مجلة كلية التربية

فاعلية برنامج الكتروني قائم علي تطبيقات التعلم المنتشر في تنمية الوعي بالأمن السيبراني لدي الطلاب المعلمين بكلية التربية النوعية (شعبة الحاسب الآلي)

The Effectiveness of an Electronic Program Based on Ubiquitous -Learning Applications in Developing Cyber security among Student teachers at the Faculty of Specific Education (Computer Department)

بحث مستل من رسالة دكتوراه

إعداد

آيات منصور إبراهيم صالح

مسئول مركز المعلومات ودعم اتخاذ القرار

مديرية التربية والتعليم بالدقهلية

أ. د. فريال عبده أبو ستة

أستاذ المناهج وطرق تدريس

الرياضيات (المتفرغ)

ورئيس قسم المناهج وطرق التدريس السابق

أ. د. محمد عبده راغب عماشة

أستاذ استخدامات الحاسب في التعليم

وعميد كلية التربية النوعية

جامعة دمياط

د. شيماء سمير أنور حميدة

مدرس المناهج وطرق تدريس الرياضيات

كلية التربية – جامعة دمياط

١٤٤٥هـ – ٢٠٢٤م

مستخلص البحث:

هدف البحث إلى الكشف عن فاعلية برنامج مقترح قائم علي تطبيقات التعلم المنتشر فى تنمية الوعي بالأمن السيبراني لدي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي، وكانت عينة البحث مكونة من (٣٢) طالب وطالبة من الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي بدمياط، وتمثلت المواد التعليمية في برنامج الكتروني قائم على تطبيقات التعلم المنتشر (من إعداد الباحثة)، مدونة الكترونية تحتوي علي المنهج المقترح، وتمثلت أدوات القياس في مقياس الوعي بالأمن السيبراني، وأسفرت نتائج المعالجة الإحصائية عن وجود فروق ذات دلالة إحصائية عند مستوي (٠.٠٥) بين التطبيق القبلي والبعدي في مقياس الوعي بالأمن السيبراني لصالح التطبيق البعدي، مما يدل علي فاعلية البرنامج الالكتروني المقترح والقائم علي تطبيقات التعليم المنتشر في تنمية الوعي بالأمن السيبراني لدي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي، وأوصت الباحثة بضرورة توسيع استخدام تطبيقات التعلم المنتشر في تدريس المواد الدراسية المختلفة، وتطبيق البرنامج على فئات أخرى من الطلاب والمعلمين في مختلف التخصصات.

الكلمات المفتاحية: تطبيقات التعلم المنتشر، الوعي بالأمن السيبراني، طلاب شعبة الحاسب الآلى.

The Effectiveness of an Electronic Program Based on Ubiquitous -Learning Applications in Developing Cyber security among Student teachers at the Faculty of Specific Education (Computer Department)

Abstract:

This research aimed to reveal the effectiveness of a proposed program based on Ubiquitous learning applications in developing cybersecurity awareness among student teachers at the Faculty of Specific Education, Computer Department. The research sample consisted of (32) male and female students from the student teachers at the Faculty of Specific Education, Computer Department in Damietta. The educational materials were represented by an electronic program based on Ubiquitous learning applications (prepared by the researcher), an electronic blog containing the proposed curriculum, and the measurement tools were represented by the cybersecurity awareness scale. The results of the statistical processing showed statistically significant differences at the level of (0.05) between the pre- and post-application in the cybersecurity awareness scale in favor of the post-application, which indicates the effectiveness of the proposed electronic program based on Ubiquitous learning applications in developing cybersecurity awareness among student teachers at the Faculty of Specific Education, Computer Department. It was recommended that the use of Ubiquitous learning applications be expanded in teaching various subjects, and that the program be applied to other categories of students and teachers in various specializations.

Keywords: Ubiquitous learning applications, cybersecurity awareness, computer science students.

مقدمة:

تلعب الثقافة الرقمية دورًا حيويًا في تعزيز الوعي الأمني وحماية الأفراد والمجتمعات من التهديدات الرقمية المتزايدة في العصر الحالي من خلال التمكين من فهم كيفية تأمين البيانات الشخصية أو المؤسسية، وتجنب التهديدات والجرائم المعلوماتية مثل الاحتيال والاختراقات، وتسهم الثقافة الرقمية في بناء مجتمع واعٍ ومدرك لمخاطر العالم الرقمي، هذا الوعي لا يعزز فقط الأمان الشخصي، بل يساهم أيضًا في بناء مجتمع رقمي متكامل يدعم التنوع والتفاعل الثقافي، وحماية الأوطان ككل.

ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي في القرن (٢١) وما نتج عنه من تداعيات عديدة بسبب ظهور تهديدات وجرائم معلوماتية ترافق تطبيقات الثقافة الإلكترونية المتزامنة أصبحت تشكّل تحديًا كبيرًا للأمن القومي وكذلك الدولي، لدرجة اعتبارها بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني (Cybersecurity) كبُعد جديد ضمن أجندة حقل الدراسات الأمنية، ومؤخرًا الدراسات التربوية (Singer .,& Friedman, 2014) [١]. ويعد الأمن السيبراني من أكثر المواضيع جذبًا للانتباه لا سيما مع التطور التقني الكبير والمتسارع الذي يشهده عالمنا اليوم، حيث يبحث الأفراد والشركات والمنشآت الكبيرة بشكل خاص اليوم عن وسائل وتقنيات تمكّنهم من حماية معلوماتهم التي في تهديد، ويتطلب التمكن من الأمن السيبراني امتلاك الخبرة والمهارة، وليس فقط مجرد المعرفة النظرية (تامر متولي وآخرون، ٢٠٢٢).

[١] **يسير التوثيق في البحث الحالي وفق A P A (اسم ولقب المؤلف ، سنة النشر ، رقم الصفحة)**

والأمن السيبراني هو استخدام تقنيات وعمليات ووسائل حماية لحماية الأنظمة والشبكات والبرامج والأجهزة والبيانات من الهجمات الإلكترونية، بهدف تقليل خطر الهجمات الإلكترونية والحماية من الاستغلال غير المصرح به للأنظمة والشبكات والتقنيات (IT Governance, 2021).

وعلي ذلك فلابد من تحقيق قدر من المهارات المطلوبة للحماية من هذه المخاطر، والتدريب على الأدوات والإجراءات اللازمة لضمان هذه الحماية مثل تعلم إنشاء كلمة مرور قوية، وكيفية مراقبة الحسابات الشخصية واكتشاف أي تصيد أو هجوم إلكتروني، وحماية إعدادات الخصوصية في مواقع التواصل الاجتماعي والحذر من الرسائل الانتحالية، وغيرها من وسائل الحماية (YTH, 2015).

ويأتي دور المؤسسات التربوية في إعداد الطلاب بصفة عامة بشكل يمكنهم من التعامل مع كافة التطورات التكنولوجية، وما يتطلبه هذا التعامل من درجة وعي كافية بالأمن السيبراني الذي يؤدي إلي تنمية الوعي لديهم نحو أمنهم علي المستوي الشخصي من جهة وعلي المستوي القومي من جهة أخري.

وبالنسبة للطلاب المعلمين، يتضاعف الاهتمام بالأمن السيبراني نظرًا لدورهم المستقبلي كقادة تربويين ومسؤولين عن توجيه الأجيال القادمة، وإن فهم الطلاب المعلمين لمبادئ الأمن السيبراني يمكنهم من خلق بيئة تعليمية آمنة لتلاميذهم، وتعزيز ممارسات الأمان الرقمي في المؤسسات التعليمية، حيث أظهر تقرير من مؤتمر الأمن السيبراني والتعليم أن تدريب المعلمين على الأمن السيبراني يمكن أن يحسن من استجابة المدارس للهجمات السيبرانية بنسبة تصل إلى ٥٠% (Cybersecurity and Education Conference, 2021).

وفي مجال البحث العلمي التربوي أكدت العديد من الدراسات علي أهمية تضمين الأمن السيبراني في المؤسسات التعليمية، ومنها:

دراسة بيكاك وليو وميرفي Bicak, Liu., & Murphy (2015) التي أشارت إلى أهمية وعي المعلمين بكافة التطورات المتعلقة بتحديات ومفاهيم الأمن السيبراني، وحيوية هذا الدور بالنسبة لإعداد الطلاب في التعامل مع البيئات السيبرانية في المستقبل، وأن تطوير مناهج الأمن السيبراني يجب أن يكون عملية مستمرة ومرنة، تستجيب للتغيرات السريعة في مجال الأمن السيبراني وتلبي احتياجات سوق العمل المتطورة، واقترحوا إدخال تخصصات محددة في برامج الدراسات العليا يمكن أن يساعد في إعداد الخريجين بشكل أفضل للتحديات المستقبلية في مجال الأمن السيبراني.

ودراسة بلاك وشابمان وكلارك Blake, Chapman, & Clark (2018) التي أكدت على أهمية مشاركة المعلمين لمعارفهم وخبراتهم التقنية ونقلها إلى الطلاب عبر بيئة تعليمية تفاعلية تمكنهم من ممارسة المهارات النظرية عمليًا باستخدام آلات افتراضية، كما سلطت الضوء على بعض القيود مثل غياب آليات تقييم تقدم المستخدمين، مما يشير إلى الحاجة لمزيد من التحسينات المستقبلية، وتعكس هذه الدراسة الدور الحيوي للتكنولوجيا في تعزيز الوعي بالأمن السيبراني وتطوير أساليب تعليمية مبتكرة وفعّالة.

ودراسة أميرة غوص وباسم الشريف (٢٠٢٢) التي تناولت فاعليَّةُ تَوظيفِ بعضِ التَّطبيقاتِ التّعليميَّةِ الذَّكيَّة في تقديم وحدَّة مقترَحة عن الْأَمْنِ السيبراني على التَّحصيل المعرفي والْاتِّجاهات نحوهُ لدى طالباتِ المرحلةِ المتوسِّطةِ بِالمدينَةِ المُنوَّرةِ، وتكونت عينة الدراسة من (٦٣) طالبة من طالبات الصف الثانى المتوسط، وتوصلت الدِّراسَة إلى وجود فرق ذي دلالةٍ إحصائيَّة عند مستوى (٠.٠١) بين متوسِّطي درجات طالبات المجموعتين التجريبيَّة والضابطة في التطبيق البعدي لمستويات التذكُّر، والفهم، والتطبيق، وكذلك الدرجة الكليَّة للاختبار التحصيلي، لصالح المجموعة التجريبيَّة، وأوصت الدِّراسَة بضرورة تضمين وحدة عن الأمن السيبراني،

في منهج الحاسب الآلي للمرحلة المتوسِّطة، والاستفادة من التطبيقات الذكيَّة في توضيح مفاهيم الأمن السيبراني، واستخدام نظريات التعلُّم الموقفي في تصميم محتوى وأنشطة منهج الحاسب الآلي في المرحلة المتوسِّطة.

وحيث يفرض عصر الانفجار المعرفي تمكين الطلاب من استيعاب واستخدام المعرفة ومهاراتها، وتنمية مهارات التعلم الذاتي بطرق متنوعة، أدت التطورات في تكنولوجيا التعليم الإلكتروني إلى ظهور التعليم عبر الهواتف الذكية وأجهزة الحاسب اللوحية، مما زاد من التفاعل الاجتماعي والإبداع مع تطور أدوات التعلم النقال، انتقل التعليم الإلكتروني إلى التعليم المنتشر (Jung, 2014).

واستنادًا إلى التقارب بين التعلم الإلكتروني، والتعلم النقال والتكنولوجية اللاسلكية التي جعلت التعلم المنتشر ممكنًا للطلاب في أي وقت وأي مكان، حيث أن أحد الفروق الكبيرة بين التعلم التقليدي والتعلم المنتشر هو أن التعلم المنتشر يوفر المحتوى العلمي للطالب وفقًا لحالته من خلال الحصول على معلومات من سياقات التعلم المختلفة، مما يجعل من استخدام التكنولوجيا النقالة مثل الهواتف الذكية التي توفر للطلاب فرص التعلم ذاتيا دون فرض قيود الوقت والمكان (Joiner., et al., 2006)

وحيث أشار محمد خميس (٢٠٠٨) إلى أنه ترجع فكرة التعلم المنتشر إلى أواخر الثمانينيات عندما استخدم مارك ويزر مصطلح الحوسبة المنتشرة للإشارة إلى وجود أجهزة الحاسب الآلي في كل مجالات الحياة، فهو حولنا في كل مكان أينما نذهب فلم يعد يقتصر الأمر على أجهزة الحاسب المعتادة بل أصبح كثير من الأجهزة والمعدات تعمل بالمعالجات الدقيقة.

ويعتبر التعلم المنتشر توسيعًا وامتدادًا لفكرة الحاسب المنتشر Ubiquitous مما يصف الوجود النافذ لأجهزة الحاسب في تعلمنا، ويساعد في تكوين بنية معرفية

جديدة اصبحت ممكنة بواسطة موفري الوسائط المتعددة (إيمان سحتوت، زينب جعفر،٢٠١٤).

وأوضح محمد عماشة وسالم الخلف (٢٠١٥) أن مكونات بيئة التعليم المنتشر، كالآتى:

١. المعالجات الدقيقة: ويقصد بها الأجهزة الذكية محمولة كانت او ثابته، تتيح للطالب التفاعل المباشر من خلال جهاز الإحساس وتبادل المعلومات المناسبة للموقف التعليمي.

٢. وحدة الخادم: ويقصد بها الأجهزة الرئيسية التي تستضيف نظام التعلم المنتشر وتوفر الأدوات لقواعد البيانات وأدوات التحليل والاكتشاف وتتضمن المعايير والأساليب لعمل النظام كما يجب مثل (المخولين بدخول البيئة– التحديث – سلامة الأداء).

٣. التكنولوجيا اللاسلكية:ويقصد بها التكنولوجيا التي تتيح للأجهزة الحركة بحريه دون وجود ارتباط مادي لنقل المعلومات، وهذه التكنولوجيا تعتبر سببا أساسيا في فاعلية التعليم المنتشر ليكون في كل مكان وزمان ولكن يعيبه ضرورة وجود مزود خدمه أو جهاز موزع شبكي يحمل ذات الخواص، كما انه يستهلك الطاقة ولو بشكل خفيف.

٤. أجهزة الإحساس:هي مستشعرات منتشرة في البيئة المحيطة متجانسة مع الأجهزة التي يحملها الطالب متصلة مع وحدة الخادم لتستجيب للإشارات وتعكس ذلك تفاعلًا مع جهاز الطالب بمجرد الاقتراب منها، أي بواسطة استخدام أجهزة الإحساس تستطيع وحدة الخادم تحدد كل طالب داخل فضاء التعلم المنتشر مجرد أن يقترب الطالب منها.

وعلي ذلك تشكل مكونات بيئة التعليم المنتشر أساسًا لتوفير تجربة تعليمية متكاملة وفعالة. تسهم المعالجات الدقيقة في التفاعل الفوري مع المحتوى عبر

الأجهزة الذكية، بينما تدير وحدة الخادم النظام التعليمي بالكامل، بما في ذلك إدارة البيانات وتحليلها. تضمن التكنولوجيا اللاسلكية الوصول إلى التعليم في أي وقت وأي مكان، وتلعب أجهزة الإحساس دورًا في تحديد مواقع المتعلمين وتوفير تفاعل تلقائي. مجتمعة، تتيح هذه المكونات تجربة تعليمية تدعم التعلم الذاتي والتفاعلي.

وأشار فيرتانين وسوكي (Suki., & Suki (2011); Virtanen (2018 إلى أن تطبيقات التعلم المنتشر، تتمثل فى:

١. تقنية بودكاست Podcast :

من تقنيات ويب ٢ تتكون من تسجيلات صوتية أو مرئية تحتوي على حوار كلامي أو ملفات موسيقية أو ملفات فيديو يتم تحميلها من خلال تطبيقات Apps أو من خلال شبكة الإنترنت، فيمكن استثمارها في تحميل المحاضرات وبالتالي القدرة على سماعها في أي وقت وتقديم التغذية الراجعة داخل المحاضرة، ومن ثم تُعرف المقررات بشكل أوسع، وتتميز بزيادة تفاعل الطلاب عن طريق سهولة مشاهدته أو سماعه في أي مكان مما يزيد من تحكم الطالب.

٢. تقنية Remote Response System (RRS) :

نظام الاستجابة عن بعد هو نظام يستخدم للتفاعل عن بعد، مما يمكن الطلاب من المشاركة في الفصول الدراسية والاختبارات والمناقشات من أي مكان وفي أي وقت باستخدام التكنولوجيا الحديثة مثل الإنترنت والأجهزة المحمولة. هذا النظام يعزز من التفاعل بين الطلاب والمعلمين ويسمح بتقديم ملاحظات فورية، ويمكن الطلاب من التفاعل مع المحتوى التعليمي عن بعد وتقديم ردود فورية تعزز التفاعل، ويُستخدم RRS في الفصول الدراسية الافتراضية والاختبارات عبر الإنترنت، مما يزيد من التفاعل والمشاركة.

٣. تقنية RFID:

تعتمد على تحديد هوية المتعلم تلقائيا من خلال شريحة إلكترونية من السليكون مثبته في جهاز المتعلم والتي تقوم بإرسال البيانات والاستعلامات لخادم التعلم المنتظر من خلال موجات الراديو.

٤. تقنية Context Aware:

تقوم بتوفير موقف تعليمي يعتمد على وضع المتعلم في سلسلة من الدروس التي تربط بين البيئات الحقيقية والبيئات الإفتراضية، وبالتالي ترتبط بحالة الطالب المكانية والزمانية أثناء التعلم.

٥. نظم إدارة التعلم Learning Management Systems :

تقدم خدمات الويب الحديثة في نظم إدارة التعلم (LMS) إمكانيات متكاملة لإدارة المتعلمين، مثل تسجيل الدخول، إنشاء الملفات الشخصية، ومتابعة الأنشطة، وتتيح هذه النظم إنشاء وإدارة المحتوى التعليمي والمقررات الدراسية والاختبارات الإلكترونية، مع أدوات تفاعل تزامنية وغير تزامنية، مثل Moodle و .Blackboard تطورت هذه النظم لتصبح أكثر توافقًا مع احتياجات المتعلمين، مما أتاح تقديم محتوى تعليمي أكثر تخصيصًا عبر نظم إدارة التعلم المنتشر(ULMS) .

تعزز تطبيقات التعلم المنتشر، مثل البودكاست ونظام الاستجابة عن بعد(RRS)، من تجربة التعلم الذاتي والتفاعل الفوري بين الطلاب والمعلمين، كما تسهم تقنيات RFID وContext Awareفي تخصيص تجربة التعلم وفقًا لظروف الطالب، هذه الابتكارات تدعم التعلم المستدام والشامل، مما يعكس تطور الأدوات التعليمية لتلبية احتياجات العصر الرقمي، وتبنت الباحثة هذا النموذج من التعلم المنتشر، لما يقدمه من توافق تلقائي مع احتياجات وخصائص الطلاب، مستفيدًا من الأجهزة النقالة المتصلة بالإنترنت والمتاحة للجميع.

وقد اهتمت العديد من الدراسات بالأمن السيبرانى، مثل:

دراسة عبد العال السيد ورشا إبراهيم (٢٠١٨) التي هدفت إلى تقصي أثر تطبيقات التعلم المنتشر على تنمية مهارات تصميم قواعد البيانات الإلكترونية لدى طلاب المرحلة الثانوية، وتم اختيار عينة الدراسة من ٥٦ طالبًا بالصف الثانى الثانوى بمدينة الرياض، وتوصلت نتائج الدراسة إلى وجود فروق دالة إحصائيًا لصالح المجموعة التجريبية في التحصيل الدراسي، ملاحظة الأداء، وتقييم المنتج النهائي.

وهدفت دراسة أحمد علي وآخرون (2023) إلى استكشاف تأثير بيئة التعلم المنتشر على تطوير مهارات محددة في تصميم قواعد البيانات لدى طلاب المرحلة الثانوية، وتكونت عينة الدراسة من (٦٠) طالبًا وطالبة بالصف الثالث الثانوى التجارى، وقد أظهرت نتائج البحث أن استخدام بيئة التعلم المنتشر أدى إلى زيادة التحصيل المعرفي والأدائي في مهارات وحدتي إنشاء قواعد البيانات والاستعلامات في برنامج اكسيس Access ضمن مقرر الحاسب الآلي على الصف الثالث الثانوي التجاري

وتشير هذه الدراسات إلى أن التعلم المنتشر ليس مجرد وسيلة تعليمية حديثة، بل هو أداة فعالة تعزز من جودة التعليم، وتساعد في التغلب على التحديات التعليمية المختلفة، خاصة في ظل الظروف الصعبة مثل جائحة كورونا.

وعلي ذلك فلابد من البحث عن سبل تطوير التكنولوجيا، وملاءمتها مع السياق المحلي، مسترشدين بالتجارب الدولية المختلفة، فعندما يكون التدريس في الفصول الدراسية صعبًا، فإن التعلم على الهاتف المحمول كأحد تطبيقات التعلم المنتشر قد يكون ممكناً، في ظل توافر سبل تحقق أمن المعلومات وأمن الشبكة متمثلًا في الأمن السيبراني.

الإحساس بالمشكلة:

وذلك من خلال:

أولًا: الاطلاع على نتائج بعض البحوث والدراسات السابقة وتوصيات المؤتمرات علي ضرورة الاهتمام بالأمن السيبراني وتنمية الوعي بكيفية الحفاظ على المعلومات والبيانات الرقمية لكل مواطن، ووضع برامج لتوعية الشباب بأهمية الأمن السيبراني في مرحلتي التعليم الأساسي والجامعي:

الدراسات والأبحاث:

Bicak, Liu, & Murphy (2015) ، حازم صالح (٢٠١٨) ، (2018) Virtanen., et al، فاطمة المنتشري (٢٠١٩).

المؤتمرات العلمية:

- مؤتمر القاهرة السابع للأمن الإلكترونى" Cairo Security Camp" في نوفمبر ٢٠١٦.

ثانيًا: بمراجعة مناهج الحاسب الآلي وتكنولوجيا المعلومات في جميع مراحل وفئات التعليم قبل الجامعي فانها لا تتطرق لأي من المواضيع المتعلقة بالأمن الإلكتروني فيما عدا وحدة إثرائية في الصف الثاني الإعدادي تحتوي بعض الإرشادات للتعامل الآمن مع الإنترنت.

ثالثًا: الدراسة الاستكشافية التي قامت بها الباحثة لعينة عشوائية قوامها (٤٠) طالب وطالبة من طلاب شعبة الحاسب الآلي– كلية التربية النوعية – جامعة المنصورة بهدف التعرف علي مدي استيعاب طلاب المرحلة الجامعية لمفاهيم ومهارات الأمن السيبراني ومدي وعيهم تجاهه من خلال تطبيق استطلاع رأي يتضمن أسئلة حول المفاهيم المبدئية لأمن المعلومات وأمن الشبكات، وعن مدي قدرة الطلاب علي حماية أجهزتهم الشخصية (موبايل، جهاز كمبيوتر، لابتوب) وعن مدي احساسهم بالأمان تجاه بياناتهم الشخصية ومرفقاتهم (صور، ملفات، .... إلخ)علي هذه الأجهزة،

واتضح للباحثة من النتائج تدني لمهارات الأمن السيبراني لدي أفراد العينة علي الرغم من امتلاكهم جميعًا لأجهزة ذكية وحسابات إلكترونية مفعلة واستخدامهم لتطبيقين علي الأقل من تطبيقات الإنترنت.

مشكلة البحث:

تتضح مشكلة البحث الحالي في تدني مستوي الوعي بالأمن السيبراني لدي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي.

وتتحدد مشكلة البحث في السؤال الرئيسي التالي:

ما فاعلية برنامج الكتروني قائم علي تطبيقات التعليم المنتشر في تنمية الوعي بالأمن السيبراني لدي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي؟

وتفرع من السؤال الرئيسي الأسئلة الفرعية التالية:

١. ما مستوى وعي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي بالأمن السيبرانى؟
٢. ما صورة البرنامج الإلكتروني بعنوان "مقدمة في الأمن السيبراني" القائم علي تطبيقات التعلم المنتشر؟
٣. ما فاعلية برنامج الكتروني قائم علي تطبيقات التعليم المنتشر في تنمية الوعي بالأمن السيبراني لدي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي؟

مصطلحات البحث:

١- الأمن السيبراني Cybersecurity:

يشير مفهوم الأمن السيبراني إلى ممارسات حماية الأنظمة والشبكات والبيانات من الهجمات الرقمية. تهدف هذه الهجمات إلى الوصول إلى المعلومات الحساسة أو تعديلها أو تدميرها، أو ابتزاز الأموال، أو تعطيل العمليات التجارية العادية. تشمل

المفاهيم الأساسية في الأمن السيبراني ثلاثية "السرية، السلامة، والتوافر"، والتي تضمن حماية المعلومات من الوصول غير المصرح به، والحفاظ على دقتها، وضمان توفرها عند الحاجة. علاوة على ذلك، تبرز التهديدات المستجدة مثل البرمجيات الخبيثة، والهجمات التصيدية، وبرامج الفدية أهمية الحذر المستمر والابتكار في استراتيجيات الحماية (Christen et al., 2020, 13).

تعرفه الباحثة إجرائيًا بأنه مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية المجال السيبراني (الشبكات، الأجهزة، البرمجيات، البيانات الشخصية، والمؤسسية) من التهديدات السيبرانية علي مستوي الفرد، والمؤسسة.

٢- الوعي بالأمن السيبراني Cybersecurity Awareness**:**

يشير مفهوم التوعية بالأمن السيبراني إلى فهم ووعي الأفراد والمؤسسات بالتهديدات والمخاطر السيبرانية. يتضمن ذلك تثقيف الأشخاص حول أهمية حماية بيئاتهم الرقمية من خلال التعرف على التهديدات المحتملة مثل هجمات التصيد الاحتيالي والبرمجيات الخبيثة وانتهاكات البيانات. تساهم التوعية الفعالة في تعزيز الممارسات الآمنة مثل إنشاء كلمات مرور قوية، وتجنب الروابط المشبوهة، وتحديث الأنظمة بانتظام. مع تطور العالم الرقمي، يعد تعزيز ثقافة الوعي بالأمن السيبراني أمرًا حيويًا لتقليل المخاطر وتحسين مستوى الأمان للأفراد والمنظمات (Christen et al., 2020, 161).

تعرفه الباحثة إجرائيًا بأنه مدي إحتياج الطلاب المعلمين لاكتساب المهارات الأساسية للحفاظ علي البيانات الشخصية أو المؤسسية في المجال السيبراني.

٣- التعلم المنتشر:

هو نمط تعليمي يمكن من خلاله أن يحدث التعلم في أي وقت وأي مكان باستخدام تقنيات الحوسبة المنتشرة (Yahya., et al., 2010, 120).

تعرفه الباحثة إجرائيًا بأنه أسلوب للتعلم باستخدام تطبيقات (RRS, Podcast, LMS, RFID, Context Aware) يقوم به الطالب المعلم بكلية التربية النوعية– شعبة الحاسب الآلي– الفرقة الرابعة بغرض اكتساب الوعى بالأمن السيبراني.

٤– تطبيقات التعلم المنتشر:

تطبيقات التعلم المنتشر (Pervasive Learning Applications) تشمل مجموعة من الأدوات والتقنيات التي تسهم في توفير تجربة تعليمية مرنة وشخصية، بحيث يمكن للمتعلمين الوصول إلى المحتوى التعليمي في أي وقت وأي مكان، من خلال الأجهزة المتصلة بالإنترنت والأنظمة التي تتفاعل مع السياق المحيط بالمتعلم. تشمل هذه التطبيقات:

- أنظمة إدارة التعلم (LMS): هي منصات مركزية تسهل إدارة المحتوى التعليمي، التفاعل مع الطلاب، ومتابعة تقدمهم. توفر وصولاً سهلاً إلى المواد التعليمية وتتيح التعلم عن بُعد في أي وقت ومن أي مكان (Jones & Jo, 2004, 470).
- تقنية RFID: تُستخدم لتعقب الأجسام والأشخاص في بيئات التعلم الذكية باستخدام موجات الراديو. تسمح بتحديد مواقع المتعلمين أو المواد التعليمية، مما يتيح تخصيص الأنشطة التعليمية وفقًا للسياق(Ogata et al., 2005, 208).
- البودكاست (Podcasts): توفر وسيلة لنشر المحتوى التعليمي على شكل ملفات صوتية يمكن الوصول إليها في أي وقت. تسهم في تعزيز التعلم المتنقل وتتيح للمتعلمين الاستماع إلى المحاضرات أو النقاشات أثناء التنقل (Sharples et al., 2009, 340).
- التعلم المعتمد على السياق (Context-aware Learning): هو نظام يستخدم تقنيات مثل أجهزة الاستشعار لتحليل بيئة المتعلم (مثل المكان أو النشاط) وتخصيص المحتوى بناءً على تلك البيانات، مما يتيح تجربة تعلم مخصصة لكل متعلم وفقًا لسياقه الخاص(Li et al., 2013, 365) .

تتفاعل هذه التطبيقات مع بعضها البعض لتشكيل بيئة تعليمية مدمجة ومتصلة، مما يعزز التعلم الذاتي ويزيد من إمكانية تخصيص التجربة التعليمية حسب احتياجات كل طالب.

اجرائيًا: هي تطبيقات رقمية تعتمد على التكنولوجيا الحديثة لتمكين التعلم في أي وقت وأي مكان باستخدام الأجهزة المحمولة والذكية. هذه التطبيقات تتيح للطلاب التفاعل مع المحتوى التعليمي بشكل مستمر دون الحاجة للتواجد في بيئة تعليمية تقليدية، تتنوع تطبيقات التعلم المنتشر بين تطبيقات إدارة التعلم، بودكاستات تعليمية، أنظمة الاستجابة عن بعد، وتقنيات تحديد الهوية باستخدام موجات الراديو، وتوفر جميعها تجارب تعليمية متكاملة وتفاعلية.

أهداف البحث:

- التعرف علي مستوى وعي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي بالأمن السيبرانى.
- تفسير أسباب التدني في مستوي الوعي بالأمن السيبراني، لدي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي.
- التنبؤ بفاعلية برنامج الكتروني قائم علي تطبيقات التعليم المنتشر في تنمية الوعي بالأمن السيبراني لدي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي.

أهمية البحث:

- تتماشى مع الاتجاهات الحديثة في بناء وتطوير المناهج من حيث تفعيل دور الطالب في العملية التعليمية، واكسابه مهارات التعلم الفردي، والتعلم الجماعي في ذات الوقت.

- الإسهام في تزويد المسئولين عن تطوير المناهج بوزارتي التعليم العالي والبحث العلمي والتربية والتعليم بأهمية هذه الجزئية من علوم الحاسب وتضمينها بكافة مراحل التعليم.
- الإسهام في لفت أنظار القائمين بوزارتي التعليم العالي والبحث العلمي والتربية والتعليم نحو أهمية تطوير تطبيقات التعلم المنتشر، والحد من التهديدات السيبرانية.
- الإسهام في تغيير نظرة الطلاب إلى مادة الحاسب الآلي تغييراً إيجابياً من حيث تزويده بمعلومات غالبا يحتاجها في واقع حياته العملية، وليس مجرد تأصيل دراسي تخصصي فقط .
- الإسهام في جعل تطبيقات التعلم المنتشر أكثر تأثيرا بتوظيفها عبرمختلف المواد الدراسية عبر مراحل التعليم المختلفة.
- تنمية الوعى بالأمن السيبراني للطلاب في مختلف المراحل التعليمية، وبالتالي نقل هذه الثقافة للمجتمع ككل.
- تقديم مقياس وعى بالأمن السيبرانى يمكن الاستعانة به في معرفة وعى طلاب المرحلة الجامعية بالأمن السيبرانى، وما قبلها.
- تقديم بعض التوصيات والمقترحات التي قد تفتح مجالاً لبحوث ودراسات مستقبلية أخرى لتطويرتعليم وتعلم الحاسب الآلى وفق تطبيقات التعلم المنتشر في تنمية متغيرات تابعة أخرى وتنفيذها في مراحل تعليمية أخرى .

محددات البحث: اقتصر البحث الحالي على الحدود التالية:

حدود موضوعية: المفاهيم والمهارات الأساسية للأمن السيبراني فيما يخص حماية البيانات الشخصية والمؤسسية.

حدود بشرية: عينة عشوائية مكونة من ٣٢ طالب وطالبة من الطلاب المعلمين بالفرقة الرابعة بكلية التربية النوعية جامعة دمياط شعبة الحاسب الآلي.

حدود زمنية: الفصل الدراسي الثاني للعام الدراسي ٢٠٢٣ / ٢٠٢٤.

حدود مكانية: كلية التربية النوعية جامعة دمياط.

متغيرات البحث:

المتغير المستقل : برنامج إلكتروني قائم علي تطبيقات التعلم المنتشر.

المتغير التابع: الوعي بالأمن السيبراني.

منهجا البحث:

استخدمت الباحثة المنهج الوصفى لتفسير، ووصف، وتحليل الدراسات السابقة المتعلقة بالتعلم المنتشر والأمن السيبراني، والمنهج التجريبي القائم على المجموعة الواحدة؛ لقياس أثر المتغير المستقل (البرنامج الإلكتروني بإحدي تطبيقات التعلم المنتشر) على المتغير التابع (الوعي بالأمن السيبراني لدي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي).

أدوات ومواد البحث:

١- البرنامج الإلكتروني القائم علي تطبيقات التعلم المنتشر في مهارات الأمن السيبراني.

٢- مقياس الوعي بالأمن السيبراني لدي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي.

إجراءات البحث:

للإجابة على أسئلة البحث والتحقق من صحة فروضها اتبعت الباحثة الإجراءات التالية :

أولاً : للإجابة على السؤال الأول ونصه:

ما مستوى وعي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي بالأمن السيبرانى؟

قامت الباحثة بالآتي:

- اعداد مقياس وعي يقيس وعي الطلاب بالأمن السيبراني.
- عرض مقياس الوعي علي السادة المحكمين للتأكد من صلاحيته للتطبيق ثم إجراء التعديلات المطلوبة وفقًا لآرائهم ومقترحاتهم، ووضع المقياس في صورته النهائية.
- تطبيق مقياس الوعي علي عينة استطلاعية للبحث من الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي من أجل الضبط الإحصائيً.
- اختيار عينة البحث من الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي.
- تطبيق مقياس الوعي قبليًا علي عينة البحث من الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي

ثانيا : للإجابة على السؤال الثاني ونصه هو:

ما صورة برنامج إلكتروني في مهارات الأمن السيبراني قائم علي تطبيقات التعلم المنتشر ؟

قامت الباحثة بالآتي:

- دراسة متطلبات إعداد البرنامج الإلكتروني المقترح القائم علي تطبيقات التعلم المنتشر وتشمل:
  - دراسة تطبيقات التعلم المنتشر

- دراسة لغات البرمجة وبرامج التصميم التي سيتم إعداد البرنامج الإلكتروني بها.
- إعداد محتوي البرنامج وصياغته الصياغة التربوية المناسبة.

- إعداد البرنامج الإلكتروني في صورة Mobile Application القائم علي تطبيقات التعلم المنتشر.
- عرض البرنامج الإلكتروني المقترح على مجموعة من السادة المحكمين للتأكد من صلاحيته للتطبيق.
- تعديل البرنامج الإلكتروني المقترح فى ضوء أراء السادة المحكمين، والتوصل للصورة النهائية.

ثالثا: للإجابة على السؤال الثالث ونصه:

ما فاعلية برنامج الكتروني قائم علي تطبيقات التعليم المنتشر في تنمية الوعي بالأمن السيبراني لدي الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي؟

قامت الباحثة بالآتي:

- تطبيق مقياس الوعي قبليًا على مجموعة البحث.
- تطبيق البرنامج الإلكتروني المقترح على مجموعة البحث.
- تطبيق مقياس الوعي بعديًا على مجموعة البحث.
- جدولة النتائج وتحليلها إحصائياً.
- اختبار صحة الفروض من خلال المعالجات الإحصائية.
- تفسير نتائج البحث والتعليق عليها فى ضوء الأدبيات والدراسات والبحوث السابقة.
- تلخيص نتائج البحث وتقديم التوصيات والمقترحات في ضوء ما أسفرت عنه نتائج البحث الحالية لإجراء دراسات وبحوث مستقبلية.

أدبيات البحث:

المحور الأول: تطبيقات التعلم المنتشر Ubiquities Learning**:**

التعلم المنتشر هو ذلك النوع من التعلم الموجود حولنا دائمًا في كل مكان وزمان ولكننا لا نشعر به، ويمكن بلوغه بسهولة باستخدام أجهزة التعلم المتنقل-m learningوأجهزة الحاسب النقال، وحاسب الجيب، والتليفونات المحمولة، وجهاز المساعدات الرقمية الشخصي (PDAs) وجهاز قراءة الكتب الإلكترونية (جمال الدهشان ومجدي يونس، ٢٠٠٩).

والتعلم المنتشر(Ubiquitous learning) هو نمط تعليمي يمكن من خلاله أن يحدث التعلم في أي وقت وأي مكان باستخدام تقنيات الحوسبة المنتشرة (Yahya, et al., 2010).

وعرفه عصام الحسن (٢٠١٥، ٨٢) بأنه: تعلم سياقي حقيقي وظيفي وتكيفي يتم من خلاله توصيل كائنات التعلم الإلكتروني المناسبة إلى مجموعة من الطلاب المتواجدين في أماكن مختلفة ومتباعدة وتتم إدارة التعلم والأنشطة التعليمية الوظيفية المناسبة في الوقت والمكان المناسب.

وتعرفه الباحثة إجرائيا بأنه أسلوب للتعلم باستخدام تطبيقات (RSS, Podcast, LMS, RFID, Context Aware) يقوم به الطالب المعلم بكلية التربية النوعية– شعبة الحاسب الآلي– الفرقة الرابعة بغرض تنمية الوعي تجاه الأمن السيبراني.

بيئة التعلم المنتشر:

تُعرف بيئة التعلم المنتشر بأنها: وسيط مناسب يتيح للطلاب الانغماس بشكل كامل في عملية التعلم، بتقديم الدعم والمحفزات المطلوبة التي تشجع على مشاركة الطلبة دون الحاجة إلى لفت انتباه نشط منهم (محمد عماشة وسالم الخلف، ٢٠١٥).

ويقول فيرتانين Virtanen., et al (2018) أن هذه البيئة تتميز بنظام واعٍ بالسياق، حيث يمكنه معرفة واستشعار معلومات الطلاب والمعلومات المحيطة بهم

في العالم الحقيقي، وتقديم خدمات مخصصة، مما يسمح للطلاب بتعلم المعرفة والمهارات وحل المشكلات أثناء تفاعلهم مع العالم الحقيقي من خلال سيناريوهات واقعية.

وبالتالي تتميز بيئة التعلم المنتشر بقدرتها على خلق أنشطة تعلم أكثر نشاطًا وتكيفًا في العالم الحقيقي، حيث يمكن للطلاب التعلم في الوقت المناسب، في المكان المناسب، باستخدام الأدوات والمحتوى المناسب.

أهداف وأهمية التعلم المنتشر:

يتميز التعلم المنتشر بالقدرة على تكييف العملية التعليمية لتلبية الاحتياجات الفردية لكل طالب، مما يعزز من فرص النجاح الأكاديمي والتطور الشخصي، وفقًا لدراسة أجراها جونز وجو Jones & Jo (2004)، فإن التعلم المنتشر يسهم في خلق بيئة تعليمية مرنة تتناسب مع أساليب التعلم المتنوعة، مما يزيد من مشاركة الطلاب وتحفيزهم.

كما أن هذا النمط من التعلم يتيح للطلاب الوصول إلى المحتوى التعليمي في الوقت المناسب والمكان المناسب، مما يسهم في تحسين نتائج التعلم (Sharples., et al., 2005).

كذلك تعزيز الوصول إلى التعليم، وجعل التعليم أكثر سهولة، من خلال إزالة قيود الوقت والمكان، يضمن التعلم المنتشر أن يتمكن الطلاب من التعامل مع المواد التعليمية في أي وقت ومن أي مكان، مما يستوعب أساليب التعلم والجداول الزمنية المختلفة (Virtanen, et.al, 2018).

وعلي ذلك فيبرز التعلم المنتشر كتحول جوهري في التعليم، حيث يستغل التكنولوجيا المتقدمة لخلق بيئة تعليمية مرنة ومخصصة تلبي احتياجات المتعلمين المتنوعة. هذا التحول يعزز من التفاعل والمشاركة بين الطلاب، ويتيح لهم التعلم في أي وقت وأي مكان، مما يسهم في تحسين نتائجهم الأكاديمية وتطوير مهاراتهم

الشخصية. كما يدعم كلا من التعلم الفردي والتعلم التعاوني معًا، مما يزيد من دافعية الطلاب من خلال تقديم تجارب تعلم مخصصة وملائمة لاحتياجاتهم

خصائص التعلم المنتشر:

حددت شركة SMOWL وهي شركة تقنية أوروبية متخصصة في تطوير حلول مراقبة الامتحانات عبر الإنترنت، خصائص التعلم المنتشر في الآتي: Smowltech (2022)

- إمكانية الوصول غير المحدود Unlimited accessibility :

حيث يمكن الوصول إلي المادة العلمية باستمرار، مما يعزز التعلم مدى الحياة وديمقراطية المعرفة.

- التنقل Mobility :

إمكانية الوصول إلى المعلومات من أي مكان في المجال المهني والشخصي، مما يجعله شاملاً ويزيل أي عوائق جغرافية أو معمارية.

- التكيف Adaptability:

يتكيف مع جميع أنماط المتعلمين وتسهيل تخصيص المحتوى.

- التفاعلية Interactivity :

يسمح بتواصل ثنائي الاتجاه بين المعلم والطالب، مما يحفز كلا الطرفين.

- الفورية Immediacy:

الوصول الفوري إلى الإجابات والوثائق يقلل من وقت البحث ويحسن استيعاب المعلومات.

- عدم الرسمية Informality:

يحدث التعلم في الظروف التي يختارها الفرد دون الحاجة إلى الالتزام بقواعد أو بيئات صارمة.

- التعاون Collaboration:

عززت تقنيات المعلومات والاتصالات تطوير منصات التعلم التعاوني التي يمكن من خلالها للأشخاص التفاعل ببساطة واستمرار، وتبادل الأفكار وتعزيز التواصل الاجتماعي.

مما سبق نجد أن التعلم المنتشر يشير إلى أسلوب تعليمي يتميز بقدرته على التكيف مما يمثل تحولًا نحو نهج أكثر مرونة واتصالًا وتخصيصًا في التعليم، مستفيدًا من التكنولوجيا لتعزيز تجربة التعلم، ومن خلال فهم ودمج هذه خصائصه في الممارسات التعليمية، يمكننا تعزيز بيئة تعليمية ليس فقط فعالة ولكن أيضًا مشوقة وملهمة لجميع المتعلمين التي تجعل التعلم المنتشر قوة تحويلية في تشكيل مستقبل التعليم من وجهة نظر بعض المتخصصين في هذا المجال.

تطبيقات التعلم المنتشر:

تتنوع تطبيقات التعلم المنتشر لتشمل مجالات متعددة، مثل التعليم الرسمي في المدارس والجامعات، والتدريب المهني في المؤسسات والشركات، والتعليم غير الرسمي عبر منصات التعلم عبر الإنترنت(Georgouli, et al., 2008).

التعلم عبر الأجهزة المحمولة (Mobile Learning):

التعلم المنتشر يستفيد بشكل كبير من الأجهزة المحمولة مثل الهواتف الذكية والأجهزة اللوحية، مما يتيح للمتعلمين الوصول إلى المحتوى التعليمي في أي وقت وأي مكان. ويشمل ذلك:

أ) المنصات التعليمية (Educational Apps): مثل منصة كورسيرا (Coursera)
الموقع الرسمي: [coursera.org](https://www.coursera.org)

ب) *تطبيقات إدارة التعلم* (Learning Management Systems - LMS): مثل

- مودل (Moodle): وهو نظام مفتوح المصدر لإدارة التعلم يستخدم في العديد من المؤسسات التعليمية حول العالم لتوفير بيئة تعليمية تفاعلية وشاملة.
- الموقع الرسمي: moodle.org

- **التعلم المدعوم بالسياق (Context-Aware Learning):**

هو نهج تعليمي يستخدم تقنيات مثل تحديد المواقع (GPS) والبيانات البيئية لتقديم محتوى تعليمي مخصص يتناسب مع الظروف المحيطة بالمتعلم. يهدف هذا النوع من التعلم إلى تحسين تجربة التعلم من خلال تكييف المواد التعليمية والأنشطة مع السياق الفعلي للمتعلم. ويشمل:

مثل: تطبيق GeoGebra: هو تطبيق رياضي تفاعلي يتيح للطلاب استكشاف الموضوعات الرياضية والجغرافية بشكل تفاعلي، مما يعزز فهم الطلاب للموضوعات الجغرافية والرياضية.

الموقع الرسمي: geogebra.org

- الفصول الدراسية الافتراضية (Virtual Classrooms):

هي بيئات تعليمية عبر الإنترنت تتيح للمعلمين والطلاب التفاعل في الوقت الفعلي من خلال مؤتمرات الفيديو، الدردشات، والأنشطة التفاعلية الأخرى. هذه الفصول تمكّن المعلمين من تقديم الدروس والمحاضرات، وتنظيم المناقشات، وإجراء التقييمات، والتواصل مع الطلاب بطرق مماثلة للفصول التقليدية. (Google Workspace Updates, 2023; Google for Education, 2024).

مثل:

أ) التعلم المتزامن (Synchronous Learning):

يتيح للمعلمين والطلاب عقد الاجتماعات والدروس الافتراضية في الوقت الفعلي، مما يوفر بيئة تعليمية تفاعلية عبر منصات تمكن للطلاب حضور الدروس الحية والمشاركة في المناقشات والتفاعل مع الزملاء والمعلمين في الوقت الفعلي بشكل فوري.مثل:

- **Google Meet:** هو تطبيق مؤتمرات الفيديو من جوجل، يستخدم لعقد الاجتماعات والدروس الافتراضية في الوقت الفعلي.

- الرابط الإلكتروني: (https://meet.google.com)[meet.google.com].

ب) التعلم غير المتزامن (Asynchronous Learning):

يتيح الوصول إلى المحاضرات المسجلة والمواد التعليمية في أي وقت من خلال منصات تمكن للطلاب مراجعة المواد التعليمية وإكمال الواجبات في الوقت الذي يناسبهم. مثل:

- **Google Classroom:** هو نظام إدارة تعلم من جوجل، يتيح للمعلمين إنشاء الدروس، توزيع الواجبات، والتواصل مع الطلاب، ويوفر للمعلمين إمكانية تحميل المحاضرات والواجبات، مما يتيح للطلاب الوصول إليها وإكمالها حسب جداولهم الزمنية.

- الرابط الإلكتروني:

(https://classroom.google.com)[classroom.google.com]

- التعلم التفاعلي والمخصص (Interactive and Personalized Learning)

التعلم التفاعلي والمخصص هو نهج تعليمي يستخدم تقنيات مثل الذكاء الاصطناعي والتعلم الآلي لتقديم تجارب تعليمية مخصصة بناءً على احتياجات واهتمامات كل طالب. يهدف هذا النهج إلى جعل التعليم أكثر تفاعلية وجاذبية وملائمة لكل متعلم بشكل فردي (Chou, 2013)، مثل:

أ) نظم التوصية (Recommendation Systems):

أنظمة تقدم توصيات لمحتوى تعليمي معين، ودورات تعليمية مخصصة بناءً على اهتمامات وتفضيلات المستخدم، أو الطالب وأدائه السابق (Duitama, Defude, Lecocq, & Bouzeghoub, 2006)، مثل:

- **Coursera**: هي منصة تعليمية تقدم دورات تعليمية عبر الإنترنت بالتعاون مع جامعات ومؤسسات عالمية. وتستخدم نظم التوصية لتقديم دورات مخصصة لكل مستخدم بناءً على اهتماماته وأدائه.

الرابط الإلكتروني: (https://www.coursera.org)[coursera.org].

ب) التقييمات التكيفية (Adaptive Assessments):

أنظمة تقوم بتقييم أداء الطالب وتعديل مستوى الصعوبة بناءً على نتائجه السابقة، وتقديم تحديات تعليمية تتناسب مع مستوى تقدمهم (Knewton, 2023)، مثل:

- **Knewton**: هي منصة تعليمية تستخدم الذكاء الاصطناعي والتقييمات التكيفية لتقديم تجارب تعليمية مخصصة تساعد على تحسين أداء الطلاب.

الرابط الإلكتروني: (https://www.knewton.com)[knewton.com]

التحديات التي تواجه توظيف تطبيقات التعلم المنتشر في التعليم:

يواجه التعليم المنتشر عدة تحديات مهمة تؤثر على فعاليته وتطبيقه في النظام التعليمي، تشمل هذه التحديات (Zawacki-Richter et al., 2019; SMOWL, 2024):

- البنية التحتية التقنية: ضرورة توفر اتصال إنترنت عالي السرعة وأجهزة ملائمة للطلاب والمعلمين.
- المهارات الرقمية: الحاجة لتدريب المعلمين والطلاب على استخدام التقنيات الحديثة بفعالية.
- ضمان الجودة والأمان: حماية البيانات ومنع الغش في البيئات الرقمية.
- التفاعل والمشاركة: تطوير أساليب تدريس تفاعلية لزيادة مشاركة الطلاب.
- إدارة الوقت والانتباه: توجيه الطلاب لإدارة وقتهم وتجنب الانحرافات الرقمية.
- تكلفة المعدات: تكلفة الأجهزة قد تشكل عبئًا على بعض الطلاب.

- سوء استخدام التكنولوجيا: الاستخدام غير المناسب للتكنولوجيا يمكن أن يؤدي لمشكلات تعليمية.
- صعوبة تجميع المعرفة: قد يواجه الطلاب صعوبة في استيعاب المعرفة من مصادر متنوعة.
- مشكلة الأمان: عدم الكشف عن هوية المشاركين قد يسبب مخاطر أمنية.

تسلط هذه التحديات الضوء على الجوانب المتعددة التي يجب معالجتها لضمان نجاح التعليم المنتشر، من خلال تعزيز البنية التحتية، وتحسين المهارات الرقمية، وضمان الجودة والأمان، يمكن التغلب على العقبات وتحقيق تجربة تعليمية شاملة وفعالة.

وهناك العديد من الدراسات التي اهتمت بالتعلم المنتشر، كالآتى:

هدفت دراسة مجيد وعلى Majeed, A., & Ali (2018) اقتراح نموذجًا لتطوير حرم جامعي ذكي يعتمد على تكنولوجيا إنترنت الأشياء (IoT) يعزز استخدام إنترنت الأشياء في التعليم التواصل عبر الإنترنت بين المتحكمات والمستشعرات والأشياء المادية، هذا المشهد للتكنولوجيا الحديثة يحدث تغييرات كبيرة في التعليم الجامعي، حيث يتم دمج العديد من الأشياء مع المستشعرات، وجمع البيانات باستخدام التكنولوجيا القابلة للارتداء، ويتم التواصل الداخلي من خلال الحوسبة السحابية، هذا النموذج يحدد مجموعة متنوعة من المعايير للجامعات، مما يتيح فرصًا لجعلها ذكية، ويعزز التفاعل الجديد بين الأشياء والأشخاص، و يركز هذا البحث على جعل الغرف الذكية، ومواقف السيارات الذكية، بالإضافة إلى تقديم التعليم الذكي للطلاب.

كما تناولت دراسة سوارتاما وآخرون Suartama., et al. (2020) إلى تطوير بيئة التعلم المنتشرة (ULE) استنادًا إلى نظام إدارة التعلم(LMS) ، تُركز الدراسة على تطوير بيئة تعلم منتشرة باستخدام نظام إدارة التعلم Moodle تهدف إلى إنشاء

نظام يدعم التعلم الشخصي والمتكيف مع السياق، بحيث يكون متاحًا في أي وقت وأي مكان، تستعرض الدراسة مراحل التصميم والتطوير والتقييم لهذه البيئة، وتُبرز قدرتها على تعزيز تفاعل الطلاب الجامعيين وتحسين أدائهم الأكاديمي، مما ساهم في تحسين مفاهيم التعلم المنتشرة واستخدامها بشكل أكثر فعالية، وقد أوضحت الدراسة أن تطوير بيئة تعليمية مخصصة يعزز من مرونة التعلم ويقدم مفاهيم تعلم مبتكرة.

وفي نفس العام، تناولت دراسة ستويانوفيتش وآخرون Stojanović., et al. (2020)استخدام بيئات التعلم التفاعلية المنتشرة في التعليم الثانوي، حيث تم استغلال رموز QR كأداة قوية للتفاعل مع الطلاب وتحسين العملية التعليمية، وأظهرت الدراسة أن هذه الأدوات يمكن أن تلعب دورًا مهمًا في تحسين التفاعل وتقديم تعليم تفاعلي وفعّال.

المحور الثاني: الأمن السيبراني

نشأة الأمن السيبراني:

في أوائل القرن الحادي والعشرين، بدأ الباحثون في استكشاف إمكانات تقنيات الحوسبة المنتشرة في التعليم، ومن بين المشاريع البارزة في هذا المجال تجربة "Ambient Wood" التي أجرتها جامعة ساكس في عام ٢٠٠٣، حيث تم استخدام مزيج من الأجهزة المحمولة والمستشعرات وشبكات الأسلاك اللاسلكية لإنشاء بيئة تعليمية تفاعلية للأطفال الذين يستكشفون منطقة الغابات (Ogata, et al., 2010) .

ومنذ ذلك الحين، تم تنفيذ العديد من المشاريع البحثية والمبادرات لتطوير مفهوم التعلم المنتشر، مما أدى إلى ظهور تقنيات ونهج متنوعة مثل التعلم النقال، التعلم القائم على السياق، والتعلم التكيفي (Dey, 2001).

وأصبح التعلم المنتشر مجالًا بحثيًا وممارسة راسخة مع تطبيقات متعددة في مختلف البيئات التعليمية، بدءًا من التعليم الابتدائي والثانوي وصولًا إلى التعليم العالي والتدريب المؤسسي(Yahya., et al., 2010; Ogata, et al., 2010) .

وساهمت التطورات السريعة في تكنولوجيا الهواتف المحمولة والاتصالات اللاسلكية، بالإضافة إلى تزايد انتشار الأجهزة المتصلة بالإنترنت، في تعزيز نمو التعلم المنتشر، مما أتاح للمتعلمين الوصول إلى المحتوى التعليمي أثناء التنقل .(Dirceli., & Calik, 2018)

علاوة على ذلك، أدى دمج تقنيات الذكاء الاصطناعي وتعلم الآلة وتحليلات البيانات الضخمة، والواقع المعزز وإنترنت الأشياء إلى تخصيص تجارب التعلم وتكييفها لتلبية الاحتياجات والتفضيلات الفردية للمتعلمين (هاني البمباوي، ٢٠٢٣)

ويُتوقع أن يشهد التعلم المنتشر تطورًا أكبر في إنشاء تجارب تعلم سلسة وشخصية مع تزايد توافر هذه التقنيات.

أهمية وأهداف الأمن السيبراني:

يلعب الأمن السيبراني دورًا حيويًا في حماية كافة جوانب الحياة، سواء كانت تعليمية، اجتماعية، اقتصادية، أو إنسانية، إنه يعكس قدرة الدولة على حماية مصالحها وشعبها، ويعزز القدرة على الإبداع والتنافس بأمان في العصر الرقمي (راشد المري، ٢٠٢٣).

١. على المستوى الفردي:

الأمن السيبراني ضروري لحماية البيانات الشخصية والحساسة مثل المعلومات الشخصية والصحية (PHI) ومعلومات التعريف الشخصية (PII) من السرقة والاحتيال، يتطلب ذلك ممارسات مثل إدارة كلمات المرور القوية وتحديث البرامج والحذر من محاولات الاحتيال عبر البريد الإلكتروني.

٢. على المستوى المؤسسي:

الأمن السيبراني يحمي الشركات من هجمات البرمجيات الضارة والتصيد وسرقة البيانات الشخصية والملكية الفكرية. كما يحمي أنظمة الكمبيوتر من الفيروسات التي قد تتسبب في تلف البيانات والأنظمة. الاستثمار في تقنيات الأمان المتقدمة وتدريب الموظفين ضروري لحماية الأصول الرقمية من الهجمات الإلكترونية المتزايدة على الخدمات السحابية الضعيفة(Agrawal, Zhu, & Carpenter, 2020) .

٣. على المستوى الحكومي:

يحمي الأمن السيبراني السيادة الوطنية من خلال حماية البنية التحتية الحرجة والأنظمة الحكومية، ويعد ضروريًا لضمان سلامة الأنظمة والمعلومات الحساسة، الحكومات وصناع السياسات يلعبون دورًا حيويًا في تعزيز الأمن السيبراني من خلال وضع أطر تنظيمية وتنسيق الجهود مع القطاع الخاص.

٤. على المستوى الدولي:

التعاون الدولي في مجال الأمن السيبراني أصبح بالغ الأهمية نظرًا لتجاوز الهجمات الإلكترونية للحدود الوطنية، والثورة التكنولوجية أدت إلى ظهور الفضاء السيبراني كساحة جديدة للصراع بين الدول والجهات غيرالحكومية، مما يستدعي استجابة عالمية منسقة لمواجهة الحروب السيبرانية المتزايدة، والتي تشكل تهديدًا حقيقيًا على المستوى الدولي، ونخلص من ذلك إلى أنه في القرن الحادي والعشرين، أصبح الأمن السيبراني مسألة بالغة الأهمية، مع استمرار اعتمادنا على التقنيات الرقمية في النمو، تزداد الحاجة إلى تدابير فعالة لحماية أنفسنا من التهديدات الإلكترونية، من خلال اتباع نهج شامل وتعاوني للأمن السيبراني، يمكننا ضمان مستقبل رقمي أكثر أمانًا للجميع(Taha, 2022) .

مبادئ الأمن السيبراني:

تعليم مبادئ الأمن السيبراني للأفراد والمؤسسات بات ضرورياً في العصر الرقمي مع تزايد التهديدات السيبرانية، و يعتمد الأمن السيبراني على ثلاثة مبادئ رئيسية تُعرف بمثلث (CIA) (Khidr, 2021).

١.سرية المعلومات(Confidentiality) :

ضمان أن المعلومات متاحة فقط للأشخاص المصرح لهم، وحجبها عن غير المصرح لهم. يتم تحقيق ذلك من خلال التشفير والمصادقة الثنائية وإدارة الوصول.

٢. سلامة المعلومات:(Integrity)

ضمان عدم تغيير أو استبدال البيانات من قبل أشخاص غير مصرح لهم أو نتيجة لأحداث غير متوقعة. يتحقق ذلك باستخدام أذونات الملفات، والتشفير، والنسخ الاحتياطية.

٣. توافر المعلومات:(Availability)

ضمان وصول المعلومات للأشخاص المصرح لهم عند الحاجة. يتطلب ذلك صيانة الأجهزة، وجود خطة استعادة بعد الكوارث، وحماية البيانات من الهجمات.

إذن سرية، سلامة، وتوافر المعلومات هي المبادئ الأساسية للأمن السيبراني، حيث تضمن حماية البيانات من الوصول غير المصرح به، الحفاظ على دقتها، وضمان الوصول إليها عند الحاجة. تعتمد استراتيجيات الأمن السيبراني الناجحة على تحقيق توازن بين هذه المبادئ لحماية الأنظمة والمعلومات بشكل شامل.

أنواع الأمن السيبراني:

يشمل الأمن السيبراني عدة أنواع تهدف جميعها إلى حماية الأنظمة والشبكات والبيانات من التهديدات السيبرانية، يمكن تقسيمها إلى عدة أنواع رئيسية، كما يوضح

كل من ستالنج، وويتمان وماتورد Stallings(2018), Whitman & Mattord (2018)

أمن الشبكات:

يركز على حماية البنية التحتية للشبكات من الاختراقات والهجمات عبر جدران الحماية، وأنظمة كشف ومنع التسلل.

١. أمن المعلومات:

يحمي البيانات الحساسة من الوصول غير المصرح به والتلف عبر تقنيات التشفير وإدارة الهوية والسياسات الأمنية

٢. أمن التطبيقات:

يضمن سلامة التطبيقات من الثغرات التي قد يستغلها المهاجمون من خلال البرمجة الآمنة والتحديثات المنتظمة

٣. الأمن السحابي:

يحمي البيانات والتطبيقات الموجودة في السحابة باستخدام تقنيات التشفير وإدارة الهوية.

٤. أمن الأجهزة المحمولة:

يركز على حماية الهواتف الذكية والأجهزة اللوحية من التهديدات السيبرانية عبر تأمين التطبيقات وإدارة الأجهزة.

٥. الأمن السيبراني الحيوي:

يحمي الأنظمة التي تتفاعل مع العالم الفيزيائي مثل أنظمة التحكم الصناعي وشبكات الكهرباء.

١. أمن نقطة النهاية:

يؤمن الأجهزة المتصلة بالشبكة مثل أجهزة الكمبيوتر والهواتف من التهديدات باستخدام برامج مكافحة الفيروسات وجدران الحماية.

إذن تلعب أنواع الأمن السيبراني دورًا حاسمًا في حماية البيانات والأنظمة من التهديدات المتنوعة، كل نوع يركز على جانب محدد، مما يعزز الدفاع الشامل ضد الهجمات السيبرانية ويضمن أمان العمليات الرقمية في مختلف البيئات.

الوعي بالأمن السيبراني:

تتضمن الجهود الحالية في مجال الأمن السيبراني تطوير تقنيات وأساليب جديدة للتعامل مع التهديدات المتزايدة والمعقدة. يعتبر الوعي والتدريب من العناصر الأساسية في تعزيز الأمن السيبراني، حيث يمكن للموظفين والمستخدمين النهائيين أن يكونوا خط الدفاع الأول ضد الهجمات السيبرانية.

١. الوعي بالأمن السيبراني في البيئات التعليمية:

يشير الوعي بالأمن السيبراني إلى فهم الطلاب للمخاطر التي يمكن أن تنشأ عند استخدامهم للتكنولوجيا والإنترنت في بيئات التعلم التكنولوجية ومنها في البحث الحالب التعلم المنتشر، وذلك مع تزايد الاعتماد على التعليم الرقمي والتعلم الإلكتروني، فيصبح من الضروري أن يكتسب الطلاب مهارات ومعرفة تمكنهم من حماية بياناتهم وأجهزتهم من التهديدات السيبرانية.

ويشمل الوعي بالأمن السيبراني المعرفة بالممارسات الجيدة مثل استخدام كلمات مرور قوية، التعرف على التهديدات مثل التصيد الاحتيالي، والحفاظ على تحديث الأنظمة والتطبيقات بشكل مستمر(Taha, 2022).

أهمية الوعي بالأمن السيبراني في البيئات التعليمية:

يتعرض الطلاب في البيئات التعليمية، للعديد من المخاطر السيبرانية، خاصة مع الانتشار الواسع للأجهزة المتصلة بالإنترنت والاستخدام المكثف للمنصات التعليمية الرقمية. لذا، يصبح من الضروري أن يمتلك الطلاب وعيًا كافيًا بالأمن السيبراني وذلك لـــ:

- حماية المعلومات الأكاديمية والشخصية :يساعد الطلاب والمعلمين في حماية معلوماتهم من التهديدات السيبرانية.
- الوقاية من الاحتيال الإلكتروني :يعزز من قدرة الطلاب والمعلمين على التعرف على التهديدات وتجنب الاحتيال السيبراني.

٢. الوعي بالأمن السيبراني في مؤسسات التعليم العالي

تلعب مؤسسات التعليم العالي دورًا محوريًا في تعزيز الوعي بالأمن السيبراني بين طلابها؛ لأن عليها تقديم برامج تعليمية وتدريبية تستهدف زيادة الوعي السيبراني بين الطلاب والمعلمين. يتضمن ذلك دمج موضوعات الأمن السيبراني في المناهج الدراسية وتنظيم ورش عمل لتدريب الطلاب على كيفية حماية أنفسهم في البيئات الرقمية(Bada., et al., 2019) .

أهمية الوعي بالأمن السيبراني في مؤسسات التعليم العالي

- تطوير جيل من الخبراء في الأمن السيبراني :من خلال تعليم وتدريب الطلاب على كيفية التعامل مع التهديدات السيبرانية.
- تعزيز الأمان داخل المؤسسات التعليمية :من خلال تبني سياسات أمنية شاملة وتقديم التدريب المستمر.

٣.الوعي بالأمن السيبراني في كليات التربية بصفة خاصة

يعد الوعي بالأمن السيبراني أمرًا بالغ الأهمية للطلاب المعلمين في كليات التربية. يتم تدريب هؤلاء الطلاب على كيفية حماية المعلومات الشخصية والأكاديمية والتعامل مع التهديدات السيبرانية بفعالية في بيئات التعلم التي تعتمد بشكل كبير على التكنولوجيا(Garba, 2021).

أهمية الوعي بالأمن السيبراني في كليات التربية، والتربية النوعية:

- حماية المعلومات الأكاديمية والتربوية :يساعد الطلاب المعلمين على حماية أبحاثهم وبياناتهم الأكاديمية من السرقة أو التلاعب.

- الاستعداد لسوق العمل: يعزز من فرص توظيف الطلاب المعلمين في المؤسسات التي تتطلب معرفة بالأمن السيبراني.

دور مؤسسات التعليم العالي في تعزيز الوعي بالأمن السيبراني:

أولًا: التعليم والتدريب يُعدان من أبرز المهام التي تضطلع بها الجامعات، حيث تقدم برامج تعليمية متخصصة في مجال الأمن السيبراني. هذه البرامج، التي تشمل دورات أكاديمية وشهادات معترف بها، تهدف إلى تأهيل جيل جديد من الخبراء في مجال الأمن السيبراني القادرين على مواجهة التحديات المستقبلية (Akter et al., 2022)

ثانيًا: تدعم مؤسسات التعليم العالي البحث والتطوير من خلال إنشاء مراكز بحثية متخصصة. تتعاون هذه المراكز مع الحكومات والصناعة لتطوير تقنيات وأساليب جديدة تساهم في التصدي للتهديدات السيبرانية، مما يعزز من أمان الفضاء الرقمي على مستوى أوسع (Taha, 2022).

ثالثًا: تعمل الجامعات على التوعية ونشر المعرفة عبر تنظيم ندوات وورش عمل ومؤتمرات تهدف إلى تعزيز الوعي بالأمن السيبراني بين الطلاب والمجتمع. هذه الجهود تشمل أيضًا إنتاج مواد توعوية مثل المقالات والفيديوهات التعليمية التي تُسهم في نشر ثقافة الأمن السيبراني (Bada., et al., 2019) .

رابعًا: توفر المؤسسات التعليمية التطبيق العملي والتدريب المهني من خلال مختبرات متخصصة وأدوات عملية تتيح للطلاب تطبيق ما تعلموه في بيئات واقعية. هذه التجارب تُعزز من قدرة الطلاب على التعامل مع التهديدات السيبرانية بشكل فعّال، كما تساهم في إقامة شراكات مع شركات تكنولوجيا المعلومات لتوفير فرص تدريب عملي ووظائف مستقبلية(Akter et al., 2022) .

خامسًا: أيضًا تمثل السياسات والإجراءات جزءًا لا يتجزأ من دور مؤسسات التعليم العالي. يتم تطوير سياسات داخلية تهدف إلى حماية بيانات الطلاب والموظفين من

التهديدات السيبرانية. هذه السياسات تشمل استخدام أدوات مثل التحقق متعدد العوامل (MFA) وأنظمة الكشف عن التهديدات والاستجابة لهاEDR) ، مما يضمن بيئة تعليمية آمنة وموثوقة(Garba, 2021) .

سادسًا: في إطار التعاون والشراكة، تتعاون الجامعات مع مؤسسات أخرى وجهات حكومية وصناعية لتبادل المعرفة والخبرات. هذه الشراكات تشمل المشاركة في الشبكات الدولية والمشاريع البحثية المشتركة، مما يعزز من تأثير هذه المؤسسات في مجال الأمن السيبراني.(Akter et al., 2022)

إذن تلعب مؤسسات التعليم العالي دورًا محوريًا في نشر ثقافة الأمن السيبراني من خلال مجموعة من الأنشطة والمبادرات المتنوعة، وتسعى هذه المؤسسات إلى تعزيز الوعي الأمني لدى الطلاب والمعلمين وتزويدهم بالمهارات والمعرفة الضرورية لمواجهة التهديدات السيبرانية المتزايدة، ويتم ذلك عبر مجموعة من الاستراتيجيات المتكاملة التي تشمل التعليم، التدريب، البحث والتطوير، بالإضافة إلى السياسات والإجراءات العملية.

استراتيجيات تعزيز الوعي بالأمن السيبراني في البيئات التعليمية:

تعتمد الجامعات استراتيجيات محددة لتعزيز الوعي بالأمن السيبراني في البيئات التعليمية، مثل التدريب والتوعية التي تركز على تنظيم برامج ودورات تعليمية تستهدف تعزيز وعي الطلاب والمعلمين بأهمية الأمن السيبراني ,.Akter et al) (2022، ودمج الأمن السيبراني في المناهج الدراسية من خلال تطوير وحدات تعليمية تركز على حماية البيانات وإدارة الهوية الرقمية(Khidr, 2021) ، وكذلك التطبيق العملي باستخدام التكنولوجيا التعليمية لتعزيز الوعي السيبراني عبر دروس تفاعلية ومحاكاة سيناريوهات واقعية(Garba, 2021).

من خلال هذه الجهود المتكاملة، تساهم مؤسسات التعليم العالي بشكل كبير في تعزيز الثقافة الأمنية السيبرانية، مما يساعد على حماية البيانات والمعلومات في العصر الرقمي الحديث.

فروض البحث:

١. "توجد فروق دالة إحصائياً عند مستوى دلالة (**α** ≤٠.٠٥) بين متوسطات درجات الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي في التطبيقين القبلي والبعدي في مقياس الوعي بالأمن السيبراني ككل وفي كل بُعد على حدة لصالح التطبيق البعدي."

٢. "يثبت استخدام البرنامج المقترح القائم على تطبيقات التعلم المنتشردرجة كبيرة من الفاعلية في تنمية الوعي بالأمن السيبراني للطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي ، عند مستوى (≤ ١.٢) كما تمثل نسبة الكسب المعدل لبليك، وعند مستوى (≤ ٠.٦)، كما تمثل بنسبة الفاعلية لماك جوجيان."

أدوات ومواد البحث:

استخدمت الباحثة الأدوات والمواد البحثية الآتية:

أ) اعداد مقياس وعي يقيس وعي الطلاب بالأمن السيبراني

الهدف من مقياس الوعي:

يهدف المقياس إلى التعرف على وعي الطلاب المعلمين شعبة الحاسب الآلي في كلية التربية النوعية نحو الأمن السيبراني.

طريقة بناء مقياس الوعي:

تم اتباع طريقة "ليكرت" Likert ثلاثي البعد في إعداد المقياس، وهي تعتمد على تقديم مفردات محايدة يقوم الطالب بالتعبير عن وعيه بها، وتم بناء المقياس في صورة عبارات موجبة تعكس استحسان وعي الطالب نحو الأمن السيبراني،

وعبارات سالبة. تعكس عدم وعي الطالب نحو الأمن السيبراني، ويجيب الطلاب باختيار العبارة الملائمة من البدائل التالية: (موافق، محايد، معارض).

تحديد أبعاد مقياس الوعي:

قامت الباحثة بإعداد مقياس الوعي في ضوء الاطلاع على الأدبيات والدراسات السابقة التي تناولت وعي الطلاب نحو أمن المعلومات بصفة عامة ، الأمن السيبراني بصفة خاصة.

وجاء مقياس الوعي في ثلاث أبعاد فرعية هي :

- البعد الأول: الوعي بالتعامل الآمن مع الشبكات و الأجهزة.
- البعد الثاني: الوعي بالتعامل الآمن مع نظام التشغيل والبرامج.
- البعد الثالث: الوعي بالتعامل الآمن مع المتصفحات، ووسائل التواصل الإجتماعي.

تتكامل معا لتوضيح البعد الرئيسي وهو" قياس وعي الطلاب المعلمين بالأمن السيبراني"

ضبط المقياس:

تم عرض الصورة الأولية للمقياس على مجموعة المحكمين من المتخصصين في مجال علم النفس، والمناهج وطرق التدريس، وتكنولوجيا التعليم.

١- حساب صدق الاتساق الداخلي:

تم حساب صدق الاتساق الداخلي لمقياس الوعي نحو الأمن السيبراني بحساب معامل الارتباط بين درجة كل عبارة بمجموع درجات البعد الذي تنتمي إليه، ومن خلال النتائج التي أسفرت عنها معاملات الارتباط اتضح أن جميع معاملات الارتباط موجبة ودالة عند مستوي ٠.٠٠٥ علي الأقل، حيث تراوحت قيم معاملات كل عبارة بالدرجة الكلية للبعد الذي تنتمي إليه كالآتي:

- في البعدالأول: (الوعي بالتعامل الآمن مع الشبكات والأجهزة): تراوحت قيم معاملات الارتباط بين(٠.٣٨،٠.٦٥) ويدل ذلك علي وجود علاقة مقبولة بين درجة كل عبارة ودرجة البعد الذي تنتمي إليه.
- في البعد الثاني: (الوعي بالتعامل الآمن مع نظام التشغيل والبرامج): تراوحت قيم معاملات الارتباط بين (٠.٣١، ٠.٩٢) ويدل ذلك علي وجود علاقة مقبولة بين درجة كل عبارة ودرجة البعد الذي تنتمي إليه.
- في البعد الثالث: (الوعي بالتعامل الآمن مع المتصفحات، ووسائل التواصل الإجتماعي): تراوحت قيم معاملات الارتباط بين(٠.٤٦، ٠.٧٤) ويدل ذلك علي وجود علاقة مقبولة بين درجة كل عبارة ودرجة البعد الذي تنتمي إليه.

٢- حساب معامل ثبات مقياس الوعي:

- تم حساب ثبات مقياس الوعي نحو الأمن السيبراني على مجموعة تجربة البحث التي بلغ عددها (٥٠) طالب وطالبة من الطلاب المعلمين بكلية التربية النوعية (شعبة الحاسب الآلي).
- وقد تحققت الباحثة من ثبات المقياس بطريقة معامل ألفاكرونباخ Alpha-Cronbach، وبلغت قيمة الثبات للمقياس (٠.٨٤) وهي قيمة ثبات عالية ومقبولة احصائيًا، مما يعني أن مقياس الوعي ثابت إلى حد كبير، وأنه سوف يعطى نفس النتائج إذا أعيد تطبيقه على نفس المجموعة التجريبية في نفس الظروف، كما يعنى خلوه من الأخطاء التي يمكن أن تغير من استجابات الفرد من وقت لأخر على نفس المقياس، ومن ثم يمكن الوثوق بالنتائج التي تم الحصول عليها.

ب) اعداد البرنامج الإلكتروني باستخدام تطبيقات التعلم المنتشر

قامت الباحثة بالآتي:

- دراسة متطلبات إعداد البرنامج الإلكتروني المقترح القائم علي تطبيقات التعلم المنتشر وتشمل:
  - دراسة تطبيقات التعلم المنتشر
  - دراسة لغات البرمجة وبرامج التصميم التي سيتم إعداد البرنامج الإلكتروني بها.
  - إعداد محتوي البرنامج وصياغته الصياغة التربوية المناسبة.
- إعداد البرنامج الإلكتروني في صورة Mobile Application القائم علي تطبيقات التعلم المنتشر.
- عرض البرنامج الإلكتروني المقترح على مجموعة من السادة المحكمين للتأكد من صلاحيته للتطبيق.
- تعديل البرنامج الإلكتروني المقترح فى ضوء أراء السادة المحكمين، والتوصل للصورة النهائية.

عينة البحث:

العينة الاستطلاعية: تكونت العينة من ٥٠ طالباً وطالبة من الفرقة الرابعة شعبة الحاسب الآلي بكلية التربية النوعية، تم إرسال نموذج Google Form للتحقق من توفر بريد إلكتروني، اتصال بالإنترنت، جهاز كمبيوتر أو لابتوب، وهاتف أندرويد لكل منهم. كما تم من خلال العينة الاستطلاعية تحديد الزمن المناسب لاختبار الجوانب المعرفية في مهارات الأمن السيبراني، والتحقق من صدق وثبات الاختبارات والمقاييس ذات الصلة، بالإضافة إلى معرفة معاملات السهولة والصعوبة والتمييز للاختبار.

مجموعة البحث:

- تكونت من (٣٢) طالباً وطالبة بالفرقة الفرقة الرابعة شعبة الحاسب الآلي بكلية التربية النوعية.

نتائج البحث:

للتحقق من صحة الفرض الأول الذى ينص على:

"توجد فروق دالة إحصائياً عند مستوى دلالة (a≤٠.٠٥) بين متوسطات درجات الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي في التطبيقين القبلي والبعدي في مقياس الوعي بالأمن السيبراني ككل وفي كل بُعد على حدة لصالح التطبيق البعدي.

للتحقق من صحة هذا الفرض استخدمت الباحثة:

- اختبار "t- Test" :لدلالة الفرق بين متوسطي درجات المجموعة التجريبية في التطبيقين القبلي والبعدي لمقياس الوعي بالأمن السيبراني كما هي موضحة بجدول (١):

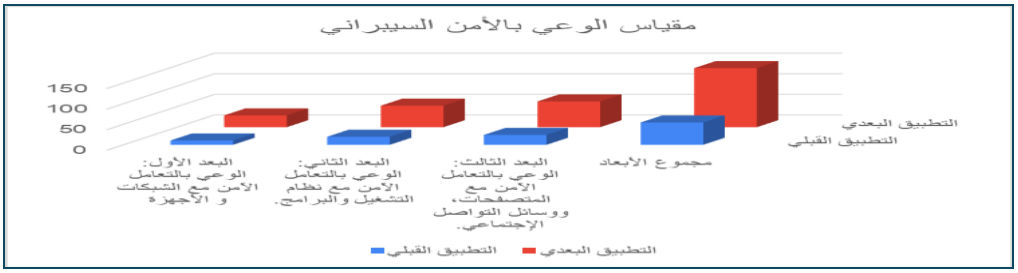
جدول (١): نتائج اختبار "t- Test" لدلالة الفرق بين متوسطي درجات المجموعة التجريبية في التطبيقين القبلي والبعدي لمقياس الوعي بالأمن السيبراني.

البعد	القياس	العينة	المتوسط	الانحراف لمعياري	درجات الحرية	معدل الارتباط	قيمة "ت"	مستوى الدلالة
البعد الأول: الوعي بالتعامل الآمن مع الشبكات و الأجهزة	القبلي	٣٢	10.5	٨1.589	٣١	.86٠	٨٢.٠٦	دالة عند ٠.٠٥
	البعدي		28.6875	٩0.7				
البعد الثاني: الوعي بالتعامل الآمن مع نظام التشغيل والبرامج.	القبلي	٣٢	19.625	1.71	٣١	.81٠	102.5	دالة عند ٠.٠٥
	البعدي		52.3125	٧1.894				
البعد الثالث: الوعي بالتعامل الآمن مع المتصفحات، ووسائل التواصل الإجتماعي.	القبلي	٣٢	24.3	٦1.811	٣١	٠.60	72.53	دالة عند ٠.٠٥
	البعدي		62.625	3.82222				
مجموع الأبعاد	**القبلي**	**٣٢**	**٨54.18**	**١3.042**	**٣١**	**٠.٧٣**	**127.13**	**دالة عند ٠.٠٥**
	البعدي		**143.625**	**٢4.735**				

وتشير النتائج كما يوضحها جدول (١) إلى ان:

قيمة "ت" المحسوبة للتطبيقين: القبلي والبعدي لمقياس الوعي بالأمن السيبراني ككل بلغت (127.13)، ومستوى دلالة (٠.٠٥)، كما تراوحت قيمة "ت" المحسوبة لكل بعد على حدي ما بين(٧٢.٥٣ ، 102.50) عند مستوى دلالة (٠.٠٥)، مما يدل على أنه توجد فروق دالة إحصائياً عند مستوى (٠.٠٥) بين متوسطات درجات الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي الذين درسوا البرنامج في التطبيقين القبلي والبعدي لمقياس الوعي بالأمن السيبراني ككل وكل بعد على حدة صالح التطبيق البعدي. ويشير ذلك إلى أن المتغير المستقل المتمثل في البرنامج الإلكتروني المقترح كان له أثر دال في تنمية الوعي بالأمن السيبراني.

ويوضح الشكل التالي التمثيل البياني للفروق بين متوسطات درجات طلاب مجموعة البحث في التطبيقين القبلي والبعدي لمقياس الوعي بالأمن السيبراني ككل وكل بعد على حدي:



شكل (١) التمثيل البياني للفروق بين متوسطات درجات الطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي في التطبيقين القبلي والبعدي لمقياس الوعي بالأمن السيبراني ككل وبأبعاده الفرعية

ويتبيّن من شكل (١) السابق ارتفاع متوسطات درجات الطلاب في التطبيق البعدي عن التطبيق القبلي في مقياس الوعي بالأمن السيبراني ، مما يدل على فاعلية البرنامج المقترح في تنمية الوعي بالأمن السيبراني.

ويتبين أن متوسطات درجات الطلاب فى التطبيق البعدى لمقياس الوعي بالأمن السيبراني ككل، وكل بعد على حده دالة عند مستوى دلالة (٠.٠٥) لصالح التطبيق البعدى، وعلّيه يتم قبول الفرض الأول. ليصبح النص على النحو التالي: "وجود فرق دال إحصائياً عند مستوي (α ≤٠.٠٥) بين متوسطي درجات طلاب المجموعة التجريبية في التطبيق القبلي والبعدي لمقياس الوعي بالأمن السيبراني لصالح التطبيق البعدي."

للتحقق من صحة الفرض الثانى الذى ينص على:

"يثبت استخدام البرنامج المقترح القائم على تطبيقات التعلم المنتشردرجة كبيرة من الفاعلية في تنمية الوعي بالأمن السيبراني للطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي ، عند مستوى (≤ ١.٢) كما تمثل نسبة الكسب المعدل لبليك، وعند مستوى (≤ ٠.٦)، كما تمثل بنسبة الفاعلية لماك جوجيان."

للتحقق من صحة هذا الفرض استخدمت الباحثة:

تحديد الدلالة التطبيقية للبرنامج الإلكتروني المقترح على الوعي بالأمن السيبراني:

يوضح جدول (٢) حجم تأثير البرنامج الإلكتروني المقترح في تنمية الوعي بالأمن السيبراني كما يقيسه مربع (η^2) كما يلي:

جدول (٢) حجم تأثير البرنامج الإلكتروني المقترح في تنمية الوعي بالأمن السيبراني كما يقيسه مربع (η2)

البعد	قيمة ت	درجة الحرية	قيمة (η2)
البعد الأول: الوعي بالتعامل الآمن مع الشبكات و الأجهزة.	82.06	31	0.995
البعد الثاني: الوعي بالتعامل الآمن مع نظام التشغيل والبرامج.	102.5	31	0.998
البعد الثالث: الوعي بالتعامل الآمن مع المتصفحات، ووسائل التواصل الإجتماعي.	72.53	31	0.994
مجموع الأبعاد	**127.13**	**31**	**0.998**

يتضح من جدول (٢) أن قيمة مربع ايتا (η^2) لمقياس الوعي بالأمن السيبراني > 0.14 ؛ حيث كانت (٠.٩٩٨) للمقياس ككل، بينما كانت قيمة مربع إيتا للابعاد الفرعية مابين (٠.٩٩٤، ٠.٩٨٨)، مما يدل على فاعلية البرنامج في تنمية الوعي بالأمن السيبراني لكل الأبعاد الفرعية، وللمقياس ككل.وهذا يعني أن حجم تأثير البرنامج الإلكتروني المقترح على الوعي بالأمن السيبراني لدي طلاب المجموعة التجريبية يعد كبيرا، مما يشير إلى فاعلية البرنامج الإلكتروني المقترح في تنمية الوعي بالأمن السيبراني لدي طلاب المجموعة التجريبية.

العلاقة بين مربع إيتا وحجم التأثير(d):

يوضح جدول (٣) قيم مربع ايتا (η2)، وقيمة (d) المقابلة لها، وحجم التأثير في تنمية الوعي بالأمن السيبراني لدي عينة البحث

جدول (٣): قيم مربع ايتا (η2)، وقيمة (d) المقابلة لها، وحجم التأثير في تنمية الوعي بالأمن السيبراني لدي عينة البحث

البعد	قيمة (ت)	درجات الحرية	قيمة (η2)	الدلالة	قيمة (d)	حجم التأثير
البعد الأول: الوعي بالتعامل الأمن مع الشبكات و الأجهزة	82.06	31	٠.٩٩٥	دالة عند ٠.٠٥	28.2134	كبير
البعد الثاني: الوعي بالتعامل الأمن مع نظام التشغيل والبرامج.	102.5	31	٠.٩٩٨	دالة عند ٠.٠٥	44.6766	كبير
البعد الثالث: الوعي بالتعامل الأمن مع المتصفحات، ووسائل التواصل الإجتماعي.	72.53	31	٠.٩٩٤	دالة عند ٠.٠٥	28.2134	كبير
مجموع الأبعاد	١٢٧.١٣	٣١	٠.٩٩٨	دالة عند ٠.٠٥	44.6766	كبير

ويتضح من نتائج جدول (٣) أن قيمة (η2) لنتائج التطبيقين القبلي والبعدي لمقياس الوعي بالأمن السيبراني ككل بلغت (١٢٧.١٣)، بينما تراوحت قيمة مربع

إيتا لأبعاده الفرعية بين (٠.٩٩٨ ، ٠.٩٩٤)، مما يدل على فاعلية البرنامج في تنمية الوعي بالأمن السيبراني ككل و لكل أبعاده الفرعية.

نسبة الكسب المعدل لبليك:

يوضح جدول (٤) نتائج حساب نسبة الكسب المعدل لمقياس الوعي بالأمن السيبراني:

جدول (٤): نسبة الكسب المعدل لبليك نسبة الفاعلية لـــ "ماك جوجيان" لمقياس الوعي بالأمن السيبراني

البعد	متوسط التطبيق القبلي	متوسط التطبيق البعدي	النهاية العظمى للدرجات	نسبة الكسب المعدل لبليك	نسبة الفاعلية ماك جوجيان
البعد الأول: الوعي بالتعامل الآمن مع الشبكات والأجهزة	10.53125	28.6875	30	1.538	0.933
البعد الثاني: الوعي بالتعامل الآمن مع نظام التشغيل والبرامج.	19.625	52.3125	54	1.556	0.951
البعد الثالث: الوعي بالتعامل الآمن مع المتصفحات، ووسائل التواصل	24.03125	62.625	66	1.504	.919
مجموع الأبعاد	54.1875	143.625	150	1.530	.934

ويتضح من جدول (٤) السابق أن نسبة الكسب المعدل لبليك بالنسبة لمقياس الوعي بالأمن السيبراني ككل بلغت (١.٥٣٠)، وتراوحت ما بين (١.٥٠٤ – ١.٥٥٦) للأبعاد الفرعية، وجميعها نسب مقبولة؛ لأنها أكبر من النسبة المحكّية التي حددها بليك لمقياس الفاعلية، وهي (١.١٢)، أن نسبة الفاعلية لـــ "ماك جوجيان" بالنسبة لمقياس الوعي بالأمن السيبراني ككل بلغت (٠.٩٣٤)، وتراوحت ما بين (٠.٩١٩ – ٠.٩٥١) للأبعاد الفرعية، وجميعها نسب مقبولة؛ لأنها أكبر من النسبة المحكّية التي حددها "ماك جوجيان" لمقياس الفاعلية، وهي (٠.٦)، وهذا يدل على فاعلية البرنامج في تنمية لمقياس الوعي بالأمن السيبراني لدى الطلاب. وبهذا، يتم قبول الفرض الثاني.

ليصبح الفرض على النحو التالي: "يُظهر استخدام البرنامج المقترح القائم تطبيقات التعلم المنتشر درجة كبيرة من الفاعلية في تنمية الوعي بالأمن السيبراني للطلاب المعلمين بكلية التربية النوعية شعبة الحاسب الآلي ، عند مستوى (≤ 1.2) كما تُقاس نسبة الكسب المعدل "لبليك"، وعند مستوى (≤ 0.6) كما تُقاس نسبة الفاعلية لـــ "ماك جوجيان".

تفسير نتائج البحث:

وتوضح الباحثة أن تنمية الوعي بالأمن السيبراني يعود إلى عدة عوامل، منها:

- توفير بيئة تعليمية غنية تشجع على التعلم الإلكتروني وتعزز مشاركة الطلاب بشكل إيجابي.
- تعزيز شعور الطالب بالمسؤولية الذاتية نحو تعلمه، مما يزيد من دافعيته واستعداده للتحصيل.
- استخدام وسائل التعلم الحديثة التي تتيح تعدد الأنشطة وتنوع المهام، مما يزيد من تفاعل الطلاب مع المادة العلمية.
- الاستفادة من تكنولوجيا الكمبيوتر في توفير بيئة تعليمية مرنة تسمح للطلاب بالتعلم حسب وتيرتهم الخاصة، مما يعزز من دافعيتهم وإقبالهم على المادة.
- أهمية الشعور بأهمية الكمبيوتر في التعليم، حيث يوفر البرنامج الإلكتروني تجربة تعلم متكاملة ومستقلة تلبي احتياجات الطلاب الفردية.

واتفق البحث الحالي مع الدراسات السابقة في استخدام التكنولوجيا الحديثة لتحسين البيئة التعليمية وتنمية مهارات محددة لدى الطلاب، كما هو الحال في دراسة بيكاك، ليو، وميرفي (٢٠١٥) التي اهتمت بتطوير مناهج تعليمية في مجال الأمن السيبراني، ودراسة بلاك وشابمان وكلارك (٢٠١٨) التي ركزت على استخدام مختبر افتراضي معزز لتنمية الوعي بالأمن السيبراني.

توصيات البحث:

- تطبيق البرنامج المقترح لتدريس مهارات الأمن السيبراني لجميع طلاب شعبة الحاسب الآلي وتوسيع نطاقه ليشمل كافة تخصصات كلية التربية، والتربية النوعية.
- إجراء بحوث إضافية لاستكشاف وتطوير مهارات الأمن السيبراني لدى الطلاب والمعلمين.
- تطوير بيئات تعلم إلكترونية تفاعلية وتطبيق استراتيجيات التعلم المنتشر لتعزيز التفاعل والإبداع.
- توسيع تطبيق البرنامج المقترح ليشمل فئات أخرى من الطلاب، مثل طلاب التعليم الفني والثانوي.
- رفع وتحسين الكفاءات التعليمية من خلال دمج تطبيقات التعلم المنتشر في المقررات الدراسية.
- إعداد خطة تدريبية شاملة وتطوير أدوات تقييم مبتكرة لقياس فعالية البرنامج وتحسين جودة التعليم.

مقترحات بحثية:

- برنامج تدريبي قائم على التعلم المنتشر لتطوير مهارات لغات البرمجة لدى طلاب شعبة الحاسب الآلي بكلية التربية النوعية.
- برنامج تدريبي قائم على التعلم المنتشر لتنميه مهارات تدريس الرياضيات لدى طلاب شعبة الرياضيات بكلية التربية.
- دراسة أثر استخدام برامج تعليمية قائمة على التعلم المنتشر في تنمية مهارات الأمان الرقمي والوعي السيبراني لدى الطلاب في مرحلة الثانوي العام.

- تطوير برنامج إعداد معلم الحاسب الآلي في ضوء معايير إعداد معلمي الحاسب وفقاً لمتطلبات الأمن السيبراني.
- دراسة فعالية برنامج قائم على استراتيجيات التعلم المدمج لتنمية الوعي السيبراني لدى معلمي الحاسب الآلي.
- فاعلية مواقع الويب التعليمية في تنمية مهارات الأمن السيبراني لدى الطلاب في مراحل التعليم المختلفة.

مراجع البحث:

المراجع العربية:

أحمد عدلي علي، حمدي محمد البيطار، على سيد عبد الجليل، ماريان ميلاد منصور (٢٠٢٣). أثر بيئة إلكترونية قائمة على التعلم المنتشر لتنمية بعض مهارات تصميم قواعد البيانات لدى طلاب المرحلة الثانوية التجارية. **مجلة كلية التربية (أسيوط)**، 39(٤)، ١٠٣-١٣٦.

أميرة عبد الرحمن غوص، باسم نايف الشريف (٢٠٢٢). فاعليَّةُ تَوظيفِ بعضِ التَّطبيقاتِ التّعليميَّةِ الذَّكِيَّة في تقديم وحدَّة مقترَحة عن الْأَمْنِ السيبراني على التَّحصيل المعرفي والْاتِّجاهات نحوهُ لدى طالباتِ المرحلةِ المتوسِّطةِ بِالمدينَةِ المُنوَّرةِ. التربية (الأزهر): **مجلة علمية محكمة للبحوث التربوية والنفسية والاجتماعية**، ٤١(١٩٥)، ٦٨٥٧٣٤. مسترجع من: https://doi.org/10.21608/jsrep.2022.261430

ايمان محمد سحتوت، زينب عباس جعفر (٢٠١٤). **استراتيجيات التدريس الحديثة** (نسخة الكترونية). الرياض: مكتبة الرشد.

هاني إبراهيم البمباوي. (٢٠٢٣). دور تقنيات الذكاء الاصطناعي والبيانات الضخمة في رفع كفاءة الأساليب التسويقية الرقمية من وجهة نظر خبراء التسويق. **المجلة المصرية لبحوث الأعلام**, ٢٠٢٣(٨٢) , ١٤٣١-١٤٦٧ Doi: 10.21608/ejsc.2023.300438. مسترجع من:
https://ejsc.journals.ekb.eg/article_300438.html

تامر محمد متولي، حسناء فوزي بسيوني، محمد محمد يوسف. (٢٠٢٤). فاعلية بيئة للتعلم المصغر الهجين في تنمية بعض مهارات الأمن السيبراني لدى تلاميذ المرحلة الإعدادية.

مجلة كلية التربية: جامعة كفر الشيخ كلية التربية، (١١٥)، ٣٣٣٣٦٢. مسترجع من: http://demo.mandumah.com/Record/1471683

جمال الدهشان ومجدي ويونس (٢٠٠٩). التعليم الجوال: صيغة جديدة للتعلم عن بعد، بحث مقدم الى الندوة العلمية الاولى لكلية التربية، بعنوان نظم التعلم العالي الافتراضي، جامعة كفر الشيخ، مصر

حازم صالح (٢٠١٨). تطوير تطبيقات التعلم المنتشر عبر الأجهزة اللوحية وأثرها على تنمية مهارات تصميم قواعد البيانات الإلكترونية لدى طلاب المرحلة الثانوية. **الجمعية المصرية للكمبيوتر التعليمي، ٦(١)**، يوليو، ٣٣١٣٩٨.

راشد محمد المري. (٢٠٢٣). الأمن السيبراني وحماية الأنظمة الإلكترونية دراسة تحليلية تأصيلية. المقالة ١٢، ٩(١)، مارس، Doi: 959-1008 مسترجع من: https://doi.org/10.21608/jdl.2023.188855.1109

عبدالعال عبد الله السيد، رشا أحمد إبراهيم (٢٠١٨). تطوير تطبيقات التعلم المنتشر عبر الأجهزة اللوحية وأثرها على تنمية مهارات تصميم قواعد البيانات الإلكترونية لدى طلاب المرحلة الثانوية. **المجلة العلمية المحكمة للجمعية المصرية للكمبيوتر التعليمي، ٦(٢)**، ٢٥٣٠.

عصام إدريس الحسن (٢٠١٥). التعلم الإلكتروني المنتشر نقلة جديدة نحو تفريد التعليم الجامعي: من تعلم كل المجموعة إلى التعلم كل فرد في المجموعة. **دراسات تربوية، ١٦(٣١)**، ٧٦٩٤. مسترجع من: http://search.mandumah.com/Record/861815

فاطمة يوسف المنتشري (٢٠١٩). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. **المجلة العربية للتربية النوعية، (١٤)**، ٩٥١٤٠.

محمد راغب عماشة، سالم صالح الخلف، (مارس، ٢٠١٥). ورشة التعلم المنتشر .المؤتمر الدولي الرابع للتعلم الإلكتروني والتعليم عن بعد، الرياض.

محمد عطية خميس (٢٠٠٨). من تكنولوجيا التعلم الإلكتروني إلى تكنولوجيا التعلم المنتشر. **مجلة تكنولوجيا التعليم. الجمعية المصرية لتكنولوجيا التعليم**، ٩١٢.

المركز العربي الإقليمي للأمن السيبراني. (٢٠١٦-٢٠٢٠). المؤتمرات الإقليمية للأمن السيبراني. الاتحاد الدولي للاتصالات. مسترجع من: https://arcc.om/

مؤتمر القاهرة السابع للأمن الإلكتروني "Cairo Security Camp." (2016). القاهرة، نوفمبر ٢٠١٦.

المراجع الأجنبية:

Agrawal, N., Zhu, F., & Carpenter, S. (2020). Do you see the warning? Cybersecurity warnings via nonconscious processing. In *Proceedings of the 2020 ACM Southeast Conference (ACMSE '20)* (pp. 260–263). Association for Computing Machinery. Retrieved from: https://doi.org/10.1145/3374135.3385314

Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research*, 1-26.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behavior? *Proceedings of the International Conference on Cyber Security for Sustainable Society*. Retrieved from: https://www.researchgate.net/publication/274663655_Cyber_Security_Awareness_Campaigns_Why_do_they_fail_to_change_behaviour

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

Black, M., Chapman, D., & Clark, A. (2018). The enhanced virtual laboratory: Extending cyber security awareness through a web-based laboratory. *Information Systems Education Journal (ISED)*, 16(6), 4-12.

Chou, C. (2013). Interactive and personalized learning: Emerging technologies and smart pedagogies. *Educational Technology & Society*, 16(4), 1-3.

Christen, M., Gordijn, B., & Loi, M. (Eds.). (2020). *The ethics of cybersecurity*. Springer. Retrieved from: https://doi.org/10.1007/978-3-030-29053-5

Cybersecurity and Education Conference. (2021). Enhancing school response to cyber threats through teacher training. Ann Johnson, Corporate Vice President of Security, Compliance & Identity (SCI) Business Development, Microsoft.

Dey, A. K. (2001). Understanding and using context. *Personal and Ubiquitous Computing*, 5(1), 4-7.

Dirceli, F., & Calik, T. (2018). Ubiquitous learning: Concept, characteristics, and implications. *International Journal of Contemporary Educational Research*, 5(1), 1-12.

Duitama, J., Defude, B., & Lecocq, C., & Bouzeghoub, A. (2006). Learning objects: Applications, implications, and future directions. Retrieved from: https://www.researchgate.net/publication/259481144_Learning_Objects_Applications_Implications_Future_Directions

Garba, A. (2021). Case study on cybersecurity awareness among university students. *Journal of Cybersecurity Education*, 8(3), 67-80.

Georgouli, K., Skalkidis, I., & Guerreiro, P. (2008). A framework for adopting LMS to introduce e-learning in a traditional course. *Educational Technology & Society*, 11(2), 227-240. Retrieved from: https://doi.org/10.2307/jeductechsoci.11.2.227

Google for Education. (2024). Retrieved from: https://edu.google.com/

Google Workspace Updates. (2023). Retrieved from: https://workspaceupdates.googleblog.com/2023/

Cisco. (n.d.). What is cybersecurity? Retrieved from: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

IT Governance. (n.d.). What is cybersecurity? Retrieved October 20, 2023, Retrieved from: https://www.itgovernance.co.uk/whatiscybersecurity

Joiner, R., Nethercott, J., Hull, R., & Reid, J. (2006). Designing educational experiences using ubiquitous technology. *Computers in Human Behavior*, 22(1), 67-76.

Jones, V., & Jo, J. H. (2004). Ubiquitous learning environment: An adaptive teaching system using ubiquitous technology. In *Proceedings of the 21st ASCILITE Conference* (pp. 468-474.

Jung, H. J. (2014). Ubiquitous learning: Determinants impact learners' satisfaction and performance with smartphones. *Journal of Language Learning & Technology*, 18(3), 97-119.

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, 2019(7), 11-14. Retrieved from: https://doi.org/10.1016/S1361-3723(19)30085-5

Khidr, M. (2021). Developing a framework to enhance cybersecurity awareness in academic institutions. *Journal of Academic Security*, 12(1), 35-49.

Kim, L. (2017). Cybersecurity awareness: Protecting data and patients. *Nursing Management*, 48(4), 16-19.

Knewton. (2023). Knewton - Adaptive learning technology. Retrieved from: https://www.knewton.com/

Majeed, A., & Ali, M. (2018). How Internet-of-Things (IoT) making the university campuses smart? QA higher education (QAHE) perspective. In *Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 646-648). IEEE. Retrieved from: https://doi.org/10.1109/CCWC.2018.8301774

Ogata, H., & Yano, Y. (2010). Knowledge awareness for a computer-assisted language learning using handheld. *International Journal of Continuing Engineering Education and Lifelong Learning*, 145. Retrieved from: https://doi.org/10.1504/IJCEELL.2004.005731

Sharples, M., Taylor, J., & Vavoula, G. (2005). Towards a theory of mobile learning. In *Proceedings of mLearn*. 1(1), 1-9.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Smowltech. (2022). Ubiquitous learning: Characteristics, advantages, and disadvantages. Learning and Development. Retrieved from: https://smowl.net/en/blog/ubiquitous-learning/

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.

Stojanović, D., Bogdanović, Z., Petrović, L., Mitrović, S., & Labus, A. (2020). Empowering learning process in secondary education using pervasive technologies. *Interactive Learning Environments*, 31(2), 779-792. Retrieved from: https://doi.org/10.1080/10494820.2020.1806886

Suartama, I., Setyosari, P., Sulthoni, S., & Ulfa, S. (2020). Development of ubiquitous learning environment based on Moodle learning management system. *International Journal of Interactive Mobile Technologies (iJIM)*, 14(2), 182-204. Retrieved from: https://doi.org/10.3991/ijim.v14i02.11593

Suki, N. M., & Suki, N. M. (2011). Users' behavior towards ubiquitous M-learning. *The Turkish Online Journal of Distance Education*, 12(3), 118-129.

Taha, N. (2022). Evaluating the effectiveness of practical cybersecurity practices in developing information security skills among female students at Umm University College. *Journal of Cybersecurity and Information Management*, 9(1), 85-100.

Virtanen, M. A. (2018). The development of ubiquitous 360 learning environment and its effects on students' satisfaction and histotechnological knowledge. Graduate School, University of Oulu.

Whitman, M. E., & Mattord, H. J. (2019). *Principles of information security* (6th ed.). Cengage Learning.

Yahya, S., Ahmad, E., & Abd Jalil, K. (2010). The definition and characteristics of ubiquitous learning: A discussion. *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, 6(1), 117-127. Retrieved from: https://www.researchgate.net/publication/272139764_The_definition_and_characteristics_of_ubiquitous_learning_A_discussion

YTH. (2015). What you need to know about teens and online privacy. Retrieved from: https://yth.org/whatyouneedtoknowaboutteensandonlineprivacy

Zawacki-Richter, O., Marín, V. I., & Bond, M. (2019). Systematic review of research on artificial intelligence applications in higher education: Where are the educators? *International Journal of Educational Technology in Higher Education*, 16(39). Retrieved from: https://doi.org/10.1186/s41239-019-0174-0