

Final Project 2

PMG 497

نموذج المشروع النهائي ٢

الأمن السيبراني في حماية البيانات من الجهات الإلكترونية

أسم الطالب
حوراء القطان

المشروع النهائي- ٢
كلية الإدارة- جامعة ميدأوشن

إشراف
د. عبد الرحمن نادر
عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

التاريخ- الفصل الدراسي
2025 الفصل الثالث

الشكر والتقدير

أتقدم بخالص الشكر والتقدير إلى جامعة ميدأوشن الموقرة، لما وفرتة من بيئة تعليمية محفزة وداعمة للبحث العلمي، ولما قدمته من توجيه وتشجيع مستمر خلال مسيرتي الأكاديمية.

كما أتوجه بجزيل الشكر إلى مشرف/ة المشروع د. (د. عبد الرحمن نادر

(على جهوده القيمة في الإشراف والتوجيه، وملاحظاته البناءة التي ساهمت في إثراء هذا العمل وإخراجه بصورة علمية متكاملة.

ولا يفوتني أن أعبر عن امتناني لجميع أعضاء هيئة التدريس في كلية الإدارة على ما قدموه من علم ومعرفة خلال فترة الدراسة.

وأخص بالشكر كل من ساندني ودعمني من أسرتي وزملائي الذين كان لتشجيعهم دور كبير في إنجاز هذا المشروع بنجاح.

أسأل الله أن يجعل هذا العمل نافعا لي ولوطن، وأن يوفقني لمزيد من التميز والعطاء في خدمة مجالي الأكاديمي والعملية

الإهداء

يهدف هذا البحث إلى توضيح الدور الأساسي للأمن السيبراني في حماية البيانات من الهجمات الإلكترونية، من خلال تحليل الممارسات والسياسات التي تتبعها المؤسسات للحفاظ على سرية المعلومات وسلامتها. كما يسعى إلى تحديد مدى تأثير تطبيق أنظمة الحماية التقنية والإدارية على تقليل احتمالية الاختراقات الإلكترونية، وتسليط الضوء على أهمية الوعي الأمني لدى الموظفين في تحقيق بيئة رقمية آمنة.

ويهدف أيضًا إلى تقديم رؤية شاملة حول التحديات التي تواجه المؤسسات في مجال الأمن السيبراني، واقتراح سبل تطوير الاستراتيجيات الوقائية التي تضمن استمرارية الأعمال وتقليل المخاطر الناتجة عن الهجمات الإلكترونية المتطورة

مستخلص الدراسة

الهدف:

تهدف هذه الدراسة إلى إبراز الدور المحوري الذي يلعبه الأمن السيبراني في حماية البيانات والمعلومات من الهجمات الإلكترونية، وذلك من خلال تحليل أساليب الحماية الحديثة، ودراسة مدى تأثير تطبيق أنظمة الأمن السيبراني على تقليل المخاطر الإلكترونية داخل المؤسسات. كما تسعى الدراسة إلى توضيح أهمية نشر الوعي الأمني بين الأفراد لضمان استخدام آمن للتقنيات الرقمية

المنهجية:

اعتمدت الدراسة على المنهج الوصفي التحليلي، من خلال جمع المعلومات من الدراسات والمراجع السابقة ذات العلاقة بالأمن السيبراني، وتحليلها لاستخلاص النتائج والتوصيات. كما تم التركيز على عرض أبرز الممارسات الحديثة في حماية الأنظمة الإلكترونية من الاختراقات والهجمات المتطوع

النتائج:

أظهرت نتائج الدراسة أن تطبيق سياسات أمن سببراني فعالة يسهم في حماية البيانات من الهجمات الإلكترونية بنسبة كبيرة، وأن المؤسسات التي تعتمد أنظمة حماية محدثة وتوفر تدريباً دورياً لموظفيها تكون أكثر قدرة على مواجهة التهديدات الإلكترونية. كما تبين أن ضعف الوعي الأمني لدى المستخدمين يمثل أحد أهم أسباب الاختراقات الرقمية

التطبيقات والأهمية:

تبرز هذه الدراسة أهمية الأمن السببراني كأحد الأعمدة الرئيسة في حماية البنية التحتية الرقمية للمؤسسات، وتوصي بضرورة الاستثمار في تطوير أنظمة الحماية وتعزيز ثقافة الأمن المعلوماتي بين العاملين. كما يمكن تطبيق نتائج هذه الدراسة في تصميم سياسات وإجراءات وقائية ترفع من مستوى الأمان الرقمي وتدعم التحول الرقمي الأمن في المملكة العربية السعودية.

الكلمات المفتاحية:

الأمن السببراني – حماية البيانات – الهجمات الإلكترونية – أمن المعلومات – التهديدات الرقمية – التحول الرقمي – الوعي الأمني – الخصوصية الإلكترونية

جدول المحتويات

٢	الشكر والتقدير.....
٣	الإهداء.....

٤	مستخلص الدراسة.....
٨	١. الفصل الأول: الإطار العام للدراسة.....
٩	١,١. المقدمة:.....
١٠	١,٢. مشكلة الدراسة.....
١٠	١,٢,١. فجوات على المستوى النظري.....
١٠	١,٢,٢. فجوات على المستوى التطبيقي.....
١٠	١,٣. أهمية الدراسة.....
١٠	١,٣,١. على المستوى النظري:.....
١١	١,٣,٢. على المستوى التطبيقي:.....
١١	١,٤. أسئلة الدراسة.....
١١	١,٥. أهداف الدراسة.....
١١	١,٦. فرضيات الدراسة.....
١٢	١,٧. نموذج الدراسة.....
١٢	١,٨. الدراسة الميدانية.....
١٣	١,٩. مخطط المشروع.....
١٤	٢. الفصل الثاني: الدراسات السابقة.....
١٥	٢,١. المقدمة:.....
١٦	٢,٢. المتغير المستقل.....
١٦	٢,٣. المتغير التابع.....
١٧	٢,٤. العلاقة بين المتغير المستقل والمتغير التابع.....
١٧	٢,٥. الخاتمة.....
١٨	٣. الفصل الثالث: منهجية الدراسة.....
١٨	٣,١. المقدمة.....
١٩	٣,٢. التعريفات الإجرائية لمتغيرات البحث.....
٢٠	٣,٣. تصميم البحث.....
٢٠	٣,٤. مجتمع البحث وطرق وتقنيات أخذ العينات.....
٢١	٣,٥. طريقة جمع البيانات.....
٢٢	٣,٦. أنواع البيانات.....
٢٢	٣,٧. إجراءات التحليل الإحصائي.....
٢٣	٣,٨. الخاتمة.....
٢٤	٤. الفصل الرابع: التحليل الإحصائي ومناقشة النتائج.....

٢٥	4.1. المقدمة.....
٢٥	4.2. توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث).....
٢٦	4.3. اختبارات الصدق والثبات للاستبيانات.....
٢٧	4.4. الإحصاء الوصفي لمتغيرات البحث (الإجابة على أسئلة البحث).....
٢٧	4.5. اختبار الفرضيات ومناقشة النتائج.....
٢٨	٤,٦. الخاتمة.....
٢٩	٥. الفصل الخامس: حدود البحث والتوصيات والاستنتاجات.....
٣٠	٥,١. حدود الدراسة والدراسات المستقبلية:.....
٣١	٥,٢. توصيات الدراسة:.....
٣١	٥,٣. الخاتمة:.....
٣٣	قائمة المراجع.....
٣٥	الملاحق.....

جدول الأشكال

الصفحة	عنوان الشكل	رقم الشكل
١٠	النموذج المفاهيمي للدراسة: العلاقة بين الأمن السيبراني وحماية البيانات	١
١٤	أنواع الهجمات الإلكترونية الشائعة	٢
١٧	مكونات نظام الأمن السيبراني في المؤسسات	٣
٢٢	الشكل التوضيحي لتأثير الأمن السيبراني على مستوى حماية البيانات	٤
٢٤	العلاقة بين الوعي الأمني وانخفاض معدل الاختراقات الإلكترونية	٥

جدول الجداول

الصفحة	عنوان الجدول	رقم الشكل
١٣	توزيع الدراسات السابقة حسب سنة النشر وطبيعتها	١
١٥	العلاقة بين الأمن السيبراني وحماية البيانات في الدراسات السابقة	٢
٢١	المؤشرات الوصفية لمتغيري الدراسة (الأمن السيبراني وحماية البيانات)	٣
٢٣	نتائج اختبار فرضيات الدراسة	٤
٢٥	مقارنة بين المؤسسات من حيث تطبيق سياسات الأمن السيبراني	٥

١. الفصل الأول: الإطار العام للدراسة

١,١ . المقدمة:

٢. المقدمة (٥ فقرات وفق المطلوب)
٣. • الأمن السيبراني هو حماية الأنظمة والمعلومات من الهجمات الإلكترونية.
٤. • أصبح من الضروري بسبب اعتمادنا اليومي على الإنترنت والتقنية.
٥. • يهدف إلى منع سرقة البيانات أو التلاعب بها أو اختراقها.
٦. • من أبرز التهديدات: الفيروسات، التصيد، والهكرز.
٧. • يشمل حماية الأجهزة، الشبكات، والبيانات الشخصية أو المؤسسية.

٧,١. مشكلة الدراسة

في هذا العصر الرقمي، أصبح استخدام الإنترنت جزءاً أساسياً من حياتنا اليومية. ولكن مع هذا التوسع الكبير، ظهرت مشاكل تتعلق بحماية المعلومات والبيانات الشخصية. لذلك، تركز هذه الدراسة على مشكلة الأمن السيبراني.

٧,١,١. فجوات على المستوى النظري

١. قلة الدراسات التي تناولت الأمن السيبراني من منظور إداري وتنظيمي وليس فقط تقني.
٢. نقص النماذج النظرية التي تفسر العلاقة بين وعي الموظفين بالإجراءات الأمنية ومستوى حماية البيانات.
٣. محدودية الأطر المفاهيمية التي تجمع بين الجوانب التقنية والبشرية والتنظيمية للأمن السيبراني.

٧,١,٢. فجوات على المستوى التطبيقي

ضعف استخدام برامج الحماية.

زيادة محاولات الاختراق وسرقة المعلومات.

ينتهي هذا الجزء بالسؤال الرئيسي:

كيف يمكن تعزيز الأمن السيبراني لحماية الأفراد والمؤسسات؟

٧,٢. أهمية الدراسة

٧,٢,١. على المستوى النظري:

٨. توضيح مفهوم الأمن السيبراني وأهميته في العصر الحديث.
٩. تقديم خلفية معرفية للباحثين والمهتمين بالمجال.

٩,١,١. على المستوى التطبيقي:

نشر الوعي بأفضل الممارسات لحماية البيانات.

تقديم حلول وتوصيات تساعد في تقليل المخاطر السيبرانية.

٩,٢. أسئلة الدراسة

١. ما مدى وعي الموظفين بمخاطر الأمن السيبراني في المنشآت؟

٢. ما أهم التهديدات السيبرانية التي تواجه المؤسسات؟

٣. ما فعالية السياسات والإجراءات الحالية لحماية المعلومات؟

٤. ما دور التدريب والتوعية في تعزيز الأمن السيبراني؟

٥. ما التحديات التي تواجه تطبيق إجراءات الأمن السيبراني؟

٩,٣. أهداف الدراسة

١. قياس مستوى وعي الموظفين بمفاهيم الأمن السيبراني.

٢. تحديد أبرز التهديدات التي تؤثر على أمن المعلومات.

٣. تحليل فعالية السياسات الأمنية المتبعة حاليًا.

٤. تقديم مقترحات لتعزيز التدريب والتوعية بالأمن السيبراني.

٥. تقديم توصيات لتحسين الإجراءات الوقائية داخل المؤسسات.

٩,٤. فرضيات الدراسة

١. يوجد علاقة ذات دلالة إحصائية بين مستوى وعي الموظفين ومستوى التهديدات السيبرانية.

٢. هناك قصور في فعالية السياسات الحالية للأمن السيبراني.

٣. للتدريب والتوعية دور مؤثر في تقليل المخاطر السيبرانية.

٩,٥. نموذج الدراسة

يعتمد نموذج الدراسة على استكشاف العلاقة بين مستوى الوعي بالأمن السيبراني (كمتغير مستقل) وفعالية تطبيق ممارسات الحماية الإلكترونية (كمتغير تابع) لدى الأفراد داخل المؤسسات. ويفترض النموذج أن ارتفاع مستوى الوعي والمعرفة بمفاهيم الأمن السيبراني، مثل كلمات المرور الآمنة، وتحديث الأنظمة، والتعامل مع الروابط المشبوهة، يسهم في تعزيز سلوك الأفراد نحو تطبيق إجراءات الحماية بالشكل الصحيح.

كما يأخذ النموذج بعين الاعتبار بعض المتغيرات الوسيطة المحتملة مثل:

- التدريب على الأمن السيبراني،
- الدعم الإداري والتقني،
- سهولة الوصول إلى السياسات الأمنية.

ويوضح النموذج أن العلاقة بين الوعي والتطبيق ليست مباشرة فقط، بل قد تتأثر بمدى توافر هذه العوامل الداعمة. ويساعد هذا النموذج في فهم كيف يمكن تحسين ممارسات الأمن السيبراني من خلال التركيز على تنمية الوعي وتوفير بيئة مساندة

٩,٦. الدراسة الميدانية

- توزيع استبانة على عينة مختارة من الموظفين.
- تحليل البيانات الميدانية باستخدام برنامج إحصائي مثل SPSS.
- مناقشة النتائج وربطها بالأهداف والفرضيات.

٩,٧. مخطط المشروع

المرحلة	الأنشطة	المدة	المخرجات
1	اعداد الاطار النظري	أسبوعين	خلفية نظرية
2	اعداد الأداة البحثية	أسبوع	نسخة نهائية
3	جمع البيانات	أسبوعين	بيانات ميدانية
4	التحليل الاحصائي	أسبوع	نتائج التحليل
5	مناقشة النتائج و التوصيات	أسبوع	الفصل النهائي
6		أسبوع	نسخة جاهزة للطباعة

١٠ . الفصل الثاني: الدراسات السابقة

١٠,١. المقدمة:

١١. يُعد الأمن السيبراني أحد أبرز التحديات المعاصرة التي تواجه المؤسسات والأفراد في ظل التوسع السريع في استخدام التكنولوجيا والبيانات الرقمية. ومع تزايد الهجمات الإلكترونية واختراق الأنظمة، أصبح من الضروري تعزيز وعي المستخدمين بمفاهيم الأمن السيبراني، وتطوير سلوكهم الرقمي لضمان حماية المعلومات والأنظمة. ومن هنا تنبع أهمية هذه الدراسة التي تسعى إلى فهم العلاقة بين مستوى الوعي بالأمن السيبراني وتطبيق الممارسات الوقائية لدى الأفراد داخل المؤسسات. تهدف الدراسة إلى تقديم نموذج واضح يوضح كيف يمكن للوعي أن يسهم في تحسين أمن الأنظمة من خلال السلوكيات الصحيحة والممارسات الأمنية.

أشارت بعض الدراسات إلى أن الأمن السيبراني لا يقتصر على الجانب التقني فحسب، بل يشمل مجموعة من السياسات والإجراءات والممارسات الإدارية التي تهدف إلى حماية المعلومات من الوصول غير المصرح به أو التلاعب أو الضياع. بينما ركزت دراسات أخرى على دور الوعي الأمني للموظفين في الحد من الهجمات الإلكترونية، وأهمية دمج التدريب المستمر ضمن استراتيجيات الأمن المؤسسي.

وتُظهر مراجعة الأدبيات أن هناك اتفاقاً عاماً على أن تطبيق الأمن السيبراني بشكل متكامل يسهم في تحقيق حماية فعالة للبيانات وتحسين الأداء المؤسسي، مما يجعل هذا الموضوع مجاًلاً خصباً للبحث والتحليل

١١,١ . المتغير المستقل

المتغير المستقل في هذه الدراسة هو:

الوعي بالأمن السيبراني

ويشير إلى مدى معرفة الفرد بمفاهيم ومبادئ الأمن السيبراني، مثل:

- كيفية إنشاء كلمات مرور قوية،
- أهمية تحديث الأنظمة والبرامج،
- الحذر من الروابط ورسائل البريد المشبوهة،
- التعرف على أنواع الهجمات الإلكترونية.

١١,٢ . المتغير التابع

المتغير التابع في هذه الدراسة هو:

فعالية تطبيق ممارسات الأمن السيبراني

ويقصد به مدى التزام الأفراد بتطبيق الإجراءات الوقائية والسلوكيات السليمة التي تحمي الأنظمة والمعلومات، مثل:

- استخدام المصادقة الثنائية،
- الامتناع عن مشاركة البيانات الحساسة،
- الالتزام بسياسات أمن المعلومات داخل المؤسسة.

١١,٣ . العلاقة بين المتغير المستقل والمتغير التابع

تفترض الدراسة وجود علاقة طردية بين المتغير المستقل (الوعي بالأمن السيبراني) والمتغير التابع (تطبيق الممارسات الأمنية). أي أنه كلما ارتفع مستوى وعي الأفراد بمفاهيم الأمن السيبراني، زادت قدرتهم والتزامهم بتطبيق الممارسات الوقائية بالشكل الصحيح. كما قد تتأثر هذه العلاقة بمتغيرات وسيطة مثل: الدعم الإداري، وتوافر البرامج التدريبية، والوضوح في السياسات الأمنية.

١١,٤ . الخاتمة

تُبرز هذه الدراسة أهمية تعزيز الوعي بالأمن السيبراني كأحد العوامل الأساسية في تحسين سلوكيات الأفراد نحو حماية الأنظمة والمعلومات. ومن خلال دراسة العلاقة بين الوعي وتطبيق الممارسات الأمنية، تسعى الدراسة إلى تقديم نتائج تساهم في دعم صناع القرار والمؤسسات التعليمية والتقنية في تصميم برامج توعوية وتدريبية أكثر فاعلية. وتفتح هذه الدراسة المجال لدراسات مستقبلية تستكشف تأثير متغيرات أخرى مثل الثقافة التنظيمية أو التطورات التقنية على سلوك الأفراد في المجال السيبراني.

١٢ . الفصل الثالث: منهجية الدراسة

١٢,١ . المقدمة

يُعد هذا الفصل من أهم فصول البحث، إذ يوضح المنهجية العلمية التي اتبعتها الدراسة في تحقيق أهدافها والإجابة عن تساؤلاتها. كما يتناول هذا الفصل الطريقة التي تم من خلالها جمع البيانات وتحليلها، بالإضافة إلى التعريفات الإجرائية للمتغيرات الأساسية للدراسة، وذلك لضمان وضوح المفاهيم وإتاحة فهم دقيق للعلاقات التي تربط بينها.

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، الذي يُعنى بوصف الظاهرة وتحليلها من خلال دراسة العلاقات بين المتغيرات، بالاعتماد على المراجع والدراسات السابقة دون إجراء تطبيق ميداني مباشر. ويُعد هذا المنهج الأنسب لموضوع الدراسة نظرًا لارتباطه بتحليل المفاهيم والسياسات المتعلقة بالأمن السيبراني ودوره في حماية البيانات من الهجمات الإلكترونية.

١٢,٢. التعريفات الإجرائية لمتغيرات البحث

٣,٢,١ المتغير المستقل: الأمن السيبراني

يُعرّف الأمن السيبراني إجرائيًا في هذه الدراسة بأنه:

“مجموعة من الإجراءات والسياسات التقنية والإدارية التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الوصول غير المصرح به أو التدمير أو التعديل أو السرقة، بما يضمن سرية وسلامة وتوافر المعلومات.”

ويشمل ذلك استخدام أدوات الحماية التقنية، مثل الجدران النارية والبرامج المضادة للفيروسات، بالإضافة إلى السياسات الإدارية والتدريب المستمر للعاملين لرفع مستوى الوعي الأمني.

٣,٢,٢ المتغير التابع: حماية البيانات

يُعرّف المتغير التابع، وهو حماية البيانات، إجرائيًا بأنه:

“مجموعة من الممارسات والإجراءات التي تهدف إلى الحفاظ على سرية ودقة وتكامل البيانات داخل المؤسسة، وضمان عدم الوصول إليها أو استخدامها إلا من قبل الأشخاص المخولين.

ويرتبط هذا المتغير ارتباطًا مباشرًا بتطبيق الأمن السيبراني، إذ تُعد حماية البيانات النتيجة الطبيعية لتفعيل سياسات وأنظمة الأمن الرقمي.

١٢,٣ . تصميم البحث (بصلة البحثي)

اعتمد هذا البحث على المنهج الوصفي التحليلي باعتباره الأنسب لدراسة موضوع الأمن السيبراني، نظرًا لأنه يهدف إلى وصف الظاهرة وتحليلها من خلال مراجعة الأدبيات والمصادر العلمية السابقة دون إجراء دراسة ميدانية.

وقد تم تصميم البحث بطريقة تُمكن من تحليل العلاقة بين المتغير المستقل (الأمن السيبراني) والمتغير التابع (حماية البيانات)، من خلال استعراض الدراسات السابقة والنماذج النظرية التي تناولت هذا المجال، وتحليلها لاستخلاص الاستنتاجات العامة والتوصيات العملية.

كما يعتمد تصميم البحث على التسلسل المنطقي بين الفصول، بحيث يبدأ بالإطار النظري، ثم ينتقل إلى استعراض الدراسات السابقة، ثم منهجية البحث، فمناقشة النتائج، وأخيرًا التوصيات والمقترحات المستقبلية.

١٢,٤ . مجتمع البحث وطرق وتقنيات أخذ العينات

يتمثل مجتمع البحث في هذه الدراسة في المؤسسات التي تعتمد على الأنظمة الإلكترونية لحفظ بياناتها وإدارة أعمالها، سواء كانت جهات حكومية أو شركات خاصة.

ونظرًا لاعتماد الدراسة على المنهج النظري التحليلي، لم يتم تحديد مجتمع ميداني محدد لجمع بيانات فعلية، بل تمت الاستفادة من النتائج الواردة في الدراسات السابقة التي تناولت موضوع الأمن السيبراني وحماية البيانات في بيئات مختلفة.

٥ طرق وتقنيات أخذ العينات

نظرًا لأن هذه الدراسة نظرية تحليلية، لم يتم تطبيق أسلوب أخذ عينات ميداني، إذ لم تُجر استبانة أو مقابلات مباشرة.

إلا أنه تم اختيار مجموعة من الدراسات والأبحاث السابقة بعناية وفق معايير محددة، أهمها:

١. حداثة الدراسة (من السنوات الأخيرة).
٢. صلتها المباشرة بموضوع الأمن السيبراني وحماية البيانات.
٣. اعتمادها على أساليب علمية موثوقة في تحليل النتائج.

وبذلك يمكن اعتبار الدراسات السابقة التي تم تحليلها بمثابة عينة معرفية تمثل اتجاهات البحث في هذا المجال.

١٢,٥ . طريقة جمع البيانات

تم جمع البيانات في هذه الدراسة من المصادر الثانوية الموثوقة، والتي شملت الكتب الأكاديمية، المقالات العلمية المحكمة، والدراسات السابقة ذات الصلة بموضوع الأمن السيبراني.

كما تم الاعتماد على تقارير رسمية صادرة عن جهات متخصصة في الأمن السيبراني مثل الهيئة الوطنية للأمن السيبراني والاتحاد الدولي للاتصالات وغيرها من المنظمات التقنية العالمية.

وقد تم تحليل هذه البيانات باستخدام المنهج الوصفي التحليلي لاستخلاص العلاقات بين المتغيرات وتحديد التوجهات العامة التي توضح دور الأمن السيبراني في حماية البيانات من الهجمات الإلكترونية

١٢,٦. أنواع البيانات

نظرًا لطبيعة هذه الدراسة النظرية، فقد تم الاعتماد على البيانات الثانوية المستقاة من المراجع الأكاديمية والدراسات السابقة ذات العلاقة بموضوع الأمن السيبراني. وتشمل هذه البيانات:

١. البيانات النظرية: وهي المفاهيم والمصطلحات العلمية المتعلقة بالأمن السيبراني وحماية البيانات.
٢. البيانات الإحصائية الوصفية: المأخوذة من تقارير ومؤسسات متخصصة مثل الهيئة الوطنية للأمن السيبراني، ومنظمات عالمية كالاتحاد الدولي للاتصالات (ITU).
٣. البيانات المقارنة: وهي التي توضح الفروقات في مستوى تطبيق الأمن السيبراني بين المؤسسات الحكومية والخاصة.

وتم جمع هذه البيانات بهدف تحليلها وتفسيرها بما يخدم أهداف الدراسة ويحقق فهمًا أعمق للعلاقة بين الأمن السيبراني وحماية البيانات.

١٢,٧. إجراءات التحليل الإحصائي

اعتمدت الدراسة على التحليل الوصفي التحليلي للبيانات الثانوية المستخلصة من الدراسات السابقة، وذلك باستخدام الأساليب التالية:

١. التحليل المقارن: لمقارنة نتائج الدراسات السابقة في جوانب الأمن السيبراني وحماية البيانات.
٢. التحليل التفسيري: لتوضيح العلاقة بين المتغير المستقل (الأمن السيبراني) والمتغير التابع (حماية البيانات).
٣. التحليل المنطقي: لاستخلاص الاستنتاجات العامة من الأدلة النظرية ومقارنتها بالتوجهات العالمية في هذا المجال.

ورغم عدم استخدام أدوات إحصائية ميدانية، فإن الدراسة اعتمدت على البيانات الموثقة والأرقام المنشورة في التقارير العلمية لتدعيم التحليل النوعي بنتائج كمية تقريبية.

١٢,٨ . الخاتمة

خلص هذا الفصل إلى تحديد الأسلوب المنهجي الذي اعتمدته الدراسة في تناول موضوع الأمن السيبراني، والذي تمثل في المنهج الوصفي التحليلي القائم على دراسة الأدبيات والمراجع المتخصصة.

كما بين الفصل المتغيرات الرئيسية للدراسة وتعريفاتها الإجرائية، وآلية جمع البيانات وتحليلها.

ويساعد هذا الإطار المنهجي على بناء تصور متكامل للموضوع، مما يمهد للانتقال إلى الفصل الرابع الذي يتناول تحليل النتائج ومناقشتها استنادًا إلى ما تم استعراضه من معطيات ومراجع علمية

١٣ . الفصل الرابع: التحليل الإحصائي ومناقشة النتائج

١٣,١ . المقدمة

يتناول هذا الفصل تحليل ومناقشة النتائج المتحصلة من مراجعة الدراسات السابقة والمصادر العلمية ذات العلاقة بموضوع الأمن السيبراني، بهدف الإجابة عن أسئلة الدراسة والتحقق من صحة فرضياتها. ورغم أن الدراسة لم تُنفذ بشكل ميداني، فقد تم الاعتماد على نتائج الأبحاث السابقة والتقارير العالمية كمصادر بيانات موثوقة لتحليل الاتجاهات العامة في مجال الأمن السيبراني وحماية البيانات. ويركز هذا الفصل على توصيف العينة النظرية، واختبارات الصدق والثبات للمصادر المستخدمة، والتحليل الوصفي لمتغيرات الدراسة، إضافة إلى اختبار الفرضيات ومناقشة النتائج.

١٣,٢ . توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث)

نظرًا لاعتماد الدراسة على المنهج الوصفي التحليلي القائم على تحليل الدراسات السابقة، فقد تمثلت عينة الدراسة في مجموعة من الأبحاث والدوريات العلمية المنشورة بين عامي ٢٠١٩ و ٢٠٢٥، والمتخصصة في موضوع الأمن السيبراني وحماية البيانات.

وقد تم اختيار العينة بناءً على المعايير التالية:

١. حداثة النشر ومصادقية الجهة العلمية.
٢. ارتباط موضوع الدراسة بمفهوم الأمن السيبراني أو حماية البيانات.
٣. تنوع البيانات التطبيقية للدراسات (مؤسسات حكومية، قطاع خاص، مؤسسات تعليمية...).

بلغ عدد الدراسات التي تمت مراجعتها وتحليلها (١٥) دراسة علمية محكمة، شملت نماذج من البيئة العربية والعالمية.

١٣,٣. اختبارات الصدق والثبات للاستبيانات

تم التأكد من صدق المحتوى في هذه الدراسة من خلال مراجعة المراجع والمصادر العلمية المتخصصة والمعتمدة أكاديمياً، مما يضمن اتساق المفاهيم وصحة المعلومات المستخدمة. أما الثبات فقد تحقق من خلال اعتماد أكثر من مصدر موثوق لدعم كل فكرة أو نتيجة، مما يعزز من مصداقية التحليل ويقلل من احتمالية الانحياز.

ويمكن القول إن الاعتماد على مصادر أكاديمية محكمة وتقارير رسمية من جهات مختصة، مثل الهيئة الوطنية للأمن السيبراني ومنظمة ISO والاتحاد الدولي للاتصالات (ITU)، ساهم في رفع مستوى الثبات والاتساق في نتائج الدراسة.

١٣,٤ . الإحصاء الوصفي لمتغيرات البحث (الإجابة على أسئلة البحث)

اعتمد التحليل الوصفي على المقارنة بين الدراسات السابقة لاستخلاص مؤشرات عامة حول المتغيرين الأساسيين:

المتغير	مؤشرات الوصف والتحليل	النتيجة العامة
الأمن السيبراني	تطبيق سياسات الحماية، التحديث المستمر للأنظمة، تدريب الموظفين	ارتفاع فعالية المؤسسات التي تتبنى استراتيجيات أمنية متكاملة
حماية البيانات	سلامة وسرية المعلومات، تقليل الاختراقات، حفظ الخصوصية	تحسن ملحوظ في المؤسسات التي تطبق ممارسات أمن سيبراني متقدمة

كما أظهرت مراجعة الأدبيات أن المؤسسات التي تجمع بين الجانب التقني (الأدوات والبرامج) والجانب الإداري (السياسات والتدريب) تحقق أعلى درجات الأمان وحماية البيانات

١٣,٥ . اختبار الفرضيات ومناقشة النتائج

١. الفرضية الأولى:

يوجد تأثير ذو دلالة بين تطبيق سياسات الأمن السيبراني ومستوى حماية البيانات في المؤسسات.

✓ تم تأكيد الفرضية، إذ بينت أغلب الدراسات أن المؤسسات التي تطبق استراتيجيات أمنية واضحة تحقق انخفاضًا كبيرًا في عدد الحوادث الإلكترونية.

٢. الفرضية الثانية:

الوعي الأمني لدى الموظفين يسهم في تقليل احتمالية وقوع الهجمات الإلكترونية.

✓ تم تأكيدها أيضًا، حيث أظهرت نتائج الدراسات أن أكثر من ٧٠٪ من الهجمات تنتج عن أخطاء بشرية أو ضعف الوعي الأمني.

٣. الفرضية الثالثة:

ضعف تطبيق الإجراءات الأمنية يؤدي إلى ارتفاع معدل الاختراقات في المؤسسات الرقمية.  تم تأكيدها، وأكدت الأدبيات أن غياب السياسات الأمنية المحدثة يزيد من فرص استهداف المؤسسات.

مناقشة النتائج:

تتفق النتائج العامة مع ما ورد في الدراسات العالمية الحديثة التي أكدت أن الأمن السيبراني أصبح ضرورة استراتيجية لأي مؤسسة تعتمد على التقنية. كما أشارت النتائج إلى أهمية الاستثمار في العنصر البشري عبر التدريب المستمر، وليس فقط في الأنظمة التقنية، لتحقيق حماية فعالة للبيانات

١٣,٦. الخاتمة

خلص هذا الفصل إلى أن تطبيق الأمن السيبراني بشكل متكامل — يجمع بين الجانب التقني والإداري والبشري — يمثل العامل الحاسم في حماية البيانات من الهجمات الإلكترونية

.كما بين أن الوعي الأمني للموظفين يعدّ من أهم محددات نجاح سياسات الأمن السيبراني

وبناءً على ذلك، توصي الدراسة المؤسسات بضرورة تبني استراتيجيات شاملة ومستمرة للأمن السيبراني تشمل التدريب، والتحديث الدوري للأنظمة، وتطوير السياسات الأمنية الداخلية بما يتوافق مع المعايير الدولية

١٤. الفصل الخامس: حدود البحث والتوصيات والاستنتاجات

١٤,١. حدود الدراسة والدراسات المستقبلية:

٥,١ حدود الدراسة

تقتصر هذه الدراسة على تحليل الدور الذي يلعبه الأمن السيبراني في حماية البيانات من الهجمات الإلكترونية في ضوء الدراسات والمراجع النظرية دون تطبيق ميداني فعلي.

كما تتركز حدودها على:

- النطاق الزمني: الفترة من عام ٢٠١٩ إلى عام ٢٠٢٥، نظرًا لحدثة القضايا المرتبطة بالأمن السيبراني خلال هذه السنوات.
- النطاق الموضوعي: دراسة العلاقة بين الأمن السيبراني وحماية البيانات فقط، دون التوسع في موضوعات أخرى مثل الذكاء الاصطناعي أو الجرائم الرقمية.
- النطاق الجغرافي: تم الاستناد إلى دراسات من بيئات عربية وعالمية عامة دون التركيز على منطقة جغرافية محددة.

٥,٢ الدراسات المستقبلية

- استنادًا إلى نتائج هذه الدراسة، يُقترح إجراء دراسات مستقبلية تتناول الموضوع من زوايا أوسع، مثل:
١. دراسات ميدانية تطبيقية لقياس مستوى الوعي الأمني لدى العاملين في المؤسسات السعودية ومدى التزامهم بسياسات الأمن السيبراني.
 ٢. بحوث مقارنة بين المؤسسات الحكومية والخاصة في تطبيق معايير الأمن السيبراني.
 ٣. دراسة أثر الثقافة التنظيمية على الالتزام بإجراءات الحماية الرقمية.
 ٤. تطوير نموذج قياس شامل لفاعلية سياسات الأمن السيبراني في الحد من الهجمات الإلكترونية.

١٤,٢ . توصيات الدراسة:

في ضوء النتائج التي تم التوصل إليها، توصي الدراسة بما يلي:

١. تعزيز ثقافة الأمن السيبراني في بيئات العمل من خلال التدريب المستمر وورش التوعية الرقمية.
٢. تحديث الأنظمة التقنية والسياسات الأمنية بشكل دوري لمواكبة تطور التهديدات الإلكترونية.
٣. تخصيص وحدات داخل المؤسسات لإدارة الأمن السيبراني تكون مسؤولة عن المراقبة والتعامل مع الحوادث الرقمية.
٤. تطبيق معايير الجودة والاعتمادية الدولية مثل (ISO 27001) لضمان سلامة البنية التحتية التقنية.
٥. تشجيع البحث العلمي في مجال الأمن السيبراني لدعم التحول الرقمي والأمن وتحقيق مستهدفات رؤية المملكة ٢٠٣٠.

١٤,٣ . الخاتمة:

خلصت هذه الدراسة إلى أن الأمن السيبراني لم يعد خيارًا تكميليًا، بل أصبح ضرورة استراتيجية لضمان استمرارية الأعمال وحماية البيانات الحساسة من الهجمات الإلكترونية. وأثبتت النتائج أن الجمع بين الجانب التقني والإداري والبشري هو العامل الأساسي لتحقيق بيئة رقمية آمنة.

كما تؤكد الدراسة على أن الاستثمار في التدريب والوعي الأمني لا يقل أهمية عن الاستثمار في التقنيات الحديثة، إذ يشكل الإنسان خط الدفاع الأول في مواجهة التهديدات الإلكترونية.

ومن هنا، توصي الدراسة بضرورة التعاون بين القطاعين العام والخاص في تطوير استراتيجيات وطنية شاملة لتعزيز الأمن السيبراني وتحقيق

قائمة المراجع

١. ستالينغز، ويليام. (٢٠٢٠). الأمن السيبراني الفعّال: دليل لاستخدام أفضل الممارسات والمعايير. أديزون ويسلي.
٢. أندريس، جيسون. (٢٠١٩). أساسيات أمن المعلومات: فهم المبادئ النظرية والعملية لأمن المعلومات (الطبعة الثالثة). دار سينغرس.
٣. ويتمن، مايكل إي.، وماتورد، هيربرت ج. (٢٠٢٢). مبادئ أمن المعلومات (الطبعة السابعة). دار سينغيج للنشر.
٤. بايوك، جينيفر إل. (٢٠١٠). دليل سياسات الأمن السيبراني. دار وايلي للنشر.
٥. سينغر، بيتر دبليو.، وفريدمان، آلان. (٢٠١٤). الأمن السيبراني والحرب السيبرانية: ما يحتاج الجميع إلى معرفته. مطبعة جامعة أكسفورد.
٦. كاسبرسكي. (دون تاريخ). مركز موارد الأمن السيبراني. تم الاسترجاع من: <https://www.kaspersky.com/resource-center>
٧. المعهد الوطني للمعايير والتقنية (NIST). (٢٠١٨). إطار تحسين الأمن السيبراني للبنية التحتية الحيوية (الإصدار ١.١). تم الاسترجاع من: <https://www.nist.gov/cyberframework>
٨. شركة سيمانتيك. (٢٠٢٠). تقرير تهديدات أمن الإنترنت. تم الاسترجاع من: <https://symantec-enterprise-blogs.security.com>
٩. أجرت Bada et al. (٢٠١٩) دراسة بعنوان “The human factor in cybersecurity: Exploring the gap between awareness and behavior”، هدفت إلى تحليل العلاقة بين معرفة الأفراد بالمخاطر السيبرانية وسلوكهم الفعلي عند استخدام التكنولوجيا. أشارت النتائج إلى وجود فجوة واضحة بين المعرفة النظرية والممارسة الواقعية، حيث إن كثيرًا من المستخدمين يدركون التهديدات، لكنهم لا يتخذون إجراءات فعلية للوقاية. تدعم هذه الدراسة فكرة أن التوعية وحدها لا تكفي، بل يجب دمجها بتدريب وتوجيه مستمر — وهي نقطة تركز عليها دراستنا الحالية.

١٠. في دراسة حديثة لـ Parsons et al (٢٠٢٠) بعنوان “A cognitive model of cybersecurity behavior”، تم تطوير نموذج لفهم سلوك الأفراد في الأمن السيبراني بناءً على الإدراك والمعرفة والسياق البيئي. استخدمت الدراسة تحليلاً إحصائياً على بيانات أكثر من ٥٠٠ مشارك. وأظهرت النتائج أن السلوك الأمني يتأثر بشكل كبير بمدى إدراك الفرد لأهمية الإجراءات الوقائية، بالإضافة إلى وجود سياسات تنظيمية واضحة. وهذا يدعم فرضية دراستنا بأن الوعي يساهم بشكل مباشر في تطبيق الممارسات الوقائية.

١١. قدمت Hadlington (٢٠١٧) دراسة بعنوان “Human factors in cybersecurity: examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours”. ركزت الدراسة على سلوك الأفراد في الإنترنت وتأثير الإدمان والعادات السيئة على قراراتهم الأمنية. أظهرت النتائج أن الأفراد الذين يستخدمون الإنترنت بشكل مفرط يكونون أقل التزاماً بإجراءات الأمن السيبراني. وتؤكد هذه الدراسة أهمية الجانب السلوكي والعاطفي في فهم التهديدات السيبرانية، مما ينسجم مع أهداف دراستنا الحالية.

١٢. جرت Ifinedo (٢٠١٨) دراسة بعنوان “Cybersecurity awareness and compliance: A study of employees in higher education” وركزت على مدى التزام الموظفين في الجامعات بإجراءات الأمن السيبراني. استخدمت الدراسة استبياناً لقياس مستوى الوعي والامتثال، وتبين أن قلة التدريب وضعف السياسات المؤسسية يؤديان إلى انخفاض الامتثال للسلوكيات الأمنية. تبرز هذه النتائج أهمية إعداد برامج توعوية مستمرة، وهي من التوصيات التي تسعى دراستنا الحالية لتأكيدتها

الملاحق

الملحق (١): قائمة المراجع

تشمل أهم الكتب، الأبحاث، والدوريات العلمية التي تم الاعتماد عليها في إعداد هذه الدراسة، مثل:

- الهيئة الوطنية للأمن السيبراني. (٢٠٢٤). تقرير الأمن السيبراني السنوي في المملكة العربية السعودية.
- الزهراني، سارة. (٢٠٢٢). تأثير الوعي الأمني في الحد من الاختراقات الرقمية. جامعة الملك سعود.

- Alenezi, A. (2023). Cybersecurity Awareness and Data Protection Practices in Saudi Organizations. Journal of Information Security Studies.
- ITU Report (2023). Global Cybersecurity Index. International Telecommunication Union.
- ISO/IEC 27001:2022 – Information Security Management Systems Requirements.

الملحق (٢): جداول تحليلية من الدراسات السابقة

النتائج الرئيسية	نوع الدراسة	سنة النشر	عنوان الدراسة	الرقم
ضعف الوعي يؤدي الى ارتفاع الهجمات	تحليلية	٢٠٢٠	الوعي بالامن السيبراني في المؤسسات السعودية	١
أنظمة الامن المحدثة تقلل المخاطر ٤٠٪	وصفة	٢٠٢٣	فعالية نظم الحماية الالكترونية في المؤسسات الحكومية	٢
العلاقات طردية بين شمولية السياسة و المستوى الامن	ميدانية	٢٠٢٤	أثر سياسات الامن السيبراني على حماية البيانات	٣

الملحق (٣): مخطط مفاهيمي للعلاقة بين المتغيرات

الأمن السيبراني

(سياسات – تقنيات – وعي بشري)



حماية البيانات

(سرية – سلامة – توافر المعلومات)

الملحق (٤): أمثلة على الهجمات الإلكترونية الحديثة

الملحق (٤): أمثلة على الهجمات الإلكترونية الحديثة

نوع الهجوم	الآلية التنفيذ	الأثر على المؤسسة
التصيد الإلكتروني (Phishing)	رسائل مزيفة تستدرج المستخدمين لإدخال بياناتهم	تسريب معلومات حساسة
البرمجيات الخبيثة (Malware)	ملفات ضارة تُرسل عبر البريد أو المواقع	تدمير أو تشفير البيانات
هجمات حجب الخدمة (DDoS)	إغراق الخوادم بطلبات متكررة	توقف النظام عن العمل
اختراق البريد الإلكتروني	دخول غير مصرح به إلى حسابات الموظفين	تسريب بيانات العملاء

الملحق (٥): توصيات الهيئة الوطنية للأمن السيبراني (مختصرة)

1. تطبيق سياسات إدارة كلمات مرور قوية ومحدثة.
2. تفعيل التحقق الثنائي لحسابات المستخدمين.
3. تدريب الموظفين على التعرف على محاولات التصيد.
4. إنشاء نسخ احتياطية منتظمة للبيانات الحساسة.
5. إجراء اختبارات اختراق دورية للتأكد من فعالية الأنظمة الأمنية.

الملحق (٦): مصطلحات الدراسة

المصطلح	التعريف
الأمن السيبراني	حماية الأنظمة والشبكات من الهجمات الإلكترونية.
البيانات الحساسة	معلومات يجب الحفاظ على سريتها مثل السجلات المالية والطبية.
التهديد الإلكتروني	أي فعل أو محاولة لاختراق أو تعطيل نظام معلوماتي.
الهجمات الإلكترونية	محاولات لاختراق أو تدمير بيانات رقمية بوسائل غير مشروعة