# تصميم بيئة تعلم إلكترونية تكيفية لتنمية مهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم

# Designing an adaptive e-learning environment to develop cybersecurity skills among educational technology specialists

**إعداد:**

**سيد نوح سيد عبدالجواد**

رئيس قسم الموهوبين والتعلم الذكي بإدارة الموهوبين والتعلم الذكي – الفيوم

**ا.د/ حسام الدين حسين ابو الهدى**

أستاذ المناهج وطرق تدريس الدراسات الاجتماعية ومستشار رئيس الجامعة لشئون البيئة والمجتمع سابقاً – جامعة الفيوم

**ا.د/ الغريب زاهر اسماعيل**

أستاذ تكنولوجيا التعليم ووكيل كلية التربية لشئون التعليم والطلاب السابق جامعة المنصورة

**د/ أيمن جبر محمود**

مدرس تكنولوجيا التعليم

كلية التربية النوعية جامعة الفيوم

## المستخلص باللغة العربية

هدف البحث الحالي إلى تنمية مهارات الأمن السيبراني لدى أخصائي تكنولوجيا التعليم، من خلال تصميم بيئة تعلم إلكترونية تكيفية، وتكونت عينة البحث من (60) أخصائي تكنولوجيا التعليم من أخصائيين المرحلة الإعدادية والثانوية، وقسمت عينة البحث إلى مجموعتين (تجريبية، وضابطة) المجموعة التجريبية الأولى استخدمت بيئة تعلم إلكترونية تكيفية، وكان عددها(30) أخصائي، أما المجموعة الضابطة الثانية استخدمت بيئة تعلم إلكترونية، وكان عددها(30) أخصائي، وتمثلت أدوات البحث في: اختبار تحصيل معرفي لقياس الجوانب المعرفية لمهارات الأمن السيبراني

لدى أخصائي تكنولوجيا التعليم، وبطاقة ملاحظة لقياس الجوانب الأدائية لمهارات مهارات الأمن السيبراني لدى أخصائي تكنولوجيا التعليم، وبعد تطبيق أدوات البحث قبليًا وبعديًا وباستخدام المعالجات الإحصائية تم التوصل إلى النتائج التالية: تفوق طلاب المجموعة التجريبية على نظرائهم طلاب المجموعة الضابطة في التطبيق البعدي للجانب المعرفي والأداء المهاري لمهارات الأمن السيبراني.

**الكلمات المفتاحية:** بيئة تعلم إلكترونية تكيفية– الأمن السيبراني.

## Abstract

The current research aimed to develop the cybersecurity skills of educational technology specialists, through designing an adaptive electronic learning environment. The research sample consisted of (60) educational technology specialists from middle and high school specialists. The research sample was divided into two groups (experimental and control), the first experimental group. An adaptive electronic learning environment was used, and its number was (30) specialists. As for the second control group, it used an electronic learning environment, and its number was (30) specialists. The research tools were: a cognitive achievement test to measure the cognitive aspects of the cybersecurity skills of an educational technology specialist, and a note card. To measure the performance aspects of the cybersecurity skills of educational technology specialists, and after applying the research tools pre- and post-application and using statistical treatments, the following results were reached: The students of the experimental group outperformed their counterparts, the students of the control group, in the post-application of the cognitive aspect and skill performance of cybersecurity skills.

Keywords: adaptive e-learning environment - cybersecurity.

## المقدمة:

يشهد التعليم في جميع أنحاء العالم تحولات نموذجية كبيرة في الممارسات التعليمية للتدريس والتعلم تحت مظلة بيئة التعلم التي تدعم تكنولوجيا المعلومات والاتصالات، ويشهد العالم نموًا تلقائيًا في تكنولوجيا الاتصالات وشبكات الكمبيوتر وتكنولوجيا المعلومات، وأدى إلى تطوير خدمات اتصالات جديدة ذات نطاق عريض وتقارب الاتصالات السلكية واللاسلكية مع أجهزة الكمبيوتر، ويمكن القول بأن بيئات التعلم الإلكترونية هي خلق إمكانيات عديدة لاستخدام مجموعة متنوعة من أدوات التكنولوجيا الجديدة لنظام التعليم والتعلم.

وفي السنوات الأخيرة، تقدمت تكنولوجيا التعليم بمعدل سريع، فبمجرد تخصيص تجارب التعلم، يصبح محتوى التعلم الإلكتروني أكثر ثراءً وتنوعًا، وينتج التعلم الإلكتروني نتائج تعليمية بناءة، لأنه يسمح للطلاب بالمشاركة بنشاط في التعلم في أي وقت وفي أي مكان، وأصبح التعلم الإلكتروني التكيفي نهجًا يتم تنفيذه على نطاق واسع من قبل مؤسسات التعليم، ومن خلال ذلك ظهرت بيئات التعلم الإلكترونية التكيفية، وأصبح التعلم الإلكتروني التكيفي نهجًا يتم تنفيذه على نطاق واسع من قبل مؤسسات التعليم.

بيئة التعلم الإلكتروني التكيفي مجال بحثي يتعامل مع نهج التطوير لتلبية أنماط التعلم لدى الطلاب من خلال تكييف بيئة التعلم داخل نظام إدارة التعلم لتغيير مفهوم تقديم المحتوى الإلكتروني، فعملية التعلم يتم فيها تعليم المحتوى أو تكييفه بناءً على استجابات أنماط التعلم أو تفضيلات المتعلمين، ومن خلال تقديم محتوى مخصص تعمل بيئات التعلم الإلكتروني التكيفية على تحسين جودة التعلم عبر

الإنترنت (Truong, 2016) [1]، وفي بيئات التعلم الإلكتروني التقليدية الحالية، اتبع التعليم نهج "نمط واحد يناسب الجميع"، مما يعني أن جميع الطلاب يتعرضون لنفس إجراءات التعلم، ولا يأخذ هذا النوع من التعلم في الاعتبار أنماط التعلم المختلفة وتفضيلات الطلاب حاليًا، استوعب تطوير أنظمة التعلم الإلكتروني ودعم التعلم الشخصي، حيث يتم تكييف التعليم مع الاحتياجات الفردية للطلاب وأنماط التعلم، تتيح بعض الأساليب الشخصية للطلاب اختيار المحتوى الذي يتناسب مع شخصيتهم، ويعد تقديم مواد الدورة قضية مهمة في التعلم الشخصي، علاوة على ذلك، يمثل تصميم نظام تعليم إلكتروني مصمم جيدًا وفعال وقابل للتكيف تحديًا بسبب تعقيد التكيف مع الاحتياجات المختلفة للمتعلمين بغض النظر عن استخدام التعلم الإلكتروني التي تفيد بأن التحول إلى بيئات التعلم الإلكتروني التكيفية قادر على تعزيز مشاركة الطلاب، ومع ذلك، لا يمكن اعتبار بيئة التعلم متكيفة إذا لم تكن مرنة بما يكفي لاستيعاب أنماط التعلم لدى الطلاب ( Ennouamani & Mahani, 2017)، وفي بيئات التعلم الإلكتروني، يتم بناء التكيف على سلسلة من العمليات المصممة جيدًا لتناسب المواد التعليمية، ويحاول إطار التعلم الإلكتروني التكيفي مطابقة المحتوى التعليمي لاحتياجات وأساليب المتعلمين، وتعتمد بيئات التعلم الإلكتروني التكيفية (AEL) على بناء نموذج لاحتياجات وتفضيلات وأساليب كل متعلم، ومن المعروف جيدًا أن مثل هذا السلوك التكيفي يمكن أن يزيد من تطور وأداء المتعلمين، وبالتالي إثراء جودة تجربة التعلم، لبيئات التعلم الإلكتروني التكيفية من خلال التنوع والتفاعلية والقدرة على التكيف والتغذية الراجعة والأداء والقدرة على التنبؤ (Nuankaew et al., 2019).

[1] اتبع الباحث نظام التوثيق APA Style 6th Edition، ولكن في الأسماء العربية تكتب كما هي.

تخلق استراتيجيات التعلم التكيفي تجربة للطلاب يتم تعديلها بناءً على أداء الطالب وتفاعله مع مواد التعلم، وفي جوهره هو نهج للتعليم يعتمد على التكنولوجيا والبيانات حول أداء الطالب للتكيف والاستجابة بالمحتوى والمنهجيات التي تطور مسارًا لإتقان المتعلم هدف تعليمي معين، والتعلم التكيفي يشير إلى التعليم الذي يتم فيه تحسين وتيرة التعلم والنهج التعليمي لتلبية احتياجات كل متعلم، وقد تختلف أهداف التعلم والنهج التعليمية والمحتوى التعليمي (وتسلسله) بناءً على احتياجات المتعلم (Waters, 2014).

توفر التطورات التكنولوجية الحديثة في التدريس والتعلم أدوات ديناميكية مطلوبة لتلبية الاحتياجات التعليمية للعصر الرقمي، ومع ذلك يواجه المعلمون وغيرهم من المعلمين بشكل متزايد التهديدات السيبرانية أثناء التدريس عبر الإنترنت، مما يؤثر على جودة التدريس وكذلك نتائج التعلم، وفي الآونة الأخيرة كانت هناك تقارير عن انقطاع التعلم الناجم عن مجرمي الإنترنت الذين يستخدمون هجمات مثل برامج الفدية، ورفض الخدمة، وسرقة البيانات، وفي هذا السياق، يجب أن يكون أخصائي التكنولوجيا قادرين على تسخير الأدوات والموارد والممارسات التعليمية الصحيحة لضمان الاستمرارية، و الجودة والفعالية في التعلم.

وفي تلك الأنظمة التي تعتمد على التقنيات الحديثة يتم الحفاظ على البيانات المختلفة التي يتم نقلها عبر شبكة الإنترنت، وتتكون بشكل رئيسي من أجهزة مختلفة متصلة بها، حيث تبدأ هذه الأجهزة في قياس وجمع البيانات من الطلاب، مما يعرض أمن خصوصية الطالب للخطر، ويمكن لأي خرق للسلامة أن يكشف عن بيانات الطالب الخاصة المرتبطة بالسجل الطبي للفرد، أو الخلفية الاقتصادية للأسرة، أو أي بيانات سرية أخرى، ويجب أن تكون التطبيقات المستخدمة في السياق التعليمي آمنة وموثوقة، ويجب أن يكون الطلاب والمعلمون على دراية ببروتوكولات

السرية والأصالة عند استخدام الأدوات والأجهزة التكنولوجية، وأن يكونوا على دراية بالاستخدام الآمن لهذه التقنيات وحماية أنفسهم من أي تهديدات إلكترونية محتملة، وتقع على عاتق السلطات المدرسية قبل استخدام التكنولوجيا الجديدة إبلاغ موظفي المدرسة والطلاب بالوظائف وكيفية الاستفادة من تلك التقنيات بأمان، ويجب أن تؤخذ في الاعتبار إدارة جميع حقوق المستخدمين والامتثال لحماية البيانات واللوائح القانونية الأخرى(Sollins, H., 2019).

ومع ذلك، فإن عالم الفضاء الإلكتروني المتنامي قد يكون له أيضًا آثار سلبية على مستخدمي الإنترنت، مثل الجرائم الإلكترونية، لذلك ينبغي احتواء مثل هذه القضايا في وقت مبكر حتى لا يكون لها تأثير كبير، وفي هذا السياق يعد تنفيذ الأمن السيبراني بين مستخدمي الإنترنت أمرًا مهمًا للغاية، ويعد التثقيف في مجال الأمن السيبراني ضروريًا لأن قضايا الجرائم الإلكترونية يمكن أن تحدث في أي مكان بغض النظر عن الأفراد والمؤسسات والأماكن، ويعريف الأمن السيبراني بأنه حالة الحماية ضد الاستخدام الإجرامي أو غير المصرح به للبيانات الإلكترونية، أو التدابير المتخذة لتحقيق ذلك(Oxford University Press, 2014).

ومع استخدام تكنولوجيا المعلومات والاتصالات في قطاع التعليم عالميًا خلال العقود القليلة الماضية، ليصبح جزءًا لا يتجزأ من التدريس والتعلم، والاتصالات وادى ذلك إلى الاعتماد على التعلم الرقمي، ومع ذلك، فإن استيعاب التكنولوجيا في المدارس قد خلق مخاطر جديدة، وخاصة فيما يتعلق بالعامل البشري وقد تفاقم هذا الأمر بسبب التغيرات التكنولوجية السريعة التي لم يواكبها المعلمون بعد تؤدي زيادة الرقمنة في التعليم إلى ظهور تحديات تتعلق بالأمن السيبراني على جميع مستويات التعليم (von Solms & von Solms, 2014)، والمؤسسات التعليمية بما في ذلك المدارس الثانوية، والكليات والجامعات، وتشمل التحديات البرامج الضارة وبرامج

الفدية والتصيد الاحتيالي وحجب الخدمة والكشف غير المصرح به والسرقة الفكرية والخصوصية وحماية بيانات الهوية، ويتم استهداف المدارس بسبب البيانات القيمة التي تحتفظ بها عن الطلاب وأولياء الأمور والخريجين وأعضاء هيئة التدريس والموظفين والأبحاث( Impact Networking, 2021; Pusey & Sadera, 2011).

ويمكن الإشارة إلى أسباب الهجمات إلى هفوات بشرية وفنية، فيستخدم الطلاب وأعضاء هيئة التدريس والموظفين أحيانًا الأجهزة الشخصية للتعامل مع بيانات المدرسة، وقد لا يكون أمان أجهزة الكمبيوتر هذه كافيًا لحماية المعلومات التي يتم الوصول إليها (Richardson et al., 2020)، وقد لا يكون المتعلمون في الفضاء الإلكتروني على دراية بالمخاطر المتعلقة بسلامتهم الشخصية وبياناتهم نظرًا لضعف الوعي بين مستخدمي الإنترنت (Amankwa, 2021)، ومن الناحية الفنية لا توجد إجراءات أمنية كافية لحماية مجموعة متنوعة من البيانات – الأكاديمية والبحثية والطبية والمصرفية والسكنية وما إلى ذلك – الموجودة في هذه المؤسسات، وتشمل عواقب الهجمات السيبرانية فقدان البيانات، وبطء أو عدم الوصول إلى أنظمة الكمبيوتر، والتسلط عبر الإنترنت، والتعرض لمحتوى غير لائق، وتعطيل الفصول الدراسية، وإلغاء الامتحانات، والخسائر المالية، والإجراءات القانونية، وقد لوحظت حوادث متكررة تشير إلى فشل محتمل في التعلم من الهجمات السابقة ( Impact Networking, 2021)، وعلى الرغم من احتوائها على معلومات لا تقدر بثمن، لا تمتلك المدارس قدرات كافية للتعامل مع الأمن السيبراني.

والأمن السيبراني هو الحل الأمثل لمتابعة الاستخدام الواسع للإنترنت وتطبيقاته وأنظمته المختلفة للتقليل من المخاطر التي تنشأ من سوء الاستخدام، حيث توجد محتويات غير مشروعة وغير مرغوب بها ذات تأثير سلبي على أخلاقيات وقيم

المجتمع وتؤدي إلى تغيرات في شخصية الأفراد، وميل البعض منهم لسلوكيات منحرفة وبالتالي كثرة الجرائم من خلال التقليد أو ممارسة ألعاب معينة تشجع على ذلك، ولهذا فلابد من بناء مجتمع واعي مسئول ومدرك لهذه المخاطر ليستطيع التعامل معها وفقا لقواعد السلامة مع إدراكه للعواقب القانونية للتصرفات اللامسؤولة والتي تعرض الاخرين للخطر أو للسرقات (منى الأشقر جيور، 2016).

وأن قطاع التعليم يواجه تحديات الأمن السيبراني التي تتطلب الاهتمام لما له من تأثير في الحد من الخسائر المالية، وتعطيل التعلم، وسرقة الملكية الفكرية، وينبغي إدراج الأمن السيبراني في برامج تدريب المعلمين قبل الخدمة وأثناء الخدمة (UNESCO, 2018)، ويجب أن يمتلك المعلمون المهارات اللازمة للتعامل مع الأمن السيبراني في الفصل الدراسي، لذلك من الضروري إنشاء دورات تدريبية حول الأمن السيبراني تحتوي على محتوى يمكن للمعلمين فهمه بسهولة ووضعه موضع الاستخدام (Ivy et al., 2019).

وعلى المعلمين ومتخصصي التكنولوجيا بالمدرسة فهم أساسيات الأمن السيبراني أثناء استخدامهم للفضاء الرقمي للتعليم والتعلم وهذا ليس من أجل سلامتهم فحسب، بل من أجل سلامة طلابهم أيضًا، الذين قد لا يكون الكثير منهم على دراية كاملة بالمخاطر الموجودة في الفضاء الإلكتروني، حيث إنهم يميلون إلى تجاهل قواعد السلامة عبر الإنترنت، وبالتالي يجدون أنفسهم في مواقف لا يفهمها المعلمون وأولياء الأمور بشكل كامل (Pencheva et al., 2020)، ويتمتع معظم المعلمين بمعرفة محدودة في مجال الأمن السيبراني، مما يجعل تعزيز السلامة عبر الإنترنت عند التدريس والتعلم تحديًا (von Solms, 2014)، بينما يتعلم المعلمون قبل الخدمة دمج التكنولوجيا في التدريس، فإنهم غير مستعدين لوضع نموذج أو تدريس الأمن السيبراني بسبب عدم كفاية المعرفة ومهارات التدريس في هذا المجال،

وبالتالي، فإنهم غير قادرين على تحديد التهديدات التي تهدد أنفسهم وطلابهم ومؤسساتهم (Pusey & Sadera, 2011)، ومن ناحية أخرى، فإن المدارس لديها ميزانية وموارد محدودة لأن الدعم الحكومي في مجال السلامة السيبرانية في المدارس غير موجود أو في حده الأدنى.

ومع ضعف التمويل والخبرة والقدرات الكافية للاستعداد لمواجهة التهديدات السيبرانية، يحتل التعليم مرتبة منخفضة في مؤشر الأمن حسب القطاع على الرغم من كونه من بين أهم القطاعات المستهدفة (Impact Networking, 2021)، ومن الواضح أن استخدام التكنولوجيا يمكن أن يؤدي إلى ضرر جسدي وعاطفي للمستخدمين وبياناتهم ومؤسساتهم، ولذلك يجب أن يكون المعلمون مزودين بالمعرفة والمهارات المتعلقة بالأمن السيبراني لتطبيق مهاراتهم الرقمية بأمان في التدريس والتعلم (Pusey & Sadera, 2011).

ويتم تصنيف تقنيات البيئات التكيفية إلى ثلاثة أجزاء: التقنيات التي تسمح للكائنات بالحصول على معلومات؛ والتقنيات التي تمكن الكائنات من معالجة المعلومات؛ وتقنيات لتعزيز الأمن والخصوصية (Sintef & Norway, 2014)، ومن خلال تلك التقنيات يسعي الباحث إلى تصميم بيئة تعلم إلكترونية تكيفية لتنمية مهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم.

**الإحساس بالمشكلة:**

نبع الإحساس بالمشكلة من خلال ما يلي:

**من خلال عمل الباحث:** كرئيس قسم الموهوبين والتعلم الذكي ومن قبلها مسئول التعلم الذكي بإدارة الموهوبين والتعلم الذكي ومن قبلها كمتابع ومدرب بمركز التطوير التكنولوجي بمديرية التربية والتعليم ومن قبلها اخصائي تكنولوجي بمدارس تابعة لادارة سنورس التعليمية ووجد أن هناك قصور في مهارات الأمن

السيبراني لدى اخصائي تكنولوجيا التعليم، والحاجة الضرورية لدمج بيئة تعلم إلكترونية تكيفية في الأنشطة اليومية للجامعات والمدارس.

**مراجعة الأدبيات والدراسات السابقة:**

أكدت العديد من الدراسات على قوة التعلم الإلكتروني التكيفي في تقديم المحتوى الإلكتروني للمتعلمين بطريقة تتناسب مع احتياجاتهم وأساليب تعلمهم، مما يساعد على تحسين عملية اكتساب الطلاب للمعرفة والخبرات وتنمية مهارات المختلفة لديهم **مثل :**

دراسة (Palmisano .S. J, 2008)، ودراسة (Chun–Hui et al., 2017)، ودراسة (Dominic et al., 2015)، ودراسة (Vassileva, 2012 )، ودراسة( Mahnane et al., 2013)، ودراسة (Cletus, D., & Eneluwe, D, 2020)، وقد استفاد الباحث من الجوانب التالية:

- أهمية استخدام البيئات التكيفية كآلية جديدة في التعليم بشكل عام.
- أهمية تنمية مهارات الأمن السيبراني لدى أخصائي تكنولوجيا التعليم لتعزيز قدراتهم الأدائية والمهارية على الإبقاء على الأجهزة بحالة جيدة والاحتفاظ بها سليمة دون اعطال.
- على حد اطلاع الباحث لا توجد دراسة تناولت تنمية مهارات الامن السيبراني لدى أخصائي تكنولوجيا التعليم.

**مشكلة البحث:**

لاحظ الباحث وجود قصور لدى اخصائي تكنولوجيا التعليم في مهارات الأمن السيبراني، وحيث أن من المسئوليات والواجبات الرئيسية للتوصيف الوظيفي كما جاء في الكتاب الدوري رقم 164 لسنة 2016م، بشان بطاقات التوصيف الوظيفي لاخصائي تكنولوجيا التعليم هي الحفاظ على الأجهزة التعليمية بالمدرسة بما يضمن

استمرارية صلاحيتها، لذلك؛ يجب على اخصائي تكنولوجيا التعليم الذين يرغبون في تقديم المساعدة لحماية الأجهزة والطلاب اتخاذ خطوة كبيرة نحو الأمام من خلال تنمية أنفسهم والطلاب وأولياء الأمور لتطبيق مبدأ التفكير الوقائي على الأنشطة عبر الإنترنت، فأمن المعلومات مخيفًا حتى بالنسبة للمحترفين الأكثر مهارة من الناحية الفنية، وأصبح يمثل أحد التحديات التي تواجه اخصائي تكنولوجيا التعليم أثناء محاولة حماية الطلاب، وألاجهزة من الهجمات الاحتيالية المحتملة من الشبكة العنكبوتية، وحيث أن الأمن السيبراني من المواضيع البحثية الحديثة في العالم العربي التي لم تحظى بالقدر الكافي من الاهتمام على مستوى البحث العلمي، ولا يمكن إغفال بعض الجهود القليلة، وخاصة في الجانب التعليمي، برغم أنه من أهم الكفايات لاخصائي تكنولوجيا التعليم؛ لذا يهتم البحث الحالي بالتأكيد على مهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم، مما دعى الباحث بإجراء دراسة استكشافية على عينة من اخصائي تكنولوجيا التعليم وذلك من خلال بطاقة ملاحظة أعدها الباحث، وأكدت نتائج الدراسة الإستكشافية وجود قصور لديهم في مهارات الأمن السيبراني، وأنهم بحاجة إلى مصادر معرفة أكثر ثراءاً توفر الدقة والسرعة بها لتنمية هذه المهارات لديهم، ويرى الباحث أن تصميم بيئة إلكترونية تكيفية وبها مجموعة من المصادر التعليمية الإثرائية قد يزيد من مهارات الامن السيبراني لديهم.

ويرجع ايضاً الباحث هذا القصور من وجهة نظره إلى عدم دراسة تلك المهارات في المرحلة الجامعية لاخصائي تكنولوجيا التعليم، والنظم التعليمية القائمة لا تتماشى مع تعلم تلك المهارات حيث فقدان الدقة والسرعة المطلوبة لاداء تلك المهارات ويرى الباحث أن تصميم بيئة إلكترونية تكيفية لاخصائي تكنولوجيا التعليم، وبها مجموعة من المصادر التعليمية الإثرائية قد يزيد من مهارات الامن السيبراني لديهم وقد يزيد من الدقة والسرعة في اداء المهام المنوطه بهم.

ومن ثم فإن البحث الحالي يسعى لحل تلك المشكلة من خلال طرح السؤال التالي: كيف يمكن **تصميم بيئة تعلم إلكترونية تكيفية لتنمية مهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم؟** ولذلك يجب علينا إلقاء بعض التساؤلات الفرعية حول هذا الموضوع:

1- ما التصميم التعليمى المناسب لبيئة تعلم إلكترونية تكيفية لتنمية مهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم؟

2- ما أثر تصميم بيئة تعلم إلكترونية تكيفية في تنمية الجانب المعرفي لمهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم؟

3- ما أثر تصميم بيئة تعلم إلكترونية تكيفية في تنمية الجانب الأدائي لمهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم؟

**أهداف البحث:**

يهدف البحث الحالي إلى:

علاج القصور فى مهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم وذلك من خلال بيئة تعلم تكيفية وبدلالة التالى:

1- قياس أثر تصميم بيئة تعلم إلكترونية تكيفية لتنمية الجانب المعرفي لمهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم

2- قياس أثر تصميم بيئة تعلم إلكترونية تكيفية لتنمية الجانب الأدائي لمهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم.

**أهمية البحث:**

تتضح أهمية البحث في أنه قد يفيد في:

- تقديم نظام تعلم الكتروني جديد يتيح الاستغلال الأمثل للانترنت والأجهزة التكنولوجية وغيرها في العملية التعليمية.

- تطوير نظم التعليم المختلفة من خلال اتاحة نظام تعليمي إلكتروني تكيفي لمجالات تعليمية أخرى.
- توفير الكثير من الوقت والتكلفة حيث البيئة التكيفية تتعامل مع الأشياء الموجودة بالفعل وربطها عن طريق شبكة الانترنت المتوفرة أيضا الان.
- امتلاك اخصائي تكنولوجيا التعليم لمهارات الامن السيبراني.

**فروض البحث:**

يحاول البحث التحقق من صحة الفروض التالية:

1- يوجد فرق دال احصائيا عند مستوى (0.05) بين متوسطي درجات المجموعة التجريبية ودرجات المجموعة الضابطة في الجانب المعرفي لمهارات الامن السيبراني في التطبيق البعدي للاختبار التحصيلي لصالح المجموعة التجريبية.

2- يوجد فرق دال احصائيا عند مستوى (0.05) بين متوسطي درجات المجموعة التجريبية ودرجات المجموعة الضابطة في الجانب الادائي لمهارات الامن السيبراني في التطبيق البعدي لبطاقة الملاحظة لصالح المجموعة التجريبية.

**حدود البحث:**

يقتصر البحث على الحدود التالية:

- **حدود بشرية:** اخصائي تكنولوجيا التعليم
- **حدود محتوى:** تمثل محتوى الامن السيبراني.
- **حدود مكانية:** محافظة الفيوم- إدارة سنورس التعليمية- مدرسة الدكتور لطفي الثانوية بنات التعلم (عن طريق الإنترنت كلٌ في منزله، ومعامل الحاسب

الآلي ومعامل الخاضعة للتطوير التكنولوجي وذلك لما يتوفر بالمعامل من عدد كافي من الأجهزة الحديثة ذات المواصفات العالية التي تتناسب مع طبيعة بيئة التعلم الإلكترونية التكيفية أثناء تطبيق بطاقة الملاحظة).

- **حدود زمانية:** من المتوقع العام الدراسي 2023/ 2024 م، الفصل الدراسي الثاني.
- **حدود موضوعية:**
  - بيئة تعلم إلكترونية تكيفية.
  - الامن السيبراني، وتتحدد مهارات الامن السيبراني في:

1- حماية بياناتك وخصوصيتك، وتضم:

- يحمي أجهزة الحوسبة- يدير نظام التشغيل والمتصفح - يحمي جميع الاجهزة- يستخدم الشبكات اللاسلكية بأمان- يستخدم كلمات مرور مميزة لكل حساب عبر الإنترنت.

2- كيفية تشفير البيانات، وتضم:

- يقوم بتشفير بياناته.

3- كيفية نسخ البيانات احتياطيًا، وتضم:

- ينسخ بياناته احتياطيًا- يحذف بياناته نهائياً- يستخدم المصادقة الثنائية - يستخدم المصادقة المفتوحة (OAuth)- يتقن خصوصية مستعرض الويب والبريد الإلكتروني.

4- كيفية مشاركة المعلومات الشخصية عبرالإنترنت وتضم:

- يكتشف السلوكيات الخطيرة عبر الإنترنت- يشارك المعلومات الشخصية عبر الإنترنت بطريقة امنه0

**منهج البحث:**

يستخدم البحث:

1- المنهج الوصفي لمراجعة البحوث والدراسات السابقة وإعداد الاطار النظري للبحث.

2- المنهج التجريبي والتصميم شبة التجريبي، للتعرف على أثر تصميم بيئة تعلم إلكترونية تكيفية لتنمية مهارات الامن السيبراني لدى اخصائي تكنولوجيا التعليم.

**أدوات البحث:**

يستخدم البحث الأدوات التالية:

1- اختبار تحصيلي لقياس الجانب المعرفي المرتبط بمهارات الامن السيبراني.

2- بطاقة ملاحظة الأداء العملي لمهارات الامن السيبراني.

**مجموعة البحث:**

مجموعة البحث (60) اخصائي تكنولوجيا التعليم، مُقسمةً إلى مجموعتين ضابطة وتجريبية، كل مجموعة مكونة من ( 30) اخصائي.

**متغيرات البحث:**

1. **المتغير المستقل:** تصميم بيئة تعلم إلكترونية تكيفية.
2. **المتغير التابع:** تنمية الجانب المعرفي والأدائي لمهارات الامن السيبراني.

**التصميم التجريبي للبحث:**

في ضوء موضع البحث استخدم المنهج التجريبي والتصميم شبة التجريبي، بحيث يتم تطبيق أدوات القياس على عينة البحث :التجريبية والضابطة جدول ( 1 ).

**جدول ( 1 ): التصميم التجريبي للبحث**

| المجموعات | القبلي | المعالجة التجريبية | البعدي |
|---|---|---|---|
| **المجموعة الضابطة** | الاختبار التحصيلي لمهارات الامن السيبراني. بطاقة ملاحظة لمهارات الامن السيبراني. | التعلم بالأسلوب التقليدي | - الاختبار التحصيلي لمهارات الامن السيبراني. -بطاقة ملاحظة لمهارات الامن السيبراني. |
| **المجموعة التجريبة** | | التعلم عبر بيئة تعلم إلكترونية تكيفية. | |

**خطوات البحث:**

يتبع البحث الخطوات التالية وفق المنهج التجريبي:

- تحديد المهارات اللازمة للتعامل مع الامن السيبراني.
- مراجعة الدراسات السابقة المرتبطة بمهارات التعامل مع الامن السيبراني.
- تحديد المهارات المستخدمة للتعامل مع الامن السيبراني.
- اعداد قائمة تفصيلية بالمهارات.
- اعداد بيئة تعلم إلكترونية تكيفية.
- اعداد قائمة بالمعايير والمواصفات تفصيليا للامن السيبراني.
- الحصول على المحتوى الرقمي من المتخصصين.
- التأكد من مطابقة المحتوى الرقمي للمعايير والمواصفات المتفق عليها.
- انشاء الاتباطات الخاصة بالأجهزة وأجهزة الاخصائيين.
- وضع المحتوى الرقمي.
- تصميم أدوات القياس (الاختبار التحصيلي لتقييم الجانب المعرفي الخاص بمهارات الامن السيبراني - بطاقة ملاحظة مهارات الامن السيبراني - والعرض على المحكمين، وإجراء التعديلات المقترحة للوصول لصورتهم النهائية، لإجازتها وحساب صدقها وثباتها.

- إجراء التجربة الإستطلاعية للبحث للتأكد من وضوح الأهداف والمحتوى وتحديد زمن الاختبار ومعرفة الصعوبات والتحديات التي قد تواجه عينة البحث والعمل على التغلب على هذه الصعوبات قبل بدء التجربة الأساسية.
- تطبيق تجربة البحث الأساسية على مجموعة البحث.
- اختيار عينة البحث الأساسية على اخصائي تكنولوجيا التعليم .
- تم تقسيم اخصائي تكنولوجيا التعليم إلى مجموعتين ضابطة وتجريبية.
- تطبيق الاختبار التحصيلي على اخصائي تكنولوجيا التعليم مجموعتي البحث.
- تطبيق مادة المعالجة التجريبية على المجموعة التجريبية
- تطبيق أدوات القياس (الاختبار التحصيلي، بطاقة الملاحظة) على اخصائي تكنولوجيا التعليم عينة البحث تطبيقًا بعديًا.
- رصد النتائج وإجراء المعالجة الإحصائية لها.
- تحليل وتفسير النتائج في ضوء رؤية الباحث، والتصميم التعليمي المستخدم، ونظريات التعلم، والدراسات والبحوث السابقة المرتبطة بالمتغيرات قيد البحث.
- تقديم التوصيات والبحوث المقترحة في ضوء نتائج البحث الحالي.

**مصطلحات البحث:**

**التعلم التكيفي:**

هو جزء من التعلم التفاعلي الذي يعالج احتياجات الأفراد من خلال مسارات التعلم، وردود الفعل الفعّالة، والموارد التكميلية (Kurt, S, 2021).

**بيئات التعلم الإلكتروني التكيفية:**

عملية تعلم يتم فيها تدريس المحتوى أو تكييفه بناءً على استجابات أنماط التعلم أو تفضيلات المتعلمين، ومن خلال تقديم محتوى مخصص تعمل بيئات التعلم الإلكتروني التكيفية على تحسين جودة التعلم عبر الإنترنت، و تكون البيئة المخصصة قابلة للتكيف بناءً على احتياجات وأنماط التعلم لكل متعلم ( Truong, 2016).

**الأمن السيبراني Cyber security:**

**ويعرفه الباحث بأنه:**

قدرة اخصائي تكنولوجيا التعليم على حماية مكونات المنظومة التعليمية من اى خطر او تهديد يلحق بهم ضرر من الفضاء السيبراني0

**الإطار النظري:**

**اولاً بيئة التعلم التكيفية:**

**مفهوم بيئة التعلم التكيفية في التعليم** ( Peng, H., Ma, S., & Spector, J.M, 2019):

التعلم التكيفي هو أسلوب لاستخدام التعليم القائم على البيانات لتعديل وتخصيص تجارب التعلم لتلبية الاحتياجات الفردية لكل متعلم، ويمكن لأنظمة التعلم التكيفي تتبع البيانات مثل تقدم الطلاب ومشاركتهم وأدائهم واستخدام البيانات لتوفير تجارب تعليمية مخصصة، وتوفر فرص التعليم المتساوية للأفراد، وإمكانية الوصول المتساوية إلى الموارد، فإن التعليم العادل يعترف بالاختلافات بين المتعلمين ويعالجها من خلال توفير المواد المناسبة المتوافقة مع كل منهم للوصول إلى مساعيهم الأكاديمية، ويسعى التعلم التكيفي جنبًا إلى جنب مع التدريس والتقييم التكيفيين إلى توفير المساواة في التعليم لجميع المتعلمين، والتعلم التكيفي هو جزء من التعلم

التفاعلي الذي يعالج احتياجات الأفراد من خلال مسارات التعلم، وردود الفعل الفعّالة، والموارد التكميلية؛ على عكس المناهج الدراسية التي تناسب الجميع (Kurt, S, 2021).

**خصائص البيئة التكيفية** (Redmon, M., Wyatt, S., & Stull, C , 2021 ):

- يجعل التقدم التكنولوجي التعلم التكيفي أسهل في التنفيذ، وهناك ثلاثة مجالات يمكن للمرء أن ينفذ فيها التعلم التكيفي: المحتوى التكيفي، والتسلسل التكيفي، والتقييم التكيفي.
- يوفر المحتوى التكيفي ردود فعل على استجابة الطلاب المحددة (على سبيل المثال، التلميحات، ومواد المراجعة حول المهارة ذات الصلة، والمزيد من الدعم) دون تغيير التسلسل العام للمهارات.
- يجمع التسلسل التكيفي بيانات الطلاب ويحللها باستمرار لتغيير ما يراه الطالب بعد ذلك تلقائيًا.
- يغير التقييم التكيفي الأسئلة التي يراها الطالب بناءً على استجابته للسؤال السابق، وستزداد صعوبة الأسئلة عندما يجيب الطالب عليها بدقة، بينما إذا واجه الطالب صعوبة تصبح الأسئلة أسهل.
- تتضمن برامج التعلم التكيفي جميع المجالات الثلاثة، وهي تقوم بتقسيم مادة الدورة إلى أقسام يمكن إدارتها بناءً على كل هدف تعليمي، ثم تقدم للمتعلمين المساعدة الفورية والموارد الخاصة باحتياجاتهم التعليمية والملاحظات ذات الصلة، يضبط البرنامج المحتوى والتسلسل والتقييم وفقًا للاستجابات التفاعلية المخزنة في النظام، علاوة على ذلك، يمكن للمدرسين تكييف التعليمات من خلال اتخاذ قرارات مستنيرة في الوقت المناسب ومستندة إلى البيانات لتلبية احتياجات كل فرد.

**فوائد التعلم عبر البيئة التكيفية:**

يتمتع التعلم التكيفي بالعديد من الفوائد منها (Kurt, S, 2021):

-يمكّن التعلم التكيفي المتعلمين من أن يصبحوا أكثر نجاحًا وتوجيهًا ذاتيًا من خلال توفير نظرة ثاقبة لمستوى إتقانهم والسماح لهم بالعمل بالسرعة التي تناسبهم.

- يحسن من مشاركة المتعلمين من خلال توفير دروس وأنشطة مصممة خصيصًا لاحتياجاتهم.

-يمكن استخدامه كبديل فعال من حيث التكلفة للكتب المدرسية باهظة الثمن.

- يوفر هيكلًا يحافظ على أهداف الدورة والدروس وأنشطة التدريب والتقييمات في محاذاة ويُظهر للمتعلمين كيف يرتبط كل عنصر من عناصر الدورة بأهداف الدورة، وبالمثل، عندما يواجه المتعلمين صعوبة في إتقان مفهوم ما، يمكن لأعضاء هيئة التدريس مراجعة ما إذا كانت بعض العناصر التعليمية غير متوافقة بشكل جيد مع الأهداف.

- يوفر بيانات ذات صلة في الوقت المناسب يمكن لأعضاء هيئة التدريس والإداريين استخدامها لتحديد أداء الفئات الفرعية المستهدفة .

-يتيح التعلم التكيفي لأعضاء هيئة التدريس والإداريين تقديم الدعم المستهدف في الوقت المناسب من خلال تحديد الأفراد، أو حتى الأقسام المحددة في دورة متعددة الأقسام، والتي تحتاج إلى الاهتمام.

- يتيح لأعضاء هيئة التدريس والإداريين إجراء تحسين مستمر من خلال مقارنة البيانات عبر الفصول الدراسية.

-يتيح التعلم التكيفي تقديم التعلم الشخصي على نطاق واسع، كما يقلل من الغش لأن المحتوى والتقييمات يمكن أن تختلف لكل متعلم.

- يمكن للتعلم التكيفي تعظيم نتائج التعلم حيث يمكن للمدرسين أن يكون لديهم إحساس أفضل بالمجالات التي يعاني منها المتعلمين والذين يحتاجون إلى مزيد من المساعدة وتوفير التدخل قبل أن يتعرض الطلاب لخطر الانسحاب.

**أفضل الممارسات لجعل التعلم التكيفي ناجحًا**( McGuire, R, 2021 ):

-يتطلب التعلم التكيفي التخطيط والتفاعل البشري ليكون ناجحًا، ولا يزال وجود المدرب ضروريًا لحدوث التعلم التكيفي حيث يساعد الطلاب في فهم قيمة النظام التكيفي ويساعدهم في الانتقال من المتعلمين السلبيين إلى النشطين.

-يوصى باختيار البيئة التكيفية التي توفر للمدرسين القدرة على تحديد أنشطة وتقييمات تعليمية محددة للتأكد من أن المحتوى يتماشى مع الأهداف.

-يجب على المعلمين التخطيط مسبقًا عند تصميم التعلم التكيفي وتحديد الأشخاص الذين يمكنهم التواصل معهم للحصول على الدعم.

- يجب على المعلمين أن يأخذوا الوقت الكافي لفهم كيفية عمل النظام التكيفي ونقل هذه المعلومات إلى الطلاب.

-تقديم التوقعات بوضوح للمقرر وعملية المشاركة في المواد التكيفية.

-التعرف على تحليلات التعلم التي توفرها أداة التعلم التكيفي، واستخدام تحليلات التعلم بشكل فعال لإعلام المعلمين بالتدخلات وتنفيذ التدريس الذي يركز على المتعلم.

**مفهوم الأمن السيبراني:**

يُعد مفهوم الأمن السيبراني من المفاهيم الحديثة نسبيًّا، والتي ظهرت في الثورة الرقمية والتكنولوجية المعاصرة، والتي أدت إلى تدفق المعلومات بشكل كبير وغير مسبق، مع تعدد وسائل الاتصال إلى مصادر المعلومات عبر أجهزة الحواسيب،

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 والباحثين.

ويُعرفه بوسي وسادير (Pusey & Sadera , 2011) بأنه الإجراءات التقنية الهادفة إلى حماية البيانات، والهوية الشخصية، والمعدات التقنية من أي شكل من أشكال الوصول غير المسموح به إلى تلك المعلومات أو المعدات، فان الأمن السيبراني يمثل العملية أو الحالة التي تكون بموجبها المعلومات وأنظمة المعلومات محمية بشكل تام ضد أي شكل من أشكال الإتلاف أو الوصول غير المسموح به لتلك المعلومات والأنظمة، أو التلاعب بها أو إساءة استادامها Crompton, (Thompson and Zou , 2016).

وفي ضوء ما سبق، يتضح الاتفاق على أن الأمن السيبراني يمثل مفهوم أمني خاص بحماية المعلومات، وكل ما له صلة بتلك المعلومات من عمليات وخدمات وأجهزة وتقنيات، ضد أي شكل من أشكال الوصول غير المسموح به، أو استخدام تلك المعلومات بشكل سلبي، أو بما يمثل خطرا على الجهات أو الأفراد ذوي الصلة بتلك المعلومات.

**الأهمية التربوية للأمن السيبراني:**

ساهم انتشار استخدام وسائل الوصول إلى شبكة الإنترنت عبر العديد من الأجهزة المحمولة بالإضافة إلى الحواسيب، واعتماد الحياة المعاصرة في معظم مجالاتها على التكنولوجيا الرقمية، على وقوع العديد من المعلمين حول العالم ضحية لأحد أشكال المخاطر والانتهاكات السيبرانية، ويترتب على تلك المخاطر والانتهاكات العديد من الأضرار المادية والنفسية والمعنوية التي تؤثر على المعلم، وعلى المؤسسة التعليمية التربوية، وهذه الأضرار تُكسب الأمر السيبراني أهمية خاصة بالنسبة لكل

معلم في عالم اليوم (Wilson, 2014)، ومما يزيد من الأهمية التربوية للأمن السيبراني أنه قد يتعرض المعلمون إلى الانتهكات والمخاطر السيبرانية دون أن يكون لديهم دراية بتلك المخاطر والانتهاكات، ومدى خطورتها على التصفح الأمن للإنترنت، وهو ما يدعو إلى ضرورة رفع مستوى الوعي بأهمية الأمن السيبراني لدى هؤلاء المعلمين، وضرورة تضافر الجهود من قبل المدرسة ووزارة التعليم في هذا الشأن( Solms. R & Solms. S, 2015).

ذكر ستوارد وشلينجفورد (stewart & Shilingford, 2011) الأهمية التربوية للأمن السيبراني على النحو التالي:

- ضمان سرية وخصوصية الوثائق التعليمية والحفاظ على سلامتها بشكل مستمر.
- متابعة ومراقبة وتطوير وضبط نظام المعلومات والأمن في المدرسة.
- حماية المعلمات والمدرسة من الهجمات السيبرانية في الفضاء السيبراني.

ومن السرد السابق يتضح الأهمية التربوية للأمن السيبراني في حماية المعلومات المهمة والحساسة لدى المعلمين والمؤسسات التربوية، واذلك تثقيف المعلمين بعدم التعرض للانتهاكات والمخاطر السيبرانية، وتوفيرطرق الوقاية ضد الهجمات السيبرانية؛ للحفاظ على أمن المؤسسة التعليمية والمعلم.

وتنعكس تلك الأهمية بشكل خاص على طلبة المدارس، باعتبارهم يمثلون الجيل الرقمي، اي الجيل الذي بدأ استخدام تقنيات الاتصال المختلفة منذ سنوات عمره المبكرة، ويزداد أعداد الطلبة مستخدمي الإنترنت بشكل كبير سنويًّا لأغراض متعددة ومنها: التعليم، واللعب، والتواصل الاجتماعي، وتبلغ نسبة الطلبة الذين لديهم إمكانية الوصول إلى الإنترنت نحو40%من الطلبة حول العالم، وعلى الرغم من مزايا استخدامهم للإنترنت، إلا أن فرص وقوعهم كضحايا للجرائم السيبرانية كبيرة جدًّا؛

لعدم امتلاكهم الوعي الكافي بتلك الجرائم وكيفية تجنبها، وهو ما يزيد أهمية الأمن السيبراني في مجال التعليم والتعلم (Kritizinger, Bada & Nurse,2017).

وبالإضافة إلى ما سبق من أهمية تربوية للأمن السيبراني للمعلمين وللطلبة، فإن هناك جانب خاص يتمثل في ضرورة ضمان سرية وخصوصية الوثائق التعليمية والحفاظ على سلامتها بشكل مستمر، ومتابعة ومراقبة وتطوير وضبط نظام المعلومات والأمن في المدرسة، ومراقبة أي محاولات للتسلل إلى شبكات المعلومات الخاصة بالمدرسة كمؤسسة تربوية.(Stewart & Shilingford, 2011).

**إجراءات تعزيز الأمن السيبراني:**

هناك العديد من الإجراءات التي يُمكن لكل مستخدم للإنترنت ولرواد الفضاء السيبراني، ومن هذه الإجراءات (Tiwari et. al., 2016) :

1- المحافظة على تحديث جدران الحماية، والتي تمثل أنظمة الدفاع عن البنية التحتية للبيئة المعلوماتية.

2- التأكد من إعدادات الحاسوب وشبكة الإنترنت.

3- اختيار كلمات مرور قوية، وعمليات تحقق أمنية لمواقع التواصل الاجتماعي، والبريد الإلكتروني، والحسابات الشخصية على الحاسوب أو الهواتف.

4- عدم الاستجابة لأي رسائل مجهولة المصدر ترد إلى البريد الإلكتروني.

5- استخدام برامج الحماية ومضادات الفيروسات وتحديثها باستمرار.

6- حماية المعلومات الشخصية ومنع الآخرين من الاطلاع عليها.

7- تحديث كلمات المرور بشكل مستمر، على الأقل مرة أو مرتين شهرياً.

8- عدم إرسال أي معلومات شخصية عبر البريد الإلكتروني، أو الإفصاح عن معلومات خاصة عبر مواقع التواصل الاجتماعي.

وبالإضافة إلى ما سبق من إجراءات عامة، فإن هناك بعض الإجراءات التي

يجب اتخاذها من قبل الإدارة التعليمية بمختلف مستوياتها، والقيادة المدرسية على وجه الخصوص، ومنها (Kritzingler & Bada, 2017) :

1- وضع خطط على مستوى المدارس بشكل عام للتوعية بالأمن السيبراني، والتحذير من المخاطر والانتهاكات السيبرانية، بما يشمل الطلبة والمعلمين.

2- التأكد من تطبيق جميع المدارس لسياسات واضحة بالنسبة للتعامل مع التكنولوجيا الرقمية، بما يشمل الأمن السيبراني، ويجب تعميم تلك السياسات على جميع المدارس، والإشراف على تطبيقها من قبل بعض الجهات المختصة في وزارة التعليم.

3- يجب أن يكون لدى المدرسة خطة عمل واضحة للتعامل مع المخاطر والانتهاكات السيبرانية، وأن تتضمن تلك الخطة الجهات والمؤسسات التي يُمكن للمدرسة التواصل معها لمواجهة تلك المخاطر والانتهاكات.

4- عقد دورات تدريبية لجميع المعلمين في المجالات التالية: الوعي بالأمن السيبراني لدى الطلبة، الاجراءات التي يُمكن للطلبة اتباعها في حال وقوعهم ضحية للمخاطر والانتهاكات السيبرانية.

5- التعاون مع بعض المؤسسات الأكاديمية كالجامعات، أو المؤسسات الاقتصادية ومؤسسات المجتمع المدني في وضع خطط التوعية بالأمن السيبراني، وتوفير المصادر والدعم اللازم للتدريب ونشر الوعي بالأمن السيبراني.

6- إشراك الآباء في خطط وبرامج عمل المدرسة ذات الصلة بالأمن السيبراني.

7- العمل على نشر الاهتمام بموضوع الأمن السيبراني على نطاق واسع، وذلك من خلال عقد ورشات عمل، ندوات، أيام مفتوحة مخصصة للأمن السيبراني، وضع ملصقات أو توزيع كتيبات أو نشرات للتوعية، أو عبر مواقع التواصل الاجتماعي.

8- إدراج موضوع الأمن السيبراني ضمن أدلة المعلمين.

9- اعتبار الوعي بالأمن السيبراني من المهارات الحياتية اللازمة للطلبة، وإدراجه ضمن القضايا المثارة اثناء التدريس والأنشطة المدرسية.

**التصميم التعليمي:**

## التصميم التعليمي لبيئة تعلم إلكترونية تكيفية لتنمية مهارات الأمن السيبراني لدى اخصائي تكنولوجيا التعليم

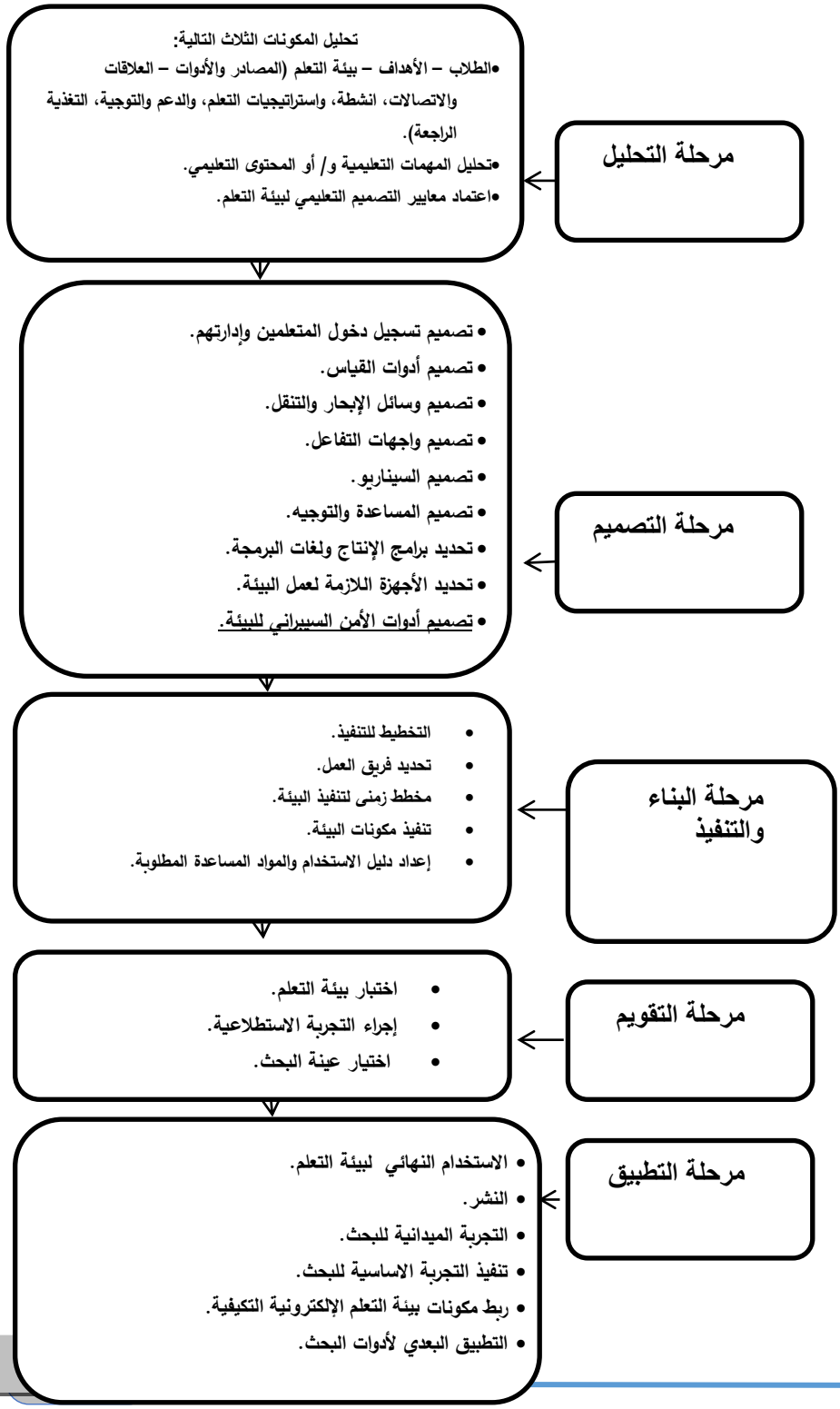
يندرج في التصميم التعليمي تصميم أدوات القياس المستخدمة من اختبار تحصيلي لقياس الجانب المعرفي لمهارات الامن السيبراني لدى اخصائي تكنولوجيا التعليم، وبطاقة ملاحظة لقياس الجانب العملى لمهارات الامن السيبراني لدى اخصائي تكنولوجيا التعليم، وتم تحديد نموذج التصميم المناسب للتصميم التعليمي **لبيئة تعلم إلكترونية تكيفية**، حيث اطلع الباحث على عديد من نماذج التصميم وهي:

نموذج الغريب زاهر اسماعيل (2021)، نموذج محمد ابراهيم الدسوقي (محمد الدسوقي، 2015)، نموذج عبد اللطيف الجزار المطور (2014)، نموذج عبد اللطيف الجزار (عبد اللطيف الجزار، 2013)، نموذج محمد عطية خميس (محمد عطية خميس، 2003، ص125)، نموذج نبيل جاد عزمي ( نبيل جاد عزمي، 2001، ص ص17-48)، النموذج العام لتصميم التعليم ADDIE Model، نموذج كافاريل (Caffarella, 1994)، نموذج بيلى وثرنتون ( Bally & Thornoton, 2009)، نموذج بوث روبرانس ( Roberance, Both & Lucas, Rbert, Jr, 2002).

بعد إطلاع الباحث على النماذج السابقة سوف يتبني الباحث نموذج الغريب زاهر اسماعيل (2021)؛ لتصميم البحث الحالي ومحاولة الباحث من وضع تصور

من هذا التصميم الشامل بما يخدم موضوعه المحدد والموضح بالشكل رقم (1)؛ وذلك للأسباب الآتية:

- تصميم بيئة التعلم التي تتضمن مجموعة متنوعة من المصادر التى يمكن أن تتغير لتلبية الاحتياجات التعليمية لأنها تتطور مع مرور الوقت والتفاعلات التعليمية الالكترونية النشطة وهو ما يتوفر في **بيئة التعلم الإلكترونية التكيفية**، على عكس التصميمات التعليمية التي تركز على مجموعة محددة من الاهداف التعليمية، واقتراح تصميم محدد لا يتغير معتمدا على أسلوب الدمج لتدريس المعلومات الرئيسة المحددة أو المهارة0
- حيث أن البحث الحالي يسعى إلى تصميم بيئة تعلم إلكترونية تكيفية لتنمية مهارت الامن السيبراني لدى اخصائي تكنولوجيا التعليم، ونلاحظ أن تلك المهارات تتم في أوقات متغيرة واماكن كذلك متغيرة، وهذا ما تضمنه نموذج الغريب زاهر على عكس النماذج السابقه حيث تراعي عمليات التعلم فيه أن تتم عمليات التعلم في أماكن الدراسة المتغيرة، وبما يتناسب مع اوقات المتعلمين0
- من الملاحظ تجاهل نماذج التصميم التعليمي الأمن المعلوماتي، وإمكانية اختراق البيئة التعليمية وإلحاق الضرر بها، تم إضافة الأمن السيبراني في تصميم البيئة.


مرحلة التحليل
تحليل المكونات الثلاث التالية:
•الطلاب – الأهداف – بيئة التعلم (المصادر والأدوات – العلاقات والاتصالات، انشطة، واستراتيجيات التعلم، والدعم والتوجية، التغذية الراجعة).
•تحليل المهمات التعليمية و/ أو المحتوى التعليمي.
•اعتماد معايير التصميم التعليمي لبيئة التعلم.
مرحلة التصميم
• تصميم تسجيل دخول المتعلمين وإدارتهم.
• تصميم أدوات القياس.
• تصميم وسائل الإبحار والتنقل.
• تصميم واجهات التفاعل.
• تصميم السيناريو.
• تصميم المساعدة والتوجيه.
• تحديد برامج الإنتاج ولغات البرمجة.
• تحديد الأجهزة اللازمة لعمل البيئة.
• تصميم أدوات الأمن السيبراني للبيئة.
مرحلة البناء والتنفيذ
• التخطيط للتنفيذ.
• تحديد فريق العمل.
• مخطط زمنى لتنفيذ البيئة.
• تنفيذ مكونات البيئة.
• إعداد دليل الاستخدام والمواد المساعدة المطلوبة.
مرحلة التقويم
• اختبار بيئة التعلم.
• إجراء التجربة الاستطلاعية.
• اختيار عينة البحث.
مرحلة التطبيق
• الاستخدام النهائي لبيئة التعلم.
• النشر.
• التجربة الميدانية للبحث.
• تنفيذ التجربة الاساسية للبحث.
• ربط مكونات بيئة التعلم الإلكترونية التكيفية.
• التطبيق البعدي لأدوات البحث.

ويضم هذا النموذج المراحل التالية:

**المرحلة الأولى التحليل وتشمل:**

تم فيها تحليل المكونات الثلاث التالية:

**أولا: تحليل: الطلاب – الأهداف – بيئة التعلم** (المصادر والأدوات – العلاقات

**شكل (1): نموذج لتصميم بيئة التعلم الإلكترونية التكيفية مستند إلى نموذج تصميم بيئة التعلم الإلكترونية المتمركزة حول الطالب للغريب زاهر (الغريب زاهر، 2021)**

والاتصالات، انشطة، واستراتيجيات التعلم، والدعم والتوجية، التغذية الراجعة).

**1: الطلاب:**

التحليل الدقيق وبإحكام في خصائص الطلاب، لتحديد الأهداف التي ستتحقق من خلالهم والمحتوى التعليمي المناسب لهم0

تحديد خصائص المتعلمين وسلوكم المدخلي:

- الخصائص العامة والقدرات الخاصة:

حدد الباحث الخصائص الأساسية للمتعلمين كالمرحلة العمرية، وعدد المتعلمين، ونوعهم، وهم اخصائي تكنولوجيا التعليم وتتراوح اعمارهم من 30 إلى 45 عاماً وتقع هذه الفئة في مرحلة الرشد، كما أنهم يتميزون بقدرات عقلية ولغوية جيدة، ومستوى الدافعية والمستوى الاجتماعي متوسط.

إن بعض القدرات العقلية المعرفية تصل إلى قمتها خلال مرحلة الرشد، وأن المهام التي تتطلَّب السرعة في زمن الاستجابة أو زمن الرجع وذاكرة المدى القصير، والقدرة على إدراك العلاقات المعقدة، تُؤَدَّى بطريقة عالية الكفاءة، كما أن بعض القدرات

الابتكارية وخاصةً تلك التي تتطلَّبُ إنتاج أفكار، أو متنوعة "المرونة"، تصل إلى أعلى مستوياتها أيضًا؛ فالقدرات العقلية المرتبطة بالنشاط اللغوي والسلوك الاجتماعي مثلًا تظل في حالة نموٍ مستمرٍ وهذه هي المهارات والقدرات التي تتحسن بالتعلم والخبرة0

وتم تحديد خصائص المتعلمين في ضوء النقاط التالية:

– انهم في نفس المرحلة العمرية مرحلة الرشد: وتتسم هذه المرحلة العمرية بحب إظهار الذات والتميز و الميل إلى ما هو جديد ومبتكر وتتسم بالميل إلى الثبات الانفعالي .

– لديهم القدرة على استخدام الإنترنت، والتفاعل من خلالها والتعامل مع البرامج المختلفة0

– لديهم الدافعية لتحصيل المحتوى التعليمي حيث أنه من مهامهم الوظيفية والمحتوى نابع من احتياجاتهم.

- **مستوى السلوك المدخلي:**

يتمثل في المهارات التي يمتلكها الاخصائيين بالفعل قبل البدء في التعلم الجديد، ومن خلال عمل الباحث وعمل مقابلات شخصية مع زملائه للتعرف على ما لديهم من معارف ومهارات الامن السيبراني، وما لديهم من خبرات سابقة، تبين قدرتهم على التعامل مع الشاشة التفاعلية بصورة جيدة، وبعض المعارف البسيطة في الامن السيبراني، ولكن يوجد ضعف واضح في مهاراتالامن السيبراني.

**2: الأهداف:**

تهتم بتحديد إطار عام الأداء وما يجب تنفيذه من قبل الطلاب0

تصنيف الأهداف التعليمية، وتحليلها:

تم تصنيف الهدف العام للموضوع الذي سيتم تدريسه باستخدام النموذج، ثم تم ذكر الأهداف التعليمية للموضوعات حسب مستوى بلوم بعد تحليلها، والأهداف العامة المراد تحقيقها:

**الامن السيبراني**

الموضوع الاول: حماية بياناتك وخصوصيتك:

الاهداف الرئيسة

- يحمي أجهزة الحوسبة
- يدير نظام التشغيل والمتصفح
- يحمي جميع الاجهزة
- يستخدم الشبكات اللاسلكية بأمان
- يستخدم كلمات مرور مميزة لكل حساب عبر الإنترنت

الموضوع الثاني: كيفية تشفير البيانات

الهدف الرئيس

- يقوم بتشفير بياناته

الموضوع الثالث: كيفية نسخ البيانات احتياطيًا

الاهداف الرئيسة

- ينسخ بياناته احتياطيًا
- يحذف بياناته نهائياً
- يستخدم المصادقة الثنائية
- يستخدم المصادقة المفتوحة (OAuth)

الموضوع الرابع: إتقان خصوصية مستعرض الويب والبريد الإلكتروني

- يتقن خصوصية مستعرض الويب والبريد الإلكتروني
- يكتشف السلوكيات الخطيرة عبر الإنترنت.

الموضوع الخامس: كيفية مشاركة المعلومات الشخصية عبرالإنترنت

الهدف الرئيس

- يشارك المعلومات الشخصية عبر الإنترنت بطريقة امنه0

وتم صياغة الأهداف الفرعية المنبسقة من الأهداف العامه السابقة، وقد صيغت الأهداف في عبارات تصف سلوك اخصائي تكنولوجيا التعليم المتوقع منهم بعد دراستهم لكل موضوع من مواضيع المحتوى التعليمي المقدم، حيث تم إعداد قائمة للأهداف السلوكية، وتم عرضها على السادة المحكمين وتم التعديل بها حيث كان هناك بعض الأفعال تم تعديلها لتصف السلوك بصورة دقيقة.

3: **بيئة التعلم:**

ويتم فيها تحليل العناصر الاربعة وهى المصادر والأدوات والعلاقات والاتصالات والأنشطة واستراتيجيات التعليم، والدعم والتوجيه والتغذية الراجعة0

**ثانياً: تحليل المهمات التعليمية و/أو المحتوى التعليمي:**

وتم الحصول على المحتوى الخاص بمهارات الامن السيبراني من خلال موقع سيسكو https://lms.netacad.com/course/view.php?id=1233628،

ومن ثم تم تحديد المهارات الرئيسية والمهارات الفرعية من خلال التحليل الهرمي القهقري من أعلى إلى أسفل، وتحليل الغايات والأهداف العامة للمحتوى إلى أهداف رئيسية وأهداف فرعية وفيما يلي عرض لتحليل المهمات التعليمية.

**ثالثاً: اعتماد معايير التصميم التعليمي لبيئة التعلم الإلكترونية التكيفية:**

تم وضع مجموعة من المعايير لتصميم بيئة التعلم الإلكترونية التكيفية لتنمية مهارات الأمن السيبراني، وتتضمن مجموعة من المؤشرات لتطبيق تلك المعايير0

**أ- التأكد من صدق قائمة المعايير:**

عرض قائمة المعايير على مجموعة متخصصة في تكنولوجيا التعليم، وذلك لابداء الرأي فى الصياغة اللغوية، ومدى صلة كل مؤشر بالمعيار الرئيس، السلامة العلمية (سليم- غير سليم)، أهمية البنود (مهم- غير مهم)، وإضافة أو حزف اى معيار أو مؤشر وفقا لما يرونه0

**ب-اراء المحكمين:**

تم عمل التعديلات وفقا لما تم تجميعة من السادة المحكمين من اضافة وحذف، وذلك للبدء في تجربتها مبدئياً0

**ج-المعالجة الإحصائية:**

حساب الوزن النسبي لكل معيار، ومتوسط الوزن النسبي، وتم الإبقاء على الموشرات التي حصلت على نسبة أكثر من 70% من اراء السادة المحكمين.

**د- قائمة المعايير في صوتها النهائية:**

تم وضع الصورة النهائية لقائمة معايير فنية لتصميم بيئة التعلم الإلكترونية التكيفية لتنمية مهارات الامن السيبراني، وتم عمل كافة التعديلات للسادة المحكمين سواء إضافة ، أو حذف، أو تعديل.

**المرحلة الثانية التصميم:**

ويتم فيها وضع تصور كامل للبيئة التعليمية، ويراعى في مكونات التصميم أن تعزز بعضها البعض، مع مراعاة تحديد الأولويات والعلاقات المتبادلة بين جميع المكونات0

**أولاً: تصميم تسجيل دخول المتعلمين، وإدارتهم.**

**ثانياُ: تصميم أدوات القياس.**

**ثالثاً: تصميم وسائل التنقل والإبحار.**

**رابعاً: تصميم واجهات التفاعل.**

**خامساً: تصميم السيناريو.**

**سادساً: تصميم المساعدة والتوجيه.**

**سابعاً: تحديد برامج الانتاج ولغات البرمجه.**

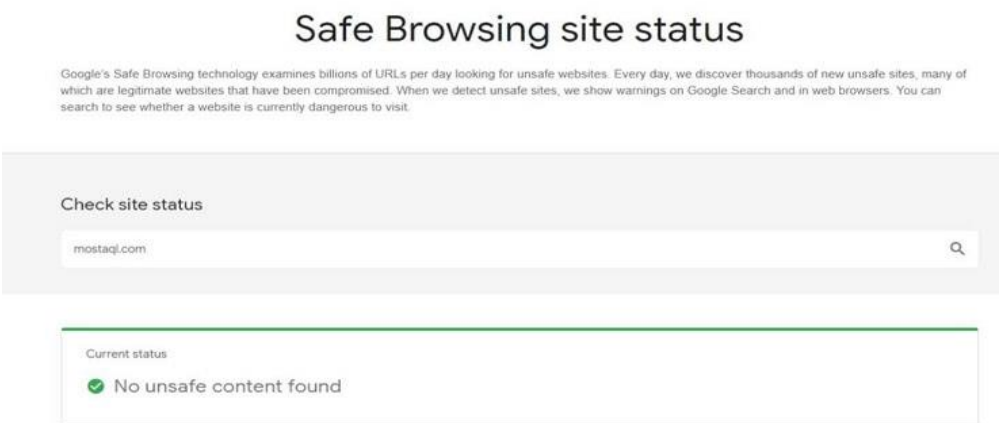
**ثامناً: تحديد الاجهزة اللازمة لعمل البيئة.**

**تاسعاً: تصميم ادوات الامن السيبراني للبيئة:**

- الحماية المتقدمة باستخدام مفتاح أمان للتحقق من هويتك وتسجيل الدخول إلى حسابك على البيئة لن يتمكن المستخدمون غير المصرح لهم من تسجيل الدخول بدون اسم المستخدم وكلمة المرور0
- تأمين البيئة على الويب من خلال التشفير للملفات.
- تأمين البيئة على الويب من خلال التشفير باستخدام تشفير بروتوكول 0HTTPS

- فحص رابط URL للتأكد من صحة صفحة الويب:

الانتقال من شاشة البيئة إلى شاشة متصفح google بمجرد الضغط على مهمة فحص رابط URL للتأكد من صحة صفحة الويب ينتقل إلى اداة google Safe Browsing شكل رقم (2)0




**شكل (2): اداة google Safe Browsing**

- التحميل من مصدر موثوق مثل googleplay، يحافظ على معلوماتك الشخصية آمنة:

يحميل من متجر جوجل وهما Google Photos و Google Drive.

يفتح برنامج الصور Photos.

يضغط على السماح Allow للدخول.

يقوم بإدخال حساب جوجل0

يفتح برنامج الصور و يضغط على زر المساعد 0Assistant

يختار من النافذة المجلدات المراد عمل نسخ احتياطي لها وننقر على 0Device Folders

يقوم بتفعيل كل الخيارات عن طريق سحب الازرار إلى اليمين ثم الرجوع إلى الخلف.

ينقر على زر الصور Photos وسوف تظهر الصور التي سوف يتم تحميلها وعمل نسخة احتياطية منها

- يمنع المتسللين من الدخول على الشبكة اللاسلكية للبيئة:

يغيير معرف SSID المعين مسبقاً وكلمة المرور الافتراضية للواجهة الإدارية المستندة إلى المتصفح0

يشفر الاتصال اللاسلكي من خلال تمكين الأمان اللاسلكي وميزة تشفير WPA2 على الموجه اللاسلكي.

يستخدام خدمة VPN الموثوق بها لمنع الوصول غير المرخص به للبيانات أثناء استخدام الشبكة اللاسلكية0

يتحقق من تكوين الجهاز بمشاركة الملفات والوسائط وأنه يتطلب مصادقة المستخدم من خلال التشفير لمنع التنصت0

يوقف تشغيل تقنية Bluetooth في حالة عدم استخدامه.

**المرحلة الثالثة البناء والتنفيذ:**

- **التخطيط للتنفيذ.**
- **تحديد فريق العمل.**
- **مخطط زمنى لتنفيذ البيئة.**

- **تنفيذ مكونات البيئة.**
- **إعداد دليل الاستخدام والمواد المساعدة المطلوبة.**

**المرحلة الرابعة التقويم:**

**1: اختبار بيئة التعلم التكيفية:**

- تم عمل حساب على البيئة لكل اخصائي بحيث يكون له بريد الكتروني وكلمة مرور خاصة به وذلك بالضغط على اضافة اخصائي وتسجيل البريد الالكتروني وكلمة المرور ، وتم إضافة (60) اخصائي.
- تجربة جميع حسابات المسجلين على البيئة، وذلك بإدخال البريد الالكتروني وكلمة المرور.

**2: إجراء التجربة الاستطلاعية:**

إجراء التجربة الاستطلاعية على عينة ممثلة من اخصائي التكنولوجيا وعددهم (20) اخصائي، بحيث تكون من خارج العينة الرئيسة للبحث، وذلك للتأكد من مدى سلامة المحتوى، والروابط، وإجراء التعديلات ليكون جاهز للتجريب النهائي.

**3: اختيار عينة البحث:**

تمثلت عينة البحث الأساسية من 60 اخصائي من أخصائي تكنولوجيا التعليم بإدارة سنورس التعليمية بمحافظة الفيوم والتي تم اختيارها بطريقة عشوائية، وقد تم التطبيق فى الفصل الدراسي الثاني من العام الدراسي 2024/2023م، وتم تقسيمهم إلى مجموعتين (ضابطة وتجريبية):

- **المجموعة التجريبية**: والتي تطبق عليها تجربة البحث ويتم استخدام البيئة الإلكترونية التكيفية.

- **المجموعة الضابطة:** والتي يتم التدريب باستخدام بيئة إلكترونية.

**التحقق من تكافؤ أفراد العينة:**

قام الباحث بالتأكد من تجانس أفراد المجموعتين (التجريبية– الضابطة) فيما يتعلق بالاختبار التحصيلى وبطاقة الملاحظة ، وتم رصد الدرجات ومعالجتها إحصائيا.

**المرحلة الخامسة التطبيق:**

**أولاً: الاستخدام النهائي لبيئة التعلم الإلكترونية التكيفية.**

**ثانياً: النشر:**

تم نشر الرابط الخاص بالاخصائيين.

**ثالثاً: التجربة الميدانية للبحث:**

بعد التأكد من سلامة البيئة وانها تعمل بكفاءة، وتجربة الاختبار المعرفي بها، تم التطبيق الميداني لتجربة البحث كما يلى:

**1- الحصول على أذونات التطبيق:**

بعد عرض ادوات البحث على سيمنار القسم والموافقة بالتطبيق، تم أخذ الموافقة بالتطبيق من الجهاز المركزي للتعبئة العامة والاحصاء بالقاهرة،، وأخذ موافقة وزارة التربية والتعليم بالقاهرة، وأخذ موافقة مديرية التربية والتعليم بالفيوم وموافقة إدارة سنورس التعليمية.

**2- التطبيق القبلي لأدوات البحث:**

- الاجتماع مع السادة الاخصائيين (عينة البحث) وإعلامهم بإجراءات البحث وعنوانه وأهدافه، وكيفية التعامل مع البيئة الإلكترونية التكيفية.

- تم أخذ موافقة كتابية لافراد عينة البحث على إجراء البحث والمشاركة في البحث والتصوير لتوثيق التجربة.

**رابعاً: تنفيذ التجربة الاساسية للبحث:**

- التأكد من تسجيل جميع افراد عينة البحث وان حساباتهم تعمل.
- التأكد من أن جميع أفراد عينة البحث تم الانتهاء من إجراء الاختبار القبلي، ومتابعة اجراءات الاختبار القبلي وظهور نتيجة تفصيلية لإجابة كل مفردة من مفرادات الاختبار لدي الباحث.
- بعد الانتهاء من الاختبار القبلي من جميع افراء العينة وعددهم (60) اخصائي، تم تقسيم أفراد العينة إلى مجموعتين مجموعة تجريبية أكملت التجربة بإستخدام البيئة الإلكترونية التكيفية وعددهم (30) أخصائي، والمجموعة الثانية مجموعة ضابطة لم تكمل التجربة البيئة الإلكترونية التكيفية ولكن تم تدريبهم على بيئة تعلم إلكترونية.
- تطبيق بطاقة الملاحظه قبلياً باستعانة الباحث بمساعدين له في تسجيل بيانات الملاحظة لافراد عينة البحث.

**خامساً: ربط مكونات البيئة الإلكترونية التكيفية:**

**سادساً: التطبيق البعدي لأدوات البحث:**

- بعد الإنتهاء من فترة التدريب المحددة وإكمال افراد العينة التدريب على بيئة التعلم الإلكترونية التكيفية، تم إجراء الاختبار البعدي وبطاقة الملاحظة على أفراد عينة البحث.

تجميع البيانات التى تم رصدها تمهيداً لإجراء المعالجات الاحصائية.

## نتـائـج البـحث

يهدف هذا الفصل إلي عرض النتائج التى أسفر عنها البحث، والتحقق من صحة فروض البحث وتفسيرها، وتقديم التوصيات والبحوث المقترحة.

## اختبار صحة فروض البحث:

### أولاً: اختبار صحة الفرض الأول:

بالنسبة للفرض الأول من فروض البحث والذي ينص على ما يلي: " توجد فروق ذات دلالة إحصائية بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي للاختبار المعرفي للامن السبيراني لصالح المجموعة التجريبية "

للتحقق من صحة هذا الفرض قام الباحث بحساب قيمة (ت) للمقارنة بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي للاختبار المعرفي للامن السبيراني، ويتضح ذلك من الجدول التالي:

جدول (2) قيمة (ت) ودلالتها الإحصائية للفرق بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي للاختبار المعرفي للامن السبيراني ككل

| البيانات الإحصائية / المجموعة | العدد (ن) | المتوسط الحسابي (م) | الانحراف المعياري (ع) | درجة الحرية | قيمة (ت) الجدولية | | قيمة(ت) المحسوبة | مستوى الدلالة الإحصائية | حجم التأثير (d) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | 0.05 | 0.01 | | | |
| التجريبية | 30 | 27.23 | 0.97 | 58 | 2.00 | 2.66 | 44.04 | 0.01 | 11.57 |
| الضابطة | 30 | 6.63 | 2.37 | | | | | | |

يتضح من الجدول السابق أن قيمة (ت) المحسوبة (44.04) وقيمة (ت) الجدولية تساوي (2.00)عند مستوى ثقة 0.05 وتساوي (2.66) عند مستوى ثقة

0.01 عند درجة حرية (58)، وكذلك يتضح أن حجم التأثير كبير حيث أنه أكبر من 0.8 وهو يساوي (11.57).

مما سبق يتضح أن قيمة (ت) المحسوبة أكبر من قيمة (ت) الجدولية مما يدل على وجود فرق ذو دلالة إحصائية لصالح المجموعة التجريبية، وبذلك تم التحقق من صحة الفرض الثاني.

ولقد قام الباحث بحساب قيمة (ت) للمقارنة بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي للاختبار المعرفي للامن السبيراني فى كل بعد من الابعاد التى يقيسها كما يلي:

جدول (3) قيمة (ت) ودلالتها الإحصائية للفرق بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي للاختبار المعرفي للامن السبيراني فى كل بعد من الابعاد

| الابعاد | المجموعة | العدد | المتوسط | الانحراف المعياري | قيمة (ت) | مستوى الدلالة | حجم التأثير (d) |
|---|---|---|---|---|---|---|---|
| تذكر | التجريبية | 30 | 3.70 | 0.47 | 10.60 | 0.01 | 2.78 |
| | الضابطة | 30 | 1.30 | 1.15 | | | |
| فهم | التجريبية | 30 | 4.70 | 0.53 | 19.59 | 0.01 | 5.14 |
| | الضابطة | 30 | 0.93 | 0.91 | | | |
| تطبيق | التجريبية | 30 | 14.27 | 0.83 | 28.55 | 0.01 | 7.50 |
| | الضابطة | 30 | 3.37 | 1.92 | | | |
| تحليل | التجريبية | 30 | 1.77 | 0.43 | 9.16 | 0.01 | 2.40 |
| | الضابطة | 30 | 0.37 | 0.72 | | | |

| الابعاد | المجموعة | العدد | المتوسط | الانحراف المعياري | قيمة (ت) | مستوى الدلالة | حجم التأثير (d) |
|---|---|---|---|---|---|---|---|
| تركيب | التجريبية | 30 | 2.80 | 0.41 | 14.26 | 0.01 | 3.75 |
| | الضابطة | 30 | 0.67 | 0.71 | | | |

يتضح من الجدول السابق أن قيمة (ت) المحسوبة أكبر من قيمة (ت) الجدولية ، وكذلك يتضح أن حجم التأثير كبير حيث أنه أكبر من (0.8) في كل بعد من الابعاد والمجموع الكلي، مما يدل على وجود فرق ذي دلالة إحصائية بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي للاختبار المعرفي للامن السيبراني فى كل بعد من الابعاد لصالح المجموعة التجريبية.

**ثانياً: اختبار صحة الفرض الثاني:**

بالنسبة للفرض الثاني من فروض البحث والذي ينص على ما يلي : " توجد فروق ذات دلالة إحصائية بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي لبطاقة ملاحظة الامن السيبراني لصالح المجموعة التجريبية ".

للتحقق من صحة هذا الفرض قام الباحث بحساب قيمة (ت) للمقارنة بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي لبطاقة ملاحظة الامن السيبراني، ويتضح ذلك من الجدول التالي:

جدول (4) قيمة (ت) ودلالتها الإحصائية للفرق بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي لبطاقة ملاحظة الامن السيبراني ككل

| البيانات الإحصائية / المجموعة | العدد (ن) | المتوسط الحسابي (م) | الانحراف المعياري (ع) | درجة الحرية | قيمة (ت) الجدولية | | قيمة(ت) المحسوبة | مستوى الدلالة الإحصائية | حجم التأثير (d) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | 0.05 | 0.01 | | | |
| التجريبية | 30 | 106.87 | 1.91 | 58 | 2.00 | 2.66 | 130.84 | 0.01 | 34.36 |
| الضابطة | 30 | 15.43 | 3.32 | | | | | | |

يتضح من الجدول السابق أن قيمة (ت) المحسوبة (130.84) وقيمة (ت) الجدولية تساوي (2.00)عند مستوى ثقة 0.05 وتساوي (2.66) عند مستوى ثقة 0.01 عند درجة حرية (58)، وكذلك يتضح أن حجم التأثير كبير حيث أنه أكبر من 0.8 وهو يساوي (34.36).

مما سبق يتضح أن قيمة (ت) المحسوبة أكبر من قيمة (ت) الجدولية مما يدل على وجود فرق ذو دلالة إحصائية لصالح المجموعة التجريبية، وبذلك تم التحقق من صحة الفرض الثاني.

ولقد قام الباحث بحساب قيمة (ت) للمقارنة بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي لبطاقة ملاحظة الامن السيبراني فى كل بعد من الابعاد التى يقيسها كما يلي:

جدول (5) قيمة (ت) ودلالتها الإحصائية للفرق بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي لبطاقة ملاحظة الامن السيبراني فى كل بعد من الابعاد

| الابعاد | المجموعة | العدد | المتوسط | الانحراف المعياري | قيمة (ت) | مستوى الدلالة | حجم التأثير (d) |
|---|---|---|---|---|---|---|---|
| كيفية حماية بياناتك وخصوصيتك | التجريبية | 30 | 55.27 | 0.58 | 100.67 | 0.01 | 26.44 |
| | الضابطة | 30 | 8.70 | 2.47 | | | |
| كيفية تشفير البيانات | التجريبية | 30 | 11.87 | 0.68 | 47.49 | 0.01 | 12.47 |
| | الضابطة | 30 | 1.67 | 0.96 | | | |
| كيفية نسخ البيانات احتياطيًا | التجريبية | 30 | 28.03 | 1.61 | 60.76 | 0.01 | 15.96 |
| | الضابطة | 30 | 2.67 | 1.63 | | | |
| كيفية مشاركة المعلومات الشخصية عبر الانترنت. | التجريبية | 30 | 11.70 | 0.47 | 34.42 | 0.01 | 9.04 |
| | الضابطة | 30 | 2.40 | 1.40 | | | |

يتضح من الجدول السابق أن قيمة (ت) المحسوبة أكبر من قيمة (ت) الجدولية، وكذلك يتضح أن حجم التأثير كبير حيث أنه أكبر من (0.8) في كل بعد من الأبعاد والمجموع الكلي، مما يدل على وجود فرق ذي دلالة إحصائية بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي لبطاقة ملاحظة الامن السيبراني فى كل بعد من الابعاد لصالح المجموعة التجريبية.

## تفسير نتائج البحث:

الفرض الأول يوجد فرق دال احصائيا عند مستوى (0.05) بين متوسطي درجات المجموعة التجريبية ودرجات المجموعة الضابطة في الجانب المعرفي لمهارات الامن السيبراني في التطبيق البعدي للاختبار التحصيلي لصالح المجموعة التجريبية، يتضح أن قيمة (ت) المحسوبة أكبر من قيمة (ت) الجدولية، وكذلك يتضح أن حجم التأثير كبير حيث أنه أكبر من (0.8) في كل بعد من الابعاد والمجموع الكلي، مما يدل على وجود فرق ذي دلالة إحصائية بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي للاختبار المعرفي للامن السيبراني فى كل بعد من الابعاد لصالح المجموعة التجريبية، ويرجع ذلك إلى إستخدام بيئة تعلم إلكترونية تكيفية و تميز وتوجه عملية التعلم الشخصي المستمر من خلال خرائط المعرفة ومراقبة أنشطة المتعلمين، والاستجابة لها في الوقت الفعلي، وتتفق النتائج مع نظرية التدريس بالآلة لسكينر (Wleklinski. N,. 2017)، حيث اكتساب خصائص القدرة على التكيف، وباعتباره محدودًا بمستوى التكنولوجيا، وإن التعلم التكيفي المدعوم بالتكنولوجيا، يعتمد بشكل أساسي على قواعد أو معايير بسيطة ويتلخص جوهره في مجرد نقل الطالب إلى مكان ما من مسار التعلم المحدد مسبقًا وفقًا لمعلومات التغذية الراجعة الخاصة به، واتفقت النتائج مع نتائج الدراسات السابقة مثل دراسة (Peng, Z.T. Zhu, 2017)، حيث التطبيقات المستخدمة في السياق التعليمي آمنة وموثوقة، والتأكيد على أن استخدام بيئة تعلم إلكترونية تكيفية يجعل الطلاب والمعلمون على دراية ببروتوكولات السرية والموثوقية عند استخدام الأدوات والأجهزة التكنولوجية، ويكونوا على دراية بالاستخدام الآمن لهذه التقنيات وحماية أنفسهم من أي تهديدات إلكترونية محتملة، وتقع على عاتق السلطات

المدرسية قبل استخدام التكنولوجيا الجديدة إبلاغ موظفي المدرسة والطلاب كيفية الاستفادة من تلك التقنيات بأمان.

الفرض الثاني يوجد فرق دال احصائيا عند مستوى (0.05) بين متوسطي درجات المجموعة التجريبية ودرجات المجموعة الضابطة في الجانب الادائي لمهارات الامن السيبراني في التطبيق البعدي لبطاقة الملاحظة لصالح المجموعة التجريبية، يتضح أن قيمة (ت) المحسوبة أكبر من قيمة (ت) الجدولية، و يتضح أن حجم التأثير كبير حيث أنه أكبر من (0.8) في كل بعد من الأبعاد والمجموع الكلي، مما يدل على وجود فرق ذي دلالة إحصائية بين متوسطى درجات المجموعة التجريبية والمجموعة الضابطة فى التطبيق البعدي لبطاقة ملاحظة الامن السيبراني فى كل بعد من الابعاد لصالح المجموعة التجريبية، ويرجع ذلك حيث تجعل البيئة التكيفية من الممكن تسجيل وتفسير الخصائص الفردية للأخصائي وحالته في الوقت الفعلي في جميع جوانب التعلم، واستخدام بيانات التعلم المسجلة بشكل أكثر فعالية في تقييم عمليات التعلم والتنبؤ بالأداء المستقبلي وتحديد المشكلات الأمنية المحتملة التي يمكن أن يتعرض لها، وبهذه الطريقة يمكن للأخصائيين باستخدام البيئة التكيفية على اتخاذ قرارات ذات قيمة، وبالتالي توفير المزيد من المعلومات المفيدة بدلاً من مجرد الإبلاغ عن البيانات الأولية سترسل البيئة التكيفية معلومات ذات مستوى أعلى إلى الاخصائيين لمزيد من التقييم واتخاذ القرار بشكل أسرع، ويتفق ذلك مع دراسة ( Zhu & Shen 2013)حيث صمم نظامًا تعليميًا تكيفيًا مخصصًا بثلاث حلقات تغذية مرتدة من تدفقات البيانات، ومن خلال البيانات المكثفة، أصبح التعلم التكيفي نموذجًا جيدا للتكنولوجيا التعليمية، وتتفق النتائج مع دراسة (Waters, 2014) حيث يخلق التعلم التكيفي تجربة للأخصائيين للتعامل مع البيئة التكيفية حسب تقدمه في أداء المهارة، ويتم تعديلها بناءً على أداء الأخصائي وتفاعله مع محتوى البيئة

التكيفية، ففي جوهره كما ذكرت الدراسة هو نهج للتعليم يعتمد على التكنولوجيا والبيانات حول أداء المتعلم للتكيف والاستجابة بالمحتوى والمنهجيات التي تطور مسارًا لإتقان المتعلم لهدف تعليمي معين، وتجاوز الثغرات الأمنية أو المخاوف المتعلقة بالخصوصية، وتوكد الدراسة على أنه عند الإبلاغ عن مسائل انتهاك الخصوصية والثغرات الأمنية في بيئة تعلم تكيفية تزداد قدرة المستخدمين في مواجهة الثغرات الأمنية.

**التوصيات:**

بعض التوصيات لإستخدام بيئات التعلم الإلكترونية التكيفية في التعليم:

عندما يتم دمج الإنترنت مع تقنيات مثل انظمة الاندرويد والتعلم النقال وتحليلات البيانات، فإنه يجلب نموذجًا جديدًا في التعليم، لتمكّن بيئات التعلم الإلكترونية التكيفية المؤسسات من:

- تغيير الطريقة التي يقدم بها المعلمون الدروس واختبار التحصيل باستخدام بيئة تعلم إلكترونية تكيفية، والاختبار عبر الإنترنت.
- توظيف انظمة الاندرويد وغيرها من الوسائط الرقمية التفاعلية التي يمكنها جمع وتحليل البيانات للمعلمين والطلاب لاستخدامها في الفصل الدراسي، أو في أي مكان آخر، وفي أي وقت مما يؤدي إلى تحسين التدريس وتحسين نتائج التعلممن خلال بيئة تعلم إلكترونية تكيفية.
- تعليم تصميم بيئات التعلم الإلكترونية التكيفية وكيفية استخدامه لطلبة تكنولوجيا التعليم.
- توظيف بيئة تعلم إلكترونية تكيفية في تشكيل خطط الدروس الذكية والفصول الدراسية الذكية والحرم الجامعي الذكي.

**المقترحات:**

1. تصميم بيئة تعلم إلكترونية تكيفية لتنمية مهارات التفكير الناقد لدى الطلاب ذوى الإعاقة السمعية.
2. تصميم بيئة تعلم إلكترونية تكيفية لتنمية مهارات صيانة الحاسب الالي لدى طلبة تكنولوجيا التعليم.
3. تصميم بيئة تعلم إلكترونية تكيفية لتنمية مهارات انتاج برمجيات الاندرويد لدى اخصائي تكنولوجيا التعليم.

**المراجع:**

**أولا المراجع العربية:**

منى الأشقر جيور (2016) السيبرانية هاجس العصر، لبنان: جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية.

**ثانياً المراجع الأجنبية:**

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security, 12(4).

Chun-Hui, Wu., Chen, Y.-S., & Chen, T. C. (2017). An adaptive e-learning system for enhancing learning performance: based on dynamic scaffolding theory. Eurasia Journal of Mathematics, Science and Technology Education. https:// doi. org/ 10.12973/ ejmste/ 81061.

Chweya, R.; Ibrahim, O.; Nilashi, M.(2019) IoT in Higher Learning Institutions: Opportunities and Challenges. J. Soft Comput. Decis. Support Syst.

Cletus, D., & Eneluwe, D. (2020). The impact of learning style on student performance: mediate by personality. International

Journal of Education, Learning and Training. https:// doi. org/ 10. 24924/ ijelt/ 2019. 11/ v4. iss2/ 22. 47Des mond.

Crompton, B., Thompson, D., Reyes, M., Zhou, X., and Zou., X. (2016). Cybersecurity awareness Shrewsbury public schools. School of professional studies. Paper 3.

Ennouamani, S., & Mahani, Z. (2017). An overview of adaptive e-learning systems. Eighth International ConfeRence on Intelligent

impact Networking. (2021). 15 Cybersecurity In Education Stats You Should Know. https://www.impactmybiz.com/blog/cybersecurity-in-education-stats/

Ivy, J., Lee, S. B., Franz, D., & Crumpton, J. (2019). Seeding Cybersecurity Workforce Pathways With Secondary Education. Computer, 52(3), 67–75. https://doi.org/10.1109/MC.2018.2884671

King.L. (2018). The intenet of things and libraries. En ligne sur: http://www.davidleeking.com/the-internet-of-things-iot-and-libraries.

Kritizinger, E., Bada, M., & Nurse, J. (2017). A study into the cybersecurity awareness initiatives for school learners in south africa and the uk. 10th world conference on information security education. Rome.

Kurt, S. (2021). Adaptive learning: What is it, what are its benefits and how does it work? EducationalTechnology. https://educationaltechnology.net/adaptive-learning-what-is-it-what-are-its-benefits-and-how-does-it-work/

Mahnane, L., Laskri, M. T., & Trigano, P. (2013). A model of adaptive e-learning hypermedia system based on thinking

and learning styles. International Journal of Multimedia and Ubiquitous Engineering.

McGuire, R. (2021). What is adaptive learning and how does it work to promote equity in higher education. Every Learner Everywhere. https://www.everylearnereverywhere.org/blog/what-is-adaptive-learning-and-how-does-it-work-to-promote-equity-in-higher-education/

Nengdi, Wu (2016). Wireless Communication Technologies in Internet of Things(IOT), master thesis, University of Vaasa, Faculty of Technology, Communication and Systems Engineering

Nuankaew, P., Nuankaew, W., Phanniphong, K., Imwut, S., & Bussaman, S. (2019). Students model in different learning styles of academic achievement at the University of Phayao, Thailand. International Journal of Emerging Technologies in Learning (iJET)., 14, 133. https:// doi. org/ 10. 3991/ ijet. v14i12. 10352.

Oxford University Press. (2014). Oxford Online Dictionary. Oxford: Oxford University Press. [Online]. Available:http://www.oxforddictionaries.com/definition/english/Cybersecuri y

Palmisano .S. J. (2008). A smarter Planet: The Next Leadership Agenda.https://www.ibm.com/ibm/cioleadershipexchange/us/ en/pdfs/SJP_Smarter_Planet.pdf.

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education. IEEE Security & Privacy, 18(2), 68–74. https://doi.org/10.1109/MSEC.2020.2969409

Peng, H., Ma, S., & Spector, J.M. (2019). Personalized adaptive learning: an emerging pedagogical approach enabled by a smart learning environment. Smart Learning Environment, 6(9). https://doi.org/10.1186/s40561-019-0089-y

Peng, Z.T. Zhu, (2017) Measuring to assist learning: A Core mechanism of precision instruction in smarter education. E-Educ.

Pusey, P., & Sadera, W. A. (2011). Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. Journal of Digital Learning in Teacher Education, 28(2), 82–85. https://doi.org/10.1080/21532974.2011.10784684

Redmon, M., Wyatt, S., & Stull, C. (2021). Using personalized adaptive learning to promote industry-specific language skills in support of Spanish internship students. Global Business Languages, 21, 92-112. https://doi.org/10.4079.gbl.v21.6

Sintef & Norway.( 2014). Internet of Things–From Research and Innovation to Market Deployment. Aalborg, Denmark: River Publishers.

Sollins, H. (2019)."IoT big data security and privacy versus innovation," IEEE Internet of Things Journal, vol. 6, no. 2.

Solms, S., & Solms, R. (2014). Towards Cyber Safety Education in Primary Schools in Africa. HAISA.

Stewart, K., & Shilingford, N. (2011). Cyber girls Sumer camp: Exposing middle school females to Internet security. Unpublished master thesis. University of Minnesota.

Truong, H. (2016). Integrating learning styles and adaptive e-learning system: current developments, problems, and opportunities. Computers in Human Behavior, 55(2016), 1185–1193. https:// doi. org/ 10. 1016/j. chb. 2015. 02. 014.

UNESCO. (2018). UNESCO ICT Competency Framework for Teachers Version 3. https://unesdoc.unesco.org/ark:/48223/pf0000265721

Valentina Terzieva, Svetozar Ilchev, Katia Todorova. (2022) The Role of Internet of Things in Smart Education, Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Bulgaria, https://www.sciencedirect.com/science/article/pii/S2405896322011466?ref=pdf_download&fr=RR-2&rr=88a946309b4c0ff2

von Solms, S., & von Solms, R. (2014). Towards Cyber Safety Education in Primary Schools in Africa. HAISA, Wange. Yunxiao (2017). IOT Device Management and Configuration, master thesis, Department of Computer Science, University of Saskatchewan Saskatoon, SaskatchewanCanada.

Waters (2014). The Great Adaptive Learning Experiment. https://campustechnology.com/articles/2014/04/16/the greatadaptive learning-experiment.aspx

Wilson, C. (2014). Cybersecurity education the emergence of an accredited academic discipline. Journal of the colloquium information system security education. 2(1) .

Wleklinski. N. (2017). Skinner's Teaching Machine and Programmed Learning Theory. http://people.ischool.illinois.edu/~chip/ projects/timeline/1954teaching_machine.html

Zhu, D.M. Shen, New paradigm of educational technology research based on Big Data. E-Educ. Res. (10).