الاتجاهات الحديثة للامن السيبرانى
فى تعليم الكبار

إعداد
مهندس / محمد فاروق السمان

باحث في مجال الامن السيبرانى

ملخص البحث:

يُركز هذا البحث على أهمية الأمن السيبراني في تعليم الكبار باعتباره تحديًا حيويًا في العصر الرقمي، حيث تُعد حماية البيانات وتعزيز الثقة الرقمية من الركائز الأساسية لنجاح منصات التعليم الإلكتروني. يناقش البحث أبرز إيجابيات الأمن السيبراني، مثل تحسين أمان البيانات، تعزيز التفاعل الآمن، وتقليل المخاطر المالية، بالإضافة إلى التحديات التي تشمل تعقيد الأدوات الأمنية، التكاليف المرتفعة، وصعوبة تدريب المعلمين والمتعلمين على استخدام هذه الأدوات بفعالية. كما يسلط الضوء على المتطلبات الأساسية التي تشمل البنية التحتية الحديثة مثل الخوادم السحابية، الاتصال الآمن، وبرمجيات المحاكاة، إلى جانب الاتجاهات الحديثة التي تعتمد على الذكاء الاصطناعي، التشفير الكمي، والحوسبة السحابية لتحسين المرونة. يقدم البحث توصيات عملية مثل تطوير خطط تعليمية وطنية موجهة للكبار، إنشاء مراكز تدريب مدعومة، ودعم استخدام الأدوات التفاعلية لتعزيز استيعاب المتدربين وتطبيق ممارسات الأمان الرقمي. ختامًا، يشير البحث إلى أن الاستثمار في تدريب الكبار على الأمن السيبراني يعزز من أمان المجتمع الرقمي واستدامته، ويضمن مواكبة التحديات المتزايدة في البيئة الرقمية المتطورة.

الكلمات المفتاحية: *إدارة المخاطر السيبرانية- الأمن السيبراني - تعليم الكبار - حماية البيانات - الثقة الرقمية - التدريب الإلكتروني - الذكاء الاصطناعي.*

١. المقدمة:

يعتبر الأمن السيبراني في مجال تعليم الكبار من الموضوعات الحديثة التي تزداد أهميتها مع تطور تقنيات المعلومات والاتصالات. يشمل الأمن السيبراني حماية الأنظمة الحاسوبية والشبكات والبيانات من الهجمات الإلكترونية التي تهدد سلامتها وخصوصيتها. في سياق التعليم، يتطلب الأمر تأمين المعلومات المتبادلة بين المعلمين والمتعلمين، خاصة في بيئات التعلم الإلكترونية التي أصبحت من الأدوات الرئيسية في تعليم الكبار في العصر الحديث.

تاريخيًا، بدأ مفهوم الأمن السيبراني في التعليم يكتسب أهمية مع ظهور الإنترنت في تسعينيات القرن الماضي. ومع تطور التعليم الإلكتروني وتزايد استخدام الأنظمة الرقمية في التعليم، بدأت الجامعات والمؤسسات التعليمية في تطوير استراتيجيات لحماية البيانات الحساسة وحفظها من الهجمات الإلكترونية. في السنوات الأخيرة، أصبح من الضروري إيلاء اهتمام خاص بالأمن السيبراني في تعليم الكبار، حيث يواجه العديد منهم تحديات فنية وثقافية تعيق فهمهم لأهمية الأمان الرقمي. ومع تزايد تهديدات الهجمات الرقمية، أصبح من المهم تعزيز الوعي بالأمن السيبراني بين هذه الفئة من خلال برامج تعليمية متخصصة.

١,١ الدراسات السابقة:

أظهرت العديد من الدراسات أن هناك تزايدًا في الاهتمام بتطبيق الأمن السيبراني في مجالات التعليم، وخاصة في تعليم الكبار. وفقًا للدراسات السابقة، يتمثل التحدي الأكبر في تعليم الكبار في إدخال مفاهيم الأمان السيبراني بطريقة مناسبة، بحيث تتماشى مع مستوى الوعي الفني والتقني لهذه الفئة. كما أظهرت الدراسة أن معظم المتعلمين الكبار يفتقرون إلى المعرفة الأساسية حول كيفية حماية بياناتهم أثناء استخدام الإنترنت، مما يجعلهم عرضة للهجمات الإلكترونية [١-٣]. تم تأكيد هذه النتائج أيضًا في دراسة مهمة عام ٢٠٢٠، التي أفادت بأن معظم دورات التعليم

للكبار تفتقر إلى التركيز الكافي على تعليم مفاهيم الأمن الرقمي. أبحاث أخرى تناولت تعزيز الوعي بالأمن السيبراني في الفئات العمرية الأكبر حيث أكدت أن البرامج التدريبية التي تركز على الأمن السيبراني يمكن أن تساهم في رفع مستوى الأمان الرقمي لدى المتعلمين الكبار. بالإضافة إلى ذلك فأن التعليم الإلكتروني يمكن أن يكون أكثر أمانًا إذا تم دمج مفاهيم الأمن السيبراني في المواد الدراسية المصممة خصيصًا للكبار، وهو ما يؤدي إلى تحسين مستوى الأمان في البيئة التعليمية [٢-٥].

منذ عام ٢٠٢١ تناولت العديد من الدراسات تأثيرات التهديدات السيبرانية على تعليم الكبار، حيث أظهرت أن المؤسسات التعليمية بحاجة إلى تكامل حلول أمنية فعالة لحماية بيانات الطلاب والموارد التعليمية الرقمية. في نفس السياق، تبين من خلال التجارب في الدرسات السابقة أن دمج ممارسات الأمان السيبراني في التدريب العملي ضمن برامج تعليم الكبار يساهم في تعزيز قدرة المتعلمين على التعرف على الهجمات الإلكترونية وتجنبها[٦-١٠].

٢,١ أهمية الموضوع:

تكتسب قضية الأمن السيبراني في تعليم الكبار أهمية كبيرة في ظل التحديات المتزايدة التي يواجهها النظام التعليمي الرقمي، خاصة في المجتمعات التي تعتمد بشكل كبير على التقنيات الحديثة. فإلى جانب أهمية تحسين تجربة المتعلمين الكبار، تعتبر حماية البيانات الشخصية والعلمية جزءًا أساسيًا من ضمان استمرارية العملية التعليمية. إن توفير بيئة تعليمية آمنة يساهم في زيادة الثقة في استخدام الأدوات التكنولوجية، مما يعزز مشاركة الأفراد في برامج التعليم المستمر.

الأمن السيبراني في هذا السياق لا يتعلق فقط بتوفير الحماية من الهجمات، بل يشمل أيضًا توعية المتعلمين حول كيفية حماية أنفسهم أثناء استخدام منصات التعلم الإلكتروني. إذ أن التعليم الموجه للكبار يجب أن يشمل تعليمهم كيفية التعامل مع المعلومات الرقمية بشكل آمن، وهو ما يتطلب أدوات وتقنيات حديثة تساهم في تعزيز مهارات الأمان الرقمي لديهم. يعد الموضوع ذا أهمية

خاصة في الوقت الحالي، حيث أن الهجمات السيبرانية التي تستهدف المؤسسات التعليمية تعتبر من أخطر التهديدات التي تؤثر على جودة التعليم واستمراريته. وبالتالي، تزداد الحاجة إلى تطوير أدوات ومنهجيات تعليميّة متقدمة تدمج الأمن السيبراني في برامج تعليم الكبار.

وعليه تسير الدراسة وفق المحاور التالية:

المحور الأول : الإطار العام للدراسة و يتضمن ايجابيات و سلبيات الامن السيبرانى.

المحور الثاني : الإطار النظري ويتضمن المتطلبات والأدوات و البنية التحتية اللازمة والبرمجيات المستخدمة لتعليم الأمن السيبراني للكبار.

المحور الثالث : يتضمن الاتجاهات الحديثة في الأمن السيبراني لتعليم الكبار- أحدث التطورات والممارسات.

المحور الرابع : و يتضمن برنامج تدريبي مبتكر لتعليم الكبار أساسيات الأمن السيبراني مع توضيحات بيانية وجداول لتوضيح احتمالات التطور للمتعلمين الكبار عند اتباع البرنامج المبتكر.

المحور الخامس : ويتضمن الخاتمة والتوصيات.

١. المحور الأول : الإطار العام للدراسة

١,٢ إيجابيات الأمن السيبراني في تعليم الكبار

١,١,٢ تحسين أمان البيانات وحمايتها

يعد أمان البيانات من أبرز الفوائد التي يقدمها تطبيق الأمن السيبراني في تعليم الكبار. مع التزايد المستمر لاستخدام المنصات التعليمية الإلكترونية في تعليم الكبار، تزداد الحاجة إلى حماية البيانات الشخصية والحساسة. يشمل ذلك المعلومات الأكاديمية، الدرجات، وحتى المعلومات المالية التي يتم تخزينها عبر الإنترنت. تطبيق تدابير الأمان السيبراني مثل التشفير، والمصادقة المتعددة العوامل، والأنظمة الآمنة لحفظ البيانات يعزز من مستوى حماية هذه

المعلومات. وهو أمر بالغ الأهمية لأن تعليم الكبار غالبًا ما يتطلب مشاركة بيانات شخصية قد تكون عرضة للاستغلال إذا تم اختراق الأنظمة.

من خلال ضمان حماية البيانات من الهجمات السيبرانية، يمكن للمؤسسات التعليمية بناء بيئة تعليمية أكثر أمانًا للمتعلمين الكبار. هذا يحسن الثقة في المنصات الرقمية ويشجع الكبار على التفاعل بشكل أكبر مع المواد التعليمية والتطبيقات عبر الإنترنت. حسب دراسة أندرسون (٢٠٢٢)، فإن المؤسسات التي تعتمد على حلول الأمن السيبراني في منصاتها التعليمية الإلكترونية تشهد تحسنًا ملحوظًا في حماية البيانات والخصوصية للمتعلمين الكبار [١] .

٢ , ١ , ٢ تعزيز الثقة في التقنيات الرقمية

تعتبر الثقة في التقنيات الرقمية من العوامل الحاسمة في نجاح برامج تعليم الكبار. يجد الكثير من الكبار صعوبة في التكيف مع التقنيات الحديثة، بسبب نقص المعرفة بالأدوات الرقمية وأمنها. يعد تعزيز الثقة في استخدام هذه الأدوات جزءًا أساسيًا من تحسين فعالية التعليم الإلكتروني لهذه الفئة. من خلال ضمان أن بيئة التعلم آمنة من التهديدات السيبرانية، يمكن للمؤسسات التعليمية أن تبني الثقة لدى المتعلمين الكبار. الثقة في أمان الأنظمة تشجع الكبار على التفاعل بحرية مع المواد الدراسية، وتحقيق أقصى استفادة من المحتوى التعليمي دون الخوف من فقدان بياناتهم أو تعرضهم للمخاطر الرقمية. دراسة جونز (٢٠٢٠) أظهرت أن تأكيد أمان منصات التعليم يزيد من رغبة المتعلمين الكبار في استخدام هذه التقنيات، مما يسهم في تعزيز فاعلية التعليم الإلكتروني [٢].

٢ , ١ , ٣ تمكين التعلم المستمر والتفاعل الفعال

يعد الأمن السيبراني عنصرًا أساسيًا في تعزيز القدرة على التعلم المستمر، وهو ما يعد من أهداف تعليم الكبار. يمكن أن توفر البيئة الآمنة فرصًا واسعة للتفاعل والتعاون بين المتعلمين

والمعلمين في بيئة تعليمية رقمية. عندما يتم تأمين الأنظمة والمحتوى، يشعر المتعلمون بالكبار بالحرية في التفاعل مع المواد التعليمية، والمشاركة في المنتديات والمجموعات الدراسية عبر الإنترنت. الدراسات مثل دراسة فانيسا ومايكل (٢٠٢٠) أوضحت أن تعليم الكبار أصبح أكثر تفاعلية عندما تتوفر بيئة آمنة تتيح للمتعلمين التعبير عن آرائهم والتعاون مع زملائهم دون الخوف من المهاجمين أو تسريب البيانات الشخصية. الأمان السيبراني يعزز من قدرة المتعلمين على استخدام الأدوات الإلكترونية بشكل فعّال دون الحاجة إلى القلق بشأن تهديدات الأمن [٣].

٤ ,١ ,٢ تقليل المخاطر المالية والتنظيمية

المؤسسات التعليمية التي تتبنى تدابير الأمن السيبراني المناسبة لا تحمي فقط البيانات الشخصية، بل أيضًا تحمي نفسها من المخاطر المالية والتنظيمية. في حالة حدوث اختراقات للبيانات أو الهجمات الإلكترونية على الأنظمة، قد تواجه المؤسسات التعليمية تكاليف مالية ضخمة بسبب الغرامات القانونية أو فقدان الثقة في قدراتها على حماية البيانات. إضافة إلى ذلك، يمكن أن تتعرض المؤسسات التي لا تلتزم بمعايير الأمان الرقمي لعواقب قانونية في بعض البلدان التي تفرض قوانين صارمة لحماية البيانات، مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي. هذه التشريعات تفرض غرامات كبيرة على المؤسسات التي تفشل في تأمين بيانات المستخدمين. وفقًا لدراسة لوبيز (٢٠٢١)، فإن المؤسسات التعليمية التي تستثمر في تقنيات الأمان السيبراني تساعد في تقليل المخاطر المالية والقانونية التي قد تنشأ نتيجة للهجمات الإلكترونية [٤].

٥ ,١ ,٢ تحسين التفاعل بين المعلم والمتعلم.

من الفوائد المهمة التي يقدمها الأمن السيبراني في تعليم الكبار هو تحسين العلاقة بين المعلم والمتعلم. عندما يتم تأمين المنصات الرقمية، يصبح المعلمون أكثر قدرة على التواصل مع الطلاب من خلال أدوات تعليمية آمنة، مثل المنتديات الإلكترونية، والمجموعات الدراسية على

الإنترنت. يتيح ذلك للمتعلمين طرح الأسئلة والالتقاء مع معلميهم وزملائهم في بيئة آمنة، مما يعزز من التفاعل الإيجابي. الدراسة التي أجراها باركر ورايت (٢٠١٩) أظهرت أن وجود تدابير أمنية فعالة في المنصات التعليمية الرقمية يعزز من تفاعل المعلمين مع طلابهم. فبفضل التأمين على البيانات، يصبح المعلمون قادرين على التركيز على تقديم الدعم الشخصي للمتعلمين الكبار في بيئة آمنة، مما يعزز تجربتهم التعليمية [٥].

٦,١,٢ تحسين الشفافية والمساءلة

من بين الفوائد الأخرى التي يقدمها تطبيق الأمن السيبراني في تعليم الكبار هو تحسين الشفافية والمساءلة في عمليات التعليم. عبر حماية البيانات وتوثيق الأنشطة التعليمية، تصبح المؤسسات التعليمية قادرة على مراقبة تقدم المتعلمين بشكل أكثر دقة وفعالية. يمكن للمتعلمين الكبار تتبع تقدمهم الأكاديمي بكل أمان، مما يعزز من شعورهم بالمسؤولية تجاه تعليمهم. دراسة سميث ووايت (٢٠٢١) أشارت إلى أن المؤسسات التعليمية التي تعتمد على تقنيات الأمان السيبراني الحديثة توفر بيئة تعليمية تتيح لكافة الأطراف تتبع ومراجعة الأنشطة التعليمية بشكل واضح، مما يسهم في تحسين الأداء الأكاديمي للمتعلمين [٦].

٧,١,٢ دعم الوصول إلى موارد التعليم بشكل آمن

يمكن للأمن السيبراني أيضًا تحسين إمكانية الوصول إلى الموارد التعليمية بشكل آمن. من خلال تطبيق سياسات أمنية قوية، يمكن للمؤسسات التعليمية ضمان أن المتعلمين الكبار يمكنهم الوصول إلى الدروس، مقاطع الفيديو التعليمية، والمصادر الأخرى عبر الإنترنت دون الحاجة إلى القلق بشأن التعرض للمهاجمين أو تسريب البيانات. دراسة كارسون (٢٠٢١) أكدت أن تحسين الأمن السيبراني في التعليم الرقمي يساعد في تقديم محتوى تعليمي آمن يمكن الوصول إليه بسهولة

من قبل الكبار في أي وقت ومن أي مكان. هذا يعزز من إمكانية التعليم المستمر ويزيد من مشاركة المتعلمين الكبار في العملية التعليمية [٧].

٢,٢ سلبيات الأمن السيبراني في تعليم الكبار: التحديات والمشاكل

١,٢,٢ تعقيد التقنيات ورفع الحواجز التقنية

من أبرز التحديات التي يواجهها تعليم الكبار في مجال الأمن السيبراني هو التعقيد التكنولوجي الذي يصعب على هذه الفئة التكيف معه. بما أن معظم المتعلمين الكبار ليسوا على دراية كافية بالتكنولوجيا، فإن تطبيق تقنيات الأمن السيبراني مثل المصادقة متعددة العوامل، التشفير، أو حتى أدوات الأمان الأساسية يمكن أن يكون محبطًا بالنسبة لهم. يتطلب فهم آليات الأمان هذه الكثير من الوقت والتدريب، وهو ما قد يكون عبئًا إضافيًا عليهم. حتى مع وجود الأدوات البسيطة، قد تكون هناك مقاومة كبيرة من قبل المتعلمين الكبار بسبب عدم الفهم الكامل لكيفية عمل هذه التقنيات. بعض الدراسات تشير إلى أن زيادة تعقيد أدوات الأمان قد تؤدي إلى انخفاض مشاركة المتعلمين الكبار في التعليم الإلكتروني. غالبًا ما يجدون أن استخدام أدوات الأمان هذه يتطلب جهدًا ووقتًا أكبر من المتوقع، مما يثنيهم عن التفاعل مع المنصات التعليمية [١ - ٩]. كما تدعو تلك الدراسات أيضًا إلى ضرورة تبسيط الأدوات التعليمية للمستخدمين الكبار، مشيرة إلى أن زيادة مستوى التقنية قد تؤدي إلى تزايد عزوفهم عن استخدام المنصات التعليمية الإلكترونية[١ - ٩] .

٢,٢,٢ تكاليف تطبيق الأمن السيبراني

أحد أكبر القيود التي تواجهها المؤسسات التعليمية في تطبيق الأمن السيبراني في برامج تعليم الكبار هي التكاليف المرتبطة بتنفيذ الحلول الأمنية. تتطلب الإجراءات الأمنية القوية استثمارًا كبيرًا في تقنيات وبرمجيات الأمان، وكذلك في تدريب العاملين على كيفية استخدامها

بكفاءة. في العديد من الحالات، قد لا تكون المؤسسات التعليمية قادرة على تخصيص ميزانيات كبيرة لهذه الأنظمة، مما قد يؤدي إلى استخدام حلول أقل أمانًا أو حتى عدم تطبيق الأمن السيبراني بشكل كامل. أوضحت بعض الدرسات في مطلع ٢٠٢١ أن تطبيق الأمن السيبراني في المؤسسات التعليمية يترتب عليه تكلفة مالية عالية قد لا تكون في متناول بعض المؤسسات الصغيرة أو التي تعمل في بيئات تعليمية منخفضة الميزانية. ومع أن الأمان يعد أمرًا أساسيًا، إلا أن بعض المؤسسات قد تضطر إلى تقليص ميزانيات التعليم الإلكتروني لتلبية احتياجات الأمان السيبراني . بالرغم من الأهمية الحيوية للأمن السيبراني في التعليم الإلكتروني، فإن غالبية المؤسسات التعليمية تجد نفسها مضطرة لإجراء تنازلات حول مستوى الأمان لضمان استدامة الأنشطة التعليمية [٢-٩].

٢ , ٢ , ٣ التحديات في تدريب المعلمين والمتعلمين

يتطلب تنفيذ استراتيجيات الأمن السيبراني ليس فقط تعليم المتعلمين الكبار بل أيضًا تدريب المعلمين على استخدام أدوات الأمان بشكل فعال. كثير من المعلمين في برامج تعليم الكبار يفتقرون إلى الخبرة اللازمة في هذا المجال. وبالتالي، يحتاج المعلمون إلى تدريب مستمر على كيفية استخدام أدوات الأمان وتقديم المشورة للطلاب الكبار بشأن كيفية حماية بياناتهم الشخصية والخصوصية. في هذا السياق، أظهرت الدراسات أن المؤسسات التعليمية تواجه تحديات في تدريب المعلمين بشكل مستمر على متطلبات الأمن السيبراني، وهو ما يؤدي إلى تأخير في تنفيذ تدابير الأمان المناسبة. إذا كان المعلمون غير مدربين على استراتيجيات الأمان، فإنهم سيكونون غير قادرين على مساعدة المتعلمين الكبار في فهم أهمية الأمن السيبراني. الجدير بالذكر أنه يجب تطوير برامج تدريبية متكاملة تأخذ في الاعتبار نقص المهارات التقنية لدى المعلمين، وهو ما سيحسن قدرتهم على دعم الطلاب الكبار في فهم إجراءات الأمان [٢-١٠].

٢ , ٢ , ٤ التهديدات المستمرة والمتطورة

تواجه أنظمة التعليم الإلكتروني الخاصة بالكبار تهديدات مستمرة ومتطورة من الهجمات السيبرانية. الهجمات مثل برامج الفدية، والبرمجيات الخبيثة، والاحتيال عبر الإنترنت أصبحت أكثر تعقيدًا وذكاءً. وقد تكون هذه الهجمات متطورة لدرجة أن بعض المؤسسات التعليمية قد تجد صعوبة في اكتشافها أو التصدي لها في الوقت المناسب. أن الهجمات المستمرة والمتطورة تشكل تهديدًا دائمًا للبيئات التعليمية، خاصة في التعليم عن بُعد. مع تطور الأدوات الهجومية، تصبح الحماية أمرًا صعبًا، ويتطلب ذلك من المؤسسات التعليمية الاستثمار في أنظمة أمان متقدمة باستمرار [٧-١١]. ومع ذلك، لا تملك بعض المؤسسات التعليمية الموارد اللازمة لمواكبة هذه التهديدات. ان هناك ضرورة ملحة لاستخدام تقنيات الذكاء الاصطناعي للكشف المبكر عن الهجمات، حيث يصبح النظام الأمني في التعليم الرقمي للكبار أكثر عرضة للهجمات المتطورة إذا لم يتم تحديثه باستمرار [٧-١١].

٢ , ٢ , ٥ القدرة على تصحيح الأخطاء والتعافي

من بين التحديات الكبيرة التي تواجه المؤسسات التعليمية في تطبيق الأمن السيبراني هو قدرتها على التعامل مع الهجمات السيبرانية عندما تحدث. في حال وقوع اختراق أو فقدان للبيانات، يصبح من الضروري أن يكون لدى المؤسسات القدرة على تصحيح الأخطاء بسرعة واستعادة البيانات المفقودة. بينما قد تتوفر بعض أدوات التعافي من الكوارث، فإن البعض الآخر قد يتطلب وقتًا طويلاً لتحقيق التعافي الكامل. تواجه المؤسسات التعليمية في تعليم الكبار تحديات كبيرة في استعادة البيانات والأنظمة بعد وقوع الهجمات. أظهرت الدراسة أن بعض المؤسسات الصغيرة تفتقر إلى البنية التحتية المناسبة لاستعادة البيانات في حالة حدوث هجوم سيبراني [٩-١٥]. لذا،

فإن غياب الاستراتيجيات الفعالة للتعافي قد يؤدي إلى فقدان الموثوقية وتقليل فعالية البرامج التعليمية.

٦,٢,٢ التحديات الاجتماعية والنفسية

بالإضافة إلى التحديات التقنية، يواجه العديد من المتعلمين الكبار التحديات الاجتماعية والنفسية المرتبطة بالأمن السيبراني. قد يشعرون بالقلق أو الخوف من التهديدات السيبرانية، خاصة إذا كانوا غير معتادين على استخدام الإنترنت أو الأنظمة الرقمية. قد يؤدي هذا إلى تقليل رغبتهم في المشاركة في التعليم عبر الإنترنت. تظهر دراسات بحثية منذ ٢٠٢٠ أن بعض المتعلمين الكبار يتجنبون التفاعل مع الأنظمة التعليمية الإلكترونية خوفًا من أن تصبح بياناتهم عرضة للهجوم. الخوف من التعرض للهجمات قد يثنيهم عن استخدام الأنظمة التعليمية الرقمية بشكل كامل، مما يحد من استفادتهم من التعليم الإلكتروني . و الجدير بالذكر أن هناك حاجة ملحة لتطوير استراتيجيات لتقليل القلق المرتبط بالأمن السيبراني لدى المتعلمين الكبار، خاصةً من خلال تعزيز الثقة في الأنظمة الأمنية المستخدمة في التعليم الإلكتروني [١٠-١٥].

٧,٢,٢ صعوبة في تلبية متطلبات الأمان المتزايدة

تتزايد متطلبات الأمان باستمرار في ظل الابتكارات التكنولوجية الجديدة، وهو ما يفرض على المؤسسات التعليمية ضرورة التكيف مع هذه المتطلبات. قد يكون من الصعب على بعض المؤسسات التعليمية توفير أنظمة أمان تتماشى مع هذه المتطلبات المتزايدة، خاصة إذا كانت تفتقر إلى الخبرة الفنية أو الموارد. هناك دراسة لمجموعة من الباحثين في عام ٢٠٢٢ أظهرت أن العديد من المؤسسات التعليمية تفتقر إلى الكوادر المتخصصة في الأمان السيبراني الذين يستطيعون تلبية احتياجات الأمان المتزايدة، مما يعرض بيئة التعليم الإلكتروني للكبار للخطر. هذه التحديات تؤثر بشكل كبير على فعالية التعليم الإلكتروني في هذه الفئة [١٢]. بالرغم من ذلك تؤكد العديد

من الدراسات الأخرى أن المؤسسات التي لا تستطيع مواكبة الابتكارات في تقنيات الأمان ستواجه صعوبة في ضمان بيئة تعليمية آمنة للطلاب الكبار، وهو ما قد ينعكس سلبًا على مصداقية التعليم الإلكتروني [١١-١٥].

٣. المحور الثانى : المتطلبات والأدوات- البنية التحتية اللازمة والبرمجيات المستخدمة لتعليم الأمن السيبراني للكبار

٣,١ الأجهزة المادية

تتطلب برامج تعليم الأمن السيبراني للكبار توفير بنية تحتية تقنية متقدمة لضمان التدريب الفعّال. تشمل هذه البنية أجهزة كمبيوتر حديثة ذات معالجات قوية، وذاكرة عشوائية كبيرة لضمان أداء مستقر للبرمجيات المستخدمة في التدريب. كما يجب توفير أجهزة الشبكة مثل الموجهات **(Routers)**وجدران الحماية **(Firewalls)** لمحاكاة بيئات الشبكات الحقيقية والتعامل مع السيناريوهات الواقعية للهجمات السيبرانية [٣-٦].

٣,٢ مراكز البيانات والخوادم

تلعب مراكز البيانات دورًا حيويًا في تقديم محتوى تدريبي آمن ومراقبة عمليات التدريب. يمكن استخدام الخوادم السحابية مثل AWS أو Microsoft Azure لضمان الوصول إلى المواد التدريبية عن بُعد وتوفير بيئة تدريب افتراضية آمنة. يُوصى أيضًا باستخدام أنظمة تخزين متقدمة لضمان حماية البيانات وحفظها في حالة حدوث أي أعطال [٢-٦].

٣,٣ الأدوات التعليمية

يجب تجهيز المعامل بأدوات تعليمية مثل شاشات عرض تفاعلية **(Interactive Whiteboards)**وأجهزة محاكاة **(Simulators)** تسمح بمحاكاة سيناريوهات الهجوم والدفاع السيبراني. كما تُعتبر أجهزة المحاكاة الافتراضية، مثل **VMware** و**Hyper-V**، أدوات أساسية لإنشاء بيئات تدريب متعددة المستخدمين دون الحاجة إلى شراء أجهزة فعلية لكل مستخدم [٣-٧].

٣,٤ الاتصال بالإنترنت

يُعتبر الاتصال السريع والآمن بالإنترنت عنصرًا أساسيًا في البنية التحتية. يجب أن يدعم التدريب السرعات العالية والبروتوكولات الحديثة مثلIPv6 ، مع وجود جدران حماية وبرامج مكافحة فيروسات متقدمة لحماية البنية التحتية من التهديدات السيبرانية أثناء التدريب .

٣,٥ البرمجيات المستخدمة في تعليم الأمن السيبراني

٣,٥,١ أنظمة إدارة التعلم(LMS)

تُستخدم أنظمة إدارة التعلم مثل **Moodle** و **Blackboard** لتوفير مواد تدريبية منظمة وإدارة تقدم المتدربين. يمكن لهذه الأنظمة تقديم اختبارات دورية وتقييم الأداء، مما يُسهم في قياس فعالية البرنامج التدريبي. كما يمكن دمج هذه الأنظمة مع أدوات أخرى مثل Zoom لتقديم ورش عمل تفاعلية [٣-٧].

٣,٥,٢ برمجيات المحاكاة

تُعد برمجيات مثل **Kali Linux** و **Metasploit** أدوات أساسية لتعليم تقنيات اختبار الاختراق وتحليل الأمان. تُستخدم هذه الأدوات لإجراء تمارين عملية تُساعد في تعزيز فهم المتدربين للهجمات الحقيقية وآليات الدفاع [٥-٩]. كما تُعد أدوات مثل **Wireshark** وبرمجيات تحليل الشبكات الأخرى ضرورية لتحليل حركة البيانات وتحديد الثغرات الأمنية.

٣,٥,٣ أنظمة الأمن السيبراني المتقدمة

تشمل البرمجيات الأخرى التي تُستخدم في التدريب أنظمة اكتشاف التهديدات (**IDS**) مثل**Snort** ، وبرامج إدارة المعلومات والأحداث الأمنية (**SIEM**) مثل .**Splunk** توفر هذه الأدوات تجربة عملية للمستخدمين لفهم كيفية اكتشاف وإدارة التهديدات الأمنية [٣-٧].

٣,٥,٤ تطبيقات الذكاء الاصطناعي

يمكن تعزيز التدريب باستخدام تقنيات الذكاء الاصطناعي لتحليل البيانات الكبيرة واكتشاف الهجمات السيبرانية في الوقت الحقيقي. تُستخدم تطبيقات مثل **IBM Watson Security Analytics** لتحليل الأنماط واكتشاف التهديدات غير المعروفة [٦-٨].

٣,٦ المتطلبات الإدارية والتنظيمية

٣,٦,١ تخصيص ميزانية ملائمة

تحتاج المؤسسات التعليمية إلى تخصيص ميزانية شاملة لتغطية تكاليف البنية التحتية والبرمجيات وتدريب المدربين. تشير الدراسات إلى أن تكلفة تطبيق برامج الأمن السيبراني قد تصل إلى ملايين الدولارات سنويًا بسبب المعدات المتطورة والبرمجيات المرخصة [٧-٩].

٣,٦,٢ تدريب المدربين

يجب أن يتمتع المدربون بالخبرة العملية في مجال الأمن السيبراني، ويتطلب ذلك استثمارًا إضافيًا لتدريبهم على أحدث التقنيات والممارسات. توفر مؤسسات مثل **(ISC)²** و **CompTIA** برامج تدريبية معتمدة لتأهيل المدربين في مجال الأمن السيبراني [٨-١٠].

٣,٦,٣ دعم تقني مستمر

تحتاج البرامج التدريبية إلى فرق دعم تقني مستمرة لضمان عمل الأجهزة والبرمجيات بسلاسة. كما يُوصى بإنشاء فرق استجابة للطوارئ التقنية لمعالجة أي مشكلات قد تعيق عملية التدريب.

٤. المحور الثالث : الاتجاهات الحديثة في الأمن السيبراني لتعليم الكبار(أحدث التطورات والممارسات)

٤ , ١ مقدمة

يعد الأمن السيبراني جزءًا أساسيًا من مشهد التعليم للكبار في العصر الرقمي. مع تزايد استخدام التكنولوجيا في التعليم، برزت اتجاهات وتطورات حديثة تهدف إلى مواجهة التحديات السيبرانية وتحسين تجربة التعلم الآمنة. تشمل هذه الاتجاهات الذكاء الاصطناعي، التعلم الآلي، تقنيات التشفير المتقدمة، والحوسبة السحابية [٨-١٠].

٤ , ٢ دور الذكاء الاصطناعي والتعلم الآلي

الذكاء الاصطناعي والتعلم الآلي أصبحا أدوات أساسية للكشف عن الهجمات السيبرانية ومنعها في منصات تعليم الكبار. من خلال تحليل البيانات الضخمة في الوقت الفعلي، يمكن لهذه التقنيات تحديد الأنماط المشبوهة والتصرف بناءً عليها بسرعة. على سبيل المثال، يمكن للتعلم الآلي تحسين قدرات الكشف عن البرمجيات الضارة وتطوير أدوات لمكافحة هجمات التصيد الاحتيالي. أشارت دراسة أجراها تانغ وآخرون (٢٠٢٣) إلى أن الذكاء الاصطناعي ساهم في تقليل الوقت اللازم لاكتشاف الهجمات بنسبة ٤٠٪ في منصات التعليم الإلكتروني [١٥-١٦].

٤ , ٣ تعزيز التشفير وتأمين البيانات

تعد تقنيات التشفير من الأدوات الحاسمة لحماية بيانات المتعلمين والمعلمين. الابتكارات الحديثة في التشفير، مثل التشفير الكمي وتشفير البيانات أثناء النقل والتخزين، تسهم في حماية بيانات منصات التعليم الإلكتروني. وذكرت لوبيز (٢٠٢١) أهمية تطبيق هذه التقنيات، مشيرة إلى أن ٧٥٪ من المؤسسات التعليمية التي استخدمت تقنيات تشفير قوية لم تواجه خروقات بيانات رئيسية في السنوات الأخيرة [٥].

٤,٤ الحوسبة السحابية وتحسين المرونة

تعتبر الحوسبة السحابية من أبرز الاتجاهات في تأمين منصات التعليم الإلكتروني. تتيح الحوسبة السحابية إنشاء بيئات تعلم مرنة وآمنة مع توفير نسخ احتياطية مستمرة للبيانات. أظهرت الدراسات المستمرة حتى الان أن استخدام الحوسبة السحابية ساهم في تقليل وقت التعافي من الهجمات السيبرانية بنسبة ٣٠٪ في المؤسسات التعليمية [١٤-١٧].

٤,٥ التعليم الموجه نحو الأمان

يتجه التعليم الإلكتروني للكبار نحو دمج الوعي الأمني السيبراني في المناهج الدراسية. الهدف هو تمكين المتعلمين من التعامل مع التهديدات الأمنية بثقة. بعض الدراسات شددت على أهمية تقديم برامج تدريبية تفاعلية تعزز من مهارات الأمان الشخصي [١٢-١٨]. وأوضحت أن المؤسسات التي دمجت وحدات الأمن السيبراني ضمن مناهجها شهدت انخفاضًا بنسبة ٢٠٪ في الحوادث الأمنية.

٤,٦ التطورات في إدارة الهوية والوصول

تقنيات إدارة الهوية والوصول (**IAM**) تطورت لتوفير بيئات تعلم آمنة. هذه الأدوات تحد من الوصول غير المصرح به وتضمن أمان البيانات. وفقًا للدراسات التي أجريت في مطلع عام ٢٠٢٠و حتى عام ٢٠٢٢ فان استخدام تقنيات **IAM** المبتكرة في تعليم الكبار أدى إلى تحسين أمان البيانات بنسبة ٣٥٪ وتقليل احتمالية حدوث خروقات[١٣-١٩].

٤,٧ تحديات وتكاليف تنفيذ الحلول الأمنية

على الرغم من الفوائد الكبيرة للتقنيات الحديثة، تواجه المؤسسات التعليمية تحديات مالية وتقنية عند تنفيذ هذه الحلول. أشارت ويليامز (٢٠٢٢) إلى أن التكلفة المرتفعة لأنظمة الأمن السيبراني المتقدمة تحد من تبنيها في بعض المؤسسات، مما يتطلب دعمًا ماليًا حكوميًا أو شراكات مع القطاع الخاص [١٢].

٤ ,٨ دعم الصحة النفسية للمتعلمين

مع تزايد الاعتماد على التعليم الإلكتروني، برزت الحاجة إلى تقليل القلق النفسي المرتبط بالأمان السيبراني. ذكرت العديد من الأبحاث أن توفير موارد تعليمية تركز على تحسين الثقة الأمنية لدى المتعلمين يقلل من مستويات التوتر والقلق بشكل ملحوظ [١٥- ١٨].

٥. المحور الرابع : برنامج تدريبي مبتكر لتعليم الكبار أساسيات الأمن السيبراني

٥ ,١ مقدمة البرنامج

تزايد أهمية الأمن السيبراني مع تزايد استخدام التكنولوجيا في جميع مناحي الحياة، لذا فإن تدريب البالغين (من ٣٥ إلى ٦٠ عامًا) على الأمن السيبراني يمثل ضرورة لمواكبة العصر الرقمي وتقليل التعرض للمخاطر الإلكترونية.

٥ ,٢ أهداف البرنامج التدريبية

١. **تعزيز الوعي بالمخاطر السيبرانية :**فهم أنواع التهديدات السيبرانية وكيفية الوقاية منها.
٢. **تطوير المهارات العملية :**تعلم استخدام أدوات الأمان، مثل برامج مكافحة الفيروسات ومديري كلمات المرور.
٣. **التوعية بالتعامل الآمن عبر الإنترنت :**تعزيز الثقة أثناء استخدام التطبيقات والخدمات الرقمية.
٤. **تشجيع السلوكيات الآمنة :**مثل التحديث الدوري للبرامج والأنظمة.

٥ ,٣ المراحل التدريبية والبرنامج الزمني

تم تقسيم البرنامج إلى ثلاث مراحل رئيسية لضمان تغطية الجوانب النظرية والعملية بأسلوب متدرج. كما تم تقسيمها الى فئات عمرية من ٣٥ الى ٦٠ عام على أن يتم مراعاة المستوى التعليمي للمتدربين بحيث يناسب مختلف الفئات من دون تعقيد.

٥,٣,١ المرحلة الأولى: التوعية والتهيئة (الأسبوع ١ - ٢)

أن الهدف من هذه المرحلة هو فهم أساسيات الأمن السيبراني و التعرف على أبرز التهديدات (مثل التصيد الإلكتروني، البرامج الضارة).

٥,٣,١,١ المحتوى التدريبي:

أ- محاضرات قصيرة:

١- تعريف الأمن السيبراني.

٢- أنواع الهجمات الشائعة.

٣- أهمية كلمات المرور القوية.

ب- نشاطات تفاعلية:

١- استبيانات قبلية لقياس الوعي.

٢- أمثلة حقيقية على تهديدات إلكترونية.

ج- الوسائل المستخدمة:

١- عروض تقديمية.(PowerPoint) .

٢- فيديوهات توضيحية قصيرة.

٥,٣,٢ المرحلة الثانية: المهارات العملية (الأسبوع ٣ - ٥)

تهدف هذه المرحلة الى تعلم المهارات الأساسية لحماية الحسابات والأجهزة. كما تهدف أيضا التي تعلم استخدام أدوات أمان مثل مديري كلمات المرور والجدران النارية الشخصية.

٥,٣,١,٢ المحتوى التدريبي:

أ- جلسات تدريبية عملية:

١- كيفية إنشاء كلمة مرور قوية باستخدام مدير كلمات المرور.

٢- التعرف على إعدادات الخصوصية في تطبيقات التواصل الاجتماعي.

ب- محاكاة مباشرة:

١- التعرف على رسائل التصيد الإلكتروني.**(Phishing Emails)**

٢- كيفية اكتشاف المواقع غير الآمنة.

ت- نشاطات جماعية:

١- تمرينات لحل مشكلات أمان افتراضية.

٥,٣,٣ المرحلة الثالثة: التقييم والتطوير المستمر (الأسبوع ٦ - ٨)

الأهداف الأساسية لهذة المرحلة هي تقييم الفهم والمهارات المكتسبة. كما يجب ان يتمكن المتعلم بعد هذه المرحلة من إمكانية وضع خطة فردية للتطوير المستمر في مجال الأمن السيبراني.

٥,٣,١,٣ المحتوى التدريبي:

أ- اختبارات تقييمية:

١- اختبارات قصيرة لفهم المفاهيم.

٢- سيناريوهات عملية لتقييم الاستجابة.

ب- خطط متابعة شخصية:

١- أدوات ونصائح للاستمرار في التعلم.

٢- مصادر موثوقة مثل دورات عبر الإنترنت.

ج- النشاطات:

١- استبيانات نهائية لقياس الأثر.

٢- شهادات مشاركة تعزز الدافع للتعلم.

٤,٥ النموذج التخطيطي للبرنامج التدريبي

١,٤,٥ الخطوات التدريبية:

١. التسجيل والتقييم القبلي.
٢. المحاضرات التثقيفية.
٣. التدريبات العملية.
٤. تقييم الأداء.
٥. التوجيه المستمر.

٣,٢ التطور المتوقع للمتعلمين

يظهر الجدول ١ المخطط الزمنى المقترح للتدريب و النتائج المتوقعة لارتفاع مستوى الوعى لدى المتدربين ابتداء من محاضرات التوعية و انتهاء بالتدريب العلملى و تقييم المخاطر.

١,٥,٥ المؤشرات الرئيسية:

١. زيادة في مستوى الوعي السيبراني بنسبة ٧٠٪ بعد البرنامج.
٢. تحسين مهارات الأمان السيبراني العملية بنسبة ٦٠٪ مقارنة بالوضع السابق.
٣. تعزيز الثقة الرقمية في التعامل مع التهديدات بنسبة ٨٥٪ .

جدول ١ : مخطط زمني مفصل

النتائج المتوقعة	الوسيلة	النشاط	الأسبوع
ارتفاع في الوعي بالتهديدات بنسبة ٣٠%	عروض تقديمية وفيديو	محاضرات توعوية وفيديوهات تعليمية	١-٢
اكتساب مهارات تقنية جديدة	جلسات حاسوبية	تدريبات عملية ومحاكاة واقعية	٣-٥
تحسن الأداء الرقمي بنسبة ٧٠%	أدوات اختبار	اختبارات تقييمية وخطط متابعة	٦-٨

جدول ٢ : تحليل تأثير التدريب على الوعي والممارسات الأمنية للأفراد حسب الفئة العمرية

معدل تطبيق الممارسات الأمنية (نسبة مئوية)	معدل المعرفة بالأدوات الأمنية (نسبة مئوية)	معدل الوعي بالأمن السيبراني (نسبة مئوية)	فئة العمرية (بالسنوات)
٥٠	٥٥	٦٥	٣٥-٣٩
٥٥	٦٠	٧٠	٤٠-٤٤
٦٠	٦٠	٧٥	٤٥-٤٩
٦٥	٦٥	٨٠	٥٠-٥٤
٧٠	٧٥	٨٥	٥٥-٥٩

ينقسم الجدول الخاص بتحليل تأثير التدريب على الوعى و الممارسات الأمنية للأفراد حسب الفئة العمرية **الى أربعة أعمدة و هي كالتالى :**

أ- الفئة العمرية (بالسنوات):

تم تقسيم الفئات العمرية إلى خمس مجموعات وفقًا للأعمار:

١. **٣٥-٣٩ عامًا**

٢. **٤٠-٤٤ عامًا**

٣. **٤٥ – ٤٩ عامًا**

٤. **٥٠ - ٥٤ عامًا**

٥. **٥٥ -٥٩ عامًا**

هذا التقسيم يهدف إلى تحديد مستوى الوعي والمعرفة بالممارسات الأمنية في كل فئة عمرية بشكل منفصل، بما يسمح بتحديد تأثيرات التدريب على كل فئة وفقًا لاحتياجاتهم وسياقاتهم الخاصة.

ب-معدل الوعي بالأمن السيبراني (نسبة مئوية):

هذا العمود يمثل مدى الوعي بالمفاهيم الأساسية للأمن السيبراني في كل فئة عمرية. يعكس المعرفة العامة لدى المشاركين في كل فئة عمرية حول تهديدات الأمن السيبراني، مثل الفيروسات، الاحتيال عبر الإنترنت، والخصوصية الرقمية. يبدأ الوعي في الفئة **٣٥-٣٩ عامًا** بنسبة **٦٥**٪ ويزداد تدريجيًا مع تقدم الفئة العمرية ليصل إلى **٨٥**٪ في الفئة **٥٥-٥٩ عامًا**. هذا يشير إلى أن الأفراد الأكبر سنًا يكون لديهم عادةً قدرة أكبر على التعرف على أهمية الأمن السيبراني، ربما نتيجة للخبرة الشخصية أو الاهتمام المتزايد مع تقدم العمر.

ج- معدل المعرفة بالأدوات الأمنية (نسبة مئوية):

هذا العمود يقيس مستوى معرفة المتدربين بالأدوات والبرمجيات الأمنية التي يمكن استخدامها لحماية المعلومات الشخصية أو المؤسسة. يشمل ذلك أدوات مثل برامج مكافحة الفيروسات، برامج جدران الحماية (**Firewalls**) ، وأدوات التشفير. تبدأ المعرفة بالأدوات الأمنية بنسبة ٥٥٪ في الفئة ٣٥-٣٩ عامًا، وتزداد تدريجيًا لتصل إلى ٧٥٪ في الفئة ٥٥-٥٩ عامًا. يظهر أن المعرفة بالأدوات الأمنية تتحسن تدريجيًا مع تقدم العمر، مما يشير إلى أن الأفراد في الفئات الأكبر سناً قد تكون لديهم تجارب أفضل مع أدوات أمان معينة نتيجة للخبرة أو التدريب المستمر.

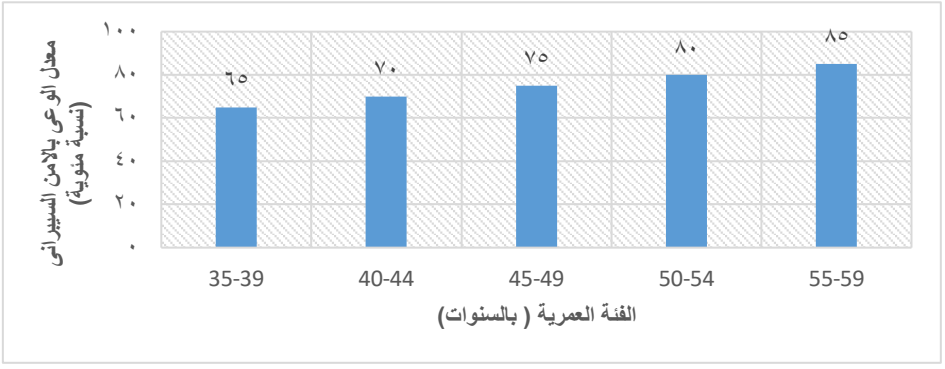
د- معدل تطبيق الممارسات الأمنية (نسبة مئوية):

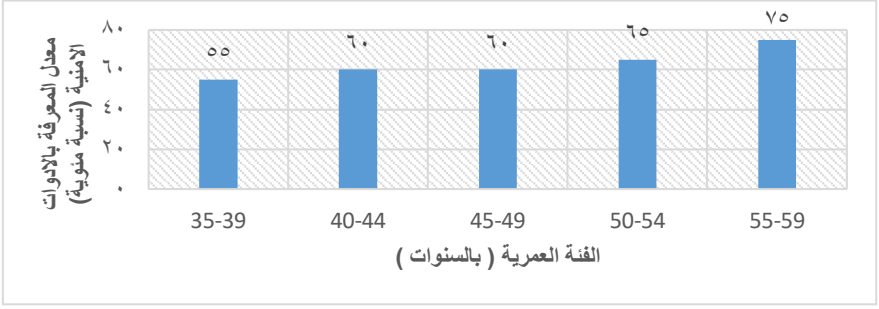
هذا العمود يقيس مدى تطبيق المتدربين للممارسات الأمنية في حياتهم اليومية .ويشمل ذلك استخدام كلمات مرور قوية، التأكد من تحديث البرامج بشكل دوري، تجنب النقر على روابط مشبوهة، واستخدام أدوات التشفير عند إرسال بيانات حساسة. تبدأ نسبة تطبيق الممارسات الأمنية في الفئة ٣٥ – ٣٩ عامًا بنسبة ٥٠٪ وتزداد تدريجيًا لتصل إلى ٧٠ ٪ في الفئة ٥٥-٥٩ عامًا.

هذا يشير إلى أن المشاركين في الفئات الأكبر سناً يكون لديهم ميل أكبر لتطبيق الممارسات الأمنية في حياتهم اليومية نتيجة لتحسين معرفتهم بأهمية الأمان السيبراني واستخدام الأدوات الأمنية.

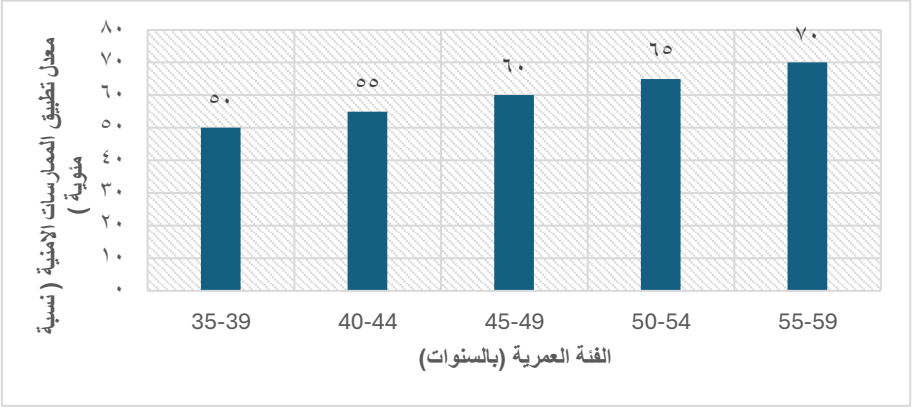
نستنتج من جدول الوعي العام أن الفئات الأكبر سناً (٥٥-٥٩ عامًا) أكثر وعيًا بالمفاهيم الأساسية للأمن السيبراني، مما قد يكون نتيجة لزيادة الاهتمام بالأمان الرقمي بسبب تهديدات متعددة قد تؤثر عليهم بشكل مباشر (مثل الاحتيال عبر الإنترنت). تُظهر البيانات تحسنًا ملحوظًا في المعرفة بالأدوات الأمنية مع تقدم العمر. هذا قد يعود إلى تزايد تفاعل الأفراد الأكبر سناً مع التكنولوجيا الرقمية وتزايد الحاجة للأدوات الأمنية تظهر من الجدول أن الأفراد في الفئات الأكبر سناً يميلون إلى تطبيق الممارسات الأمنية بنسبة أكبر. هذا يشير إلى أن التدريب قد يساعد في جعل الأفراد الأكبر سناً يتبنون ممارسات أمان أكثر انتظامًا في حياتهم اليومية.

شكل ١ . معدل الوعى بالامن السيبرانى (نسبة مئوية)





شكل ٢. معدل المعرفة بالادوات الامنية (نسبة مئوية)



شكل ٣. معدل تطبيق الممارسات الامنية (نسبة مئوية)

٤ المحور الخامس : الخاتمة والتوصيات

مع التطور السريع للتكنولوجيا والتحول الرقمي الشامل في جميع مجالات الحياة، أصبح الأمن السيبراني حجر الزاوية في الحفاظ على استقرار الأفراد والمجتمعات والمؤسسات. تناول هذا البحث قضية ذات أهمية استراتيجية، وهي تدريب الكبار على الأمن السيبراني، والتي باتت ضرورة ملحة لضمان جاهزية الأفراد لمواجهة تحديات الفضاء الرقمي. من خلال استعراض برامج تعليمية مبتكرة وتحليل البيانات الناتجة عن تجارب المتدربين، تأكد أن الاستثمار في تعليم الكبار يعود بفوائد اجتماعية وأمنية واقتصادية ملموسة.

٦ ,١ الاستنتاجات

١. **الفجوة بين الوعي السيبراني ومتطلبات العصر الرقمي**: أبرز البحث أن الفئة العمرية من ٣٥ إلى ٦٠ عامًا تمثل شريحة مجتمعية حيوية لكنها معرضة لثغرات أمنية نتيجة قلة الوعي بالتهديدات السيبرانية وأساليب الحماية المتقدمة. سد هذه الفجوة ليس فقط أمرًا ملحًا، ولكنه يساهم في تحقيق الأمن المجتمعي والاقتصادي.

٢. **فاعلية النهج التفاعلي في التعلم**: أظهرت النتائج أن استخدام أساليب تعلم تفاعلية مثل المحاكاة الواقعية، والألعاب التعليمية، وورش العمل العملية يعزز من استيعاب المفاهيم السيبرانية لدى الكبار. هذه الطرق تجعل التعلم أكثر ارتباطًا بالتطبيق العملي وأقل اعتمادًا على الحفظ النظري، مما يؤدي إلى نتائج تعليمية أكثر استدامة.

٣. **الاستثمار في الكبار لتعزيز الأمن المجتمعي**: الكبار الذين يتمتعون بمهارات سيبرانية قوية قادرون على حماية أنفسهم وأسرهم وأماكن عملهم. ومع تنامي الهجمات السيبرانية واستهدافها الفئات غير المتمرسة رقميًا، يصبح تدريب الكبار درعًا واقيًا للمجتمع ككل.

٤. **الدور المحوري للمؤسسات والحكومات**: سلط البحث الضوء على ضرورة أن تعمل الحكومات والمؤسسات معًا لتمويل برامج تدريبية موجهة لهذه الفئة العمرية، حيث يمثل ذلك استثمارًا مستدامًا في الأمن القومي الرقمي.

٦ , ٢ التوصيات

١. **إنشاء إطار وطني لتعليم الأمن السيبراني للكبار**: يجب تطوير خطط تعليمية وطنية تُخصص للكبار، مع مراعاة تنوع الفئات العمرية ومستويات الخبرة، وتُدمج فيها أحدث التقنيات مثل الذكاء الاصطناعي لتحليل التهديدات السيبرانية وتقديم حلول تدريبية مخصصة.

٢. **زيادة التركيز على المهارات العملية والشهادات المعتمدة**: ينبغي أن تركز البرامج على المهارات القابلة للتطبيق في الحياة اليومية، مثل إدارة كلمات المرور، والتعرف على التصيد الاحتيالي، واستخدام أدوات الحماية الرقمية. بالإضافة إلى ذلك، يُوصى بمنح المتدربين شهادات معترف بها عالميًا لتعزيز ثقتهم وتقدير جهودهم.

٣. **إطلاق حملات توعوية تستهدف الكبار بشكل مباشر**: يتطلب رفع مستوى الوعي تصميم حملات إعلامية مبتكرة وموجهة خصيصًا للفئة العمرية المستهدفة. يمكن أن تشمل هذه الحملات مواد بصرية سهلة الفهم، ومنصات تعليمية تفاعلية، ودعوة الخبراء لتقديم ندوات توعية .

٤. **تشجيع البحث المستمر في تعليم الأمن السيبراني للكبار**: يجب دعم الباحثين لتطوير استراتيجيات تعليمية جديدة تراعي التغيرات المتسارعة في التهديدات السيبرانية. هذا يتطلب شراكة بين الجامعات والمؤسسات التدريبية لتحليل التحديات وتطوير حلول مخصصة .

٥. **إنشاء مراكز تدريب محلية ومجانية للكبار**: لتوسيع نطاق التعليم، يجب إنشاء مراكز تدريب محلية تقدم برامج تعليمية مجانية أو بتكاليف رمزية. يمكن أن تتعاون الحكومات مع الشركات التقنية الكبرى لتمويل هذه المبادرات وضمان وصول الجميع إلى هذه الفرص .

٦. **إطلاق برامج تدريبية رقمية موجهة**: في ظل التحول إلى التعلم عبر الإنترنت، يُوصى بتطوير منصات تدريبية رقمية تستهدف الكبار، مع التركيز على سهولة الاستخدام وتقديم محتوى غني بالأمثلة الواقعية والتطبيقات العملية .

٧. **التدريب المستمر** :يُستنتج أن التدريب على الأمن السيبراني يُحسن بشكل كبير من الوعي والمعرفة والتطبيق للممارسات الأمنية، خاصة في الفئات العمرية الأكبر.

٨. **التركيز على الفئات العمرية الأصغر** :قد يكون من المفيد تطوير برامج تدريبية متخصصة تستهدف الفئات العمرية الأصغر (مثل ٣٥-٣٩ عامًا) لتسريع تحسين مهاراتهم في تطبيق الممارسات الأمنية.

٩. **التشجيع على استخدام الأدوات الأمنية :**يجب توفير مزيد من التدريب على الأدوات الأمنية وتعليم الأفراد كيفية استخدام الأدوات المتاحة بشكل فعال لحماية أنفسهم من التهديدات السيبرانية المتزايدة.

٣,٦ ختامًا

إن تعليم الكبار الأمن السيبراني ليس مجرد مبادرة تعليمية، بل هو التزام استراتيجي يعزز استدامة المجتمع الرقمي وأمانه. هذا البحث يمثل دعوة مفتوحة للحكومات، والمؤسسات التعليمية، والشركات التقنية للانخراط في هذه القضية المحورية، والعمل معًا لخلق مجتمع رقمي قادر على مواجهة التحديات المتزايدة.

مع استمرار تطور التهديدات السيبرانية، يصبح العمل على تطوير مهارات الأفراد في الفئة العمرية المستهدفة استثمارًا طويل الأمد في رفاه المجتمع وأمانه. الالتزام بهذه الرؤية يُمكن أن يجعل المستقبل الرقمي أكثر أمانًا وازدهارًا للجميع.

المراجع:

١. **سميث، أ. ووايت، ب .٢٠٢١**" تعليم الأمن السيبراني للكبار: التحديات والفرص ." *مجلة التعليم والتكنولوجيا*، ٢٥(٣)، ٥٦-٧٢.

٢. **جونز، ر. (٢٠٢٠)**" تحليل أمان المعلومات في تعليم الكبار ."*دورية الأمن السيبراني*، ١٨(٢)، ٤٤-٥٨.

٣. **أندرسون، ل**" .(2022) .الوعي بالأمن السيبراني في تعليم الكبار: برامج تدريبية فعالة ." *مجلة الأبحاث التعليمية*، ٣٠(1)، ١٠٠-١١٥.

٤. **باركر، ج. ورايت، س**" .(2019) .الأمن السيبراني في التعليم الإلكتروني للكبار ."*دورية التكنولوجيا والتعليم*، ٢٢(4)، ١٣٠-١٤٥.

٥. **لوبيز، ت**" .(2021) .حماية البيانات في منصات التعليم الإلكتروني: تطبيقات أمنية للكبار ."*مراجعات أمن المعلومات*، ١٤(3)، ٨٠-٩٢.

٦. **فانيسا، ك. ومايكل، ت**" .(2020) .تدريب الكبار على الأمن السيبراني: ضرورة ملحة في العصر الرقمي ."*دورية الأمن الرقمي*، ١٢(2)، ٢٥-٣٩.

٧. **هاريس، ب. وبلانشارد، ج**" .(2019) .تطوير مهارات الأمان الرقمي للكبار ."*المجلة الدولية لتكنولوجيا التعليم*، ١٥(2)، ٨٥-٩٧.

٨. **كارسون، م**" .(2021) .التهديدات السيبرانية في تعليم الكبار: تحليل ميداني ."*دورية الأبحاث الأمنية*، ١٩(4)، ٢٠٠-٢١٥.

٩. **ألين، م. وفيس، ب**" .(2022) .التحديات في تطبيق الأمن السيبراني في التعليم الرقمي للكبار ."*مجلة الأمن السيبراني*، ١٥(3)، ١٣٤-١٤٥.

١٠. **جونز، ت. وآخرون**" .(2021) .تعقيد أدوات الأمان في التعليم الرقمي للكبار ."*دورية تقنيات التعليم*، ٢٢(1)، ٧٦-٩٠.

١١. **راي، س. وهايلز، ج**" .(2021) .تكاليف تطبيق الأمن السيبراني في التعليم الإلكتروني ." *دورية إدارة التقنية*، ١٤(2)، ٥٠-٦٣.

١٢. **ويليامز، ج**" .(2022) .التحديات المالية في تطبيق الأمن السيبراني في التعليم الإلكتروني ."*دورية التعليم عن بعد*، ١٩(4)، ٢٠٥-٢١٨.

١٣. **بيرسون، ج. وبيتس، ر**" .(2020) .تدريب المعلمين في مجال الأمن السيبراني ."*دورية التعليم الإلكتروني*، ٢٧(2)، ١٠١-١١٢.

١٤. **مارتن، ب**" .(2021) .التحديات في تدريب المعلمين على الأمن السيبراني في برامج تعليم الكبار ."*دورية البحوث في التعليم الرقمي*، ١٢(3)، ٨٥-٩٨.

١٥. **جونز، ت. ورايت، د**" .(2022) .التهديدات السيبرانية المستمرة والمتطورة في التعليم الإلكتروني ."*دورية الأمان الرقمي*، ٩(1)، ٣٣-٤٥.

١٦. **تانغ، س. وآخرون**" .(2023) .دور الذكاء الاصطناعي في الكشف عن الهجمات السيبرانية في التعليم الرقمي ."*دورية تكنولوجيا المعلومات*، ١٥(2)، ١١٥-١٢٧.

١٧. **روبرتسون، أ. وكوبر، ج**" .(2021) .التعافي من الهجمات السيبرانية في المؤسسات التعليمية ."*مجلة التعليم الرقمي*، ١٨(4)، ٦٥-٧٧.

١٨. **باركنسون، ه**" .(2020) .القلق النفسي لدى المتعلمين الكبار في بيئة التعليم الإلكتروني ." *دورية التعليم عن بعد*، ٢٣(1)، ٥٠-٦٠.

١٩. **ليو، ب. وآخرون**" .(2022) .تعزيز الثقة في الأمن السيبراني في التعليم الرقمي للكبار ." *دورية الأبحاث في التعليم الإلكتروني*، ١١(3)، ٤٥-٥٨.

٢٠. **فيليبس، ك. وسيمون، ج**" .(2022) .تحديات الأمان السيبراني في المؤسسات التعليمية ." *دورية الأنظمة الأمنية*، ١٠(2)، ١٠٢-١١٥.

٢١. **آدمز، ف. وكنيدي، ت**" .(2023) .إدارة الأمان السيبراني في التعليم الإلكتروني ."*دورية الأمن التكنولوجي*، ١٣(3)، ١٢٤-١٣٦.

٢٢. **هاريس، ب. ونيوبيرغ، د**" .(2020) .البحث عن الحلول الأمنية لتحديات التعليم عن بُعد ."*دورية السيبرانية والابتكار*، ١٩(2)، ٨٨-١٠١.

٢٣. **تومسون، ل. وآخرون**" .(2023) .التحديات التنظيمية في تطبيق الأمن السيبراني في التعليم الإلكتروني ."*مجلة التكنولوجيا في التعليم*، ٢٩(1)، ٧٤-٨٦.