

Final Project 1

Code: MGM 496-PMG496

Project Template

Faculty of Management
Midocean University

الامن السيبراني

أسم الطالب

حوراء محمد القطان

مشروع تخرج- ١

كلية الإدارة- جامعة ميدأوشن

إشراف

د.

عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

التاريخ- الفصل الدراسي

2025 الفصل الثالث

جدول المحتويات

١. الفصل الأول: الإطار العام للدراسة..... ٣

١, ١. المقدمة:..... ٣

٥	١,٢. مشكلة الدراسة
٥	١,٢,١. فجوات على المستوى النظري
٥	١,٢,٢. فجوات على المستوى التطبيقي
٥	١,٣. أهمية الدراسة
٥	١,٣,١. على المستوى النظري
٥	١,٣,٢. على المستوى التطبيقي
٦	١,٤. أسئلة الدراسة
٦	١,٥. أهداف الدراسة
٦	١,٦. فرضيات الدراسة
٦	١,٧. نموذج الدراسة
٨	١,٨. منهجية الدراسة
٨	١,٩. الدراسة الميدانية
٨	١,١٠. مخطط المشروع المقترح
٩	٢. الفصل الثاني: الدراسات السابقة
١٠	٢,١. المقدمة
١٠	٢,٢. المتغير المستقل
١١	٢,٣. المتغير التابع
١١	٢,٤. العلاقة بين المتغير المستقل والمتغير التابع
١٢	٢,٥. الخاتمة
١٣	قائمة المراجع

١. الفصل الأول: الإطار العام للدراسة

١,١. المقدمة:

المقدمة (٥ فقرات وفق المطلوب)

- الأمن السيبراني هو حماية الأنظمة والمعلومات من الهجمات الإلكترونية.
- أصبح من الضروري بسبب اعتمادنا اليومي على الإنترنت والتقنية.
- يهدف إلى منع سرقة البيانات أو التلاعب بها أو اختراقها.
- من أبرز التهديدات: الفيروسات، التصيد، والهاكرز.
- يشمل حماية الأجهزة، الشبكات، والبيانات الشخصية أو المؤسسية.

١,٢. 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.

١,٢,١. فجوات على المستوى النظري

عدم فهم كافٍ لمفاهيم الأمن السيبراني.

نقص الوعي بأهمية حماية البيانات والمعلومات.

١,٢,٢. 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؟

١,٣. أهمية الدراسة

١,٣,١. على المستوى النظري:

توضيح مفهوم الأمن السيبراني وأهميته في العصر الحديث.

تقديم خلفية معرفية للباحثين والمهتمين بالمجال.

١,٣,٢. على المستوى التطبيقي:

نشر الوعي بأفضل الممارسات لحماية البيانات.

تقديم حلول وتوصيات تساعد في تقليل المخاطر السيبرانية.

١,٤. 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؟

١,٥. 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.

١,٦. 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.

ي@علا

١,٧. 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

١,٨ . منهجية الدراسة

- النوع: وصفية تحليلية
- أداة جمع البيانات: استبانة + مقابلات إن لزم الأمر
- العينة: موظفون في إدارات تقنية المعلومات/الأمن المعلوماتي
- طرق التحليل: تحليل إحصائي وصفي (تكرارات ونسب) وتحليل استنتاجي (اختبار الفرضيات).

١,٩ . الدراسة الميدانية

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

١,١٠ . مخطط المشروع المقترح

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

٢. الفصل الثاني: الدراسات السابقة

٢,١. المقدمة:

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 يساهم في تحسين أمن الأنظمة من خلال السلوكيات الصحيحة والممارسات الأمنية.

٢,٢. 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.

٢,٣. 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.

٢,٤. 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.

٢,٥ . 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.

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 تحليلًا إحصائيًا 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 التزامًا 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 استبيانًا 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

