الذين يتجاهلون التحذيرات حول المخاطر السيبرانية على أنهم واثقون من قدرتهم على التقليل من عواقب الاختراقات الأمنية، وهناك أدلة على أن الأشخاص ذوى هذه التحيزات المعرفية لا يغيرون استخدامهم لمواقع الشبكات الاجتماعية، حتى لو سبق اختراقها كما أنهم لا يغيرون ممارساتهم الأمنية بعد الاختراق الأمني بيد أنهم يقومون ببعض التعديلات البسيطة مع الاعتقاد بأن هذه التغييرات، تحميهم من الهجمات المستقبلية إذ يوجد القليل من الفهم بأن

نواقل التهديد، تتغير وتتطور في كثير من الأحيان إذ تصبح أكثر تعقيدًا ويصعب اكتشافها(Herath & Rao .2016) .

كما أن بعض خصائص الشخصية تؤدي دورًا في الاستهداف للتهديدات السيبرانية: منها ما أشارت إليه دراستا إجلمان وبير (Egelman& Peer,2015) إلى أن الأفراد الأكثر انبساطًا يكونون أكثر عرضة لانتهاك سياسات الأمن السيبراني.

وكشفت دراسة (Ahram, &Karwowski,2019) عن وجود علاقة بين القابلية لهجمات الهندسة الاجتماعية وعوامل الشخصية الرئيسة: مثل سمات الضمير، والانبساط، والانفتاح على الخبرة، والمقبولية وكل هذا كلن أكثر عرضة لهجمات الهندسة الاجتماعية.

إلى جانب ذلك فإن الاندفاعية بوصفها سمة في الشخصية تتنبأ بسلوكيات المحفوفة بالمخاطر التي تعوق الأمن السيبرانى وخاصة أن سمة الاندفاعية كما عرفها (Coutlee et al,2014.) بأنها "الرغبة في التصرف بشكل عفوي دون التفكير في فعل ما وعواقبه.

كما أظهرت دراسة (Egelman& Peer,2015) أن ارتفاع سمة الاندفاعية ارتبطت ارتباطًا سلبيًا بالسلوكيات الأمنية.

وتجدر الإشارة إلى أن من العوامل النفسية التي تعوق تحقيق سلوكيات الأمن السيبرانى، هى إدمان الإنترنت وإساءة استخدام الكمبيوتر؛ فقد اهتمت الأبحاث بدراسة العلاقة بين إدمان الإنترنت بإمكان الانخراط في سلوكيات محفوفة بالمخاطر في مجال الأمن السيبراني. (Greenfield & Davis، 2002؛ Young & Case، 2004). وقد قدم (Stanton, 2002) (Pee et al.2008) وأشار (Weatherbee,2010) (Panko ,2010) وأجمعت هذه الدراسات على أن إدمان الإنترنت، يتسبب في مجموعة متنوعة من المشكلات، منها تنزيل تعليمات برمجية ضارة من دون قصد أو زيارة مواقع الويب المعرضة للخطر.

ويأتي عامل إدراك المخاطر الأمنية أو تفهمها بوصفه عاملا جوهريًا في تحقيق الأمن السيبرانى أو إعاقته، إذ يتم تفهم المخاطرة وإدراكها بطرق عديدة، ومعانٍ مختلفة بين الأشخاص، وإدراك المخاطر وهي مسألة مهمة لفهم سلوك الناس، في عديد من الأنشطة اليومية؛ إذ يمكن للأفراد التعامل مع مختلف المخاطر من خلال أحكامهم الذاتية، القائمة على معالجة المعلومات لمختلف المواقف والأمور المحيطة بالفرد، إذ يتأثر الناس بما لديهم من معتقدات، وخبرات شخصية والعادات والعلاقات الشخصية والاتصالات (Sjöberg et al. 2004).

٦-العوامل النفسية المساهمة في تحقيق الأمن السيبرانى:

يشير كل من (Gcaza& von Solms,2017) إلى أن تحقيق الأمن السيبراني لا يقتصر فقط على مجرد التحكم التكنولوجي، بل الأمر يتعلق بالإنسان بما لديه من عوامل نفسية فهو النقطة المركزية في تحقيق الأمن السيبرانى، من بين العوامل (النفسية) المتعلقة بالأمن السيبراني والتى يمكن تناول بعضا منها على النحو التالي:

القيم:

القيمة لها حساسية كبيرة في المحافظة على أمن المعلومات فقد أشارت دراسة (Hadlington,2017) إلى أن الاحترام والتسامح من القيم الإنسانية التى تعزز أمن المعلومات، كما توصلت دراسة (Parsons et al,2012) إلى أن قيمة الاحترام لها تأثير إيجابي في الوعي بتوفير الأمن السيبراني الشخصي: كما أن أن قيم التسامح والسلام لها تأثير إيجابي في الوعي بالأمن السيبراني في بيئات الألعاب عبر الإنترنت.

خصائص الشخصية:

تشير النتائج إلى أن الشخصية تؤدي دورًا مهمًا في فهم سلوكيات الأمن السيبراني، إذ تشير نتائج الدراسات إلى أن بنية الشخصية مرتبطة بسلوكيات الأمن السيبراني وأن يقظة الضمير والانفتاح قد يكونان بارزين بشكل خاص في هذه العلاقة (Shappie,et al.,2020)، ويشير (Aldawood, & Skinner, 2018) إلى أن كل من الانبساط والمقبولية ويقظة الضمير والاتزان الوجداني والتفتح على الخبرة ويقظة الضمير ، والاندفاعية بوصفها خصائص للشخصية هي المسؤولة عن أن يكون الفرد أقل محافظة على المعلومات السيبرانية وأكثر استهدافًا؛ ليكون ضحية لمختلف التهديدات السيبرانية.

الدراسات السابقة:

من خلال مسح قواعد البيانات عن موضوع الدراسة الحالية كان بإمكاننا تقسيمها إلى فئتين من الدراسات وفقًا لمتغيراتها:

دراسات تناولت الوعي بالأمن السيبراني:

هدفت دراسة العبيد (٢٠١٢) إلى التعرف إلى واقع ممارسة أساليب التوعية الأمنية في مدارس المرحلة الثانوية بالمملكة العربية السعودية، ومعرفة أهمية ممارسة أساليب التوعية الأمنية فيها، إذ تكون مجتمع الدراسة من معلمي ومشرفي ومديري المدارس الثانوية الحكومية

(بنين) بمدينة بريدة بمنطقة القصيم التعليمية بالمملكة العربية السعودية في الفصل الدراسي الأول من العام الدراسي ١٤٣٠/١٤٣١ هـ.، والبالغ عددهم (١٨٠٩)، وتوصلت الدراسة في نتائجها إلى أن واقع ممارسة أساليب التوعية الأمنية في مدارس المرحلة الثانوية بالمملكة العربية السعودية هو واقع ضعيف.

كما هدفت دراسة (Halevi et al.,2016) إلى الكشف عن العلاقة بين الوعي بالأمن السيبراني، وبعض المتغيرات الثقافية والشخصية والديموغرافية، وأجريت هذه الدراسة في أربعة بلدان مختلفة، وتقدمت وجهة نظر متعددة الثقافات للأمن السيبراني، وأظهرت النتائج أن الأمن السيبراني يتأثر بالسلوك والكفاءة الذاتية وموقف الخصوصية بالثقافة وسمات الشخصية التى برزت بوضوح بوصفها متغيرات نفسية، تتبئ بسلوك المستخدم المتعلق بالأمن السيبراني عبر الثقافات المختلفة.

وكان غرض دراسة (McCormac et al.,2017) هو فحص العلاقة بين الوعي بالأمن السيبراني وكل من العمر والجنس وسمات الشخصية والميل إلى المخاطرة، وتكونت عينة الدراسة من (٥٠٥) من العاملين الأستراليين، تم قياس الجوانب البشرية لاستبيان أمن المعلومات .(HAIS-Q) وتم قياس المتغيرات النفسية والديموغرافية من مقاييس خاصة بذلك، وكشفت الدراسة عن أن كل من العمر والجنس ويقظة الضمير، والمقبولية، والاستقرار العاطفي، والميل إلى المخاطرة وكل هذا يفسر التباين الجوهري بين الأفراد في الوعي بالأمن السيبراني.

سعت دراسة نورة القحطانى (٢٠١٩) 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"، في حين جاءت جريمة "الاحتيال الإلكتروني/النصب الإلكتروني" بوصفها أكثر جريمة، يتعامل معها الأمن السيبراني، في حين تعد التوعية الإعلامية للمجتمع حول طرقه من أهم طرق الوقاية المجتمعية لمشكلات الفضاء السيبراني، كما كشفت الدراسة عن وجود معوقات اجتماعية في تحقيق الوقاية للمجتمع السعودي، وكان أهم هذه المعوقات

هو التطور الهائل في نظم المعلومات، ووسائل التكنولوجيا التي يتعامل معها أفراد الأسرة دون المعرفة الكاملة لمشكلات هذه الوسائل وكيفية تجنبها، كما كشفت الدراسة عن عدم وجود فروق ذات دلالة بين الذكور والإناث في مستوى الوعي بالأمن السيبرانى.

كما هدفت دراسة (Potgieter, 2019) إلى الكشف عن السلوك المتعلق بالوعي بالأمن السيبراني لدى الطلاب في الجامعة المركزية للتكنولوجيا بجنوب أفريقيا، واشتملت العينة على (٤٣) طالبًا، منهم (٣٣) من الذكور، و(١٠) من الإناث، 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. وفي السياق نفسه، حاولت دراسة الصفحى وسناء عسكول (٢٠١٩) الكشف عن مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينه جدة، 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 (٠,٠٥) في درجة وعي معلمات الحاسب بالأمن السيبراني، تعزى لسنوات الخبرة (المؤهل العلمي) والدورات التدريبية.

وتناولت دراسة القحطانى (٢٠٢٠) مستوى الوعي بالأمن السيبراني في مدارس بوابة المستقبل الثانوية في المملكة العربية السعودية، وتكونت عينة الدراسة، من (١٠٠) مشارك من كل قسم، مما جعل إجمالي حجم العينة (٣٠٠) مشارك، طبق عليهم استبانة لقياس الوعي بالأمن السيبرانى، وكشفت الدراسة عن فعالية نموذج نظرية الألعاب لزيادة الوعي بالأمن السيبراني بين طلاب مدارس بوابة المستقبل الثانوية في المملكة العربية السعودية.

كما سعت دراسة نورة الصانع وآخرين (٢٠٢٠) إلى معرفة درجة وعي المعلمين بالأمن السيبراني وعلاقته بتطبيق أساليب حديثة لحماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية لديهم، وتكونت العينة من (١٠٤) معلمين ومعلمات في مدارس مدينة الطائف الحكومية والأهلية، وتم بناء مقياس لتحديد درجة الوعي بالأمن السيبراني لدى المعلمين في مدارس الطائف، وأساليب حماية الطلبة من مخاطر الإنترنت، وأساليب لتعزيز القيم والهوية

الوطنية لدى الطلبة، وأظهرت نتائج الدراسة ارتفاع وعي المعلمين بالأمن السيبراني في مجال حماية الأجهزة الخاصة والمحمولة من مخاطر الاختراق الإلكتروني والهجمات السيبرانية، وفي درجة استخدامهم لأساليب حماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية بمدنية الطائف من وجهة نظرهم في مجالات الأهداف الدراسية، وطرق التدريس، والأنشطة والمشاريع، وأساليب التقويم، وكشفت الدراسة عن وجود ارتباط موجب دال إحصائيا بين وعي المعلمين بالأمن السيبراني وكل من أساليب حماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية، كما كشفت الدراسة عن عدم وجود فروق ذات دلالة إحصائية بين استجابات المعلمين حول الوعي بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت تبعًا لنوع المدرسة، بينما وكشفت الدراسة عن وجود فروق ذات دلالة إحصائية بين استجابات المعلمين حول أساليب تعزيز القيم والهوية الوطنية تبعًا لنوع المدرسة لصالح المدارس الحكومية، وتوصلت الدراسة أيضا إلى عدم وجود فروق ذات دلالة إحصائية بين استجابات المعلمين حول الوعي بالأمن السيبراني، وأساليب حماية الطلبة من مخاطر الإنترنت وأساليب تعزيز القيم والهوية الوطنية تبعًا للجنس والتخصص والمؤهل العلمى وسنوات الخبرة في التدريس.

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

كذلك استهدفت دراسة مداخل التيمانى(٢٠٢١) 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، 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 هو ضعف الوعي لدى الأفراد ومشاركتهم المعلومات الشخصية مع الآخرين دون دراية ومعرفة بطبيعة عمل هؤلاء الأشخاص.

الفئة الثانية دراسات تناولت فاعلية برامج إرشادية وتدريبية لتنمية الوعي بالأمن السيبرانى:

هدفت دراسة (Banfield, 2016) إلى معرفة مدى فاعلية برنامج الوعي بالأمن السيبراني في تنمية السلوك الأمني لدى المستخدمين بشكل نهائي في المؤسسات متوسطة الحجم، وقد تكون مجتمع الدراسة من العاملين في مؤسسة متوسطة الحجم في الولايات المتحدة، واشتملت العينة على (٤٠٠) من العاملين في المؤسسات متوسطة الحجم، واستعانت الدراسة بالأداة المسحية الإلكترونية، التي تم توزيعها على المشاركين في الدراسة، وقد توصلت الدراسة إلى عديد من النتائج كان أهمها: عدم وجود تأثير ذي دلالة لتطبيق برنامج الوعي بالأمن السيبراني على تغيير السلوكيات الأمنية لدى العاملين، كذلك وجود علاقة ارتباطية بين برنامج الوعي بالأمن السيبراني والسلوك الأمني لدى المستخدم.

وحاولت دراسة (Bada et al., 2019) 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، كما أنه يمكن قياس التغير السلوكي في بيئة الأمن السيبراني من خلال خفض المخاطر، وليس من خلال ما يعرفه ولا يعرفه الأشخاص أو من خلال ما يتجاهله الشخص، كذلك يمكن تغيير السلوك من خلال حملات الوعي بالأمن السيبراني على قدرة الأشخاص على استيعاب النصائح وتطبيقها وتحفيزهم وتعزيز رغبتهم في تنفيذ النصائح، وإحداث التغيرات في الاتجاهات والسلوكيات.

كما هدفت دراسة (Chang & Coppel, 2020) إلى تسليط الضوء على برنامج ممول من من قبل جامعة موناش في أستراليا؛ لتعزيز الوعي بالأمن السيبراني في ميانمار، واعتمدت

الدراسة على المنهج التحليلي القائم على تحليل الممارسات المتعلقة ببناء الوعي بالأمن السيبراني من خلال برامج المساعدة في التطوير بتقديم برنامج أسترال؛ لدعم الوعي والقدرات المتعلقة بالأمن السيبراني في ميانمار، وتوصلت الدراسة إلى عدة نتائج كان أهمها: تمكن البرامج التي تعزز الوعي والكفاءة المتعلقة بالأمن السيبراني في برامج دعم التطوير على حماية المواطنين من التنمر الإلكتروني وخطابات الكراهية والاحتيال كما أنها تدعم المؤسسات التي تكافح الجرائم الإلكترونية والأنشطة الحاسوبية المشبوهة، كذلك تدعم البرامج التي تعزز الوعي بالأمن السيبراني القوة في الخدمات الإلكترونية بما في ذلك التعامل المصرفي النقال والحكومة الإلكترونية ونظام المدفوعات الإلكترونية.

وهدفت دراسة منال إبراهيم (٢٠٢١) إلى الكشف عن فاعلية برنامج تدريبي لتنمية الوعي بجوانب الأمن السيبراني لدى معلمات العلوم بالمرحلة الابتدائية في المملكة العربية السعودية، وتم استخدام المنهج التجريبي ذي التصميم شبه التجريبي ذي المجموعة الواحدة، وتمثلت أداة الدراسة في مقياس الوعي بجوانب الأمن السيبراني في التعليم عن بعد، وشمل مجتمع الدراسة معلمات العلوم بالمرحلة الابتدائية، وتكونت عينة الدراسة من (٣٠) معلمة، وطبق مقياس الوعي بجوانب الأمن السيبراني في التعليم عن بعد قبليًا، وبعد تدريب المعلمات على البرنامج المقترح خلال الفصل الدراسي الأول لعام ١٤٤١/١٤٤٢هـ، بواقع (١٠) جلسات تدريبية، ثم طبق المقياس بعديًا، وأسفرت نتائج الدراسة عن وجود فرق ذي دلالة إحصائية عند مستوى (٠,٠٥) بين متوسطي درجات المعلمات في التطبيقين القبلي والبعدي لمقياس الوعي لصالح التطبيق البعدي؛ ويدل هذا على فاعلية البرنامج التدريبي المقترح.

كذلك استهدفت دراسة متولي (٢٠٢١) معرفة معدل تعرض المبحوثين من عينة الدراسة لفيديوهات الأمن الإلكتروني، ورصد أكثر الفيديوهات التي يهتمون بمشاهدتها، معرفة دوافع التماس المبحوثين للمعلومات حول الأمن الإلكتروني من خلال اليوتيوب، وكذلك رصد مستوى الوعي بالأمن الإلكتروني لديهم، بعد تعرضهم لليوتيوب، ومعرفة التأثيرات المعرفية والوجدانية والسلوكية الناتجة عن التعرض لتلك الفيديوهات، وجاءت عينة الدراسة عمدية مكونة من (٣٠٠) مبحوث من المراهقين المصريين من طالب الفرقة الأولى من (١٧-١٨) عامًا، واعتمدت الدراسة على استمارة الاستبيان لجمع بيانات الدراسة حول دور اليوتيوب في تنمية وعي المراهقين بالأمن الإلكتروني، وقد كشفت نتائج الدراسة عن وجود معدل مرتفع لتعرض

المبحوثين من عينة الدراسة لفيديوهات الأمن الإلكتروني باليوتيوب، وجاءت حماية الحسابات الشخصية في مقدمة الفيديوهات التي يفضلها المبحوثون، كما توصلت الدراسة إلى وجود علاقة موجبة ذات دلالة إحصائية بين معدل تعرض المبحوثين لفيديوهات الأمن الإلكتروني باليوتيوب ومستوى الوعي بالأمن الإلكتروني لديهم، وكشفت الدراسة عن وجود علاقة موجبة ذات دلالة إحصائية بين دوافع التماس المبحوثين للمعلومات من خلال فيديوهات يوتيوب ومستوى الوعي بالأمن الإلكتروني لديهم، وكشفت الدراسة عن وجود علاقة موجبة ذات دلالة إحصائية بين معدل تعرض المبحوثين لفيديوهات الأمن الإلكتروني باليوتيوب، وتوصلت الدراسة إلى وجود علاقة موجبة ذات دلالة إحصائية، بين معدل ارتكاب جرائم إلكترونية ضد المبحوثين، ومعدل تعرضهم لفيديوهات الأمن الإلكتروني باليوتيوب.

تعقيب على الدراسات السابقة:

من خلال عرض الدراسات السابقة، يمكن للباحث استخلاص بعض الملاحظات التي قد تسهم في دعم تحقيق أهداف الدراسة وهي:

يوجد تباين ثقافي في الدراسات المعنية بتنمية الوعي بالأمن السيبرانى، تنتمي إلى مجتمعات ذات أطر ثقافية مختلفة، والذي يمكن أن تسهم على نحو ما في اختلاف النتائج المتعلقة بفهم المشكلة ونتائجها.

وثمة تناقض بين نتائج الدراسات السابقة بشأن الفروق بين الجنسين في الوعي بالأمن السيبراني فمثلًا كشفت دراسة نورة القحطانى (٢٠١٩) عن وجود فروق ذات دلالة بين الذكور الإناث في مستوى الوعي بالأمن السيبرانى والفروق في اتجاه الذكور، بينما انتهت دراسة (McCormac et al., 2017) إلى أن كل من العمر والجنس ليس لهما تأثير في تباين الأفراد في الوعي بالأمن السيبرانى.

وخلال مسح قواعد البيانات الإلكترونية أيضا لم يجد الباحث دراسة سعودية تناولت برنامجًا إرشاديًا لتنمية الوعي بالأمن السيبرانى لدى المراهقين من خلال برامج تدريبية إرشادية.

من جهة ثانية يوجد اتفاق بين نتائج الدراسات التي تناولت تنمية الوعي بالأمن السيبرانى على أهمية العامل البشري في المحافظة على أمن المعلومات، ومما سبق يقتضي ضرورة إجراء دراسة لتنمية الوعي بالأمن السيبرانى لدى المراهقين وعلى الأخص في البيئة السعودية.

فروض الدراسة:

في ضوء ما تم عرضه من تصورات نظرية، وأيضًا في ضوء ما بينته نتائج الدراسات السابقة، فإنه يمكن صياغة فروض الدراسة الحالية على النحو الآتي:

١) توجد فروق دالة إحصائيًا عند مستوى (٠,٠٥) بين الوسط الفرضي لمقياس الوعي بالأمن السيبراني.

٢) لا توجد فروق دالة إحصائيًا في رتب متوسطات درجات أفراد المجموعة التجريبية على مقياس الوعي بالأمن السيبراني، قبل تطبيق البرنامج الإرشادي وبعده.

٣) لا توجد فروق دالة إحصائيًا في رتب متوسطات درجات أفراد المجموعة التجريبية ورتب متوسطات درجات أفراد المجموعة الضابطة على مقياس الوعي بالأمن السيبراني بعد تطبيق البرنامج الإرشادي.

٤) لا توجد فروق دالة إحصائيًا في رتب متوسطات درجات أفراد المجموعة التجريبية وعلى مقياس الوعي بالأمن السيبراني، بين التطبيق البعدي والتتبعى (بعد شهر) للبرنامج الإرشادي.

منهجية الدراسة وإجراءاتها:

منهج الدراسة: لتحقيق أهداف الدراسة استخدم الباحث المنهج التجريبي القائم على التصميم شبه التجريبي، إذ تم تعيين عينة الدراسة علي مجموعتين (تجريبية وضابطة) تعيينًا عشوائيًا، ثم اختبار المجموعتين اختبارًا قبليًا وبعد ذلك خضعت المجموعة التجريبية للمتغير المستقل والذى مثله في الدراسة الحالية برنامج إرشادي لتنمية الوعي بالأمن السيبراني، لدى المراهقين من طلاب المرحلة الثانوية بمدينة جدة ومن خلال المقارنة القبلية والبعدية لنتائج أفراد المجموعة التجريبية وبعد فترة زمنية من تطبيق البرنامج، تم إجراء القياس التتبعي للمقارنة بين الاختبار البعدي والتتبعي علي المجموعة التجريبية، ويوضح الجدول(١) هذه الإجراءات.

(١) نوع التصميم التجريبي المستخدم

مجموعة تجريبية	قياس قبلي	المتغير المستقل تطبيق (البرنامج الإرشادي)	قياس بعدى	قياس تتبعى
مجموعة ضابطة	قياس قبلي	لم يتم تطبيق البرنامج	قياس بعدى	لا يوجد قياس تتبعى

٢-**مجتمع الدراسة:** تكون مجتمع الدراسة من عينة لطلاب المرحلة الثانوية بمدينة جدة في المملكة العربية السعودية.

٣-**عينة الدراسة:** اشتملت عينة الدراسة على عينتين هما:

أ) **العينة الاستطلاعية:** تم اختيار عينة من المراهقين لطلاب المدارس الثانوية الصف الثالث الثانوي ببعض مدارس مدينة جدة قوامها (١٠٩) طالبًا وكان متوسط أعمارهم (١٨,٥) سنة بغرض التحقق من الخصائص السيكومترية لمقياس الوعي بالأمن السيبراني. والجدول التالي يوضح المدارس التى سُحبت منها هذه العينة.

جدول(٢) يوضح توزيع العينة حسب المدارس الثانوية بجدة

المدارس	العدد	النسبة المئوية
مدارس قرطبة الأهلية القسم الثانوي	١٨	%١٦,٥٢
ثانوية السروات الأهلية	٣٣	%٣٠,٢٨
مدارس التعاون الأهلية القسم الثانوي	٦	**%٥,٥**
مدرسة الفيصلية الثانوية	١١	**%١٠,١**
مدارس الإخاء القسم الثانوي	٤١	%٣٧,٦
الإجمالى	١٠٩	%١٠٠

ب) عينة التدخل الإرشادي: تم استخدامهم لغايات عينة التدخل الإرشادي، ممن انطبقت عليهم شروط المشاركة في الدراسة الحالية، والتي تمثلت فيما يلي:

- الطلاب المنتظمون بالدراسة من الصف الثالث الثانوي.
- الطلاب الذين حصلوا على درجات منخفضة على اختبار الوعي بالأمن السيبراني.

وفيما يتعلق بعدد المشاركين من أفراد عينة الدراسة الأساسية التي جرى عليها تطبيق البرنامج الإرشادي وكانت مكونة من (٣٠) طالبًا، منهم (١٥) طالبًا من عدد أفراد المجموعة التجريبية، وعدد (١٥) طالبًا من المجموعة الضابطة ومن أجل غايات تحديد أفراد المجموعتين، تم اتباع الخطوات الآتية:

أ-تطبيق اختبار الوعي بالأمن السيبراني.

ب-التحقق من تكافؤ المجموعتين من حيث (درجة اختبار الوعي بالأمن السيبراني).

أدوات الدراسة:

اختبار الوعي بالأمن السيبراني: من إعداد نورة الصانع وآخرين(٢٠٢٠). ويتكون الاختبار من (٣٠) بندًا يغطى، بعدين هما: البعد الأول (الوعي بمفهوم الأمن السيبرانى) وعدده (٧) بنود، والبعد الثانى (طرق المحافظة على أمن المعلومات) وعدد بنوده (٢٣) بندًا لقياس الوعي بالأمن السيبراني، ويتمتع المقياس في صورته الأصلية بخصائص سيكومترية جيدة من الثبات والصدق، فمن ناحية الصدق تم التحقق من صدق الاختبار من قبل معده بطريقتين: هما الصدق الظاهري وصدق الاتساق الداخلي.

وأما الثبات، فقد تم التحقق من جزء الاختبار عن طريق ثبات ألفا، والذي بلغ ٠,٩١ ويتم تصحيح المقياس من خلال بدائل خمسة وهي: تنطبق تمامًا، تنطبق، محايد، لا تنطبق، لا تنطبق تمامًا، وكانت الدرجات من (١ إلى ٥).

وللتحقق من خصائص السيكومترية للاختبار في الدراسة الحالية:

طُبق الاختبار على عينة استطلاعية التي سبق ذكرها، إذ تم التحقق من صدق اختبار الوعي بالأمن السيبرانى وثباته بالطرق الآتية:

-**حساب الصدق** تم التحقق من صدق الاختبار بالطرق التالية:

صدق المحكمين: عُرض الاختبار على (٩) محكمين من أعضاء هيئة التدريس المتخصصين في علم النفس بكلية الآداب والعلوم الإنسانية بجامعة الملك عبدالعزيز، وقسم علم النفس بكلية العلوم الاجتماعية بجامعة الإمام؛ لإبداء آرائهم وملاحظاتهم حول مناسبة فقرات المقاييس ومدى وضوح صياغتها اللغوية، وكانت نسبة الاتفاق بينهم على عبارات كل المقاييس من ٨٠-٩٠ %.

صدق التمييز لفروق المقارنة الطرفية: قام الباحث بترتيب الدرجات الكلية على اختبار الحالية لأفراد العينة الاستطلاعية ترتيبًا تنازليًا وتم تقسيم الدرجات إلى طرفين علوي وسفلى، وتم أخذ أعلى (٢٥%) من درجات الأفراد وأقل (٢٥%) من درجات الأفراد على الاختبار، وتم حساب المتوسطات، والانحرافات المعيارية للدرجات، وحساب قيمة (ت)، واختبار مستوى الدلالة، كما يوضح الجدول (٣).

جدول (٣) يوضح دلالة الفروق بين المجموعتين الطرفيتين من العينة الاستطلاعية فى درجات اختبار الوعي بالأمن السيبراني

المقاييس	المراهقون				ت	الدلالة
	الأرباعى الأعلى٢٥%		الأرباعى الأدنى٢٥%			
	م	ع	م	ع		
الوعي بالأمن السيبرانى	٢٨	١,١	١٧,١	٢,٩	١١	٠,٠١

يشير الجدول (٣) إلى أن المتوسطات الحسابية والانحرافات المعيارية للإرباعي الأعلى في الدرجات الكلية لاختبار الوعي بالأمن السيبراني تكون أعلى من المتوسطات الحسابية والانحرافات المعيارية للإرباعى الأدنى للمقاييس نفسها، كما أن قيمة (ت) كانت دالة جميعها عند مستوى (٠,٠١)، مما يدل على أن مقاييس الدراسة، تتمتع بالقدرة على التمييز بين المستويين القوى والضعيف، مما يعنى تمتع الاختبار بدرجة مقبولة من الصدق.

– **حساب الثبات:** تم التحقق من ثبات الاختبار على أفراد العينة الاستطلاعية باستخدام عدة طرق منها: حساب معامل ثبات ألفا والتجزئة النصفية، إذ بلغت معاملات ثبات ألفا كرونباخ لدرجة الكلية للمقياس (٠,٧٨) وبعد الوعي بمفهوم الأمن السيبرانى نسبة(٠,٨٨) وبعد طرق المحافظة على أمن المعلومات(٠,٨٩)، ومعاملات ثبات التجزئة النصفية للاختبار ككل بنسبة (٠,٨٨)، تتسم جميع هذه المعاملات بالقبول.

برنامج إرشادي لتنمية الوعي بالأمن السيبراني:

البرنامج الإرشادي: من إعداد الباحث حيث اعتمد الباحث على النظرية المعرفية السلوكية CBT.

ويمكن وصف خطوات البرنامج وتطبيقه على النحو الآتي:

- **الهدف:** يهدف هذا البرنامج إلى تنمية الوعي بالأمن لدى المراهقين، وتتعدد أهداف البرنامج، سواء من حيث نظرته إلى كيفية إكساب المراهقين لمجموعة من الأفكار عن الأمن السيبرانى وأهميته إلى تقديم معلومات عن مختلف التهديدات السيبرانية، وكيفية المحافظة على أمن المعلومات على جهاز الحاسب الألى.

- ❖ الاطلاع على التراث النظري والإمبريقى، الذي يتناول الأمن السيبرانى، وطرق الوعي به.
- ❖ تم تطبيق اختبار الوعي بالأمن السيبراني على العينة (التدخل الإرشادى) وبناءً على النتائج تم تحديد حاجات العينة للبرنامج، اعتمادًا على مجالات المقياس والنسبة التي تم اعتمدها بوصفها حاجة إرشادية حوالي ٥٠% في كل بند من بنود اختبار الوعي بالأمن السيبراني.
- ❖ تم بناء البرنامج الإرشادي وتنظيم محتوياته.

الأسلوب الإرشادي المتبع في تطبيق البرنامج:

اطلع الباحث على عديد من الكتابات الأجنبية والعربية، ونماذج للبرامج التدريبية لتنمية الوعي بالأمن السيبراني؛ وذلك لاختيار الأسلوب الإرشادي للبرنامج، واعتمد الباحث على النظرية المعرفية السلوكية عند تصميم البرنامج، وقد اتبع الباحث أسلوب الإرشاد الجماعي Group Counseling; في تطبيق البرنامج الحالي إذ يؤدى الإرشاد الجماعي دورًا مهمًا في التقليل من حدة تمركز العميل حول الذات ويوفر الفرصة لتحقيق أهداف للتعلم التعاوني والعصف الذهني والامتثال للحفاظ على أمن المعلومات.

الاستراتيجيات والفنيات المستخدمة في البرنامج، وهي كالآتي:

المحاضرة، والمناقشة والحوار: وذلك لما تحققه من إيجابية في التفاعل بين أفراد المجموعة وتنمية الأساليب الصحيحة للمناقشة والحوار، ولعب الأدوار، والتنفيس الانفعالي، والتعزيز والتحفيز: وتكون الإثابة المعنوية، وبحسب ما تقتضيه المواقف أثناء الجلسات، والتحصين التدريجي.

الوسائل والأدوات المستخدمة في البرنامج الإرشادي: استعان الباحث بالأدوات التالية في تطبيق البرنامج: لابتوب، بطاقات التذكير، استخدام ساعات الإيقاف، جهاز بروجكتور، استخدام أقلام سبورة.

عدد جلسات البرنامج وزمنه: تكون البرنامج من (١٣) جلسة لمدة (٦) أسابيع و(٣) أيام، وكل أسبوع عبارة عن جلستين، وكل جلسة مدتها (٤٥) دقيقة في النصف الأول من العام الدراسي (٢٠٢٢م) ويوضح الجدول التالي ملخص لجلسات البرنامج:

جدول(٤) ملخص الجلسات

رقم الجلسة	عنوان الجلسة	الأهداف	الفنيات المستخدمة	زمن الجلسة	عدد الجلسات
١	التعريف بالبرنامج ((شرح البرنامج.	بنهاية الجلسة ينبغي على الطالب أن يكون على معرفة بخطوات البرنامج وأهدافه.	الحوار. مناقشة جماعية. تعزيز إيجابي.	٤٥ دقيقة	جلسة واحدة
٢	التعريف بالأمن السيبراني.	بنهاية الجلسة ينبغي على الطالب أن يكون قادرًا على أن: ١) يفهم المقصود بالأمن السيبراني. ٢) يحدد أهمية الأمن السيبراني. ٣) يتعرف على المفاهيم المرتبطة بالأمن السيبراني.	المحاضرة. المناقشة والحوار. العصف الذهني.	٤٥ دقيقة	جلسة واحدة
٣	التعريف بالوعي بالأمن السيبراني.	بنهاية الجلسة ينبغي على الطالب أن يكون قادرًا على ١) وصف طبيعة الوعي بالأمن السيبراني) ٢) ١-التعرف على مفهوم الوعي فى إطار تكنولوجيا المعلومات والاتصالات. ٣) ٢-تحديد مفهوم الوعي بالأمن السيبراني. ٤) ٣-معرفة أهمية الوعي بالأمن السيبراني.	المحاضرة. المناقشة والحوار. العصف الذهني. لعب الأدوار.		جلسة واحدة

٤	التعريف بالتهديدات السيبرانية.	بنهاية الجلسة ينبغي على الطالب أن يكون على معرفة بـ: ١) تحديد طبيعة التهديدات السيبرانية. ٢) تحديد أشكال التهديدات السيبرانية. ٣) معرفة أهم الآثار المترتبة على التهديدات السيبرانية	المحاضرة. المناقشة والحوار	٤٥ دقيقة	جلسة واحدة
٥	البرمجيات الضارة.	تهدف الجلسة إلى: ١) التعريف بطبيعة البرمجيات الضارة. ٢) رصد أبرز صور البرمجيات الضارة. ٣) التعرف إلى أبرز البرامج التي تحمي من الهجمات السيبرانية.	المحاضرة. المناقشة والحوار.	٤٥ دقيقة	جلسة واحدة
٦	علامات الخطر التي تدل على اختراق الجهاز.	بنهاية الجلسة ينبغي على الطالب أن يكون قادرًا على أن: ٥) يحدد علامات اختراق الجهاز. ٦) يقترح الإجراءات الأمنية للحفاظ على الجهاز من الاختراق. ٧) يناقش مواعيد العناية الدورية لصيانة الجهاز.	المحاضرة. المناقشة والحوار. العصف الذهني		جلسة واحدة

		٨) يتجنب مؤشرات اختراق جهاز الحاسوب.			
٧	مخاطر إدمان الألعاب الإلكترونية	بنهاية الجلسة ينبغي على الطالب أن يكون قادرًا على أن: ١) يتعرف على ماهية الألعاب الإلكترونية. ٢) تحديد الأضرار النفسية والصحية للألعاب الإلكترونية. ٣) إعطاء أمثلة واقعية على أضرار الألعاب الإلكترونية. ٤) تحديد كيفية الوقاية من مخاطر الألعاب الإلكترونية.	المحاضرة. المناقشة والحوار. العصف الذهني. التنفيس الانفعالي. التحصين التدريجي.	٤٥ دقيقة	جلسة واحدة
٨	طرق الحماية من التهديدات السيبرانية	بنهاية الجلسة ينبغي على الطالب أن يكون قادرة على أن: ١) يراقب الدخول وأنظمة كشف التدخل. ٢) تعرف معلومات عن الحماية البرمجية للمعلومات وأنظمة المعلومات. ٣) يتنبه العنصر البشري لتحركاته وتصرفاته وحماية	المحاضرة. المناقشة والحوار. التعزيز الإيجابي.	٤٥ دقيقة	جلسة واحدة

		للمعلومات الحساسة.			
٩	الإجراءات الوقائية لتحصين الحاسوب.	بنهاية الجلسة ينبغي على الطالب أن يكون قادرة على أن: ١) يوضح الإجراءات الوقائية لتحصين الحاسب الشخصي. ٢) يحدد الإجراءات الوقائية لتحصين الهاتف الذكي. ٣) يتمهر في اتباع الإجراءات الوقائية لتحصين الحاسب. ٤) يطرح أمثلة للإجراءات الوقائية لتحصين الحاسوب.	المحاضرة. المناقشة والحوار. التعزيز الإيجابي.	٤٥ دقيقة	جلسة واحدة
١٠	(المعرفة بالقوانين وتشريعات المملكة العربية السعودية لمكافحة الجرائم المعلوماتية.	بنهاية الجلسة ينبغي على الطالب أن يكون قادرة على أن: ١) يدرك مفهوم الجريمة الإلكترونية ٢) يعرف الضوابط الرئيسة للأمن السيبرانى في المملكة العربية السعودية. ٣) يسلط الضوء على قانون مكافحة الجرائم الإلكترونية.	المحاضرة. المناقشة والحوار. العصف الذهني. ورشة العمل.	٤٥ دقيقة	جلسة واحدة

		٤) يتبين خطورة الجرائم الإلكترونية			
١١	(تعزيز الوعي بطرق المحافظة على نظام الأمن السيبراني)	١-تحقيق الامتثال لرأي الخبراء بشأن حماية أنظمة المعلومات. ٢-التوعية لتحديث برنامج الحماية من الفيروسات. ٣-التوعية باستخدام برنامج الحماية. ٤-التوعية بعمل نسخة احتياطية للملفات.	المحاضرة. المناقشة والحوار. التعزيز الإيجابي.	٤٥ دقيقة	جلسة واحدة
١٢	التقييم	١-بيان مدى الإفادة من البرنامج الإرشادي. ٢-توضيح كيفية الاحتفاظ بالمكاسب المحققة. ٣-تهيئة الطلاب لإنهاء البرنامج الإرشادي.	المناقشة الجماعية والحوار. العصف الذهني. ورشة العمل وعرض الآراء		جلسة واحدة
١٣	(ختام البرنامج الإرشادي)	١-ممارسة جلسة ختامية. ٢-مناقشة إيجابيات البرنامج الإرشادي وسلبياته. ٣-إجراء التطبيق البعدي لمقاييس الدراسة.	المناقشة الجماعية والحوار. العصف الذهني. عرض الآراء	٤٥ دقيقة	جلسة واحدة

تقويم البرنامج الإرشادي: وضع الباحث التقويم التالي:

القياس القبلي: من خلال تطبيق اختبار الوعي بالأمن السيبراني، والذي قدم لأفراد العينة وهم مجوعة الطلاب (الضابطة والتجريبية) قبل بداية تطبيق البرنامج الإرشادي.

القياس البعدى: قياس تطبيق اختبار الوعي بالأمن السيبراني، قدم لمجموعة الطلاب (الضابطة والتجريبية) بعد تطبيق البرنامج الإرشادي بهدف التأكد من فاعلية البرنامج. المعد في تنمية الوعي بالأمن السيبراني.

ج-**القياس التتبعى:** قياس اختبار الوعي بالأمن السيبراني، قدم للمجموعة (التجريبية)، بعد شهر من تطبيق البرنامج الإرشادي؛ بهدف التأكد من استمرار فاعلية البرنامج المعد لتنمية الوعي بالأمن السيبراني.

ث-المقارنة بين القياس القبلي والقياس البعدى، والقياس التتبعى.

خامساً-الأساليب الإحصائية: اختبار (ت) واختبار مان وتنى واختبار ولكوكسن.

عرض نتائج الدراسة ومناقشتها:

استعرض الباحث النتائج التي توصل إليها وفقًا للفروض التي طرحها بوصفها إجابة مؤقتة لتلك التساؤلات، كما أن الباحث يناقش كل نتيجة توصل إليها، بالإضافة إلى مناقشة عامة لتلك النتائج. وكان ذلك على النحو التالي:

نتائج الفرض الأول ومناقشتها: ينص الفرض الأول على أنه "توجد فروق دالة إحصائيًا عند مستوى(٠,٠٥) بين الوسط الفرضي لاختبار الوعي بالأمن السيبرانى، وللتحقق من صحة هذا الفرض، استخدمت الدراسة الحالية (اختبارات) للعينة الواحدة One-Sample T Test ويتم عرض النتائج بالجدول (٥)

جدول(٥) الاختبار التائى لعينة ومجتمع لإيجاد الفروق بين الوسط الفرضى لمقياس الوعي بالأمن السيبراني ومتوسط أفراد العينة(ن=١٠٩)

الوسط الفرضي	متوسط العينة	ن	درجة الحرية	قيمة ت المستخرجة	مستوى الدلالة
١٢٩,٤	٩٥,٤	١٠٩	١٠٨	٢,٩	٠,٠٠

يتبين من الجدول(٥) أن المتوسط الحسابي لدرجات العينة على مقياس الوعي بالأمن السيبراني بلغ (٩٥,٤)، في حين بلغ المتوسط الفرضي (١٢٩,٤) وهذا يعنى وجود فروق ذات دلالة إحصائية في اتجاه المتوسط الفرضى؛ مما يعنى أن وعى أفراد العينة بالأمن السيبرانى كان ضعيفًا، وتتفق هذه النتيجة مع نتائج دراسة التيمانى(٢٠٢١) ونتائج دراسة منال إبراهيم (٢٠٢١) ونتائج دراسة (Alharbi& Tassaddiq,. 2021) التي كشفت عن وجود مستوى منخفض من الوعي بالأمن السيبرانى، وفى المقابل تتناقض هذه النتيجة مع نتائج دراسات كشفت عن وجود مستوى مرتفع من الوعي بالأمن السيبراني، منها علي سبيل الذكر دراسة نورة القحطانى (٢٠١٩) التي كشفت عن مستوى مرتفع من الوعي بالأمن السيبرانى لدى

طلاب الجامعات السعودية وطالباتها، ومع دراسة الصانعي وآخرين (٢٠٢٠) التي كشفت عن درجة من الوعي الكبيرة جدًا في مجال التعامل الآمن مع خدمات الإنترنت مع نتيجة دراسة (McCormac et al.,2017) والتي توصلت إلى ارتفاع مستوى الوعي بالأمن السيبراني.

وهذه النتيجة تمثل إشارة واضحة إلى أن المراهقين من أفراد عينة الدراسة الحالية الذين يغفلون كثيرًا عن مفاهيم الأمن السيبرانى ومتطلباته، على الرغم من أن نسبة استخدام المراهقين السعوديين للإنترنت مرتفعة، إذ يستخدمه المراهقون من الجنسين في أكثر الأحيان دون موعد محدد ووفقًا لما أشارت إليه دراسة (الرويس، ٢٠١٣).

نتائج الفرض الثاني ومناقشتها: ينص الفرض الثاني على أنه "توجد فروق دالة إحصائيًا في رتب متوسطات درجات أفراد المجموعة التجريبية على اختبار الوعي بالأمن السيبراني قبل تطبيق البرنامج الإرشادي وبعده" وللتحقق من صحة هذا الفرض قام الباحث باستخدام اختبار ويلكوكسون للرتب ذات الإشارة (Wilcoxon Signed Ranks Test) والجدول التالي يوضح نتائج ذلك:

جدول (٦) يبين نتائج اختبار ويلكوكسون للفروق بين درجات المجموعة التجريبية على اختبار الوعي بالأمن السيبراني للقياس البعدي والقبلي على المجموعة التجريبية.

المجال	القياس	الرتب	ن	متوسط الرتب	مجموع الرتب	قيمةZ	الدلالة
الوعي بمفهوم الأمن السيبرانى	قبلي	الرتب السالبة	9	6.89	62.00	-2.585	.010
	بعدى	الرتب الموجبة	2	2.00	4.00		
		التداخلات	4[c]				
		الإجمالي	15				
طرق المحافظة على أمن المعلومات	قبلي	الرتب السالبة	0[a]	.00	.00	-3.414-	.001
	بعدى	الرتب الموجبة	15[b]	8.00	120.00		
		التداخلات	0[c]				
		الإجمالي	15				

يشير الجدول(٦) إلى وجود فروق دالة إحصائيًا عند مستوى دلالة (٠,٠٠١) بين درجات القياسين البعدي والقبلي في اختبار الوعي بالأمن السيبراني بعد تطبيق البرنامج الإرشادي في اتجاه القياس البعدي: بمعنى أن درجات أفراد المجموعة التجريبية في القياس البعدي على اختبار الوعي بالأمن السيبرانى كانت أعلى من درجات القياس القبلي للمجموعة نفسها، وقد جاءت هذه النتيجة في الاتجاه المتوقع وهو ما يمثل حدث تحسنٍ في مستوى الوعي بالأمن السيبراني لدى أفراد المجموعة التجريبية بعد تطبيق البرنامج الإرشادي، وتؤكد هذه النتيجة فاعلية البرنامج الإرشادي، وأنه يؤدي إلى تحسين مستوى الوعي بالأمن السيبراني، إذ يمكن تفسير هذه النتيجة بأن البرنامج الإرشادي قد أتاح الفرصة أمام أفراد المجموعة التجريبية لإمكان التعرف على الأمن السيبرانى من خلال ما تم توفيره بالبرنامج الحالي من أنشطة متكاملة تختص بالأمن المعلوماتي؛ تعزز الحماية والتثقيف بالأمن السيبرانى، وكذلك توفير فيديوهات تعليمية حول مخاطر الأمن السيبرانى وتهديداته، ووجود تعليمات للحفاظ على الأمن السيبرانى، كما تجلت المشاركة الإيجابية للطلاب بالبرنامج الإرشادي في تنمية وعيهم للحفاظ على بيئة إلكترونية آمنة، من خلال اتباع الإجراءات اللازمة لتأمين المعلومات، والعمل على تطبيق ذلك للعمل بشكل مستمر، وجاءت هذه النتيجة متسقة مع نتائج دراسة إبراهيم (٢٠٢١) التي أسفرت عن وجود فرق ذي دلالة إحصائية عند مستوى (٠,٠٥)، بين متوسطي درجات المعلمات في التطبيقين القبلي والبعدي لمقياس الوعي لصالح التطبيق البعدي، ومع نتائج دراسة متولي (٢٠٢١) التي كشفت عن وجود علاقة ارتباطية إيجابية ذات دلالة إحصائية، بين معدل تعرض المبحوثين لفيديوهات الأمن الإلكتروني باليوتيوب، ومستوى الوعي بالأمن الإلكتروني لديهم.

وتتسق النتيجة الحالية مع نتائج دراسة (Bada et al., 2019) التي كشفت عن فاعلية برنامج تدريبى في تعزيز الممارسات المتعلقة بالتفكير والثقافة المرتبطة بالأمن السيبراني، ومع نتائج دراسة (Chang & Coppel, 2020) التي كشفت عن قدرة برنامج تدريبي لتعزيز الوعي بالأمن السيبراني لدى العاملين في البنوك، في المقابل تناقضت النتيجة الحالية مع نتائج دراسة (Banfield, 2016) التى كشفت عن عدم وجود تأثير ذي دلالة لتطبيق برنامج الوعي بالأمن السيبراني قي تغيير السلوكيات الأمنية لدى العاملين. ومع نتائج من دراسة

(Proctor,2016) والتي توصلت إلى عدم فعالية برنامج تدريبي لتنمية الوعي بالأمن السيبراني.

نتائج الفرض الثالث ومناقشـــتها: والذي نصـــه "لا توجد فروق دالة إحصـــائيًا في رتب متوســـطات درجات أفراد المجموعة التجريبية ورتب متوســـطات درجات أفراد المجموعة الضـابطة على مقياس الوعي بالأمن السـيبرانى بعد تطبيق البرنامج الإرشـادي" للتحقق من صـحة هذا الفرض قام الباحث باستخدام اختبار مان ويتني للفروق بين مجموعتين مستقلتين وكانت النتائج كما في الجدول (٧)

جدول (٧) يبين نتائج اختبار مان وتني للفروق بين رتب درجات المجموعتين التجريبية والضابطة في مقياس الوعي بالأمن السيبراني بعد تطبيق البرنامج الإرشادي.

المجال	المجموعة	العدد	متوسط الرتب	مجموع الرتب	قيمة Z	مستوى الدلالة
الوعي بمفهوم الأمن السيبرانى	تجريبية	١٥	20.07	301.00	-2.891-	.004
	ضابطة	١٥	10.93	164.00		
	الإجمالى	٣٠				
طرق المحافظة على أمن المعلومات	تجريبية	١٥	8.00	120.00	-4.691	0.00
	ضابطة	١٥	23.00	345.00		
	الإجمالى	٣٠				

يتبين من الجدول السابق وجود فروق دالة إحصائيًا عند مستوى دلالة (٠,٠٠١) بين درجات المجموعتين التجريبية والضابطة في اختبار الوعي بالأمن السيبراني بعد تطبيق البرنامج الإرشادي في اتجاه المجموعة التجريبية: بمعنى أن درجات أفراد المجموعة التجريبية على اختبار الوعي بالأمن السيبراني، كانت أعلى من درجات المجموعة الضابطة، ونعزو هذه النتيجة إلى الأثر الإيجابي للبرنامج الإرشادي المعتمد على مجموعة من الجلسات المخططة والمنظمة والمتتابعة زمنيًا، ومن خلال استخدام عدة فنيات؛ بهدف تنمية الوعي بالأمن السيبراني، وهذه الفنيات مثل: المحاضرة، المناقشة، الحوار، العصف الذهني، ورشة العمل.

من جهة ثانية، وفرت هذه الفنيات فرصًا مناسبة وتجارب حية عاشها أفراد المجموعة التجريبية طوال انتظامهم في البرنامج، واكتسابهم لجملة من الممارسات كانت لازمة للمحافظة على أمن المعلومات والوعي بمختلف التهديدات السيبرانية، كما أن أفراد المجموعة التجريبية

قد شاركوا بنشاط فعال في الجلسات الإرشادية، فلم يكونوا مستقبلين فقط، بل إنهم مارسوا وتفاعلون تفاعلًا مباشرًا من خلال الأداء العلمي تحت إشراف الباحث وتوجيهه، وتتفق هذه النتيجة مع عديد من الدراسات: ومنها دراسة (Bicak et al,2015) التي خلصت إلى وجود فروق بين المجموعة الضابطة والتجريبية من طلاب الدراسات العليا في مستوى الأمن السيبرانى، وتتفق هذه النتيجة مع نتائج دراسة (Pike et al. 2020) والتي توصلت إلى فاعلية برنامج قائم على التعليم غير المنهجي والحقائب التعليمية في تنمية الوعي بالأمن السيبراني.

نتائج الفرض الرابع ومناقشتها:

والذي نصه "لا توجد فروق دالة إحصائيًا في رتب متوسطات درجات أفراد المجموعة التجريبية وعلى اختبار الوعي بالأمن السيبراني بين التطبيق البعدي والتتبعى للبرنامج الإرشادي **(بعد شهر)**" وللتحقق من صحة هذا الفرض قام الباحث باستخدام اختبار ويلكوكسون للرتب ذات الإشارة (Wilcoxon Signed Ranks Test) والجدول التالي يوضح نتائج ذلك:

جدول(٨) يبين نتائج اختبار ويلكوكسون للفروق بين درجات المجموعة التجريبية على مقياس الوعي بالأمن السيبرانى بين القياس البعدي والتتبعى على المجموعة التجريبية.

المجال	القياس	الرتب	ن	متوسط الرتب	مجموع الرتب	قيمةZ	الدلالة
الوعي بمفهوم الأمن السيبرانى	قبلي	الرتب السالبة	5	3.50	17.50	-1.633	.102
	بعدى	الرتب الموجبة	1	3.50	3.50		
		التداخلات	9[c]				
		الإجمالي	15				
طرق المحافظة على أمن المعلومات	قبلي	الرتب السالبة	5[d]	4.00	20.00	-.302	.763
	بعدى	الرتب الموجبة	3[e]	5.33	16.00		
		التداخلات	7[f]				
		الإجمالي	15				

يشير جدول(٨) إلى عدم وجود فروق ذات دلالة إحصائية بين القياس البعدي والتتبعي في الوعي بالأمن السيبراني بأبعاده المختلفة، وهذا يدل على بقاء تأثير البرنامج في تنمية الوعي بالأمن السيبراني لدى أفراد المجموعة التجريبية. وعدم زوال هذا التأثير بين التطبيقين البعدي والتتبعي.

ويمكن القول أن فنيات البرنامج الإرشادي لدى أفراد المجموعة التجريبية أسهمت في تنمية الوعي بالأمن السيبرانى لديهم؛ من خلال البرنامج الإرشاد القائم على فنيات مختلفة أهمها الحوار والمناقشة والمحاضرة والعصف الذهني في مختلف الجلسات.

كما يرجع استمرار تأثير البرنامج في تنمية الوعي بالأمن السيبراني لدى المجموعة التجريبية إلى محتوى البرنامج الذي تم تدريبهم عليه، وما تضمنه من معلومات بشأن التهديدات السيبرانية، وكيفية المحافظة على أمن المعلومات وطرق الوقاية من الاختراق والمعرفة بالتشريعات القانونية للجرائم والاختراقات السيبرانية، حيث أسهم ذلك في تنمية الوعي بالأمن السيبرانى لدى أفراد المجموعة التجريبيبة.

كما يعود السبب في استمرار فعالية البرنامج إلى ما قام به الباحث أثناء البرنامج من توفير بيئة آمنة مشجعة على الحوار قامت على الود والألفة، وهو ما حاول الباحث توفيره أثناء الجلسات والتى أسهمت بشكل أو بآخر فى استمرار فاعلية البرنامج بعد شهر من تطبيقه على المجموعة التجريبية.

إضافة إلى ذلك يدعم هذه النتيجة ما أشارت إليه نتائج دراسات المنتشري وحريري2020، والقحطاني 2019، والصحفي وعسكول 2019، وصائغ، 2018).

توصيات الدراسة:

في ضوء النتائج الحالية يوصى الباحث بما يلي:

١) تفعيل دور البرامج الإرشادية والتدريبية التي تهدف لتنمية الوعي بأصول التعامل مع الإنترنت، ومواقع التواصل الاجتماعي ومخاطر الإنترنت لمختلف الفئات العمرية من مستخدميه.

٢) دمج الأمن السيبرانى ضمن المقررات الدراسية في المدارس والجامعات.

٣) زيادة البحوث والدراسات النفسية بشأن العوامل النفسية (المعرفية والمزاجية) وتوضيح دورها في المحافظة علي أمن المعلومات السبيرانية.

٤) عمل دورات لرجال الأمن السيبرانى بشأن التوعية بالعوامل البشرية المسئولة عن قيام الفرد بالتهديدات السيبرانية، كذلك العوامل البشرية الكامنة وراء عدم المحافظة على أمن المعلومات.

٥) يمكن أن تكون برامج التوعية والتدريب في مجال الأمن السيبراني جزءًا من الأمن القومي، ويجب أن تكون منظمة بشكل جيد، لتزويد الناس بالمعرفة الأساسية للأمن السيبراني، من خلال التركيز على البيئات التعليمية وتحليل الوعي الأمني لدى مستخدمي الإنترنت بشكل دوري، وبوساطة عمل خطة شاملة للوعي الأمني والتدريب.

المراجع

إبراهيم، منال حسن محمد (٢٠٢١) الوعي بجوانب الأمن السيبرانى في التعليم عن بعد. المجلة العلمية لجامعة الملك فيصل للعلوم الإدارية، ٢٢(٢)، ٢٩٩-٣٠٧

البار، عدنان مصطفى والمرحبى، مصطفى (٢٠١٨) أمن المعلومات والأمن السيبرانى /Users/Dell/Downloads/Article-of-this-week-DrAdnan-ALBAR-and-MrKhalid-Al-Marhabi-Jan-2018.pdf

التيماني، مداخل زيد عبدالرحيم (٢٠٢١) واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني. مجلة الجمعية المصرية للأخصائيين الاجتماعيين، ٦٧ (١)، ٢٦٣-٢٧٨

السرحان، حسنين عبد المهدى. والمشاقبة، محمد ناصر (٢٠٢٠). أثر تطبيق سياسية الأمن السيبرانى على جودة المعلومات. رسالة ماجستير رسالة غير منشورة. جامعة اليرموك. الأردن.

السمحان، منى عبد الله (٢٠٢٠). متطلبات تحقيق الأَمْن السيبرانيّ لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، ع١١١

الشهري، حسن أحمد (٢٠١٧) قانون دولي موحد لمكافحة الجرائم الإلكترونية (تصور مقترح . المجلة العربية للدراسات الأمنية والتدريب، ٢٧ (٥٣)، ١-٩٠.

الصانع، نورة (٢٠٢٠) وعي المعلمين بالأمن السيبرانى وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. مجلة كلية التربية: جامعة أسيوط -كلية التربية، ٣٦(٦)٤١-٥٧

الصانع، نورة عمر؛ عسران، عواطف سعد الدين؛ السواط حمد بن حمود بن حميد؛ أبو عيشة، زاهدة جميل نمر؛ سليمان، إيناس السيد محمد (٢٠٢٠). وعي المعلمين بالأمن السيبرانيّ وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم، مجلة البحث العلمي في التربية ٣٦(٦)، ٤١-٩٠.

الصحفي، مصباح أحمد حامد والعسكول، سناء صالح (2019) مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة، مجلة

البحث العلمي في التربية، كلية البنات للآداب والعلوم والتربية، جامعة عين شمس،٢٠(١٠)، ٤٩٣- ٥٣٤

الظويفري، مشاعل شيب (٢٠٢١)، واقع الأمن السيبرانى وزيادة فاعليته في التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية، المجلة الدولية للدراسات التربوية والنفسية، المجلد العاشر العدد(٣) ٦٣٥-٦٥٥.

العريفي، محمد سعود (1996) العلاقة بين الوعي الاجتماعي والحد من انتشار العقاقير المخدرة، رسالة ماجستير، جامعة الملك سعود، الرياض، السعودية.

القحطانى، نورة بنت ناصر(٢٠١٩). مدى توافر الوعي بالأمن السيبرانى لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي :دراسة ميدانية، مجلة شؤون اجتماعية، ٨٥-١٢٠.

القيسي، محمد وائل، (2020) مستقبل الأمن الاستراتيجي العالمي في ظل التحديات التكنو –معلوماتية والفضاء السيبراني، مجلة دراسات إقليمية :جامعة الموصل، مركز الدراسات الإقليمية (٤٤)١٣، ١٣٩-١٧٣.

المنتشري، فاطمة، وحريري، رندة (٢٠٢٠) درجة وعى معلمات المرحلة المتوسطة بالأمن السيبرانى في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، المجلة العربية للتربية النوعية؛ المؤسسة العربية للتربية والعلوم والآداب، ١٤(١)، ٩٥ – ١٤٠

المنتشري، فاطمة يوسف(٢٠٢٠). درجة وعى المعلمات المرحلة المتوسطة بالأمن السيبرانى في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، المجلة العربية للتربية النوعية، مج٤، ٩٥-١٤٠.

المنيع، الجوهرة عبد الرحمن (٢٠٢٢). متطلباتُ تحقيقِ الأمْن السيبرانيّ في الجَامِعَات السعوديَّة في ضوءِ رؤية ٢٠٣٠. مجلة كلية التربية. جامعة أسيوط، ٤ (٣٨) ، ١٥٥-١٩٤.

الهيئة الوطنية للأمن السيبراني (٢٠٢٠) الاستراتيجية الوطنية للأمن السيبرانى. المملكة العربية السعودية.sa.gov.nca://:.

خليفة، إيهاب (٢٠١٧)، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، مجلة اتجاهات الأحداث، ع. ٢٢ جويلية/ أوت.

صائغ، وفاء حسن عبدالوهاب (٢٠١٨) وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم لأمنية من الجرائم الإلكترونية، المجلة العربية للعلوم الاجتماعية، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية،٣ (١٤) ١٨-٧٠.

طه، فرج عبد القادر وعبد الفتاح، مصطفى كامل ومحمد، حسين عبد القادر وقنديل، شاكر عطية، (٢٠٠٣)، موسوعة علم النفس والتحليل النفسي، ط(٢). القاهرة: دار غريب.

فرماوي، محمد (١٩٩٢): برامج التخطيط التربوية، مكتبة الأنجلو المصرية، القاهرة.

مؤنس محمد سيد (١٩٩٠): أثر استخدام التعليم في زيادة فاعلية تدريس رياضيات الثانوية المرحلة، رسالة دكتوراه، كلية التربية، جامعة أسيوط.

متولي، عمار أحمد (٢٠٢١). دور اليوتيوب في تنمية وعي المراهقين بالأمن الإلكتروني. مجلة بحوث العلاقات العامة الشرق الأوسط. ٣١ . ٣٤٩-٣٨٩.

Aakre, S., Abeynayaka, A., Aanesen, M., Abhayawansa, S., Aarnio Linnanvuori, E.,Abidin, S., ... & Achiaga Menor, B. (2021). Acknowledgment to Reviewers of Sustainability in 2020 .

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), 23.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. Int. J. Inf. Secur. Res.(IJISR), 6(2), 660-666.

Banfield, J. M. (2016). A study of information security awareness program effectiveness in predicting end-user security behavior. Eastern Michigan University.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3),

AlMindeel, R. and Martins, J.T. orcid.org/0000-0003-3906-5904 (2021) Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. Information Technology & People, 34 (2). pp. 770-788

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. Int. J. Inf. Secur. Res.(IJISR), 6(2), 660-666.

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), e06016.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education & awareness programmes for small-& medium-sized enterprises (SMEs). Information & Computer Security.

Bada, M., & Nurse, J. R. (2020). The social & psychological impact of cyberattacks. In Emerging cyber threats & cognitive vulnerabilities (pp. 73-92). Academic Press. Reicher, H. Building inclusive education on social and emotional learning: Challenges and perspectives–a review. Int. J. Inclus. Educ. 2010, 14, 213–246

Bada, M., & Nurse, J. R. (2020). The social & psychological impact of cyberattacks. In Emerging cyber threats & cognitive vulnerabilities (pp. 73-92). Academic Press.

Bhakta, R.; Harris, I.G.(2015)Semantic analysis of dialogs to detect social engineering attacks. In Proceedings of the 2015 IEEE International Conference on Semantic Computing (ICSC), Anaheim, CA, USA, 7–9 February; pp. 424–427

Bordoff, S., Chen, Q., & Yan, Z. (2017). Cyber attacks, contributing factors, and tackling strategies: the current status of the science of cybersecurity. International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 7(4), 68-82.

Cash, S. J., Thelwall, M., Peck, S. N., Ferrell, J. Z., & Bridge, J. A. (2013). Adolescent suicide statements on MySpace. Cyberpsychology, Behavior, and Social Networking, 16(3), 166-174.

Conteh, N.Y.; Schmick, P.J(.2016)Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. Int. J. Adv. Comput. Res., 6, 31

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity Awareness Enhancement: A Study of the Effects of Age & Gender of Thai Employees Associated with Phishing Attacks. Education & Information Technologies, 27(4), 4729-4752.

Fujikawa, M.; Nishigaki, M(2011). A study of prevention for social engineering attacks using real/fake organization. In Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security, Vienna, Austria, 22–26; pp. 597–602.

Gcaza, N., & Von Solms, R. (2017). A strategy for a cybersecurity culture: A South African perspective. The Electronic Journal of Information Systems in Developing Countries, 80(1), 1-17.

Hadlington, L., & Parsons, K. (2017). Can cyberloafing and Internet addiction affect organizational information security?. Cyberpsychology, Behavior, and Social Networking, 20(9), 567-571.

Hadnagy, C(2010). Social Engineering: The Art of Human Hacking; John Wiley & Sons: Hoboken, NJ, USA.

Jansson, K. A(2011) Model for Cultivating Resistance to Social Engineering Attacks. Ph.D. Thesis, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, September

Jensen, M. L., Dinger, M., Wright, R., & Thatcher, J. (2013). Training to mitigate threats from customized phishing attacks. In Proceedings of the Hawaii International Conference on System Sciences.

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018,). Game based cybersecurity training for high school students. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education (pp. 68-73).

Kumaraguru, P., Arora, S., Dagar, N., & Chen, J. (2016, November). Cultural & psychological factors in cyber-security. In Proceedings of the 18th International Conference on

Information Integration & Web-based Applications & Services (pp. 318-324).

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employee's information security awareness in private and public organisations: A systematic literature review. Computers & Security, 106, 102267

Line, M.B.; Moe, N.B. Understanding collaborative challenges in it security preparedness exercises. In Proceedings of the IFIP International Information Security Conference, Hamburg, Germany, 26–28 May 2015; pp. 311–324

Mann, I.(2017) Hacking the Human: Social Engineering Techniques and Security Countermeasures; Routledge: London, UK,

Mosteanu, N. R. Artificial intelligence and cyber security– face to face with cyber attack–a maltese case of risk management approach. Ecoforum Journal, 2020. 9 (2).

Jansson, K. A(2011) Model for Cultivating Resistance to Social Engineering Attacks. Ph.D. Thesis, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, September 2011

Odemis, M., Yucel, C., & Koltuksuz, A. (2022). Detecting User behavior in cyber threat intelligence: development of Honeypsy system. Security & Communication Networks,

.

Proctor, W. R. (2016). Investigating the efficacy of cybersecurity awareness training programs (Doctoral dissertation, Utica College)

Raineri, E. M., & Resig, J. (2020). Evaluating Self-Efficacy Pertaining to Cybersecurity for Small Businesses. Journal of Applied Business & Economics, 22(12).

Richardson, M., MacDowall, W., Burchett, H., Stansfield, C., & Thomas, J. (2020). Cyberbullying and children and young people's mental health: a systematic map of systematic reviews. Cyberpsychology, Behavior, and Social Networking, 23(2), 72-82.

Ryan T. Wright & Jason Bennett Thatcher (2017) Training to Mitigate Phishing Attacks Using Mindfulness Techniques,

Journal of Management Information Systems, 34:2, 597-626,

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2021). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. In Research Anthology on Artificial Intelligence Applications in Security (pp. 174-188). IGI Global.

Seigfried-Spellar, K. C., Flores, B. M., & Griffin, D. J. (2015, October). Explanatory Case Study of the Authur Pendragon Cyber Threat: Socio-psychological & Communication Perspectives. In International Conference on Digital Forensics & Cyber Crime (pp. 143-175)

Shostack, A. Elevation of Privilege: Drawing Developers into Threat Modeling. In Proceedings of the 3GSE, San Diego, CA, USA, 18 Auguest 2014. 61.

Solis, G. (2018). Cyber Threats Affecting Adolescents (Doctoral dissertation, Utica College) .

Tosun, N., Altinöz, M., Çay, E., Çinkiliç, T., Gülseçen, S., Yildirim, T., & Ünlü, N. (2020). A swot analysis to raise awareness about cyber security & proper use of social media: Istanbul sample. International Journal of Curriculum & Instruction, 12, 271-294.

Wiederhold, B. K., Gao, K., Sulea, C., & Wiederhold, M. D. (2014). Virtual reality as a distraction technique in chronic pain patients. Cyber psychology, Behavior, and Social Networking, 17(6), 346-352 .

Younis, Y. A., Shi, Q., & Askwith, B Topham, L., Kifayat, K.,. (2016). Cyber security teaching and learning laboratories: A survey. Information & Security, 35(1), 51.

The Effectiveness of a Counseling Program to Develop Cyber security Awareness A sample of teenagers who use the Internet in Jeddah City.

Abstract: The aim of this study is to examine the effectiveness of an effective study in developing awareness of cyber security among adolescents from high school students in Jeddah City. (15) students from the group of the experimental group, the height of (15) students from the control group from secondary school students of the third secondary grade in schools in the City of Jeddah, and the study used the security awareness test: Prepared by Noura Al-Sistan and others (2020). And an indicative program to develop awareness of cyber security prepared by the researcher. The study reached many results, including that the awareness of the respondents about cyber security was weak, and the study revealed that there were statistically significant differences at the level of significance (0.001) between the scores of the post- and pre-measurements in the cyber security awareness test after applying the counseling program in the direction of the post-measurement, as the study revealed. There are statistically significant differences at the level of significance (0.001) between the scores of the experimental and control groups in the cyber security awareness test after applying the counseling program in the direction of the experimental group.

Keywords: Cyber security; Counseling Program