

تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية مسح التعليم الجامعي: المملكة العربية السعودية

إسم الطالبة: جنان حسين المحيسن

مشروع التخرج-1

كلية الإدارة-جامعة ميداوون

إشراف:

د. منى مصطفى العشري

عضو هيئة التدريس - كلية الإدارة - جامعة ميداوون

الفصل الدراسي الأول- 2024



الشكر والتقدير

الحمد لله الذي وهبنا نعمة العقل والفكر، ومنّ علينا بنور العلم والمعرفة، والصلاة والسلام على أشرف المرسلين، سيدنا محمد وعلى آله وصحبه أجمعين.

أبدأ رسالتي بواجب الشكر لله تعالى، خالق الكون وخالق الإنسان، الذي علم الإنسان بالقلم ما لم يعلم، فهو سبحانه وتعالى المنان الذي لا ينقطع فضله، الملك القدوس السلام، مدبر الليالي والأيام، مصرف الشهور والأعوام، قدر الأمور فأجراها على أحسن نظام، ما شاء الله كان ومالم يشأ لم يكن، له الحمد والشكر على ما أنعم به على من فضله الخير الكثير والعلم الوفير، وأعانني على إنجاز هذا العمل الذي احتسبه عبادة من العبادات جعلها الله خالصة لوجهه الكريم.

أتقدم بخالص الشكر وعظيم الامتنان للدكتورة منى مصطفى العشري، أستاذة البحث، على ما قدمته لي من علم نافع وعطاء متميز وإرشاد مستمر، وعلى ما بذلته من جهد متواصل ونصح وتوجيه من بداية مرحلة البحث حتى إتمام هذه العمل.

مهما كتبت من عبارات وجمل فإن كلمات الشكر تظل عاجزة عن إيفاء حقها، فجزاها الله عني خير الجزاء وجعل ذلك في موازين حسناتها.

أرفع أسمى عبارات الشكر والتقدير إلى والديّ العزيزين اللذين غرسا فيّ حب العلم من الصغر، وقدا لي كل غالي ونفيس، وكان لهما الفضل بعد الله فيما وصلت إليه الآن. فلا أملك إلا الدعاء لهما بطول العمر وحسن العمل وبلوغ الجنان.

أشكر معالي مدير جامعة ميدا وشن وإلى جميع هيئة التدريس بجامعة ميدا وشن على ما قدموه لي من دعم وتشجيع خلال مسيرتي الدراسية.

أشكر كل من مد لي يد العون، أو أسدى لي معروفاً أو قدم لي نصيحة، أو كانت له إسهامه صغيرة أو كبيرة في إنجاز هذا العمل. فله مني خالص الشكر والتقدير.

أختم رسالتي بالحمد لله رب العالمين أولاً وآخراً، ظاهراً وباطناً، عدد خلقه ورضا نفسه وزنة عرشه ومداد كلماته، والصلاة والسلام على نبينا محمد وعلى آله وصحبه أجمعين.

اهداء

من قال "أتى لها" نالها

لم تكن الرحلة قصيرة، بل ولم يكن من المفترض أن تكون كذلك. لم يكن الحلم قريباً، ولم يكن الطريق ممهداً بالورود، لكنني فعلتها

الحمد لله حباً وشكراً وامتناناً، بفضلها أنا اليوم أنظر إلى حلم طال انتظاره، وقد أصبح واقعاً أفخر به.

إلى ملاكي الطاهر، وقوتي بعد الله، داعمتي الأولى والأبدية (أمي)، أهديك هذا الإنجاز الذي لولا تضحياتك لما كان له وجود. ممتنة لأن الله اصطفاك لي من بين البشر، فأنت خير سند وعوض.

إلى من دعمني بلا حدود وأعطاني بلا مقابل (أبي العزيز)، شكراً لك على إيمانك بي ودعمك لي في كل خطوة على طريق الحياة.

إلى من قال فيهم {سَنَشُدُّ عَضُدَكَ بِأَخِيكَ} إخواني، أدامكم الله ضلعاً ثباتاً لي، شكراً لكم على وجودكم في حياتي، وعلى كل ما تقدمونه لي من حبٍ ودعمٍ.

إلى (أخواتي العزيزات)، أنتم سندي في الشدائد، ورفيقاتي في كل لحظات الحياة. شكراً لكن على حبكم ودعمكم ليالي من آمنت بقدراتي (رفيقة دربي)، شكراً لك على إيمانك بي، ودعمك لي في كل وقتٍ وحينٍ.

أهديكم جميعاً هذا الإنجاز، ثمرة جهودي

والله ولي التوفيق.

شكر وتقدير

مستخلص

تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية ضروري لضمان سلامة وحماية البيانات والأنظمة في البيئة الجامعية في المملكة العربية السعودية. تعتبر المؤسسات التعليمية هدفاً محتملاً للهجمات السيبرانية نظراً للكمية الكبيرة من المعلومات الحساسة المخزنة فيها وتأثير هذه الهجمات على العملية التعليمية.

تتضمن خطوات تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية تحديد الأصول الحاسوبية وتصنيفها وتقييم الثغرات والتهديدات المحتملة وتحديد مدى تأثيرها واحتمالية حدوثها. ينبغي للمؤسسات التعليمية تنفيذ سياسات وإجراءات أمنية قوية مثل إدارة هوية المستخدمين وحماية البيانات وتشفيرها وتحديث البرامج، والأنظمة بانتظام، وتوفير التدريب، والتوعية.

تحليل مخاطر الأمن السيبراني يساعد المؤسسات التعليمية في تعزيز أمان البيئة التعليمية وحماية البيانات الحساسة للطلاب وأعضاء هيئة التدريس. يساعد أيضاً في الحد من تأثير الاختراقات السيبرانية مثل تسريب البيانات الشخصية والتجسس الصناعي وتلاعب النتائج الأكاديمية.

باختصار، تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية في المملكة العربية السعودية يعتبر جزءاً هاماً من استراتيجية حماية المعلومات والأنظمة. من خلال تحليل المخاطر وتنفيذ التدابير الأمنية الملائمة، يمكن للمؤسسات التعليمية تعزيز أمان البيئة الجامعية وضمان الحفاظ على خصوصية وسلامة المعلومات في سياق التعليم الجامعي في المملكة العربية السعودية.

المحتويات

١	المقدمة
٣	مشكلة البحث
٤	أهمية البحث
٥	أسئلة البحث
٦	اهداف البحث
٧	فرضيات البحث
٨	نموذج البحث
٩	منهجية البحث
١٠	الدراسة الميدانية
١٣	هيكل المشروع

(الفصل الأول) الإطار النظري

١٤	• الامن السيبراني
١٥	• تدابير الامن السيبراني
١٨	• أهمية الامن السيبراني في المؤسسات التعليمية

(الفصل الثاني) مسح التعليم الجامعي في المملكة العربية السعودية

١٩	• نظرة عامة على التعليم الجامعي في المملكة العربية السعودية
٢٠	• التدابير الامن السيبراني الجامعات السعودية
٢١	• التحديات التي تواجه الجامعات السعودية
٢٤	• التفاصيل الإضافية حول امن السيبراني في الجامعات السعودية

(الفصل الثالث) تحليل البيانات

٢٦	• تحليل المقابلات مع خبراء الامن السيبراني
٢٧	• تفسير نتائج التحليل
٢٨	• أدوات تحليل المحتوى

(الفصل الرابع) النتائج والتوصيات

٢٩	• اهم النتائج التي توصل اليها البحث
٣٠	• توصيات لتحسين الامن السيبراني في الجامعات السعودية
٣١	الدراسات السابقة
٣٢	الملخص
٣٤	الخاتمة

تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية

المقدمة:

العالم الرقمي :

يشهد العالم اليوم ثورة رقمية هائلة، حيث أصبحت تقنيات المعلومات والاتصالات جزءاً لا يتجزأ من جميع جوانب الحياة، بما في ذلك التعليم. ونتيجة لذلك، أصبحت المؤسسات التعليمية عرضة لمخاطر الأمن السيبراني بشكل متزايد.

مخاطر متزايدة :

تشمل مخاطر الأمن السيبراني التي تواجهها المؤسسات التعليمية ما يلي:

- **الاختراقات الإلكترونية:** يمكن للقراصنة اختراق أنظمة المؤسسات التعليمية وسرقة البيانات الحساسة، مثل معلومات الطلاب والموظفين.
- **البرامج الضارة:** يمكن لنشر البرامج الضارة على أجهزة الكمبيوتر التابعة للمؤسسات التعليمية أن يؤدي إلى تلف البيانات أو تعطيل الخدمات.
- **هجمات الحرمان من الخدمة:** يمكن استخدام هجمات الحرمان من الخدمة لتعطيل مواقع المؤسسات التعليمية على الإنترنت مما يمنع الطلاب والموظفين من الوصول إلى المعلومات والخدمات.
- **التنمر الإلكتروني:** يمكن استخدام الإنترنت لتنمر الطلاب على بعضهم البعض، مما قد يؤدي إلى مشاكل نفسية واجتماعية.

تأثيرات واسعة:

لا تقتصر مخاطر الأمن السيبراني على المؤسسات التعليمية فقط، بل يمكن أن تؤثر أيضاً على :

- **الطلاب :** قد تسرق بياناتهم الشخصية أو تُستخدم لارتكاب جرائم.
- **الموظفون :** قد تُسرق بياناتهم الشخصية أو تستخدم لابتزازهم.
- **المؤسسات التعليمية:** قد تلحق الضرر بسمعتها أو تُجبر على دفع غرامات كبيرة

حاجة ملحة للحلول :

في ظل هذه التحديات، هناك حاجة ملحة لتطوير حلول فعالة لضمان الأمن السيبراني في المؤسسات التعليمية تتضمن بعض الحلول :

- **رفع مستوى الوعي :** نشر الوعي بمخاطر الأمن السيبراني بين الطلاب والموظفين.
- **تطوير البنية التحتية:** الاستثمار في تطوير البنية التحتية لتقنية المعلومات والاتصالات لجعلها أكثر أمانًا.
- **تطبيق تدابير الأمن السيبراني:** تطبيق تدابير الأمن السيبراني الفعالة، مثل جدران الحماية وبرامج مكافحة الفيروسات.
- **التعاون مع الجهات الخارجية:** التعاون مع الجهات الخارجية مثل الشركات الخاصة والحكومة، لتحسين الأمن السيبراني.

المسؤولية المشتركة:

يقع ضمان الأمن السيبراني في المؤسسات التعليمية على عاتق جميع الأطراف المعنية، بما في ذلك :

- **الطلاب:** يجب على الطلاب أن يكونوا على دراية بمخاطر الأمن السيبراني وأن يتخذوا خطوات لحماية أنفسهم.
- **الموظفون:** يجب على الموظفين اتباع ممارسات الأمن السيبراني الجيدة وحماية البيانات الحساسة.
- **المؤسسات التعليمية:** يجب على المؤسسات التعليمية الاستثمار في تطوير حلول الأمن السيبراني وتطبيقها بشكل فعال.

مستقبل التعليم:

يعتمد مستقبل التعليم على قدرة المؤسسات التعليمية على ضمان أمن أنظمتها وبياناتها من خلال العمل معاً، يمكن لجميع الأطراف المعنية خلق بيئة تعليمية آمنة وفعالة للجميع.

مشكلة البحث :

تعد مخاطر الأمن السيبراني من أهم التحديات التي تواجهها المؤسسات التعليمية في المملكة العربية السعودية تشمل هذه المخاطر:

• الاختراقات الإلكترونية :

يمكن للقراصنة اختراق أنظمة المؤسسات التعليمية وسرقة البيانات الحساسة، مثل معلومات الطلاب والموظفين.

• البرامج الضارة:

يمكن لنشر البرامج الضارة على أجهزة الكمبيوتر التابعة للمؤسسات التعليمية أن يؤدي إلى تلف البيانات أو تعطيل الخدمات.

• هجمات الحرمان من الخدمة :

يمكن استخدام هجمات الحرمان من الخدمة لتعطيل مواقع المؤسسات التعليمية على الإنترنت، مما يمنع الطلاب والموظفين من الوصول إلى المعلومات والخدمات.

• التنمر الإلكتروني :

يمكن استخدام الإنترنت لتنمر الطلاب على بعضهم البعض، مما قد يؤدي إلى مشاكل نفسية واجتماعية.

أهمية البحث:

- سيساعد هذا البحث في فهم مخاطر الأمن السيبراني التي تواجهها الجامعات السعودية بشكل أفضل.
- سيساعد هذا البحث في تحديد تدابير الأمن السيبراني التي يجب على الجامعات السعودية تطبيقها.
- سيساعد هذا البحث في التغلب على التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني.
- سيساعد هذا البحث في تحسين الأمن السيبراني في الجامعات السعودية، مما سيحمي البيانات الحساسة للطلاب والموظفين.

أسئلة البحث :

- ما هي أهم مخاطر الأمن السيبراني التي تواجهها الجامعات السعودية؟
- ما ما هي تدابير الأمن السيبراني التي تتخذها الجامعات السعودية لحماية أنظمتها وبياناتها ؟
- ما هي التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني ؟
- ما هي أفضل الممارسات لتحسين الأمن السيبراني في الجامعات السعودية؟

اهداف البحث:

- لتحديد مخاطر الامن السيبراني التي يواجهها المؤسسات التعليمية بالمملكة العربية السعودية.
- لتحديد اهم التحديات التي يواجهها المؤسسات التعليمية في المملكة العربية السعودية.
- لاكتشاف الحلول التطويرية لضمان الامن السيبراني المؤسسات التعليمية في المملكة العربية السعودية.

فرضيات البحث:

١. فرضيات رئيسية:

- الفرضية الأولى: تواجه الجامعات السعودية مخاطر عالية من الأمن السيبراني.
- الفرضية الثانية: لا تتخذ الجامعات السعودية تدابير كافية لحماية أنظمتها وبياناتها من مخاطر الأمن السيبراني.
- الفرضية الثالثة: هناك العديد من التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني.

٢. فرضيات فرعية:

- الفرضية الفرعية الأولى: أكثر مخاطر الأمن السيبراني شيوعاً التي تواجهها الجامعات السعودية هي الاختراقات الإلكترونية.
- الفرضية الفرعية الثانية: لا تمتلك الجامعات السعودية الموارد المالية أو البشرية الكافية لتطبيق تدابير الأمن السيبراني الفعالة.
- الفرضية الفرعية الثالثة: نقص الوعي بمخاطر الأمن السيبراني هو أحد أهم التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني.

نموذج البحث:

١. المتغيرات:

- المتغير المستقل: مخاطر الأمن السيبراني.
- المتغير التابع: تدابير الأمن السيبراني التي تتخذها الجامعات السعودية.
- المتغيرات المتداخلة الموارد المالية والبشرية الوعي بمخاطر الأمن السيبراني، البنية التحتية لتقنية المعلومات والاتصالات.

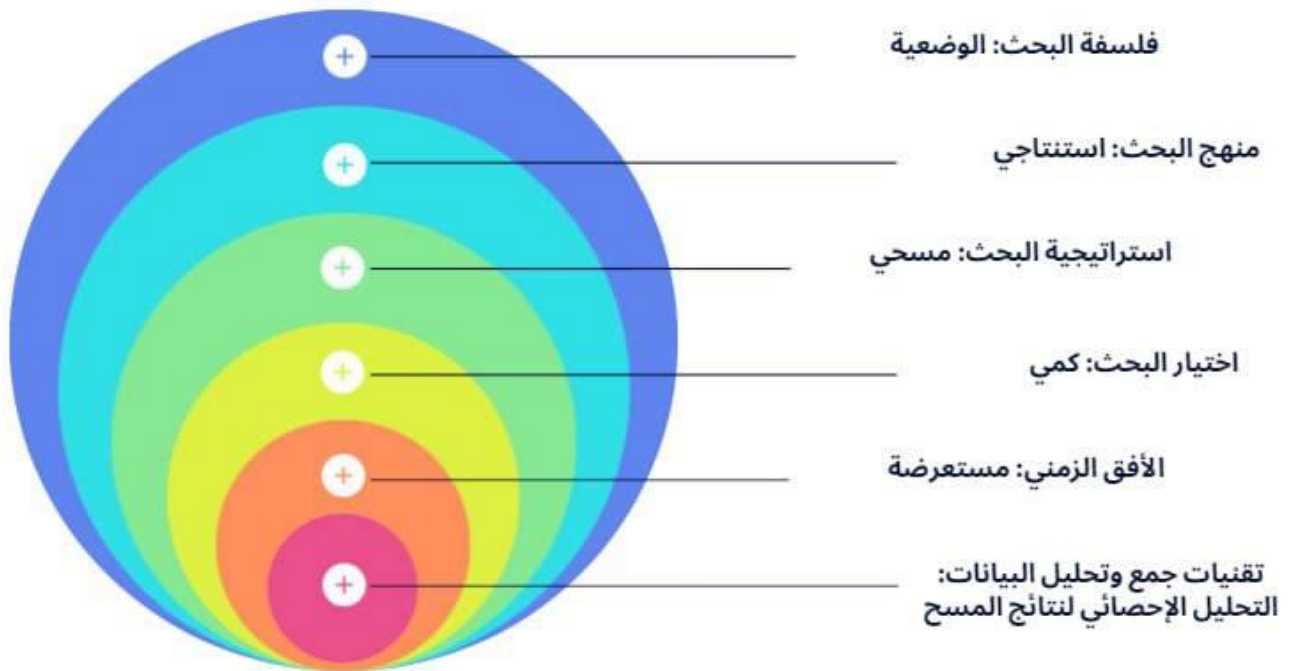
٢. العلاقات بين المتغيرات:

- العلاقة بين المتغير المستقل والمتغير التابع: تؤثر مخاطر الأمن السيبراني بشكل مباشر على تدابير الأمن السيبراني التي تتخذها الجامعات السعودية.
- العلاقة بين المتغيرات المتداخلة والمتغير التابع: تؤثر المتغيرات المتداخلة على قدرة الجامعات السعودية على تطبيق تدابير الأمن السيبراني.

منهجية البحث:

في هذي الدراسة، سيعتمد الباحث على منهجية البحث التحليلي الوصفي.

مخطط بصلة البحث



الدراسة الميدانية:

١. عنوان المشروع:

تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية دراسة حالة التعليم الجامعي في المملكة العربية السعودية

• مدة المشروع:

٦ أشهر

٢. خطوات المشروع:

أ. المرحلة التحضيرية:

- مراجعة الأدبيات ذات الصلة بمخاطر الأمن السيبراني في المؤسسات التعليمية.
- تحديد الجامعات السعودية التي سيتم دراستها.
- تصميم أدوات جمع البيانات.

ب. مرحلة جمع البيانات:

- إجراء مقابلات مع خبراء الأمن السيبراني في الجامعات السعودية.
- تحليل وثائق الجامعات السعودية المتعلقة بالأمن السيبراني.

ت. مرحلة تحليل البيانات:

- تحليل البيانات التي تم جمعها باستخدام التحليل الإحصائي.
- تفسير نتائج التحليل.

ث. مرحلة كتابة التقرير:

- كتابة تقرير نهائي يتضمن نتائج البحث وتوصياته.

٣. المخاطر والتحديات:

- نقص التعاون من قبل الجامعات السعودية.
- صعوبة الحصول على البيانات.
- نقص الموارد المالية والبشرية.

٤. خطة لإدارة المخاطر والتحديات:

- التواصل الفعال مع الجامعات السعودية.
- استخدام أدوات جمع البيانات المختلفة.
- البحث عن مصادر تمويل إضافية.

٥. نتائج المشروع المتوقعة:

- فهم أفضل لمخاطر الأمن السيبراني التي تواجهها الجامعات السعودية.
- توصيات لتحسين الأمن السيبراني في الجامعات السعودية.

٦. الفوائد المتوقعة من المشروع:

- تحسين الأمن السيبراني في الجامعات السعودية.
- حماية البيانات الحساسة للطلاب والموظفين.
- تعزيز الثقة في المؤسسات التعليمية.

٧. خطة لنشر نتائج المشروع:

- نشر التقرير النهائي في مجلات علمية محكمة.
- تقديم نتائج البحث في مؤتمرات علمية.
- مشاركة نتائج البحث مع الجامعات السعودية والجهات الحكومية والقطاع الخاص.

الجدول الزمني للمشروع:

النشاط	المدة
مراجعة الأدبيات	1 شهر
تحديد الجامعات السعودية	1 شهر
تصميم أدوات جمع البيانات	1 شهر
جمع البيانات	2 شهر
تحليل البيانات	1 شهر
كتابة التقرير	1 شهر

هيكل المشروع:

الفصل الأول: الإطار العام للدراسة

الفصل الثاني: الإطار النظري

الفصل الثالث: منهجية البحث

الفصل الرابع: التحليل الإحصائي

الفصل الخامس: المناقشة والخاتمة

الفصل الأول

الأمن السيبراني:

الأمن السيبراني هو عملية حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. تهدف هذه الهجمات عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها.

أهدافه:

- حماية البيانات الحساسة.
- ضمان استمرارية الخدمات.
- حماية سمعة المؤسسة.

مخاطر الأمن السيبراني:

١. الهجمات الإلكترونية.

- الاختراقات الإلكترونية اختراق أنظمة المؤسسات وسرقة البيانات.
- البرامج الضارة: نشر برامج ضارة على أجهزة الحاسوب لإتلاف البيانات أو تعطيل الخدمات.
- هجمات الحرمان من الخدمة: تعطيل مواقع المؤسسات على الإنترنت.

٢. الهجمات الاجتماعية:

- الاحتيال الإلكتروني: خداع الأشخاص للكشف عن معلوماتهم الشخصية أو المالية.
- التصيد الاحتيالي: إرسال رسائل بريد إلكتروني أو رسائل نصية تبدو وكأنها من مصدر موثوق به لخداع الأشخاص للكشف عن معلوماتهم الشخصية.
- الهندسة الاجتماعية: استخدام التلاعب النفسي لخداع الأشخاص للكشف عن معلوماتهم الشخصية أو اتخاذ إجراءات غير آمنة.

٣. الداخلية:

- الأخطاء البشرية: الأخطاء التي قد يرتكبها الموظفون، مثل الكشف عن معلومات سرية عن طريق الخطأ أو استخدام كلمة مرور ضعيفة.
- السلوكيات الخبيثة: سلوكيات الموظفين الخبيثة، مثل سرقة البيانات أو تعطيل أنظمة المؤسسة.

تدابير الأمن السيبراني:

١. التدابير الوقائية:

- جدران الحماية: برامج تمنع الوصول غير المصرح به إلى أنظمة المؤسسة.
- برامج مكافحة الفيروسات: برامج تكتشف وتزيل البرامج الضارة.
- تحديثات البرامج: تحديث البرامج بانتظام لإصلاح الثغرات الأمنية.
- كلمات المرور القوية: استخدام كلمات مرور قوية يصعب تخمينها.
- التوعية بمخاطر الأمن السيبراني: توعية الموظفين بمخاطر الأمن السيبراني وكيفية حماية أنفسهم.

٢. التدابير الرقابية:

- مراقبة الشبكة: مراقبة حركة الشبكة لاكتشاف الأنشطة المشبوهة.
- اختبار الاختراق: اختبار أنظمة المؤسسة بانتظام للعثور على الثغرات الأمنية.
- التحليل الجنائي الرقمي: التحقيق في الهجمات الإلكترونية لتحديد مصدرها وتأثيرها.

٣. تدابير الاسترداد:

- النسخ الاحتياطي للبيانات: الاحتفاظ بنسخ احتياطية من البيانات المهمة في مكان آمن.
- خطط الاسترداد من الكوارث: خطط لإعادة تشغيل أنظمة المؤسسة في حالة وقوع هجوم إلكتروني.

- تحديد السياسات والإجراءات ينبغي للمؤسسات والمنظمات والأفراد وضع سياسات وإجراءات أمنية فعالة لحماية البيانات والأنظمة الإلكترونية. يشمل ذلك تحديد صلاحيات الوصول، وتنفيذ تحديثات الأمان، وإجراء نسخ احتياطية منتظمة، وتوفير التدريب والتوعية الأمنية للموظفين والمستخدمين.
- استخدام التشفير: ينبغي استخدام تقنيات التشفير لحماية البيانات الحساسة والاتصالات الإلكترونية. يمكن استخدام التشفير في الاتصالات عبر الإنترنت وتخزين البيانات وحماية الأجهزة المحمولة.
- تحديث وإدارة البرمجيات: يجب تحديث الأنظمة والبرمجيات بانتظام لتصحيح الثغرات الأمنية المعروفة وتحسين الأمان. ينبغي أيضًا إدارة البرمجيات بشكل فعال من خلال تثبيت التصحيحات وتقييد البرمجيات غير المصرح بها.
- رصد الأمان والاستجابة: يجب إنشاء نظام لرصد الأنشطة السيبرانية غير العادية واكتشاف التهديدات المحتملة. يتطلب ذلك استخدام أدوات رصد الأمان وتحليل السجلات وتطبيق إجراءات استجابة فورية لمواجهة الهجمات والتهديدات.
- التوعية والتدريب يجب توفير التدريب والتوعية الأمنية للموظفين والمستخدمين للتعرف على التهديدات السيبرانية وممارسات الأمان السليمة. يشمل ذلك التوعية حول البريد الإلكتروني المشبوه والرسائل الاحتيالية وتقنيات الهندسة الاجتماعية.
- الاحتفاظ بنسخ احتياطية: ينبغي إجراء نسخ احتياطية منتظمة للبيانات للحماية من فقدان البيانات أو تلفها نتيجة لهجمات أو أخطاء فنية.

- أمن الشبكات: يشير إلى حماية الشبكات المؤسسية والاتصالات بين الأجهزة. يشمل ذلك تأمين الجدران النارية والتأكد من أن الشبكات محمية بكلمات مرور قوية واستخدام تقنيات الكشف عن التسلل والتصدي للهجمات.
- أمن الأجهزة: يتعلق بحماية الأجهزة الإلكترونية مثل الحواسيب والهواتف المحمولة والأجهزة الذكية. يشمل ذلك تأمين الأجهزة بكلمات مرور وتشفير البيانات المخزنة عليها وتحديث البرامج والتطبيقات بانتظام.
- أمن البرمجيات: يتعلق بحماية البرمجيات من الثغرات الأمنية والبرامج الخبيثة. يشمل ذلك تحديث البرامج بصورة منتظمة لتصحيح الثغرات الأمنية المعروفة واستخدام برامج مكافحة الفيروسات والحماية من البرمجيات الخبيثة.
- أمن المعلومات: يتعلق بحماية البيانات والمعلومات الحساسة من الوصول غير المصرح به والاستخدام غير المشروع. يشمل ذلك تنفيذ سياسات الوصول والتحكم في الصلاحيات وتشفير البيانات واستخدام تقنيات الحماية المتقدمة مثل التوقيع الرقمي والتوثيق المزدوج.
- أمن السحابة يشمل حماية البيانات والتطبيقات والموارد المخزنة والمستضاف على السحابة. يتطلب تأمين السحابة استخدام تقنيات التشفير والتحقق من الهوية والتحكم في الوصول ومراقبة النشاطات غير العادية.
- الاستجابة للحوادث: يتعلق بالتصدي للحوادث الأمنية والتعامل معها بفعالية. يشمل ذلك إنشاء خطة استجابة للحوادث وتوفير فريق استجابة للتحقيق في الحوادث واستعادة النظام وتقييم الأضرار وتعزيز الأمان لتجنب تكرارها في المستقبل.
- التعاون والمشاركة: يعتبر التعاون بين الجهات المختلفة ومشاركة المعلومات الأمنية ذات أهمية كبيرة في مجال الأمن السيبراني. يشمل ذلك التعاون مع الحكومة والمؤسسات الأخرى والمشاركة في منصات ومبادرات.

أهمية الامن السيبراني في المؤسسات التعليمية

تحديث البرامج والتطبيقات بانتظام له أهمية كبيرة في مجال الأمان السيبراني وحماية الأنظمة والأجهزة الإلكترونية. إليك بعض الأسباب التي تبرز أهمية تحديث البرامج والتطبيقات بانتظام:

١. إغلاق الثغرات الأمنية: يتم اكتشاف ثغرات أمنية جديدة في البرامج والتطبيقات بشكل مستمر. عند تحديث البرامج بانتظام، يتم إصلاح وإغلاق هذه الثغرات، مما يعني أن النظام يكون أكثر صلابة وأماناً ضد الهجمات السيبرانية.

٢. التصدي للبرمجيات الخبيثة: يُستغل القرصنة الثغرات الأمنية في البرامج والتطبيقات لاختراق الأنظمة وتنفيذ برامج خبيثة. تحديث البرامج يساعد في منع دخول البرمجيات الخبيثة عن طريق تصحيح الثغرات وتحسين الأمان.

٣. تحسين الأداء والوظائف: يتم تحسين البرامج والتطبيقات من خلال التحديثات لتحسين الأداء وإضافة وظائف جديدة بالاستفادة من التحديثات، يمكنك الاستفادة من أحدث الميزات والتحسينات في البرنامج أو التطبيق، مما يعزز تجربتك وقدرتك على الاستخدام الفعال والأمن للأنظمة الرقمية.

٤. التوافق مع التغييرات الأخرى: قد يتطلب تحديث البرامج والتطبيقات توافقاً مع التغييرات الأخرى في النظام الأساسي أو المكونات الأخرى. من خلال التحديث المنتظم، يمكنك ضمان التوافق بين البرامج والتطبيقات والنظام العام، مما يقلل من مشاكل التوافق ويحافظ على استقرار النظام.

٥. الحصول على دعم فني وتحديثات الأمان: عندما تقوم بتحديث البرامج بانتظام، فإنك تستفيد من الدعم الفني المستمر من الشركة المطورة. يمكنك الحصول على دعم فني في حالة وجود أي مشاكل أو استفسارات، بالإضافة إلى تلقي تحديثات الأمان العاجلة التي تحمي النظام من التهديدات الجديدة.

في النهاية، تحديث البرامج والتطبيقات بانتظام يعد إجراءً أساسياً للحفاظ على الأمان والحماية السيبرانية القوية. يوصى بتفعيل التحديثات التلقائية للبرامج والتطبيق يكون هناك تقطع في النص. كانت الجملة الأخيرة هي: " يوصى بتفعيل التحديثات التلقائية للبرامج والتطبيقات للحصول على أحدث التحديثات بشكل مستمر وبدون عناء يدوي.

الفصل الثاني

نظرة عامة على التعليم الجامعي في المملكة العربية السعودية:

- نظام التعليم الجامعي:

يتكون من ٣ مراحل البكالوريوس والماجستير والدكتوراه.

يُشرف على التعليم الجامعي وزارة التعليم.

هناك جامعات حكومية وخاصة.

- عدد الجامعات:

٣٤ جامعة حكومية.

١١ جامعة خاصة.

- عدد الطلاب:

أكثر من ٨٠٠ ألف طالب وطالبة.

- التخصصات:

تتوفر تخصصات متنوعة في مختلف المجالات، مثل العلوم والهندسة والطب والإدارة والأعمال.

مخاطر الأمن السيبراني التي تواجه الجامعات السعودية:

- الهجمات الإلكترونية

اختراق أنظمة الجامعات وسرقة البيانات الحساسة، مثل معلومات الطلاب والموظفين.

نشر البرامج الضارة على أجهزة الحاسوب التابعة للجامعات.

تعطيل مواقع الجامعات على الإنترنت.

■ الهجمات الاجتماعية:

- الاحتيال الإلكتروني على الطلاب والموظفين.
- التصيد الاحتيالي لخداع الطلاب والموظفين للكشف عن معلوماتهم الشخصية.
- التلاعب بالطلاب والموظفين للحصول على معلومات سرية.

● المخاطر الداخلية:

- الأخطاء البشرية من قبل الطلاب والموظفين.
- السلوكيات الخبيثة من قبل بعض الطلاب والموظفين.

تدابير الأمن السيبراني التي تتخذها الجامعات السعودية:

● التدابير الوقائية:

- استخدام برامج مكافحة الفيروسات وجدران الحماية.
- تحديث البرامج بانتظام.
- توعية الطلاب والموظفين بمخاطر الأمن السيبراني.

● التدابير الرقابية:

- مراقبة حركة الشبكة.
- اختبار أنظمة الجامعة بانتظام.

● تدابير الاسترداد:

- الاحتفاظ بنسخ احتياطية من البيانات.
- خطط لإعادة تشغيل أنظمة الجامعة في حالة وقوع هجوم إلكتروني.

- **التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني:**

- **نقص الموارد المالية والبشرية:**

- لا تمتلك العديد من الجامعات الموارد المالية الكافية لتطبيق تدابير الأمن السيبراني الفعالة.
- لا يوجد لدى العديد من الجامعات عدد كاف من الموظفين المتخصصين في الأمن السيبراني.

- **نقص الوعي بمخاطر الأمن السيبراني:**

- لا يدرك العديد من الطلاب والموظفين مخاطر الأمن السيبراني وكيفية حماية أنفسهم.

- **التغيرات في التكنولوجيا:**

- تتطور التكنولوجيا بسرعة، مما يجعل من الصعب على الجامعات مواكبة التهديدات الجديدة.

نظرة عامة على التعليم الجامعي في المملكة العربية السعودية:

- يتمتع التعليم الجامعي في المملكة العربية السعودية بأهمية كبيرة ويعد من أولويات الحكومة السعودية. تسعى الحكومة إلى تعزيز جودة التعليم العالي وتطوير الجامعات والمؤسسات التعليمية، وذلك من خلال استثمارات كبيرة في البنية التحتية والبرامج الأكاديمية والبحث العلمي. تتوفر في المملكة العديد من الجامعات الحكومية والخاصة التي تقدم مجموعة واسعة من التخصصات والبرامج الأكاديمية.

- **مخاطر الأمن السيبراني التي تواجه الجامعات السعودية:**

- مثل العديد من الدول الأخرى، تواجه الجامعات السعودية تحديات في مجال الأمن السيبراني. بسبب الاعتماد المتزايد على التكنولوجيا والشبكات الإلكترونية في العمليات

الأكاديمية والإدارية، تكون الجامعات عرضة للتهديدات السيبرانية المحتملة. تشمل بعض المخاطر المحتملة التي تواجه الجامعات السعودية: اختراق الأنظمة الإلكترونية، سرقة المعلومات الحساسة، القرصنة، التجسس الإلكتروني، وتعطل الخدمات الإلكتروني.

تدابير الأمن السيبراني التي تتخذها الجامعات السعودية:

تتخذ الجامعات السعودية عدداً من التدابير لتعزيز الأمن السيبراني وحماية أنظمتها وبياناتها. تشمل هذه التدابير:

١. تطوير سياسات وإجراءات الأمن السيبراني: تقوم الجامعات بوضع سياسات وإجراءات واضحة لأمن السيبراني لتوجيه الموظفين والطلاب بشأن استخدام التكنولوجيا وتعاملهم مع المعلومات الحساسة.

٢. التدريب والتوعية: تقدم الجامعات التدريب والتوعية المستمرة للموظفين والطلاب حول مخاطر الأمن السيبراني وكيفية التعامل معها، بما في ذلك تعلم كيفية التعرف على رسائل البريد الإلكتروني الاحتيالية والهجمات الإلكترونية الأخرى.

٣. تحديث البرامج والأنظمة: يتم تحديث برامج الحماية وأنظمة الجامعات بشكل منتظم لمواجهة التهديدات السيبرانية الجديدة، وتثبيت التصحيحات التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني: على الرغم من الجهود المبذولة، تواجه الجامعات السعودية تحديات في تنفيذ وتطبيق تدابير الأمن السيبراني.

التحديات التي تواجه الجامعات السعودية

١. **التكلفة:** تطبيق تدابير الأمن السيبراني يتطلب استثمارات مالية كبيرة في تكنولوجيا الحماية وتحديث الأنظمة وتدريب الموظفين. قد يكون من الصعب على الجامعات تخصيص الموارد المالية اللازمة لتلبية هذه التحديات.

٢. **نقص المهارات:** قد يواجه الجامعات نقصاً في المهارات والخبرات المتخصصة في مجال الأمن السيبراني. قد يكون من الصعب توظيف وتدريب الكوادر اللازمة لتنفيذ وإدارة برامج الأمن السيبراني.

٣. **التوافر المستمر:** تتطور تهديدات الأمن السيبراني باستمرار، وبالتالي يتطلب تطبيق تدابير الأمان السيبراني تحديثاً وتحسيناً مستمراً. يجب على الجامعات السعودية التكيف مع هذه التحديات وضمان توافر الإجراءات والتقنيات الحديثة لحماية الأنظمة والبيانات.

٤. **التحديات القانونية والتنظيمية:** تواجه الجامعات تحديات في مجال الامتثال للقوانين واللوائح المتعلقة بالأمن السيبراني، بما في ذلك حماية البيانات الشخصية للطلاب والموظفين. يجب على الجامعات السعودية الالتزام بالتشريعات المحلية ذات الصلة وتوفير الإطار القانوني والتنظيمي اللازم لتعزيز الأمن السيبراني.

التفاصيل الإضافية حول الأمن السيبراني في الجامعات السعودية:

١. التعاون والشراكات: تعمل الجامعات السعودية على تعزيز التعاون والشراكات مع الجهات المعنية بالأمن السيبراني، بما في ذلك الجهات الحكومية والشركات الخاصة والمؤسسات الأكاديمية الأخرى. يتم تبادل المعلومات والخبرات والممارسات الجيدة لتعزيز قدرات الأمن السيبراني في القطاع التعليمي.

٢. الفحص الأمني واختبار الاختراق: تقوم بعض الجامعات بإجراء فحوص أمنية دورية واختبارات اختراق لتحديد الثغرات والضعف في الأنظمة الإلكترونية. يتم استخدام هذه الاختبارات لتحسين أمان الأنظمة وإصلاح أي ثغرات مكتشفة.

٣. الحوسبة السحابية الآمنة: تعتمد بعض الجامعات السعودية على الحوسبة السحابية لتخزين ومعالجة البيانات. يتم اتخاذ إجراءات أمان متقدمة لضمان حماية البيانات المخزنة في السحابة، مثل استخدام تقنيات التشفير وتطبيق سياسات الوصول المناسبة.

٤. إدارة الهوية والوصول: يتم تنفيذ أنظمة إدارة الهوية والوصول في الجامعات للتحكم في الوصول إلى الأنظمة والموارد الحساسة. يتم تطبيق تقنيات مثل تحقق الهوية المتعددة العوامل وإعدادات الصالحيات المتقدمة للحفاظ على أمان البيانات والمعلومات.

٥. رصد واستجابة الأمن: تقوم الجامعات بإنشاء فرق الاستجابة للأمن السيبراني لرصد الأنشطة الاشتباه والتهديدات السيبرانية والتعامل معها بشكل سريع وفعال. يتم استخدام أدوات رصد الأمن وتحليل السجلات والذكاء الاصطناعي لاكتشاف الأنشطة غير العادية والتهديدات الجديدة.

٦. التوعية للمستخدمين: تعتبر التوعية الأمنية للموظفين والطالب عنصراً مهماً في الأمن السيبراني. تقوم الجامعات بتوفير تدريب مستمر للمستخدمين حول ممارسات الأمان السيبراني والوقاية من التهديدات، بما في ذلك التعرف على رسائل الاحتيال الإلكتروني ممكن أيضاً تقديم مزيد من المعلومات حول مواضيع أخرى إذا كنت ترغب في ذلك. فقط أخبرني بالموضوع الذي ترغب في معرفة المزيد عنه.

الفصل الثالث

• تحليل نتائج المقابلات مع خبراء الأمن السيبراني

١. جمع البيانات:

- ❖ إجراء مقابلات مع خبراء الأمن السيبراني من مختلف القطاعات (الحكومة، القطاع الخاص، الأكاديمية).
- ❖ تسجيل المقابلات وتحليلها.

• تحديد الموضوعات الرئيسية والنقاط الهامة التي تم طرحها من قبل الخبراء.

٢. تحليل البيانات:

- ❖ تحليل محتوى المقابلات باستخدام تقنيات تحليل المحتوى مثل: تحليل التردد: تحديد عدد مرات تكرار الكلمات والعبارات.
- ❖ تحليل السياق: فهم معنى الكلمات والعبارات في سياق الجملة والفقرة.
- ❖ تحليل المشاعر: تحديد المشاعر والآراء التي تم التعبير عنها من قبل الخبراء.

٣. تفسير النتائج:

- ❖ تفسير نتائج التحليل لتحديد الاتجاهات الرئيسية والتحديات والفرص في مجال الأمن السيبراني في المملكة العربية السعودية.
- ❖ صياغة النتائج في تقرير مكتوب أو عرض تقديمي.
- ❖ تفسير نتائج التحليل لتحديد نقاط القوة والضعف في برامج الأمن السيبراني في الجامعات السعودية.
- ❖ صياغة النتائج في تقرير مكتوب أو عرض تقديمي.

● تفسير نتائج التحليل:

١. دمج نتائج التحليلات:

- ❖ دمج نتائج تحليل المقابلات مع نتائج تحليل وثائق الجامعات.
- ❖ تحديد أوجه التشابه والاختلاف بين النتائج.

٢. تفسير النتائج:

❖ تفسير النتائج لتحديد:

- الاتجاهات الرئيسية في مجال الأمن السيبراني في المملكة العربية السعودية.
- التحديات التي تواجه المملكة العربية السعودية في مجال الأمن السيبراني.
- الفرص المتاحة للمملكة العربية السعودية في مجال الأمن السيبراني.

٣. صياغة النتائج:

- صياغة النتائج في تقرير مكتوب أو عرض تقديمي.
- تقديم توصيات لتحسين برامج الأمن السيبراني في المملكة العربية السعودية.

أدوات تحليل المحتوى:

- ❖ QDA MINER: أداة تحليل محتوى قوية تدعم العديد من تقنيات تحليل المحتوى مثل تحليل التردد وتحليل السياق وتحليل المشاعر.
- ❖ MAXQDA: أداة تحليل محتوى أخرى شائعة تدعم مجموعة واسعة من ميزات تحليل المحتوى، مثل تحليل النصوص والصور والصوت.
- ❖ NVIVO: أداة تحليل محتوى شائعة الاستخدام في العلوم الاجتماعية، وتدعم تحليل النصوص والصور والصوت والفيديو.
- ❖ ATLAS.TI: أداة تحليل محتوى قوية تدعم تحليل النصوص والصور والصوت والفيديو بالإضافة إلى تحليل الشبكات الاجتماعية.

الفصل الرابع

النتائج والتوصيات

أهم النتائج التي توصل إليها البحث:

- الوعي بالأمن السيبراني:
 - ❖ قلة وعي الطلاب وأعضاء هيئة التدريس بمخاطر الأمن السيبراني.
 - ❖ نقص البرامج التعليمية والتدريبية حول الأمن السيبراني.
- البنية التحتية للأمن السيبراني:
 - ❖ عدم كفاية أنظمة الأمن السيبراني في الجامعات.
 - ❖ نقص الاستثمار في تقنيات الأمن السيبراني.
- الممارسات الأمنية:
 - ❖ عدم اتباع أفضل الممارسات للأمن السيبراني من قبل الطلاب وأعضاء هيئة التدريس.
 - ❖ نقص الوعي بأهمية استخدام كلمات مرور قوية.
- التهديدات السيبرانية:
 - ❖ التعرض لهجمات التصيد الاحتيالي والبرامج الضارة.
 - ❖ اختراق البيانات الشخصية للطلاب وأعضاء هيئة التدريس.

توصيات لتحسين الأمن السيبراني في الجامعات السعودية:

- رفع مستوى الوعي:
 - ❖ تنظيم حملات توعية حول مخاطر الأمن السيبراني.
 - ❖ تقديم برامج تعليمية وتدريبية حول الأمن السيبراني للطلاب وأعضاء هيئة التدريس.
- تحسين البنية التحتية للأمن السيبراني:
 - ❖ الاستثمار في تقنيات الأمن السيبراني الحديثة.
 - ❖ توظيف خبراء الأمن السيبراني لإدارة أنظمة الأمن السيبراني.
- تعزيز الممارسات الأمنية:
 - ❖ تطبيق أفضل الممارسات للأمن السيبراني في جميع أنحاء الجامعة.
 - ❖ إلزام الطلاب وأعضاء هيئة التدريس باستخدام كلمات مرور قوية.
- التعاون مع الجهات الخارجية:
 - ❖ التعاون مع الجهات الحكومية والخاصة لتحسين الأمن السيبراني في الجامعات.
- موضوع البحث:
 - ❖ تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية: مسح التعليم الجامعي في المملكة العربية السعودية.

الدراسات السابقة

- متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠ " (٢٠٢٠) تحلل هذه الدراسة متطلبات تحقيق الأمن السيبراني في الجامعات السعودية من خلال تطبيق أداة بحث (الاستبانة على الموظفين التقنيين في ثلاث جامعات سعودية.
- درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة الرياض" (٢٠٢٠): تقيم هذه الدراسة مستوى وعي معلمات المرحلة المتوسطة بمخاطر الأمن السيبراني في المدارس العامة بمدينة الرياض.
- "استشارات إطار الامن السيبراني في التعليم العالي السعودي" (٢٠١٩): تقدم هذه الدراسة إطاراً عاماً للأمن السيبراني في التعليم العالي السعودي، وتتناول مبادئ التصميم الأمني ومكونات أنظمة تقنية المعلومات والتهديدات السيبرانية، والسياسات، والتشريعات والأخلاقيات.
- "الإجراءات المقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر" (٢٠١٨) تناقش هذه الدراسة أهمية إدارة المخاطر السيبرانية في المدارس الابتدائية، وتقدم إجراءات مقترحة للتحكم في هذه المخاطر.

المخلص

جاء تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية يهدف إلى تحديد وتقييم الفرص المحتملة لاختراق أنظمة المعلومات والبنية التحتية السيبرانية في المؤسسات التعليمية وتقييم التأثيرات المحتملة لهذه الاختراقات على العملية التعليمية والمعلومات الحساسة المخزنة فيها. في هذا السياق، سنلقي نظرة على دراسة حالة التعليم الجامعي في المملكة العربية السعودية.

تعد المؤسسات التعليمية في المملكة العربية السعودية هدفًا محتملاً للهجمات السيبرانية نظرًا للكمية الهائلة من المعلومات الحساسة المخزنة في أنظمتها، بما في ذلك المعلومات الشخصية للطلاب والأعضاء هيئة التدريس والبيانات البحثية والمصادر المعلوماتية الأخرى. يمكن أن يؤدي اختراق هذه المعلومات إلى تسرب البيانات الشخصية والمالية والتجسس الصناعي والتلاعب بالنتائج الأكاديمية وتعطيل الخدمات التعليمية.

يجب على المؤسسات التعليمية في المملكة العربية السعودية تنفيذ تحليل مخاطر الأمن السيبراني لتحديد الثغرات الأمنية المحتملة وتقييم مدى تأثيرها المحتمل. يشمل التحليل عادةً العديد من الخطوات مثل تحديد الأصول الحاسوبية وتصنيفها وتقييم الثغرات المحتملة وتقدير التهديدات واحتمالية حدوثها وتأثيرها، وتحديد مستوى الحماية الحالي وتحديد الإجراءات المناسبة للتخفيف من المخاطر.

بعد تحليل المخاطر، يجب على المؤسسات التعليمية تطبيق إجراءات أمنية مناسبة لحماية أنظمتها والمعلومات المخزنة فيها. يجب تنفيذ سياسات وإجراءات قوية لإدارة هوية المستخدمين ووضع قواعد وسياسات لحماية البيانات وتشفيرها وتحديث البرامج والأنظمة بانتظام وتوفير التدريب والتوعية اللازمة للطلاب وأعضاء هيئة التدريس للتعرف على التهديدات السيبرانية واتخاذ إجراءات الوقاية المناسبة.

الملخص

باختصار، تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية يلعب دور مهم في حماية المعلومات الحساسة والبنية التحتية السيبرانية في التعليم الجامعي في المملكة العربية السعودية من خلال تحليل المخاطر وتنفيذ إجراءات الأمن الملائمة، يمكن للمؤسسات التعليمية تعزيز أمان بيئة التعليم الرقمي والحفاظ على خصوصية وسلامة المعلومات للطلاب وأعضاء هيئة التدريس.

الخاتمة

اختتم بحث الذي بحث فيه عن مختلف العوامل والأسباب المؤدية إلى (تحليل مخاطر الامن السيرانى فى المؤسسات التعليمية : مسح التعليم الجامعى المملكة العربية السعودية)، حيث استعرضت تفصيليا الدوافع والمحركات التى تقف خلف هذه الإشكالية وتطرقت كذلك إلى ملخص بسيط للأفكار والنتائج والتوصيات التى تناولها البحث)، وأواجه توصية للأفراد بضرورة الالتزام بأبرز القوانين والمعايير المرتبطة بموضوع دراستي، ورفع أكف الضراعة إلى الله - عز وجل - أن يجعل هذا البحث مثقلا فى ميزان أعمالى وأعمالكم يوم الحساب، واسأل سبحانه وتعالى أن يوفقني لإنجاز المزيد من الأبحاث النافعة التى تسهم الفصل الراى فى خدمة المسلمين والأمة الإسلامية ككل، والحمد لله الذى بنعمته تتم الصالحات.

المراجع:

كتب:

- ❖ إدارة الأمن السيبراني في مؤسسات التعليم العالي، فاطمة عبد الله الشبانان، ٢٠٢١.
- ❖ الأمن السيبراني: مفاهيم وتطبيقات محمد بن عبد الرحمن آل عبد اللطيف، ٢٠٢٢.
- ❖ الأمن السيبراني وتحدياته في ظل التطورات التقنية، عبد الله بن محمد الحربي، ٢٠٢٣.

مقالات:

- ❖ التحديات التي تواجه الأمن السيبراني في الجامعات السعودية، مجلة جامعة الملك عبد العزيز، ٢٠٢٣.
- ❖ أهمية الأمن السيبراني في التعليم الجامعي، مجلة جامعة الملك سعود، ٢٠٢٢.
- ❖ الوعي بالأمن السيبراني لدى الطلاب وأعضاء هيئة التدريس في الجامعات السعودية، مجلة جامعة الملك فهد للبترول والمعادن، ٢٠٢١.

تقارير:

- ❖ التقرير الوطني للأمن السيبراني في المملكة العربية السعودية، الهيئة السعودية للبيانات والذكاء الاصطناعي، ٢٠٢٣.
- ❖ تقييم المخاطر السيبرانية في قطاع التعليم العالي، مركز الأمن السيبراني الوطني، ٢٠٢٢.
- ❖ تحليل مخاطر الأمن السيبراني في جامعة سعودية، شركة XYZ للاستشارات ٢٠٢١.