مجلة جامعة الشارقة للعلوم الإنسانية والاجتماعية

جامعة الشارقة
UNIVERSITY OF SHARJAH

مجلة جامعة الشارقة

مجلة علمية محكمة

للعلوم الإنسانية والاجتماعية

المجلد 21، العدد 3
ربيع الأول 1445هـ / سبتمبر 2024م

الترقيم الدولي المعياري للدوريات 1996-2339

سبتمبر 2024م **مجلة جامعة الشارقة للعلوم الإنسانية والاجتماعية** المجلد 21 العدد 3
https//:doi.org/10.36394/jhss/21/3/19

فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني لدى مستخدمي الإنترنت من طلاب المرحلة الثانوية بمنطقة جازان

عبد المريد عبد الجابر قاسم[1]

تركي بن بندر العنزي[2]

تاريخ الاستلام: 16-03-2023 **تاريخ القبول: 15-07-2023**

ملخص البحث:

هدفت الدراسة إلى الكشف عن فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني لدى المراهقين، وتكونت عينة الدراسة من (30) فردًا، منهم (15) طالبًا من عدد أفراد المجموعة التجريبية، وعدد(15) طالبًا من مجموعة الضابطة من طلاب المدارس الثانوية بمدارس جيزان واستعانت الدراسة باختبار الوعى بالأمن السيبراني من إعداد نورة الصانع وآخرين(2020). إضافة إلى برنامج إرشادي لتنمية الوعى بالأمن السيبراني، وكشفت الدراسة عن وجود فروق دالة إحصائيًا عند مستوى دلالة (0.001) بين درجات القياسين البعدي والقبلي في اختبار الوعى بالأمن السيبراني، بعد تطبيق البرنامج الإرشادي في اتجاه القياس البعدي، كما كشفت الدراسة عن وجود فروق دالة إحصائيًا عند مستوى دلالة (0.001) بين درجات المجموعتين التجريبية والضابطة في اختبار الوعى 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 الوعى بالأمن السيبراني بأبعاده المختلفة، وبناء على النتائج الدراسة الحالية، تم طرح مجموعة من التوصيات

الكلمات الدالة: الوعي بالأمن السيبراني، برنامج إرشادي.

(1) كلية التربية - جامعة الإمام محمد بن سعود الإسلامية (الرياض – المملكة العربية السعودية)
kasmabdo2@gmail.com

(2) أكاديمية سعد العبدالله للعلوم الأمنية (الكويت – الكويت)

المقدمة:

أحدثت تكنولوجيا المعلومات تغييرًا في استخدام التطبيقات الرقمية بأجهزة الاتصال في حياتنا اليومية في خلال العشر سنوات الماضية، 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 من الأمور البالغة الصعوبة (Alzubaidi, 2021)

وهذه التهديدات -في أبسط صورها- يقوم بها عن غير قصد أفرادٌ من ذوي المهارات التكنولوجية، بيد أن خطورة هذه التهديدات تزيد إذا تمت 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، فإن خطورة التهديدات السيبرانية تتزايد، لذلك أصبح تحقيق الأمن السيبرانى من الأهمية بمكان (Bordoff et al.,2017)

وعلى الرغم من تخصص عديد من الشركات التكنولوجيا في مجال مكافحة التهديدات الأمنية السيبرانية، إلا أن عملية إحصاء هذه التهديدات أصبحت شبه مستحيلة؛ لأنها لا تتوقف بل تُظهر أشكال جديدة وليدة اللحظة.

وعلى الرغم من استخدام تقنيات التكنولوجيا لمواجهة هذا الأمر، إلا أن التهديدات الأمنية السيبرانية باتت مستمرة، الأمر الذي نبه 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 الحد من خطر التهديدات السيبرانية ، فضلا عن أن تحقيق الأمن السيبرانى لا يتطلب التركيز على التكنولوجيا وحدها، بل يستلزم ذلك التركيز على البشر وطبيعتهم النفسية، خاصة 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 على تحقيق الأمن السيبرانى بطرق مختلفة اعتمادًا على الجوانب النفسية لمستخدمى الإنترنت، ووفقًا لتباين قدرتهم على تقييم مخاطر التهديدات، فقد أظهرت دراسة هاولينجتون وبارسونز (Hadlington & Parsons,

2017) أن نسبة 23% فقط، يتعاملون بشكل صحيح مع سيناريوهات الأمن السيبراني، ونسبة 4% فقط يمكنهم التعامل مع أكثر من 90% 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 2001 و 2013، وقد نشأوا حول إنترنت؛ فهذا الجيل أكثر الأجيال ذكاءً واستقلالية على الويب، وعلى الرغم من ذلك فإن هذا الجيل يوجه كثيرًا من الانتقاد؛ بسبب انفصاله عن المجتمع، وبسبب إهدار مقدار الوقت المبذول نظرًا لاستخدام التكنولوجيا؛ إذ يقضي هذا الجيل ما يقرب من ثلاث ساعات يوميًا عبر الإنترنت، فضلا عن أن مواقع وسائل التواصل الاجتماعي، قد تولدت في عصر هذا الجيل (Cash et al.,2013)

وفي ضوء ما تقدم، فإن الحاجة لتنيمة الوعى بالأمن السيبراني تكون جد مهمة، والتخفيف من وطأة التهديدات لأمن المعلومات، من لدن المستخدمين للإنترنت تكون كذلك، وبخاصة فيما يتعلق بفئة المراهقين عبر برامج تدريبية وإرشادية، وعلى الرغم من تدخلات علم النفس السيبراني، إلا أنه لايزال في المهد بيد أن البرامج التدريبية لتنمية الوعى بالأمن السيبرانى، قد ظهرت معتمدة على تحديد العوامل النفسية الرئيسة المتعلقة بتحقيق الأمن السيبراني أو فشله (Bordoff et al.,2017)

وهذا ما حدا بالباحثين 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

الإحساس بمشكلة الدراسة، وأسئلتها:

يشهد العالم اليوم تطورًا سريعًا في تقنيات الاتصال واستخدام الإنترنت في جميع أنحاء العالم، فضلا عن التبادل المعلوماتي، وقد صاحب هذا التزايد -أيضًا- تزايد الحروب السيبرانية التي تعد مثل الحروب التقليدية التي تصنعها الأسلحة، وأصبحت الهجمات الإلكترونية شائعة مثل الإنترنت نفسه، بل إنها تتزايد كل عام، وتشير التقارير الإخبارية، والمقالات الأكاديمية إلى تزايد حجم الهجمات والجرائم الإلكترونية، وتنوعهما، اللتان تقترنان بشكل كبير بعدم فهم المستخدمين، وإدراكهم لمخاطر الإنترنت وطرق التعامل معها (Raineri,& & Resig,2020).

وتجدر الإشارة في هذا السياق إلى أن البيئة الدراسة الحالية ، تتمثل في المملكة العربية السعودية، وهى ما سببت الهجمات الإلكترونية فيها ضررًا كبيرًا على البنية التحتية، وتمثلت أبرز الحوادث الرئيسة في الهجمات التي استهدفت شركة أرامكو السعودية، وعطلت نشاطها لمدة شهر فيها، وهو ما يعد أكبر اختراق في التاريخ. وتسببت هذه البرمجيات الخبيثة في حدوث خلل مرة أخرى بالشركة نفسها في نوفمبر 2016، ويناير 2017. (إبراهيم،2021)

والمملكة العربية السعودية، قد تبنت منهجًا متكاملا للأمن السيبرانى إضافة إلى العمل على تحقيق رؤية المملكة 2030 والأهداف الاستراتيجية الوطنية ، وهو ما سيعزز من حماية فضائها السيبراني، ومصالحها الحيوية، وهو الأمر الذي يعمل على تحقيق رؤية المملكة 2030، كما أن تطوير مبادئ الأمن السيبرانى والعمل عليها في جميع الجهات الحكومية، والقطاع الخاص والمجتمع؛ سيعزز- بدوره- من إدراك الجهات والأفراد ويزيد من مسؤولياتهم في الحفاظ على أصولهم وخدماتهم الحيوية، ويعد التعاون أساسًا لهذه المنظومة (الهيئة الوطنية للأمن السيبراني،2021)

وعلى المستوى العالمي تبذل جهود كبيرة لمواجهة مخاطر الإنترنت بوساطة المحافظة على المعلومات الحساسة 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 ما 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 قد أشارت إلى أن من أهم العوامل المؤدية إلى نجاح استهداف الهجمات السيبرانية، تعود إلى أن كثيرًا من مستخدمي الإنترنت لا يزالون يفتقرون للوعى الكافي بتهديدات الإنترنت المختلفة، والتي تُعرف -أيضًا- باسم "المخاطر الإلكترونية" فغالبًا ما يفتقد الأفراد للوعى بمخاطر الإنترنت؛ مما يؤثر سلبًا في استعدادهم لاستخدام تدابير الحماية الأمنية السيبرانية؛ لحفظ المعلومات والسرية على أجهزة الحاسوب من لدنهم انظر دراسات (Bada, & Nurse,2020,Halevi et al.,2016,Odemis et al.,2022, Seigfried-Spellar,et al.,2015

وتأسيسًا على ما سبق فقد أصبح التأكيد على تنمية الوعي بالأمن السيبراني، أمرًا لا مفر منه 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 مسؤولا في مؤسسة ما- فى التعرض لأضرار جسيمة للمؤسسة (Yunnis 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 قد تقوم بإنتاج نظم حماية، وتضع الحلول الشاملة لأي تهديد إلكترونى، فضلا عن الإفادة 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، إضافة إلى رفع مستوى الوعي بالأمن السيبرانى من لدن متابعيهم، زيادة على دور المراهقين الذين، يمثلون شريحة كبيرة من بين مستخدمي الثورة الرقمية بأدواتها المختلفة خاصة الإنترنت؛ وعليه ينبغي أن يكون الفضاء السيبرانى الذي يستخدمونه اليوم مكانًا أمنًا (متولي، 2021)

ومن اللافت لانتباه الباحث أن التقارير العلمية، قد أشارت إلى أكثر فئة عمرية مستخدمة للإنترنت، وهم المراهقون من الجنسين في بيئة الدراسة الحالية ، إذ أوضحت نتائج الدراسة السعودية التى قام بها (الرويس، 2013) أن نسبة استخدام المراهقين السعوديين للإنترنت كانت مرتفعة، إذ يستخدمه المراهقون من الجنسين في أكثر الأحيان من دون موعد محدد،

ويُعزى ذلك إلى تطور تقنيات تطبيقات مواقع التواصل الاجتماعي وسهولة استخدامها، وفقًا لما يشهده مجال الهواتف الذكية والحواسيب من تطور تقني عالي المستوى.

وتشير البيانات الحديثة إلى أن المراهقين من طلاب المدارس الثانوية الأمريكية، غالبًا ما يتعرضون للإيذاء الإلكتروني على مواقع الشبكات الاجتماعية بنسبة (62%)، وعبر الرسائل النصية، أو منصات المراسلة الأخرى40% (Waasdorp & Bradshaw ,2015)

ومن هذا المنطلق، جاءت الضرورة لبناء برامج تسهم في زيادة الوعى 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، وهو ما يعول على ضرورة تناول هذه التحديات من منظور علم النفس ، إذ إن فهم كيفية إدراك الأفراد للمخاطر السيبرانية أمرٌ بالغ الأهمية، ويستدعى حملات فعالة للتوعية، تكون قادرة على بناء الفهم والامتثال لنصائح المتخصصين بالأمن السيبرانى، و الذى 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 الوعى بالأمن السيبراني (Tosun et al.,2020)

يضاف إلى ما سبق، ما أشارت إليه نتائج بعض الدراسات السابقة، وما طرحته من توصيات قد 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،2020، والقيسى،2020 ، إبراهيم ،2021، و. Richardson et,2020 ، صائغ، 2018، القحطانى،2018)

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

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

وفي سياق الإدراك لمعالم تلك الأهمية، تبرز أهمية تنمية الوعى بالأمن السيبراني من لدن أكثر الفئات العمرية استخدامًا للإنترنت، وهم المراهقون على نحو خاص، وعلى الرغم من ذلك تندُر الدراسات التي أجريت على عينات من المراهقين في البيئة العربية بوجه عام، والمحلية بصورة خاصة -في حدود اطلاع الباحثين-

ويمكن تحديد مشكلة الدراسة الحالية في السؤال الرئيس الذى مؤداه : ما مدى فاعلية برنامج إرشادي لتنمية الوعى بالأمن السيبراني من لدن المراهقين من طلبة التعليم الثانوي في جيزان؟ ويتفرع من هذا السؤال الرئيس سؤالين فرعيين تاليين، وهما:

1. ما الفروق الدالة إحصائيًا في رتب متوسطات درجات المجموعة التجريبية، والمجموعة الضابطة على اختبار الوعى بالأمن، خاصة بعد تطبيق البرنامج الإرشادي المقترح؟
2. ما الفروق الدالة إحصائيًا بين رتب متوسطات درجات المجموعة التجريبية، وبين القياسين البعدي، والتتبعى على اختبار الوعى بالأمن ؟

أهداف الدراسة: تهدف الدراسة الحالية إلى:

1. التعرف إلى فاعلية برنامج إرشادي لتنمية مستوى الوعى بالأمن السيبراني من لدن المراهقين من طلبة التعليم الثانوي في مدارس جيزان.
2. التأكد من استمرار فاعلية البرنامج الإرشادي المقترح لتنمية مستوى الوعى بالأمن السيبراني من لدن المراهقين من طلبة التعليم الثانوي في مدارس جيزان، بعد شهر من تطبيق البرنامج.

أهمية الدراسة:

أهمية الدراسة ومبرراتها:

تجدرالإشارة إلى أن عديدًا من مستخدمي الإنترنت، لا يزالون يفتقرون إلى الوعي الكافي بتهديدات الإنترنت المختلفة، والتي تُعرف -أيضًا- باسم "المخاطر الإلكترونية"، وغالبًا ما يفشلون في امتلاك الحد الأدنى المطلوب لحماية أجهزتهم الحاسوبية في أسوأ السيناريوهات، إذ يعاني الأفراد من نقص تام في الوعي بمخاطر الإنترنت؛ ومن ثم، فإن استعدادهم لاستخدام تدابير الحماية الأمنية السيبرانية غير موجود (Emm, 2021)

ومن هنا يمكن القول إن تحقيق الأمن السيبراني، لا يقتصر فقط على مجرد التحكم التكنولوجي، بل الأمر يتعلق بوعي كل من الأفراد الذين تستهدفهم، والأفراد الذين

يستهدفونك من خلال اتباع منهج نفسي، يحقق المحافظة على الأفراد والأنظمة والبيانات الخاصة في مأمن من "الهاكرز" الذين قد يؤذون الناس (البيشي, 2021)

وعند الحديث عن الوعي بالأمن السيبراني من لدن الطلاب، فإنه يمكن ملاحظة أن البرامج الخاصة بتنمية الوعي السيبراني، تعد الأداة الأساسية التي تساعد على تحقيق ذلك الهدف (Peker et al., 2016)؛

لأنه على الرغم من أن الطلاب يمتلكون معرفة كافية بالتعامل مع الحاسوب، إلا أن مستوى الوعي بالأمن السيبراني لا يزال قاصرًا؛ لأنه لم يتم تزويدهم بخلفية عن ذلك الأمر في المقررات الأكاديمية التي تمت دراستها (Lesjak,et al., 2019).

وبناءً عليه فإنه يتحتم تعزيز الوعي بالتهديدات المختلفة، التي يمكن أن يواجهها طلاب المرحلة الثانوية في البيئات الإلكترونية، وكذلك توعيتهم بالأهمية الخاصة بالأمن السيبراني، للدفاع عن أنفسهم في حالة التعرض إلى أية هجمات (Pencheva,et al., 2019)

وتبدو الأهمية النظرية للدراسة جليه في حداثة الدراسة ،ومواكبتها للتغير المحلي والعالمي في مجال الأمن السيبراني؛ إذ تعد الدراسة الأولي على المستوى المحلي والعربي -حسب اطلاع الباحثين- إذ يتناول فاعلية البرنامج الإرشادى في تنمية الوعى بالأمن السيبراني، أى إنه يحاول توظيف الإرشاد الوقائي في معالجة قضايا معاصرة، إذ أصبح التوجّه إلى تقديم برامج إرشادية فعالة لتنمية الوعى بالأمن السيبرانى وفق أساس علمي مدروس، من العوامل التي تعمل على القيادة الواعية

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

كذلك فتح المجال للباحثين نحو إجراء دراسات نفسية تتعلق بموضوعات العلم السيبرانى وبمتغيرات الدراسة الحالية

أما الأهمية التطبيقية للدراسة الحالية، فتتمثل في:

تتقديم برنامج إرشادي لتنمية الوعى بالأمن السيبرانى من لدن المراهقين من طلاب المرحلة الثانوية، وإكسابهم المفاهيم الأساسية للأمن السيبرانى، وأنواع التهديدات السيبرانية التي يمكن أن يتم التعرض لها في الفضاء السيبرانى وهو ما يمكن تعميمه على الطلاب من مستخدمي الإنترنت في مختلف المراحل التعليمية

فضلا عن توجيه اهتمام المسؤولين في وزارة التربية والتعليم بأهمية تحقيق الوعى بالأمن السيبرانى من لدن الطلاب من مستخدمي الإنترنت في مختلف المراحل التعليمية

حدود الدراسة:

اقتصرت الدراسة الحالية على مدى فاعلية برنامج إرشادي في تنمية الوعي بالأمن السيبراني من لدن المراهقين من مستخدمي الإنترنت، وممن لديهم مستوى منخفض من الوعى بالأمن السيبراني من طلبة المدارس الثانوية من منطقة جيزان في المملكة العربية السعودية في العام الدراسي 1443/ 1444

مصطلحات الدراسة وتعريفاتها الإجرائية:

البرنامج الإرشادى: يعرف بأنه برنامج تدخل موجبة من قبل المرشد يتم تنفيذه عبر تخطيط لمجموعة من الخبرات المترابطة والمتكاملة؛ لتحقيق مجموعة من الأهداف من خلال أنشطة متنوعة. ويسعى البرنامج الإرشادى إلى تنمية الفرد الذي أعد من أجله البرنامج في جميع جوانب النمو العقلي والنفسي والجسمي، والروحي ويتضمن أسلوب العمل وأسلوب التقييم (فرماوي، 1992)

ويعرف البرنامج الإرشادى إجرا ئيًا بأنه تخطيط لمجموعة من الإرشادات والمعلومات والخبرات والمهارات المرتبطة في إطار دقيق ومحدد؛ بهدف تنمية الوعى بالأمن السيبراني وإكساب الفرد المهارات، والخبرات التي تساعده في ذلك

الوعي بالأمن السيبرانى : عرف سابيلون وآخرون (Sabillon et al.,2019) 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

ويعرف الباحثان الوعي بالأمن السيبراني إجرائيًا بأنه: 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 وواالبيانات، وكل ما يتعلق بالتقنية ذات العلاقة يتم تحديد مستوى الوعى بالأمن السيبراني من خلال المقياس المستخدم في الدراسة الحالية

الإطار النظري للدراسة والدراسات السابقة:

أولا- الوعى بالأمن السيبراني:

توجد ثلاث ركائز للأمن السيبراني وهى: المستخدمون، والنظم، وقابلية الاستخدام، وتوجد علاقة متبادلة بين الركائز الثلاثة، كما يوجد نوعان من المستخدمين: وهما (الخبراء وغير الخبراء) الذين من لدنهم خصائص مختلفة تؤثر في استخدامهم لأنظمة الأمن السيبراني (Shappie et al.,2020)

كذلك توجد ثلاثة عناصر أساسية، يعتمد عليها الأمْن السيبرانيّ، وتتمثل فيما يلى:

- **السريَّة:** ويقصد بها سرية المعلومات، للحفاظ عليها من خلال منح الإذن للمخول لهم فقط للوصول لتلك المعلومات والبيانات، مع منع الأشخاص غير المخول لهم الوصول إليها، و ضرورة التأكد من عدم الإفصاح عنها، أو تسريبها لأشخاص غير متخصصين أو مخول لهم ذلك.
- **تكامل المعلومات وسلامتها**: وتعنى الحفاظ على المحتوى من التعديل، أو التغيير، أو الحذف، أو الإضافة بوساطة الأشخاص المؤهلين والمتخصصين بالإشراف على هذا المحتوى.
- **توافرُ المعلومات وإتاحتُها**: ويقصد بها توافر المعلومات من قبل المتخصصين والمشرفين على تقديمها، وإتاحتها في الوقت المحدد (المنيع،2022).

- **-العوامل النفسية المساهمة في تحقيق الأمن السيبرانى:**

يشيرجكازا وآخرون (Gcaza, et al.,2017) إلى أن تحقيق الأمن السيبراني، لايقتصر -فقط- على مجرد التحكم التكنولوجي، بل الأمر يتعلق بالإنسان بما لديه من عوامل نفسية فهو النقطة المركزية في تحقيق الأمن السيبرانى، ومن بين العوامل (النفسية) المتعلقة بالأمن السيبراني والتى يمكن تناول بعضًا منها على النحو التالي:

- **القيم:** وهى لها حساسية كبيرة في المحافظة على أمن المعلومات؛ فقد أشارت دراسة هادلينجتون (Hadlington,2017) إلى أن الاحترام والتسامح يعدان من القيم الإنسانية التى تعزز أمن المعلومات، كما توصلت دراسة بارسونز(Parsons et al,2012) إلى أن قيمة الاحترام يكون لها تأثير إيجابي في الوعي بتوفير الأمن السيبراني الشخصي، كما أن قيم التسامح والسلام لهما 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 ترتبط بسلوكيات الأمن السيبراني، وأن يقظة الضمير والانفتاح قد يكونان بارزين بشكل خاص في هذه العلاقة (Shappie,et al.,2020).

ويشير الداود وسكينر (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

بعض النظريات المفسرة للوعى بالأمن السيبرانى:

يستخدم علماء النفس نظريات مختلفة لشرح السلوك البشري والتنبؤ به استعدادًا لبرامج الأمن السيبراني على سبيل المثال ، قد يعتمد المتخصصون في الأمن السيبراني على نظرية دافع الحماية (PMT)، والتي تشرح بشكل أساسي تأثير إدراك التهديد والكفاءة الذاتية في السلوكيات، أو المواقف الأمنية بين الأفراد (Rogers,1983)

بالإضافة إلى ذلك، تشير نظرية السلوك المخطط (TPB) إلى أن النية السلوكية تتأثر بالمعايير والمواقف الذاتية التى تساعد هذه النظريات والنماذج على تحديد العناصر السلوكية الأكثر تنبؤية؛ ليتم تضمينها في خطة الوقاية أو التدخل بشأن المحافظة على المعلومات (Ajzen,1991)

والدراسة الحالية تتبنى هاتين النظريتين في تفسير الوعى بالأمن السيبرانى.

1. نظرية دافع الحماية (PMT) :

ظهرت هذه النظرية على يد العالم رورجزRogers عام 1983وتعتمد هذه النظرية على العمليات المعرفية ،التي تتوسط السلوك في مواجهة التهديد وتفترض هذه النظرية أنه عند مواجهة تهديد ، يقوم الأشخاص بإجراء عمليتي تقييم: الأولى تركز على التهديد نفسه والأخرى على قدرتهم على التصرف ضد هذا التهديد (تقييم التهديد وتقييم المواجهة، على التوالي، ويؤثر هذا في نيتهم في اتخاذ إجراءات احترازية، ويؤدي إلى سلوكيات تكيفية أو غير قادرة على التكيف مع التهديد في تقييمهم للتهديد ، إذ يأخذ الناس في الاعتبار مدى سلبية عواقب التهديد (الخطورة المتصورة) واحتمال ظهور التهديد بطريقة، تؤثر فيهم بشكل مباشر (الضعف المتصور) فقد يؤدي تقييم التهديد هذا إلى سلوكيات غير قادرة على التكيف مثل الإنكار أو التجنب. (Haag,et al.,2021)

وفـى تقييـم التأقلـم، سـيقيم النـاس مـا إذا كان اتبـاع مسـار العمـل الموصـي بـه سـيزيل التهديـد (فعاليـة الاسـتجابة) فـصلا عـن مسـتوى ثقتهـم فـي القـدرة علـى تنفيـذ هـذا الإجـراء، ويـؤدي هـذا التقييـم إلـى السـلوكيات التكيفيـة، بشـرط ألا تكـون تكاليـف إجـراء اسـتجابة تكيفيـة (تكاليـف الاسـتجابة) مرتفعـة للغايـة.

تـم تطبيـق PMT علـى الأمـن السـيبراني ، وتحديـدًا علـى سـلوك الحمايـة مـن الفيروسـات ، والسـلوك الأمنـي بيـن الأشـخاص الذيـن يعرفـون كيفيـة حمايـة أنظمتهـم، بيـد أنهـم يفشـلون فـي القيـام بذلـك، والنوايـا السـلوكية الأمنيـة لـ مسـتخدمى الكمبيوتـر المنزلـي، وإقنـاع مسـتخدمي الإنترنـت بحمايـة أنفسـهم ، ودور المسـؤولية الشـخصية فـي السـلوك الوقائـي لـطلاب الجامعات؛ واسـتعداد المراهقيـن لتوفيـر المعلومـات عبـر الإنترنـت ، والسـلوك الأمنـي اسـتجابة لنـداءات الخـوف مـن قبـل أربـاب العمـل ، والتـزام الموظفيـن سياسـات أمـن المعلومـات (Mou et.al.,2022).

2. نظرية السلوك المخطط (TPB)

ظهـرت هـذه النظريـة علـى يـد العالـم أجـزن Ajzen عـام1985- 1991 وهـى نظريـة حـول العلاقـة بيـن المواقـف والسـلوك، وهـي تؤكـد أن حـدوث السـلوك الفعلـي، يتناسـب مـع مقـدار السـيطرة التـي يمارسـها الفـرد علـى سـلوكه وقـوة نوايـا هـذا الفـرد لتنفيـذ هـذا السـلوك،

وفقًـا (لنظريـة السـلوك المخطـط)إذ يتـم تحديـد نيـة الشـخص مـن خـلال ثلاثـة عوامـل وهـي: موقفـه مـن السـلوك المعنـى ،ونظرتـه إلـى المعاييـر الاجتماعيـة والسـيطرة إذ يعتقـد الفـرد أنـه قـادر علـى السـيطرة فـي الأوضـاع (Hong&Furnell,2021)

كمـا أنهـا علـى فهـم كيفيـة تغييـر سـلوك الأفـراد فهـذه النظريـة تتوقـع السـلوك ؛لأنـه يمكـن أن يخطـط لـه . وفـى سـياق سـلوك أمـن المعلومـات تفسـر الوعـى بالأمـن السـيبرانى مـن خـلال نيـة الفـرد فـي اعتمـاد تدابيـر أمنيـة إذ تعتمـد علـى المعتقـدات السـلوكية التـي تحـدد موقـف الفـرد تجـاه سـلوك أمـن المعلومـات، بالإضافـة إلـى المعتقـدات المعياريـة للآخريـن حـول الفـرد وهـى التـي تحـدد المعاييـر الشـخصية للفـرد لمـا هـو متوقـع مـن سـلوك، كمـا تؤثـر معتقـدات السـيطرة فـى إدراك الفـرد علـى سـلوك أمـن المعلومـات (Li et al.,2019)

ثانيًا- تنمية الوعى بالأمن السيبرانى باستخدام البرامج الإرشادية:

أصبـح تعزيـز الوعـي بالأمـن السـيبراني هدفًـا رئيسًـا لعديـد مـن المنظمـات، إذ يـؤدي زيـادة الوعـي بحالـة البيئـات إلـى تحسـين عمليـة اتخـاذ القـرار، فالوعـي هـو عمليـة تعلـم تمهـد الطريـق للتدريـب مـن خـلال تغييـر المواقـف الفرديـة والتنظيميـة؛ لإدراك أهميـة الأمـن والعواقـب السـلبية لفشـلها. والوعـي مهـم للغايـة فـي مجـال أمـن تكنولوجيـا المعلومـات والاتصـالات؛ لأن تصرفـات

الفرد يمكن أن تؤثر في المؤسسة بأكملها، ويمكن أن يتسبب عدم وعي الفرد المسؤول في أضرار جسيمة وخسارة للمؤسسة، والوعي الأمني السيبراني ، كل شيء عن نقل المعلومات (Yunos et al., 2016)

ويعد التدريب الفعال أمرًا على قدر كبير من الأهمية من أجل رفع مستوى الوعي الخاص بالأفراد،ط إزاء الأمن السيبراني، وبخاصة في ظل تزايد التهديدات السيبرانية، التي يشهدها العالم في هذه الآونة (Wray et al., 2020).

وعليه يمكن الاستعانة بالبرامج الإرشادية في تنمية الوعي بالأمن الإلكتروني من خلال بناء الوعي، والتثقيف بشأن التهديدات عبر الإنترنت وكيفية حماية البيانات ، والمساعدة في توجيه الأفراد وتوعيتهم بالمخاطر المحتملة، وتدريبهم على الكيفية التي ينبغي التصرف على ضوئها في حالة وجود خطر أمني (Official Website of Tikaj, 2022)

وعند الحديث عن الوعي بالأمن السيبراني من لدن الطلاب، فإنه يمكن ملاحظة أن البرامج الخاصة بتنمية الوعي السيبراني، تعد الأداة الأساسية التي تساعد على تحقيق ذلك الهدف (Peker et al., 2016,)؛ ذلك لأنه على الرغم من أن الطلاب يمتلكون معرفة كافية بالتعامل مع الحاسوب، بيد أن مستوى الوعي بالأمن السيبراني لا يزال مقصورًا؛ لأنه لم يتم تزويدهم بخلفية عن ذلك الأمر في المقررات الأكاديمية التي تمت دراستها (Lesjak et al., 2019). وبناءً عليه فإنه يتحتم تعزيز الوعي بالتهديدات المختلفة، التي يمكن أن يواجهها طلاب المرحلة الثانوية في البيئات الإلكترونية، وكذلك توعيتهم بالأهمية الخاصة بالأمن السيبراني للدفاع عن أنفسهم في حالة التعرض إلى أية هجمات (Pencheva et al., 2019).

إذ يمكن أن يتعرض الطلاب إلى عديد من التهديدات، والهجمات التي تهدد الأمن السيبراني، مثل: سرقة كلمات المرور الخاصة بهم، أو التهديدات التي قد يتلقونها أثناء استخدام الشبكات الاجتماعية، أو البرمجيات الخبيثة، أو الاحتيال الإلكتروني، أو الفجوات الأمنية التي تؤدي إلى تسريب بعض معلوماتهم على الشبكات (Yilmaz et al., 2017)

فقد أجريت دراسة (Banfield, 2016) بهدف بحث فاعلية برنامج الوعي بالأمن السيبراني على السلوك الأمني من لدن المستخدم النهائي في المؤسسات متوسطة الحجم، وقد تكون مجتمع الدراسة من العاملين في مؤسسة متوسطة الحجم في الولايات المتحدة، واشتملت العينة على (400) من العاملين في المؤسسات متوسطة الحجم، واعتمد الباحث على المنهج المسحي والكمي، كما استعانت الدراسة بالأداة المسحية الإلكترونية، التي تم توزيعها على المشاركين في الدراسة، وقد توصلت الدراسة إلى عديد من النتائج أهمها: عدم وجود تأثير ذي دلالة لتطبيق برنامج الوعي بالأمن السيبراني على تغيير

السلوكيات الأمنية من لدن العاملين، كذلك وجود علاقة ارتباطية بين برنامج الوعي بالأمن السيبراني، والسلوك الأمني من لدن المستخدم النهائي، كما تعد برامج الوعي المعلوماتي من العناصر المهمة في الأمن المعلوماتي الشامل؛ إذ إن التكنولوجيا من دون برنامج الوعي بالأمن السيبراني، تعد خطة أمنية غير كاملة. وأوصت الدراسة بضرورة إجراء مزيد من الدراسات المستقبلية، التي تتناول أثر برنامج الوعي بالأمن السيبراني في السلوك الأمني، وكذلك ضرورة تسليط الضوء على أساليب تفعيل برامج الوعي بالأمن السيبراني في المؤسسات، و كان الغرض من دراسة (Proctor,2016) التحقيق في فعالية برنامج تدريبي لتنمية الوعي بالأمن السيبراني، والبحث عن إجابة لأسئلة مؤداها، ما مبادئ التصميم للتدريب على التوعية بالأمن السيبراني للبرنامج؟ و ما الاهتمامات التي ينطوي عليها استخدام الوعي بالأمن السيبراني؟ وكيف تم تنفيذ برامج التدريب للتوعية بالأمن السيبراني؟ وقد أظهر التحقيق أن هناك طرقًا عديدة، لتطوير البرامج وفقًا لاحتياجات المنظمة.

أما عن الدور المطلوب من تدريب التوعية بالأمن السيبراني ، فقد تم عرض البرامج على مجموعة من الخبراء، وأظهر ذلك الإجراء عدة مخاوف أثيرت ضد استخدام البرامج التدريبية للتوعية بالأمن السيبراني، والتي تمثلت في سوء الفهم للدور المقصود من هذه البرامج. وكشفت بيانات الدراسة الحالة أن فعالية تنفيذ البرنامج كانت سيئة ، ومع ذلك فإن التوصية بتنفيذ مثل هذه البرامج، لا تزال تقدم إلى الرئيس و ضباط المعلومات على أساس الحاجة إلى توفير استراتيجية دفاع متعمقة، وهدفت دراسة (Chang & Coppel, 2020) إلى تسليط الضوء على برنامج ممول من أستراليا مقدم من قبل جامعة موناش؛ للتغلب على الإرهاب السيبراني لتعزيز الوعي بالأمن السيبراني في ميانمار، واعتمدت على المنهج التحليلي القائم على تحليل الممارسات المتعلقة ببناء الوعي بالأمن السيبراني، من خلال برامج المساعدة في التطوير بتقديم برنامج أسترالي؛ لدعم الوعي والقدرات المتعلقة بالأمن السيبراني في ميانمار، وتوصلت الدراسة إلى عدة نتائج أهمها: تقوم 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. و تدعم البرامج التي تعزز الوعي بالأمن السيبراني القوة في الخدمات الإلكترونية، بما في ذلك التعامل المصرفي النقال، والحكومة الإلكترونية، ونظام المدفوعات الإلكترونية الذي يساعد فيه برنامج Cyber Baykin بوساطة تعزيز بناء الوعي والكفاءة فيما يتعلق بالأمن السيبراني في ميانمار. وأوصت الدراسة بضرورة تطوير اللوائح المتعلقة ببرامج الوعي بالأمن السيبراني في المؤسسات المختلفة، وكذلك ضرورة توفير مزيد من الموارد المالية المطلوبة لتطوير برامج زيادة الوعي بالأمن السيبراني. كماهدفت دراسة إبراهيم(2021)

الكشف عن فاعلية برنامج تدريبي مقترح لتنمية الوعي بجوانب الأمن السيبراني في التعليم عن بعد من لدن معلمات العلوم بالمرحلة الابتدائية في المملكة العربية السعودية، واستخدم المنهج التجريبي ذو 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 (30) معلمة، وطبق مقياس الوعي بجوانب الأمن السيبراني في التعليم عن بعد قبليًا، وبعد تدريب المعلمات على البرنامج المقترح خلال الفصل الدراسي الأول لعام 1442/ 1441هـ، بواقع (10) جلسات تدريبية، ثم طبق المقياس بعديًا. وأسفرت نتائج البحث عن وجود فرق ذي دلالة إحصائية عند مستوى (0,05)، بين متوسطي درجات المعلمات في التطبيقين القبلي والبعدي لمقياس الوعي؛ لصالح التطبيق البعدي؛ ويدل هذا على فاعلية البرنامج التدريبي المقترح

كما استهدفت دراسة متولي (2021) التعرف إلى معدل تعرض المبحوثين -عينة الدراسة- لفيديوهات الأمن الإلكتروني، ورصد أكثر الفيديوهات التي يهتمون بمشاهدتها، والتعرف إلى دوافع التماس المبحوثين للمعلومات حول الأمن الإلكتروني من خلال اليوتيوب، وكذلك رصد مستوى الوعي بالأمن الإلكتروني من لدنهم، بعد تعرضهم لليوتيوب، ومعرفة التأثيرات المعرفية والوجدانية والسلوكية الناتجة عن التعرض لتلك الفيديوهات. وجاءت الدراسة وصفية معتمدة على منهج المسح الإعلامي، ويتمثل مجتمع الدراسة في المراهقين المصريين بالجامعات المصرية من (17- 18) عامًا، وجاءت عينة الدراسة عمدية مكونة من (300) مبحوث من المراهقين المصريين من طلاب الفرقة الأولى من (17 - 18) عامًا. واعتمدت الدراسة على استمارة الاستبيان لجمع بيانات الدراسة، حول دور اليوتيوب في تنمية وعي المراهقين بالأمن الإلكتروني. أما عن أهم نتائج الدراسة، فجاءت على النحو التالي: 1- ارتفاع معدل تعرض المبحوثين -عينة الدراسة- لفيديوهات الأمن الإلكتروني، باليوتيوب وجاءت حماية الحسابات الشخصية في مقدمة الفيديوهات التي يفضلها المبحوثون. 2- وأكدت الدراسة وجود عالقة ارتباطية إيجابية ذات دلالة إحصائية، بين معدل تعرض المبحوثين لفيديوهات الأمن الإلكتروني باليوتيوب، ومستوى الوعي بالأمن الإلكتروني من لدنهم. 3- توجد عالقة ارتباطية ذات دلالة إحصائية بين دوافع التماس المبحوثين للمعلومات من خلال فيديوهات يوتيوب، ومستوى الوعي بالأمن الإلكتروني من لدنهم. 4- أكدت الدراسة وجود عالقة ارتباطية إيجابية ذات دلالة إحصائية، بين معدل تعرض المبحوثين لفيديوهات الأمن الإلكتروني باليوتيوب، وتأثيراتها المختلفة عليهم. 5- توصلت الدراسة إلى وجود عالقة ارتباطية 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 الوعى بالأمن السيبرانى، تنتمي إلى مجتمعات ذات أطر ثقافية مختلفة، والذي يمكن أن تسهم -على نحو ما- في اختلاف النتائج المتعلقة بفهم المشكلة ونتائجها، وبناءً على ما سبق استعراضه من دراسات سابقة، بدى لي أن مشكلة الوعى بالأمن السيبراني، لم يتم دراستها بالتصميم على المستوى المحلى، لذلك مازالت الحاجة للبحث في البيئة المحلية، لمعرفة دور المتغيرات النفسية المؤثرة في الوعى بالأمن السيبرانى

كذلك من خلال مسح قواعد البيانات الإلكترونية عن وجود ندرة في الدراسات السعودية، التى تناولت برنامج إرشادي لتنمية الوعى بالأمن السيبرانى ، فقد ظهر من هذا المسح وجود دراسة واحدة على غرار تصميم الدراسة الحالية قام بها إبراهيم(2021).

من جهة ثانية ، يوجد اتفاق بين نتائج الدراسات التي تناولت تنمية الوعى بالأمن السيبراني على أهمية العامل البشري في المحافظة على أمن المعلومات

وما سبق يقتضي الضرورة إجراء دراسة لتنمية الوعى بالأمن السيبرانى من لدن المراهقين، وعلى الأخص في البيئة السعودية

فروض الدراسة:

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

1. توجد فروق دالة إحصائيًا في رتب متوسطات درجات أفراد المجموعة التجريبية، و رتب متوسطات درجات أفراد المجموعة الضابطة على مقياس الوعى بالأمن السيبراني بعد تطبيق البرنامج الإرشادي.
2. لا توجد فروق دالة إحصائيًا في رتب متوسطات درجات أفراد المجموعة التجريبية، و مقياس الوعى بالأمن السيبرانى، 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 تم اختبار المجموعتين اختبارًا قبليًا، وبعد ذلك خضعت المجموعة التجريبية للمتغير المستقل والذى مثله في الدراسة الحالية برنامج إرشادي لتنمية الوعى بالأمن، من لدن المراهقين من طلاب المرحلة الثانوية بمنطقة جازان، 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(1) هذه الإجراءات

(1) نوع التصميم التجريبي المستخدم

مجموعة تجريبية	قياس قبلي	متغير مستقل (برنامج إرشادي)	قياس بعدى	قياس تتبعى
مجموعة ضابطة	قياس قبلي	عدم تطبيق البرنامج	قياس بعدى	لا يوجد قياس تتبعى

1. **مجتمع الدراسة:** تكون المجتمع الأصلي للبحث من طلاب المرحلة الثانوية بمدارس إدارة تعليم جازان، والبالغ عددهم (5109) في العام الجامعي 1444.
2. **عينة الدراسة :** اشتملت عينة الدراسة على عينتين هما:

أ. **العينة الاستطلاعية**: إذ تم اختيار عينة من المراهقين من طلاب المدارس الثانوية بالصف الثالث الثانوي بمدارس في مدينة جيزان قوامها(109) طالب، وكان متوسط أعمارهم (18.5) سنة بغرض التحقق من الخصائص السيكومترية لمقياس الوعى بالأمن السيبراني.

والجدول التالي يوضح المدارس التى سُحبت منها هذه العينة.

جدول(2) يوضح توزيع العينة حسب المدارس الثانوية بجازان

المدارس	العدد	%
ثانوية الأمير عبدالمجيد	18	% 15.5
مدرسة الأمير نايف بن عبدالعزيز	33	30.2 %
مدرسة الأمير محمد بن ناصر	6	% 5.5
مدرسة الخوارزمي	11	% 10.1
مجمع صير التعليمي	41	37.6 %
الإجمالى	109	% 100

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 علي درجات منخفضة على اختبار الوعى بالأمن السيبراني.

وفيما يتعلق بعدد المشاركين من أفراد عينة الدراسة الأساسية، التي جرى عليها تطبيق البرنامج الإرشادي وكانت مكونة من (30) فردًا، منهم (15) طالبًا من عدد أفراد المجموعة التجريبية، وعدد(15) طالبًا من المجموعة الضابطة؛ ومن أجل غايات تحديد أفراد المجموعتين، تم اتباع الخطوات الآتية:

أ. تطبيق اختبار الوعى بالأمن السيبراني.

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

أدوات الدراسة:

اختبار الوعى بالأمن السيبراني: وكانت من إعداد نورة الصانع وآخرين(2020). وتكون الاختبار من (30) بندًا يغطى، بعدين هما البعد الأول (الوعى بمفهوم الأمن السيبرانى) وعدده (7) بنود، والبعد الثانى (طرق المحافظة على أمن المعلومات) وعدد بنوده (23) بندًا لقياس الوعى بالأمن السيبراني، ويتمتع المقياس في صورته الأصلية بخصائص سيكومترية جيدة من الثبات والصدق، فمن ناحية الصدق تم التحقق من صدق الاختبار من قبل معدة بطريقتين: هما الصدق الظاهري، وصدق الاتساق الداخلي.

وأما الثبات، فقد تم التحقق من جزء الاختبار عن طريق ثبات ألفا، والذى بلغ 0.91 وتم تصحيح المقياس من خلال بدائل خمسة، وهى: تنطبق تمامًا ، تنطبق، محايد، لا تنطبق، لا تنطبق تمامًا، وكانت الدرجات من(1الي 5)

التحقق من الخصائص السيكومترية للاختبار في الدراسة الحالية:

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

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

صدق المحكمين :عُرض الاختبار على مجموعة مكونة من (6) أعضاء هيئة من المتخصصين في علم النفس بكلية العلوم الاجتماعية بقسم علم النفس بجامعة الإمام؛ وأكاديمية السعد عبد الله للعلوم الأمنية؛ لإبداء آرائهم وملاحظاتهم حول مناسبة فقرات المقاييس، ومدى وضوح صياغتها اللغوية، وكانت نسبة الاتفاق بينهم على عبارات كل المقاييس من 80 - 90 %

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 (25 %) من درجات الأفراد و أقل (25 %) من درجات الأفراد على الاختبار، وتم حساب المتوسطات، والانحرافات المعيارية للدرجات، وحساب قيمة (ت)، واختبار مستوى الدلالة، كما يوضح الجدول (3)

جدول(3) يوضح دلالة الفروق بين المجموعتين الطرفيتين من العينة الاستطلاعية فى درجات اختبار الوعى بالأمن السيبراني

الوعى بالأمن السيبرانى	المراهقون					
	الأرباعى الأعلى 25 %		الأرباعى الأدنى 25 %		ت	الدلالة
	م	ع	م	ع		
	28	1.1	17.1	2.9	11	0.01

يشير الجدول(3) إلى أن المتوسطات الحسابية والانحرافات المعيارية للإرباعي الأعلى في الدرجات الكلية، لاختبار الوعى بالأمن السيبراني؛ إذ تكون أعلى من المتوسطات الحسابية، والانحرافات المعيارية للإرباعى الأدنى للمقاييس نفسها، كما أن قيمة (ت) كانت دالة جميعها عند مستوى (0,01)، مما يدل على أن مقاييس الدراسة، تتمتع بالقدرة على التمييز بين المستويين القوى والضعيف، مما يعنى تمتع الاختبار بدرجة مقبولة من الصدق

- **حساب ثبات المقاييس:** تم التحقق من ثبات الاختبار على أفراد العينة الاستطلاعية باستخدام عدة طرق، منها: حساب معامل ثبات ألفا، و التجزئة النصفية، إذ بلغت معاملات ثبات ألفا كرونباخ لدرجة الكلية للمقياس (0,78)، وبعد الوعى بمفهوم الأمن السيبرانى بنسبة (0.88) وبعد طرق المحافظة على أمن المعلومات بنسبة (0.89)، ومعاملات ثبات التجزئة النصفية للاختبار ككل بنسبة (0,88)، وتتسم جميع هذه المعاملات بالقبول.

برنامج إرشادي؛ لتنمية الوعى بالأمن السيبراني:

البرنامج الإرشادي: وهو من إعداد الباحثين، وعليه يمكن وصف خطوات البرنامج وتطبيقه على النحو الآتي:

- **الهدف** : يهدف هذا البرنامج إلى تنمية الوعى بالأمن من لدن المراهقين، وإلى تعدد أهداف البرنامج، سواء أكان من حيث نظرته إلى كيفية إكساب المراهقين لمجموعة من الأفكار عن الأمن السيبرانى أم أهميته في تقديم معلومات عن مختلف التهديدات السيبرانية، فضلا عن كيفية المحافظة على أمن المعلومات على جهاز الحاسب الآلي.
- الاطلاع على التراث النظري والإمبريقى، الذى يتناول الأمن السيبرانى، وطرق الوعى به.
- تم تطبيق اختبار الوعى بالأمن السيبراني علي العينة(التدخل الإرشادى) وبناءً على النتائج تم تحديد حاجات العينة للبرنامج، اعتمادًا على مجالات المقياس والنسبة التي تم اعتمدها بوصفها حاجة إرشادية حوالى 50 % في كل بند من بنود اختبار الوعى بالأمن السيبراني.

تم بناء البرنامج الإرشادي وتنظيم محتوياته.

الأسلوب الإرشادي المتبع في تطبيق البرنامج:

اطلع الباحثان على عديد من الكتابات الأجنبية والعربية، ونماذج للبرامج التدريبية لتنمية الوعى بالأمن السيبراني؛ وذلك لاختيار الأسلوب الإرشادي للبرنامج، وقد اتبع الباحثان 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 المستخدمة في البرنامج، وهى 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، واحتساب ما تقتضيه المواقف أثناء الجلسات، والتحصين التدريجي

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

عدد جلسات البرنامج وزمنه :تكون البرنامج من (13) جلسة لمدة (6) أسابيع و(3) أيام ، وكل أسبوع كان عبارة عن جلستين، وكل جلسة كانت مدتها (45) دقيقة في النصف الأول من العام الدراسي (2022/ م) ويوضح الجدول التالي ملخص لجلسات البرنامج:

جدول(4) ملخص الجلسات

رقم الجلسة	عنوان الجلسة	الأهداف	الفنيات المستخدمة	زمن الجلسة	عدد الجلسات
1	تعريف لبرنامج (شرح البرنامج)	بنهاية الجلسة ينبغي على الطالب الدراية بخطوات البرنامج وأهدافه	الحوار. مناقشة جماعية. تعزيز إيجابي.	45 دقيقة	جلسة واحدة
2	تعريف بالأمن السيبراني	بنهاية الجلسة ينبغي على الطالب أن يكون قادرًا على فهم المقصود بالأمن السيبراني. تحديد أهمية الأمن السيبراني. التعرف إلى المفاهيم المرتبطة بالأمن السيبراني	المحاضرة. المناقشة والحوار. العصف الذهني	45 دقيقة	جلسة واحدة

3	تعريف (الوعي بالأمن السيبراني)	بنهاية الجلسة ينبغي على الطالب أن يكون قادرًا على وصف طبيعة الوعي بالأمن السيبراني) 1. التعرف إلى مفهوم الوعي فى إطار تكنولوجيا المعلومات والاتصالات. 2. تحديد مفهوم الوعي بالأمن السيبراني. 3. معرفة أهمية الوعي بالأمن السيبراني.			
4	التعريف بالتهديدات السيبرانية	بنهاية الجلسة ينبغي على الطالب أن يكون على دراية ب: تحديد طبيعة التهديدات السيبرانية. تحديد أشكال التهديدات السيبرانية. معرفة أهم الآثار المترتبة على التهديدات السيبرانية	المحاضرة. المناقشة والحوار	45 دقيقة	جلسة واحدة
5	(البرمجيات الضارة	تهدف الجلسة إلى: التعريف بطبيعة البرمجيات الضارة. رصد أبرز صور البرمجيات الضارة. التعرف إلى أبرز البرامج التي تحمي من الهجمات السيبرانية	-العصف الذهني مناقشة وحوار	45 دقيقة	جلسة واحدة
6	علامات الخطر التي تدل على اختراق الجهاز)	بنهاية الجلسة ينبغي على الطالب أن يكون قادرًا على أن: يحدد علامات اختراق الجهاز يقترح الإجراءات الأمنية للحفاظ على هذا الجهاز من الاختراق. يناقش مواعيد العناية الدورية لصيانة الجهاز. يتجنب مؤشرات اختراق جهاز الكمبيوتر			

7	مخاطر إدمان الألعاب الإلكترونية)	بنهاية الجلسة ينبغي على الطالب أن يكون قادرًا على أن يتعرف إلى ماهية الألعاب الإلكترونية. تحديد الأضرار النفسية و الصحية للألعاب الإلكترونية. إعطاء أمثلة واقعية على أضرار للألعاب الإلكترونية. تحديد كيفية الوقاية من مخاطر الألعاب الإلكترونية	المحاضرة. المناقشة والحوار. العصف الذهني	45 دقيقة	جلسة واحدة
8	السادسة(طرق الحماية من التهديدات السيبرانية)	بنهاية الجلسة ينبغي على الطالب أن يكون قادرًا على أن يراقب الدخول وأنظمة كشف التدخل ويعرف معلومات عن الحماية البرمجية للمعلومات و أنظمة المعلومات والتنبه للعنصر البشري لتحركاته و تصرفاته وحماية المعلومات الحساسة	المحاضرة. المناقشة والحوار. التعزيز الإيجابي.	45 دقيقة	جلسة واحدة
9	الإجراءات الوقائية لتحصين الحاسب	بنهاية الجلسة ينبغي على الطالب أن يكون قادرًا على أن: يوضح الإجراءات الوقائية لتحصين الحاسب الشخصي . يحدد الإجراءات الوقائية لتحصين الهاتف الذكي. يمهر في اتباع الإجراءات الوقائية لتحصين الحاسب. يطرح أمثلة للإجراءات الوقائية لتحصين الحواسب	المحاضرة. المناقشة والحوار. التعزيز الإيجابي.	45 دقيقة	جلسة واحدة

10	(المعرفة بالقوانين التشريعات السعودية لمكافحة الجرائم المعلوماتية في المملكة العربية السعودية	بنهاية الجلسة ينبغي على الطالب أن يكون قادرًا على أن: يدرك مفهوم الجريمة الإلكترونية يعرف الضوابط الرئيسة للأمن السيبرانى في المملكة العربية السعودية. يسلط الضوء على قانون مكافحة الجرائم الإلكترونية. يتبين خطورة الجرائم الإلكترونية		45 دقيقة	جلسة واحدة
11	(تعزيز الوعى بطرق المحافظة على نظام الأمن السيبرانى)	1-تحقيق الامتثال لرأي الخبراء بشأن حماية أنظمة المعلومات. 2- التوعية لتحديث برنامج الحماية من الفيروسات. 3-التوعية باستخدام برنامج الحماية. 4- التوعية بعمل نسخة احتياطية للملفات.	المحاضرة. المناقشة والحوار. التعزيز الإيجابي	45 دقيقة	جلسة واحدة
12	التقييم	1-بيان مدى الإفادة من البرنامج الإرشادي. 2-توضيح كيفية الاحتفاظ بالمكاسب المحققة. 3-تهيئة الطلاب لإنهاء البرنامج الإرشادي.	المناقشة الجماعية والحوار. العصف الذهني. عرض الآراء		
13	(ختام البرنامج الإرشادي)	1-ممارسة جلسة ختامية. 2-مناقشة إيجابيات البرنامج الإرشادي وسلبياته. 3-إجراء التطبيق البعدي لمقاييس الدراسة	المناقشة الجماعية والحوار. العصف الذهني. عرض الآراء	45 دقيقة	جلسة واحدة

تقويم البرنامج الإرشادي: وضع الباحثان التقويم التالي:

أ. **القياس القبلي**: من خلال تطبيق اختبار الوعى بالأمن السيبراني، قُدم للطلبة(

الضابطة والتجريبية) قبل بداية تطبيق البرنامج الإرشادي.

ب. **القياس البعدى** : قياس تطبيق اختبار الوعى بالأمن السيبراني، قُدم للطلبة (الضابطة والتجريبية) بعد تطبيق البرنامج الإرشادي؛ بهدف التأكد من فاعلية البرنامج المعد لتنمية الوعى بالأمن السيبراني.

ج. **القياس التتبعى**: قياس اختبار الوعى بالأمن السيبراني، قُدم للطلبة (التجريبية)، بعد شهر من تطبيق البرنامج الإرشادي؛ بهدف التأكد من استمرار فاعلية البرنامج المعد لتنمية الوعى بالأمن السيبراني.

د. المقارنة بين القياس القبلي والقياس البعدي، والقياس التتبعى.

خامسًا- الأساليب الإحصائية: اختبار(ت) و اختبار مان وتنى و اختبار ولكوكسن.

عرض نتائج الدراسة ومناقشتها:

يستعرض الباحثان النتائج التي توصلت إليها الدراسة الحالية، وفقًا للتساؤل الذى طرحته الدراسة الحالية على النحو الآتى:

نتائج الفرض الأول و مناقشتها :

ينص الفرض الأول على أنه" توجد فروق دالة إحصائيًا في رتب متوسطات درجات أفراد المجموعة التجريبية، ورتب متوسطات درجات أفراد المجموعة الضابطة على مقياس الوعى بالأمن السبيرانى، بعد تطبيق البرنامج الإرشادي

ومن أجل التحقق من صحة هذا الفرض، تم استخدام اختبار مان ويتني للفروق بين مجموعتين مستقلتين، وكانت النتائج كما في الجدول التالي:

جدول (5)يبين نتائج اختبار مان وتنى للفروق بين درجات المجموعة التجريبية والضابطة، على اختبار الوعى بالأمن السيبراني بعد تطبيق البرنامج.

المجال	المجموعة	العدد	متوسط الرتب	مجموع الرتب	قيمة Z	مستوى الدلالة
الوعى بمفهوم الأمن السيبرانى	تجريبية	15	20.07	301.00	-2.891-	.004
	ضابطة	15	10.93	164.00		
	الإجمالى	30				
طرق المحافظة على أمن المعلومات	تجريبية	15	8.00	120.00	-4.691	0.00
	ضابطة	15	23.00	345.00		
	الإجمالى	30				

يتبين من الجدول السابق وجود فروق دالة إحصائيًا عند مستوى دلالة (0.001) بين درجات المجموعتين التجريبية، والضابطة في اختبار الوعى بالأمن السيبراني، بعد تطبيق البرنامج الإرشادي في اتجاه المجموعة التجريبية: بمعنى أن درجات أفراد المجموعة التجريبية على اختبار الوعى 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، بوساطة استخدام عدة فنيات؛ بهدف تنمية الوعى بالأمن السيبراني، وهذه الفنيات، مثل: المحاضرة، المناقشة، الحوار، العصف الذهني ، ورشة العمل

وهو ما يعني أن درجات أفراد المجموعة التجريبية - في القياس البعدي على اختبار الوعى بالأمن السيبرانى- كانت أعلى من درجات المجموعة الضابطة ، وقد جاءت هذه النتيجة في الاتجاه المتوقع ، وهو ما يمثل حدث تحسنٍ في مستوى الوعى بالأمن السيبراني من لدن أفراد المجموعة التجريبية، بعد تطبيق البرنامج الإرشادي، وتؤكد هذه النتيجة -من لدنها- فاعلية البرنامج الإرشادي، وأنه يؤدي إلى تحسين مستوى الوعى بالأمن السيبراني؛ إذ يمكن تفسير هذه النتيجة بأن البرنامج الإرشادي، قد أتاح الفرصة أمام أفراد المجموعة التجريبية؛ لإمكان التعرف إلى الأمن السيبرانى من خلال ما تم توفيره بالبرنامج الحالي من أنشطة متكاملة تختص بالأمن المعلوماتي، وهو ما يعزز الحماية والتثقيف بالأمن السيبرانى، وكذلك توفير فيديوهات تعليمية حول مخاطر الأمن السيبرانى وتهديداته، فضلا عن وجود تعليمات للحفاظ على الأمن السيبرانى، كما تجلت المشاركة الإيجابية للطلاب بالبرنامج الإرشادي في تنمية وعيهم للحفاظ على بيئة إلكترونية آمنة، من خلال اتباع

الإجـراءات اللازمـة لتأميـن المعلومـات، والعمـل علـى تطبيـق ذلـك للعمـل بشـكل مسـتمر ، وجـاءت هـذه النتيجـة متسـقة مـع نتائـج دراسـة إبراهيـم(2021) التـى أسـفرت عـن وجـود فـرق ذي دلالـة إحصائيـة عنـد مسـتوى (0,05)، بيـن متوسـطي درجـات المعلمـات في التطبيقيـن القبلي والبعـدي لمقيـاس الوعـي؛ لصالـح التطبيـق البعـدي؛ واتسـقت - أيضًـا- مـع نتائـج دراسـة متولـي (2021) التـي كشـفت عـن وجـود علاقـة إيجابيـة ذات دلالـة إحصائيـة، بيـن معـدل تعـرض المبحوثيـن لفيديوهـات الأمـن الإلكترونـي باليوتيـوب، ومسـتوى الوعـي بالأمـن الإلكترونـي مـن لدنهـم

وتتسـق النتيجـة الحاليـة مـع نتائـج دراسـة (Bada&surse,2020) التـي كشـفت عـن فاعليـة برنامـج تدريبـى فـي تعزيـز الممارسـات المتعلقـة، بالتفكيـر والثقافـة المرتبطـة بالأمن السـيبراني، مـع نتائـج دراسـة (Chang & Coppel, 2020) التـي كشـفت عـن قـدرة برنامـج تدريبـي؛ لتعزيـز الوعـي بالأمـن السـيبراني مـن لـدن العامليـن فـي البنـوك. وفـى المقابـل تناقضـت النتيجـة الحاليـة مـع نتائـج دراسـة (Banfield, 2016) التـى كشـفت عـن عـدم وجـود تأثيـر ذي دلالـة لتطبيـق برنامـج الوعـي بالأمـن السـيبراني فـي تغييـر السـلوكيات الأمنيـة مـن لـدن العامليـن. كمـا تناقصـت مـع نتائـج دراسـة (Proctor,2016) التـي توصلـت إلـى عـدم تحقيـق برنامـج تدريبـي لتنميـة الوعـي بالأمـن السـيبراني

مـن جهـة ثانيـة، وفـرت هـذه الفنيـات فرصًـا مناسـبة وتجـارب حيـة عاشـها أفـراد المجموعـة التجريبيـة طـوال انتظامهـم فـي البرنامـج، وأكسـبتهم لجملـة مـن الممارسـات كانـت لازمـة للمحافظـة علـى أمـن المعلومـات والوعـى، بمختلـف التهديـدات السـيبرانية، كمـا أن أفـراد المجموعـة التجريبيـة قـد شـاركوا بنشـاط فعـال فـي الجلسـات الإرشـادية، فلـم يكونـوا مسـتقبلين فقـط، بـل إنهـم مارسـوا وتفاعلـوا تفـاعلا مباشـرًا مـن خلال الأداء العلمـي تحـت إشـراف الباحثيـن وتوجيهمـا . وتتفـق هـذه النتيجـة مـع عديـد مـن الدراسـات: ومنهـا، دراسـة (Bicak et al,2015) التـي خلصـت إلـى وجـود فـروق بيـن المجموعـة الضابطـة، والتجريبيـة مـن طلاب الدراسـات العليـا فـي مسـتوى الأمـن السـيبرانى ، وتتفـق هـذه النتيجـة مع نتائـج دراسـة (Li et al. 2020) التـي توصلـت إلـى فاعليـة برنامـج يقـوم علـى التعليـم غيـر المنهجـي ،والحقائـب التعليميـة فـي تنميـة الوعـى بالأمـن السـيبراني

نتائـج الفـرض الثانـى و مناقشـتها: والـذى مؤداهـا" لا توجـد فـروق دالـة إحصائيًـا فـي رتـب متوسـطات درجـات أفـراد المجموعـة التجريبيـة، و و مقيـاس الوعـى بالأمـن السـيبرانى بيـن التطبيـق البعـدي والتتبعـى (بعـد شـهر) للبرنامـج الإرشـادي .وللتحقـق مـن هـذا الفـرض تـم اسـتخدام اختبـار ويلكوكسـون للرتـب ذات الإشـارة (Wilcoxon Signed Ranks Test)

جدول (6)يبين نتائج اختبار ويلكوكسون للفروق، بين درجات المجموعة التجريبية على اختبار الوعى بالأمن السيبراني، للقياس البعدي والتتبعى على المجموعة التجريبية.

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

يشير جدول(6) إلى عدم وجود فروق ذات دلالة إحصائية، بين القياس البعدي والتتبعي في الوعى بالأمن السيبراني بأبعاده المختلفة، وهذا يدل على بقاء تأثير البرنامج في تنمية الوعى بالأمن السيبراني من لدن أفراد المجموعة التجريبية، فضلا عن عدم زوال هذا التأثير بين التطبيقين البعدي والتتبعي

ويمكن القول إن فنيات البرنامج الإرشادي من لدن أفراد المجموعة التجريبية قد أسهمت، في تنمية الوعى بالأمن السيبرانى من لدنهم، من خلال البرنامج الإرشادى القائم على فنيات الحوار والمناقشة، والمحاضرة والفيديو في مختلف الجلسات.

كما يرجع استمرار تأثير البرنامج في تنمية الوعى بالأمن السيبراني من لدن المجموعة التجريبية إلى محتوى البرنامج، الذي تم تدريبهم عليه، وما تضمنه من معلومات بشأن التهديدات السيبرانية، فضلا عن كيفية المحافظة على أمن المعلومات وطرق الوقاية من الاختراق والمعرفة، بالتشريعات القانونية للجرائم والاختراقات السيبرانية، وكل هذا قد أسهم في تنمية الوعى بالأمن السيبرانى من لدن المجموعة التجريبية

ومن جهة أخرى، يرجع السبب في استمرار فعالية البرنامج إلى دور الباحثين أثناء تطبيق البرنامج من حيث توفير بيئة، تقوم على جو الود والحب والألفة والمرح، وهو ما حاول الباحثان توفيره أثناء الجلسات التى أسهمت فى هذه الأمور بوساطة استمرار فاعلية البرنامج، بعد شهر من تطبيقه على المجموعة التجريبية

إضافة إلى ذلك يدعم هذه النتيجة ما أشارت إليه نتائج دراسات المنتشري وحريري 2020 ، والقحطاني 2019 ، والصحفي وعسكول 2019 ، وصائغ2018.

توصيات الدراسة :

في ضوء النتائج الحالية يوصى الباحثان بما يأتي:

1. ضرورة التوسع في بناء البرامج الإرشادية، والتدريبية القائمة على مختلف التوجهات العلمية؛ لتنمية الوعى بالأمن السيبرانى من لدن الآباء والمعلمين، والطلاب في مختلف المراحل التعليمية.
2. تنمية وعى القائمين على الرعاية النفسية للطلاب تجاه المخاطر النفسية للتهديدات السيبرانية، وخاصة الاختصاصيين والمرشدين النفسيين بالمدارس، وتدريبهم على التدابير، والإجراءات والاحتياطات الأمنية التي يجب نقلها، وتنميتها للطلاب .
3. تصميم برامج إرشادية لرجال الأمن السيبرانى، بشأن التوعية بالعوامل البشرية المسؤولة عن قيام الفرد بالتهديدات السيبرانية، كذلك العوامل البشرية الكامنة وراء عدم المحافظة على أمن المعلومات.
4. دمج الأمن السيبرانى ضمن المقررات الدراسية في المدارس والجامعات.

البحوث المقترحة

1. دراسة العوامل النفسية(المعرفية والمزاجية) المرتبطة بالأمن السيبرانى
2. بناء أدوات نفسية ذات خصائص سيكومترية جيدة في البيئة السعودية؛ للكشف عن مستوى الوعى بالأمن السيبرانى.

قائمة المصادر والمراجع:

أولاً: المراجع العربية:

إبراهيم، منال حسن محمد (2021). الوعى بجوانب الأمن السيبرانى في التعليم عن بعد. المجلة العلمية لجامعة الملك فيصل العلوم الإدارية، *22*(2)، 307-299

خليفة، إيهاب (2017). تنامي التهديدات السيبرانية للمؤسسات العسكرية. مجلة اتجاهات الأحداث، (22)، (جويلية/ أوت). https://doi.org/10.12816/0040763

الرويس، فيصل بن عبد الله (2013). الآثار الاجتماعية لإدمان الإنترنت: دراسة ميدانية على عينة من طلاب و طالبات الصف الثالث الثانوي بمحافظة عفيف. مجلة مركز الخدمة للاستشارات البحثية، (47)، 168-128.

الصانع، نورة (2020). وعي المعلمين بالأمن السيبرانى وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. مجلة كلية التربية، *36*(6)، 57-41.

الصانع، نورة عمر و عسران، عواطف سعد الدين و السواط، حمد بن حمود بن حميد و أبو عيشة، زاهدة جميل نمر و سليمان، إيناس السيد محمد (2020). وعي المعلمين بالأمن السيبرانيّ وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. مجلة البحث العلمي في التربية، *36*(6)، 90-41

صائغ، وفاء حسن عبدالوهاب (2018). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم لأمنية من الجرائم الإلكترونية. المجلة العربية للعلوم الاجتماعية، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية، *3*(14)، 70-18

الصحفي، مصباح أحمد حامد و العسكول، سناء صالح (2019). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. مجلة البحث العلمي في التربية، *20*(10)، 493 534-. https://doi.org/10.21608/jsre.2019.56490

طه، فرج عبد القادر وعبد الفتاح، مصطفى كامل ومحمد، حسين عبد القادر وقنديل، شاكر عطية (2003). موسوعة علم النفس والتحليل النفسي (ط2). دار غريب.

الظويفري، مشاعل شيب (2021). واقع الأمن السيبراني وزيادة فاعليته في التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية. المجلة الدولية للدراسات التربوية والنفسية، *10*(3)، 655-635. https://doi.org/10.31559/EPS2021.10.3.7

فرماوي، محمد (1992). برامج التخطيط التربوية. مكتبة الأنجلو المصرية.

القحطاني، نورة بنت ناصر (2019). مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. مجلة شؤون اجتماعية، 120-85. https://doi.org/10.35217/0048-036-144-004

القيسي، محمد وائل (2020). مستقبل الأمن الاستراتيجي العالمي في ظل التحديات التكنو - معلوماتية والفضاء السيبراني. مجلة دراسات إقليمية، *13*(44)، 139--173. https://doi.org/10.33899/regs.164427.2020

متولي، عمار أحمد (2021). دور اليوتيوب في تنمية وعي المراهقين بالأمن الإلكتروني. مجلة بحوث العلاقات العامة الشرق الأوسط، (31)، 389-349

المنتشري، فاطمـة، و حريري، رندة (2020) درجـة وعـى معلمـات المرحلة المتوسطة بالأمن السيبرانى في المدارس العامة بمدينـة جـدة مـن وجهة نظر المعلمات. المجلة العربية للتربيـة النوعيـة. المؤسسـة العربيـة للتربيـة والعلـوم والآداب، *14*(1)، 95 – 140.

المنيـع، الجوهـرة عبـد الرحمـن (2022). متطلبـاتُ تحقيـقِ الأَمـن السـيبرانيّ في الجَامِعَـات السـعوديَّة في ضـوء رؤية 2030. مجلـة كليـة التربيـة، *38*(4)،194-155

الهيئـة الوطنيـة للأمـن السـيبراني (2020). الاستراتيجيـة الوطنيـة للأمـن السـيبراني. المملكـة العربية السـعودية. sa .gov. nca//:

ثانياً: المراجع الأجنبية

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. *International Journal for Information Security Research* (IJISR), *6*(2), 660-666. https://doi.org/10.20533/ijisr.2042.4639.2016.0076

Ahram, T., & Karwowski, W. (Eds.). (2019). *Advances in Human Factors in Cybersecurity*: Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity, July 24-28, 2019, *960*, Springer. https://doi.org/10.1007/978-3-030-20488-4

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 2-16. https://doi.org/10.3390/fi11030073

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), 1-13. https://doi.org/10.1016/j.heliyon.2021.e06016

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information and Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Bada, M., & Nurse, J. R. (2020). *The social & psychological impact of cyberattacks. In Emerging cyber threats & cognitive vulnerabilities* (pp. 73-92). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00004-6

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

Bicak, A., Liu, X. M., & Murphy, D. (2015). Cybersecurity curriculum development: introducing specialties in a graduate program. *Information Systems Education Journal*, *13*(3), 99-110.

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*, *7*(4), 68-82. https://doi.org/10.4018/IJCBPL.2017100106

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. https://doi.org/10.1089/cyber.2012.0098

Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. *Computers & Security*, *97*(2), 1-10. https://doi.org/10.1016/j.cose.2020.101959

Ciolan, I. M. (2014). Defining cybersecurity as the security issue of the twenty first century. A constructivist approach. *Revista de Administratie Publica si Politici Sociale*, *12*(1), 40.120-136

Coutlee, C. G., Politzer, C. S., Hoyle, R. H., & Huettel, S. A. (2014). An abbreviated impulsiveness scale constructed through confirmatory factor analysis of the Barratt. impulsiveness scale version 11. *Archives of scientific psychology*, *2*(1), 1-12. https://doi.org/10.1037/arc0000005

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review. 4*(10), 13-21. https://doi.org/10.22215/timreview/835

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. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x

Hadlington, L., & Parsons, K. (2017). Can cyberloafing and Internet addiction affect organizational information security?. C*yberpsychology, Behavior, and Social Networking*, *20*(9), 567-571. https://doi.org/10.1089/cyber.2017.0239

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. . *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks* (January 2, 2015). https://doi.org/10.2139/ssrn.2544742

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., ... & Chen, J. (2016, November). *Cultural and psychological factors in cyber-security. In Proceedings of the 18th International Conference on Information Integration and Web-based Applications and* Services (pp. 318-324). https://doi.org/10.1145/3011141.3011165

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, *18*, 106-125. https://doi.org/10.1057/ejis.2009.6

Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A *survey. ACM Computing Surveys*, *53*(1), 1-34. https://doi.org/10.1145/3372823

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*. https://doi.org/10.1016/j.cose.2021.102267

Li, J., Pang, M., Smith, J., Pawliuk, C., & Pike, I. (2020). In search of concrete outcomes—A systematic

review on the effectiveness of educational interventions on reducing acute occupational injuries. *International journal of environmental research and public health, 17*(18), 6874. https://doi.org/10.3390/ijerph17186874

Maasberg, M., Van Slyke, C., Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. *Communications of the ACM, 63*(12), 64-80. https://doi.org/10.1145/3408864

Odemis, M., Yucel, C., & Koltuksuz, A. (2022). Detecting User behavior in cyber threat intelligence: development of Honeypsy system. Security & Communication Networks, (*22)*. https://doi.org/10.1155/2022/7620125

Parsons, K., McCormac, A., Pattinson, M., Jerram, C., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others?. *Information Management & Computer Security*, *20*(1), 18-28. https://doi.org/10.1108/09685221211219173

Proctor, W. R. (2016). *Investigating the efficacy of cybersecurity awareness training programs* [Doctoral dissertation*,* Capstone Project Submitted to the Faculty of Utica College].

Raineri, E. M., & Resig, J. (2020). Evaluating Self-Efficacy Pertaining to Cybersecurity for Small Businesses. *Journal of Applied Business & Economics*, *22*(12), 13-23. https://doi.org/10.33423/jabe.v22i12.3876

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. https://doi.org/10.1089/cyber.2019.0370

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2019). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology, 21*(3), 26-39. https://doi.org/10.4018/JCIT.2019070102

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. https://doi.org/10.4018/978-1-7998-7705-9.ch008

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). https://doi.org/10.1007/978-3-319-25512-5_11

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, *9*(4), 475–480. https://doi.org/10.1037/ppm0000247

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. oup usa.

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. https://doi.org/10.1089/cyber.2014.0207

Waasdorp, T. E., & Bradshaw, C. P. (2015). The overlap between cyberbullying and traditional bullying. *Journal of adolescent health*, *56*(5), 483-488. https://doi.org/10.1016/j.jadohealth.2014.12.002

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. https://doi.org/10.11610/isij.3503

Romanized Arabic References: الترجمة الصوتية لمصادر ومراجع اللغة العربية:

ʾibrāhīmu manālu ḥasani muḥammadin (2021). alwiʻā bijawānibi alʾamni al-saybrānā fī al-taʻlīmi ʻan buʻdin almajallatu alʻilmiyyatu lijāmiʻati almaliki fayṣala alʻulūmi al-ʾidāriyyatu 22(2)، 299-307

khlyfa ʾīhāb (2017). tanāmī al-tahdīdāti al-sybrānyya lil-muʾusasāti alʻaskariyyati mijallatu attijāhāti alʾaḥdāthi) ،(22) jīlya / ʾawt https://doi.org/10.12816/0040763

alrūʾaysi fyṣl bnu ʻabdi Allāhi (2013). alʾāthāru aliājtimāʻiyyatu liʾidmāni alʾintarniti dirāsatun muydiāanaya ʻalā ʻīnatin min ṭullābi wa ṭālibāti al-ṣaffi al-thālithi al-thianwiyyi bimuḥāfaẓati ʻafīfin mijallatu markazi alkhidmati lil-iāstishārit albaḥthiyyati (47).128-168 ،

al-ṣāniʻu nawratu (2020). wuʻiyyu almuʻallimīna bi-l-ʾāmni al-saybrānā waʾasālībi ḥimāyati al-ṭalabati min makhāṭiri alʾintarnit wataʻzīzi alqiyami wa-l-haīta alwaṭaniyyati ladayhim mijallatu kulliyyati al-tarbiyati 36(6).41-57 ،

al-ṣāniʻu nūratu ʻumara wa ʻusrānu ʻawāṭifu saʻdi al-dīni wa al-sawwāṭu ḥamdu bnu ḥumūdi bni ḥumaydin wa ʾabū ʻayshata zāhidatu jamīli namirin wa sulaymānu ʾīnāsu al-sayyidi muḥammad (2020). wuʻiyyu almuʻallimīna bi-l-ʾāmni al-sībrāniyyi waʾasālību ḥimāyati al-ṭalabati min makhāṭiri alʾintarniti wataʻzīzi alqiyami wa-l-haīta alwaṭaniyyati ladayhim mijallatu albaḥthi alʻilmiyyi fī al-tarbiyati 36(6).41-90 ،

ṣāʾighun wafāʾu ḥasin ʻubdāliwhāb (2018). wuʻiyyu ʾafrādi alʾusrati bimafhūmi alʾamni al-saybrāniyyi waʻalāqatuhu biāḥtīāṭātihim liʾamniyyatin mina aljarāʾimi alʾilktrūniyyati almajallatu

al‘arabiyyatu lil-‘ulūmi aliājtimā‘iyyati almu’uassasatu al‘arabiyyatu lil-iāstishārit al‘ilmiyyati watanmiyyati almawāridi albashariyyati 3(14).18-70 ،

al-ṣaḥafiyyu miṣbāḥu ’aḥmada ḥāmidin w al‘askūlu sanā’u ṣāliḥin (2019). mustawā alwa‘yi bi-l-’āmni al-sybrānyyi ladā mu‘allamāti alḥāsibi al’ālayi lil-marḥalati al-thāniwayti bimadīnati jda mjla albaḥthi al‘ilmiyyi fī al-tarbiyati 20(10)534- 493 ،. https://doi.org/10.21608/jsre.2019.56490

ṭh farajun ‘abdu alqādiri wa‘abdu alfattāḥi muṣṭafā kāmilin wamuḥammadun ḥusaynu ‘abdu alqādiri waqandīlun shākiru ‘aṭiyyata (2003). mawsū‘atu ‘ilmi al-nafsi wa-l-taḥlīli al-nafsiyyi)t2 .(dāru gharībin

al-ẓuīfriyyu mshā‘l shyb (2021). wāqi‘u al’amni al-sybrānā wazīādatu fā‘iliyyatihi fī al-ta‘līmi al‘āmmi biminṭaqatin almadīnati almunawwarati min wijhati naẓari alqīādati almadrasiyyati almajallatu al-dawliyyatu lil-dirāsāti al-tarbawiyyati wa-l-nafsiyyati 10(3)635-655 ،. https://doi.org/10.31559/EPS2021.10.3.7

farmāwiyyun muḥammadun (1992). barāmiju al-takhṭīṭi al-tarbawiyyati mtba al-’ānjulū almiṣriyyatu

alqaḥṭāniā nwra bintu nāṣirin (2019). madā tawāfuri alwa‘yi bi-l-’āmni al-sybrānā ladā ṭilābi waṭāalbiāt aljāmi‘āti al-su‘ūdiyyati min manẓūrin ajtimā‘iyyin dirāsatun maydāniyyatin mijallatu shu’ūn ajtimā‘iyyatin 85-120. https://doi.org/10.35217/0048-036-144-004

alqaysiyyu muḥammad wā’il (2020). mustaqbilu al’amni al-astirātiyyijy al‘ālamiyyi fī ẓilli al-taḥaddīāti al-taknū - ma‘alliwwamātya wa-l-faḍā’u al-sybrānyyu mijallatu dirāsātin ’iqlīmiyyatin 13(44)-173–139 ،. https://doi.org/10.33899/regs.2020.164427

mutawallī ‘ammārun ’aḥmadu (2021). dawru alyiwtīūb fī tanmiyati wa‘yi almurāhiqīna bi-l-’āmni al’iliktirūniyyi mijallatu buḥūthi al‘alāqāti al‘āmmati al-sharqu al’awsaṭu (31).349-389 ،

al-mntshry fāṭma w ḥryry rnda (2020) drja w‘ā m‘lmāt almarḥalatu al-mtwsṭa bi-l-’āmni al-sybrānā fī almadārisi al‘āmmati bmdyna jda min wjha nẓr almu‘allamāti almajallatu al‘arabiyyatu lltrbya al-nw‘ya al-m’ussa al-‘rbya lltrbya wa-l-‘lwm wa-l-’ādāb 14(1).140 – 95 ،

almanī‘i aljawharati ‘abdi al-Raḥmāni (2022). mutaṭallabāti taḥqīqi al’amni al-saybrāniyyi fī aljāmi‘āti al-su‘ūdiyyati fī ḍaw’i ru’uyati 2030. mijallatu kulliyyati al-tarbiyati 38(4). 155-194،

al-hy’i alwaṭaniyyatu lil-’āmni al-sībrānyyi (2020). aliāstirāatyijjaya alwaṭaniyyatu lil-’āmni al-sībrānā almamlakatu al‘arabiyyatu al-su‘ūdiyyatu

The Effectiveness of a Counselling Program in Developing Awareness of Cyber Security Among Internet Users: The Case of Secondary School Students in the Province of Jazan

Abdel-Mreed Abdel-Jaber Qasim(1)

Turki Bandr Al-Enezi(2)

Abstract:

This study aimed to investigate the effectiveness of a counseling program in enhancing cybersecurity awareness among adolescents. The sample consisted of 30 individuals, with 15 students from the experimental group and 15 from the control group, all of whom were high school students in Jizan. The study utilized a cybersecurity awareness test developed by Noura Al-Saane and others (2020) and a counseling program designed to improve cybersecurity awareness. The study revealed statistically significant differences at a significance level of 0.001between the pre-test and post-test scores on the cybersecurity awareness test, with the experimental group performing better after the program was applied. Additionally, the study found statistically significant differences at the significance level of 0.001 between the experimental and control groups on the cybersecurity awareness test, after applying the counseling program, with the experimental group showing higher scores. However, there were no statistically significant differences between the post-test and follow-up measurements in the various dimensions of cybersecurity awareness.

Based on these results, a set of recommendations was proposed.

Keywords: Awareness of cyber security. Counselling Program.

(1) Faculty of Education - Imam Muhammad Ibn Saud Islamic University (Riyadh – K.S.A.)
kasmabdo2@gmail.com

(2) Saad Al-Abdullah Academy for Security Sciences Hospital (Kuwait City – Kuwait)