

أهمية الأمن السيبراني في حياتنا

اسم الطالب / ريم احمد العوفي

رقم الجامعي / 2021205013

مشروع تخرج- ١

كلية الإدارة- جامعة ميدأوشن

إشراف

د. منى مصطفى العشري

عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

الفصل الدراسي الأول- ٢٠٢٤

Contenido

الفصل الأول: الإطار العام للدراسة

١, ١	المقدمة	٤
١, ٢	مشكلة البحث	٥
١, ٢, ١	الفجوات النظرية	٥
١, ٢, ٢	الفجوات العملية	٥
١, ٣	أهمية البحث	٦
١, ٣, ١	أهمية عملية	٦
١, ٣, ٢	أهمية نظرية	٦

الفصل الثاني: الدراسات السابقة

١, ٢	الملخص	٨
٢, ٢	المقدمة	٩
٢, ٣	الصرعات	١٠
٢, ٤	الانماط	١١
٢, ٥	اثار البحث	١٣
٢, ٦	نتائج الدراسة	١٦
٢, ٧	الخاتمة	١٧
٢, ٨	المراجع	١٨
٢, ٩	جدول الاشكال	١٩

الفصل الأول

الإطار العام للدراسة

مقدمة

يحتاج كل شخص متصل بالإنترنت إلى الأمن السيبراني أو ما يعرف بالأمن الإلكتروني، حيث إنه من الخطأ اعتقاد الأفراد بأنهم غير معرضين للهجمات عبر الإنترنت، فإن الهجمات الإلكترونية تتم آليًا وتهدف بمهاجمة نقاط الضعف بدلاً من مواقع المؤسسات ومواقع الويب المحددة، أما الأمن السيبراني فهو تطبيق التقنيات والعمليات والضوابط بهدف حماية الأنظمة والشبكات والبرامج والأجهزة والبيانات من التعرض للهجمات الإلكترونية كما يعرف الأمن السيبراني بأنه ممارسة الدفاع عن أجهزة الكمبيوتر والأجهزة المحمولة والخوادم من الهجمات الضارة، ويعرف أيضًا باسم أمن تكنولوجيا المعلومات، أو أمن المعلومات الإلكترونية.

هو الأمن الذي يهدف إلى حماية الأنظمة والشبكات والبرامج والبيانات من الهجمات الإلكترونية التي قد تسبب خسائر مادية أو معنوية أو تعطيل للعمليات التجارية أو الحكومية .

بأنه يقوم بحماية البيانات من المهاجمين الذين يهدفون لإيجاد ضرر عند سرقة المعلومات حيث يمكن أن تكون هذه البيانات حساسة مثل معلومات شخصية أو حكومية أو صناعية، يعد وجود آليات للدفاع عن البنية التحتية في المجتمع أمرًا مهمًا مثل حماية بيانات المستشفيات وبرامج الخدمات المالية التي تخدم المجتمع، أما على المستوى الفردي فيحمي الأمن السيبراني المعلومات الشخصية ويساعد على الحد من محاولات سرقة الهوية والابتزاز والتي تلحق ضررًا على حياة الفرد.

على أنها عملية رصد وتقييم التهديدات الإلكترونية المستهدفة لبيانات وبرامج وأجهزة المؤسسات، إلى جانب تطبيق خطط للحد من المخاطر، بالإضافة إلى استخدام وسائل الحماية من المخاطر الإلكترونية. أما عن معنى الامتثال فيشير إلى الالتزام بالشروط الصناعية والتنظيمية، إلى جانب الشروط القانونية مثل اللائحة العامة لحماية البيانات (GDPR) ، وهي الشروط التي تتحكم في التعامل مع البيانات ومشاركتها وحفظها.

مشكلة البحث

ولا يتوقف الأمر عند هذا الحد، بل يزداد سوءا بسبب مشكلة جديدة؛ إذ يستعد أكثر من ثلث المتخصصين في الأمن السيبراني على مستوى العالم للاستقالة من أعمالهم ووظائفهم لأسباب متعددة، وهو ما سيضع الشركات والمؤسسات في خطر شديد في الوقت الذي تكافح فيه لحماية شبكاتها من الهجمات والتهديدات الأمنية التي لا تكاد تنقطع.

الفجوات النظرية ١, ٢

تحليل الفجوات هو عبارة عن آلية تساعدنا في معرفة الوضع الراهن وبناءً عليه يتم دراسة الوضع المستقبلي أو المرغوب فيه. وغالباً ما يكون الغرض الرئيسي من هذا هو تقييم مخاطر الأعمال المرتبطة، على سبيل المثال، بالأمن السيبراني والعمليات الحالية والأدوات المتاحة والموارد البشرية لمواجهة التحديات في مجال الأمن السيبراني والتطور التقني، واللوائح التشريعية، والاستعداد لحماية الموظفين والعملاء من الهجمات الحديثة، وتحديد الثغرات، وتحديد أولوياتها حسب مستوى المخاطر وتقديم توصيات لسدّ هذه الفجوات والتخفيف من المخاطر المستقبلية

2.2 الفجوات العلمية

ولكن مع ازدياد استخدام التكنولوجيا والإنترنت، تزداد أيضاً تعقيدات وتطورات الهجمات الإلكترونية، وتظهر أشكال جديدة من الجرائم والاحتمالات التي تستغل ثغرات الأمن السيبراني. لذلك، يجب على المؤسسات والأفراد توخي الحذر والوعي بأهمية الأمن السيبراني، واتباع الممارسات الجيدة للحفاظ على سلامة أنظمتهم وبياناتهم، والاستفادة من التقنيات والخبرات المتاحة لتعزيز قدراتهم في مجابهة التهديدات الإلكترونية.

سؤال البحث الرئيسي

تتناول هذي الدراسة التساؤل البحثي الرئيسي التالي:

"ما هي بعض الخطوات التي يمكنك اتخاذها لتعزيز الأمن السيبراني الخاص بك؟"

اهمية البحث

ما اهمية الامن السيبراني؟، ولماذا تستخدمها الشركات وأغلب القطاعات؟، وما هي فوائدها؟، كل تلك الأسئلة يتم طرحها من قبل العديد من الأفراد لذلك شركة لحلول الويب سوف تجيب لكم على كل تلك الأسئلة بشكل مفصل ودقيق من خلال الفقرات القادمة.

تعد شركة النور أون لاين واحدة من أفضل الشركات التي تعمل على توفير خدمات الأمن السيبراني، نعتمد على أفضل الأساليب العالمية لحماية كافة الأنظمة المتصلة بالإنترنت.

اهمية نظرية 1.3

وهو يقوم على حماية الشبكات، وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقّمه من خدمات، وما تحويه من بيانات؛ من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات، والأمن الإلكتروني، والأمن الرقمي ونحو ذلك.

اهمية العلمية ٢,٣

الأمن السيبراني أمر بالغ الأهمية للمؤسسات من جميع الأحجام. يمكن للشركات والأفراد المساهمة في تحسين الأمن السيبراني من خلال اتخاذ مجموعة من الإجراءات، مثل اتباع أفضل الممارسات الأمنية، والتدريب على الأمن السيبراني، والمشاركة في حملات التوعية.

يعتبر من أهم الفروع الخاصة بالتكنولوجيا تهدف إلى حماية كافة المعلومات الهامة الخاصة بالشركات من الهجمات الإلكترونية التي تؤدي في النهاية إلى انتهاك خصوصية المؤسسات أو حتى الأفراد.

تزداد الاسئلة عن هذا الموضوع مثل ما هي اهمية الامن السيبراني، وما هو الامن الالكتروني واسئلة اخري كثيرة سنوضح معظمها في هذا المقال

لذلك بعد التقدم الكبير الذي حدث في عالم التكنولوجيا وأيضاً مع تطور المعاملات الرقمية المختلفة أصبح الاعتماد على الأمن السيبراني من أهم الأمور في وقتنا هذا،

الفصل الثاني

الدراسات السابقة

جميع الاجراءات والتدابير والتقنيات والأدوات المستخدمة لحماية سلامة الشبكات والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به ، ويشمل كذلك حماية الأجهزة والبيانات

دراسة المعهد العربي للتخطيط (٢٠١٩) مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي

حاولت هذه الدراسة تسليط الضوء على أهمية المخاطر الالكترونية وآثارها الاقتصادية وكيفية إدارتها، وأعطت نماذج دولية لحوادث الإصابة بها .

ثم حُلّت وقيمت أوضاع دول مجلس التعاون الخليجي كنموذج أو دراسة حالة . وهدفت من ذلك الى زيادة الاهتمام بالاستثمار في الأمن الإلكتروني واستدراك الثغرات في التخطيط الاقتصادي لمجابهة هذه المخاطر، وتتصدر دول مجلس التعاون الخليجي دول العالم الأخرى في بعض أنواع الهجمات السيبرانية على الأنشطة الاقتصادية مثل معدلات البرمجيات الخبيثة بالبريد الإلكتروني ونسب البريد الإلكتروني المؤذي .

كما تفوق الخسائر الناجمة عن الهجمات الالكترونية في دول المجلس المتوسط العالمي . وعلى الرغم من تحسن أداء دول المجلس في مجال مواجهة الهجمات الالكترونية، إلا أن الدليل العالمي للأمن السيبراني الذي تصدره الأمم المتحدة يشير إلى وجود العديد من الثغرات القانونية والفنية والتنظيمية والتدريبية والتعاونية التي يجب سدها من خلال تحسين الأداء والإكمال والمراجعة للوضع الراهن في هذه الجوانب . ولا تكفي زيادة الإنفاق بمفردها في مواجهة التهديدات وتحقيق الأمن السيبراني في دول المجلس، بل لابد من تحسين الوعي والحوكمة والعمليات لأن هذه المنطقة هي إحدى أكثر مناطق العالم تقدماً في سرعة تبني واعتماد التكنولوجيا الحديثة

المقدمة

دراسة الشيتي (٢٠١٩) حول تقييم سياسات أمن وخصوصية المعلومات في مؤسسات التعليم با لملكة العربية السعودية، مع التطبيق علي جامعة القصيم . توصلت الدراسة الي ضرورة وجود برامج توعية الموظفين وتشجيع البحوث في مجال الأمن السيبراني وأهمية تكامل وصحة البيانات في مؤسسات التعليم.

حاولت الدراسة اقتراح اطار لحوكمة الأمن السيبراني في الجامعات الحكومية بالمغرب ، خلصت الدراسة الي استخدام نظام الأمن السيبراني في المؤسسات الأكاديمية سنؤدي الي فوائد عديدة ادارية ومادية وأكاديمية .

دراسة العتيبي (٢٠١٧) حول دور الأمن السيبراني في تعزيز الأمن الإنساني :

تمثلت مشكلة الدراسة في محاولة الاجابة عن سؤال رئيس : مادور الأمن السيبراني في تعزيز الأمن الانساني ؟

تكون مجتمع الدراسة من العاملين في مجال الأمن السيبراني في شركة أرامكو السعودية فرع منطقة الرياض . عينة الدراسة (٤٠٠) فرد تم اختيارهم عشوائيا ، استخدمت الدراسة المنهج الوصفي التحليلي طبقت استبانة لجمع المعلومات من عينة الدراسة ، كما استخدمت المقابلة من اهم نتائج الدراسة:

- أن الإجراءات الفنية لحماية الفضاء السيبراني للشركة متوفرة بدرجة كبيرة، حيث يتم قفل ال نظام آلياً في حالة عدم استخدامه لفترة زمنية محددة - أن الإجراءات التقنية لحماية الفضاء السيبراني الخاص بالشركة متوفرة بدرجة كبيرة، استخدام القياسات الحيوية (بصمة العين – بصمة الإصبع – بصمة الصوت) لمرور المصرح لهم.

أوصي الباحث بضرورة العمل على اتباع الوسائل العلمية والعملية لحفظ الأمن السيبراني للمؤسسات والشركات الحكومية والخاصة ، كما أوصي بالمزيد من التعمق في دراسة الربط ما بين مجال الأمن السيبراني والأمن الإنساني .

دراسة البكري (٢٠١٧) حول أمن المعلومات بالمكتبات الجامعية السودانية، هدفت التعرف علي مخاطر عدم تأمين المعلومات وكيفية تأمينها بالنسبة للمكتبات الجامعية، استخدم البحث المنهج التاريخي ن خلال الاطلاع علي الأدبيات المنشورة وأداة الملاحظة للمكتبات الجامعية بالسودان .

دراسة (Rehman) وآخرون ٢٠١٥، حول واقع أنظمة ادارة الأمن السيبراني في معاهد التعليم العالي بجامعات باكستان ، أوصت بضرورة وجود ادارة للمخاطر الموجودة، ووضع سياسات أمنية لمعالجة هذه المخاطر .

ويبدو أن الدراسات السابقة في مجال الأمن السيبراني مازالت محدودة (علي حد علم الباحثة) الا أن ماتم من أبحاث علمية أو أدبيات نظرية أكد علي أهمية دراسة الأمن السيبراني

من مختلف أبعاده، والدراسة الحالية تسير في نفس الاتجاه لتعزيز فكرة وثقافة الأمن السيبراني خاصة في المجال الجامعي حيث أنها تكاد تكون محدودة جداً.

الصرعات

تعد الهجمات السيبرانية عمليات قرصنة واختراق للأنظمة الإلكترونية، تهدف إلى الوصول إلى المعلومات الحساسة أو إلحاق الضرر بالهياكل التقنية. قد تتضمن هذه الهجمات القرصنة الإلكترونية، والبرامج الضارة، والتصيد الاحتيالي، والتجسس، والهجمات الموجهة على الشبكات.

لحماية البيانات والأنظمة الحاسوبية في السويد، يمكن اتباع بعض الإجراءات الأساسية، مثل:

١. تحديث البرامج والأنظمة الحاسوبية بانتظام لسد الثغرات الأمنية.
٢. استخدام كلمات مرور قوية وتغييرها بانتظام.
٣. تفعيل الحماية النشطة مثل "جدران الحماية النارية firewall" وبرامج مكافحة الفيروسات وبرامج مكافحة برامج التجسس.
٤. توعية الموظفين حول التهديدات السيبرانية وتدريبهم على كيفية التعامل معها.

الفجوات :

معنى كلمة سيبراني (cyber)

تطلق كلمة "سيبراني" على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، والفضاء السيبراني يعني الفضاء الإلكتروني (Cyberspace)، وهو يعني كل ما يتعلق بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة

(كالوتسآب، والفيس بوك، وغيرها من منصات التطبيقات)، وكل الخدمات التي تقوم بتنفيذها (كتحويل الأموال عبر النت، والشراء أون لاين، وغيرها من آلاف الخدمات في جميع مجالات الحياة على مستوى العالم

[\(https://www.mah6at.net/\)](https://www.mah6at.net/)

الأمن السيبراني :

-يقصد بالأمن السيبراني " Security Cyber " حماية الأشياء من خلال تكنولوجيا المعلومات مثل الأجهزة والبرمجيات ويشير إليها " ICT " وذلك اختصار Communication Technologies and Information

والقول بالأمن السيبراني يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستخدمة تقنيا وتنظيميا وإداريا في منع الوصول غير المشروع للمعلومات الإلكترونية ومنع إستغلالها بطريقة غير قانونية ونظامية، وبذلك فإنه يهدف إلى الحفاظ على إستمرارية الأنظمة والمعلومات المتوفرة بها، وحمايتها بكل خصوصية وسرية من خلال إتباع التدابير والإجراءات اللازمة لحماية البيانات

. الأمن السيبراني لغويا : الأمن السيبراني مكون من لفظتين : "الأمن"، و"السيبراني" الأمن : هو نقيض الخوف، أي بمعنى السلامة. والأمن مصدر الفعل أمن و أمناً وأماناً وأمنةً :أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أمن □ من الشر، أي سلام منه.

السيبراني :مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وكلمة "cyber" لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم . "governor" وأشار بعض المؤرخين الي أن أصلها يرجع إلى عالم الرياضيات الأمريكي

الأنماط

اصطلاحاً: هناك العديد من التعاريف التي قُدمت لمفهوم الأمن السيبراني، حيث يعرف بأنه "مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة".

وهذا ما ذهب إليه الكاتبان Martti Lehto, Pekka Neittaanmäki في كتابهما Cyber Automation and Technology :Security Analytics، حيث عرفا الأمن السيبراني أنه : "عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قرصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة".

بينما عرفه (إدوارد أمورسو) Edward Amoroso بأنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة.

وفي التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام ٢٠١٠-٢٠١١ عرف الأمن السيبراني بأنه: "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين".

وقدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني فاعتبرته " جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم : الهجمات، التخريب، التجسس والحوادث ". في حين اعتبر الإعلان الأوروبي الأمن السيبراني أنه " قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات. "

وتجدر الإشارة إلى أن الأمن السيبراني مفهوم أوسع من أمن المعلومات، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا يهتم بذلك، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية " الورقية"، بينما لا يهتم الأمن السيبراني بذلك. (الموسوعة السياسية-<https://political.encyclopedia.org/dictionary/>)

هناك العديد من المفاهيم المرتبطة بالأمن السيبراني، ومن أهمها ما يلي:

الفضاء السيبراني :عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI، بأنه: "فضاء التواصل المشكّل من خلال الربط البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية ".فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، م كون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين .

الردع السيبراني : يعرف الردع السيبراني بأنه " منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية"

الهجمات السيبرانية تعرف بأنها " :فعلاً يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكن المهاجم من التلاعب بالنظام."

الجريمة السيبرانية :مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها

(<https://political-encyclopedia.org/dictionary/>)السياسية الموسوعة

وإجمالاً يمكن القول إن الأمن السيبراني هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر (الفضاء السيبراني بصفة عامة) من مختلف الهجمات والاختراقات والتهديدات السيبرانية التي قد تهدد الأمن القومي للدول.

أمن المعلومات " Security Information "

هو حماية بيانات المؤسسة ويعتمد ذلك علي ثلاث محاور رئيسية ويرمز لها " CIA " وهي السرية " Confidentiality " سلامة المعلومة " Integrity " إتاحة المعلومة في أي وقت " Availability " أحمد عيسى ٢٠١٩،

وهو عبارة عن مجموع من الإجراءات التقنية والإدارية تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به بالتجسس أو الاختراق لاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات، كما تضمن تأمين وحماية وسرية وخصوصية البيانات الشخصية للمواطنين، كما تشمل استمرارية عمل حماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف.

اثار البحث

هناك عدد من الأسباب التي تجعل دراسة الأمن السبراني من أبرز المجالات التي تحتاج لوجود خبراء مؤهلين لحماية أمن الشركات والمؤسسات والدول أيضا، ومن أبرزها:

١ . يشهد سوق العمل حاجة مستمرة لخبراء مجال الأمن السبراني.

٢ بالعمل في مجال الأمن السبراني يمكن جني الكثير من الأرباح المالية.

٣ الخبرة في مجال الأمن السبراني ستكون غاية لكل مؤسسة مميزة.

٤ يشمل الأمن السبراني كافة المجالات العملية بالرغم من اختلافها وتنوعها.

٥ تمكين الدارس من الحصول علي امتيازات فريدة في العمل

أهم المسارات الوظيفية المتاحة بعد دراسة الأمن السبراني

يشهد هذا المجال اقبال وطلب كبير في شتى المجالات، ولذلك تشير التقارير والإحصاءات العالمية إلى زيادة كبيرة في طلب محترفي الأمن السبراني، حيث أن سوق الأمن السبراني قد نما وتطور في كافة دول العالم بشكل ملحوظ، ففي عام ٢٠٠٤ كان يقدر ب ٣,٥ مليار دولار، بينما كان في عام ٢٠١٥ يكلف ٧٥ مليار دولار، ويتوقع أن يحقق ما يقارب ١٧٠ مليار دولار في. (<https://ab7as.net>) ٢٠٢٠

عام ومن المتوقع عقب دراسة الأمن السبراني والحصول على درجة البكالوريوس سيجد الخريج العديد من الفرص الوظيفية المميزة في عدد من المجالات، وتنوع المسارات الوظيفية التابعة لتلك الدراسة، حيث تشمل : مهندس الدعم السحابي، متخصص دعم تكنولوجيا المعلومات، مهندس الدعم الفني، مطور برامج وتطبيقات -مسؤول الشبكات -مسؤول الطب الشرعي الرقمي.

أنواع الجرائم السبرانية :

تتعدد جرائم الأمن السبراني ، من أهم هذه الجرائم :

جرائم التعدي على البيانات المعلوماتية ، التعدي على الأنظمة المعلوماتية، إساءة استعمال الأجهزة أو البرامج المعلوماتية، الجرائم الواقعة على الأموال ،الاستغلال الجنسي للقاصرات، التعدي على الملكية الفكرية للأعمال الرقمية، البطاقات المصرفية والنقود الإلكترونية، جرائم تمس المعلومات الشخصية، جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية، جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت، الجرائم المعلوماتية ضد الدولة والسلامة العامة، وجرائم تشفير المعلومات. ([net.as7ab://https](https://net.as7ab.net))

المجتمع وحفظ الحقوق فيه بكافة ما يتضمن من أبعاد ويقوم الأمن السيبراني في هذا البعد على حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات

آليات (متطلبات) تحقيق الأمن السيبراني (<https://www.arageek.com/>)

قد تساعدك الخطوات البسيطة أدناه في الحفاظ على مستوى جيد من الأمان والسلامة السيبرانية :

-الموثوقية : وتعني استخدام المواقع الموثوق بها عند تقديم معلومات شخصية، والقاعدة الأساسية هي التحقق من عنوان URL، وإذا كان الموقع يتضمن https في بدايته، فهذا يعني أنه موقع آمن، أما إذا كان عنوان URL يحتوي على http بدون s؛ فيجب الحذر من إدخال أي معلومات حساسة مثل بيانات بطاقة الائتمان، أو رقم التأمين الاجتماعي.....الخ-

البريد الاحتمالي : ويعني عدم مرفقات البريد الإلكتروني أو النقر فوق روابط الرسائل من المصادر غير المعروفة، إذ إن إحدى الطرق الأكثر شيوعا التي يتعرض فيها الأشخاص للسرقة أو الاختراق هي عبر رسائل البريد الإلكتروني المتخفية على أنها رسالة من شخص موثوق به.

-التحديثات (date-to-up Always) وتعني الحرص دائما على تحديث الأجهزة ، فغالبا ما تحتوي تحديثات البرامج على تصحيحات مهمة لإصلاح مشكلات الأمان، وإن هجمات المخترقين الناجحة تتركز على الأجهزة القديمة بنسبة كبرى، والتي لا تملك أحدث برامج الأمان

- النسخ الاحتياطي : ويتطلب هذا عمل نسخ احتياطية من الملفات بانتظام لمنع هجمات الأمان على الإنترنت

الاطار الميداني:

لتحقيق هدف البحث تم تطبيق الاستبانة علي عينة قوامها (٤٧٨) تمثل نسبة حوالي (٥%) من المجتمع الأصلي من جميع العاملين بالجامعة وعددهم (٩٣٢٧) والجدول التالي يوضح توزيع أفراد العينة .

الجنس	عدد	%	المسمى الوظيفي	عدد	%
ذكور	226	47	أكاديمي	180	38
إناث	252	53	إداري	292	62
مجموع	478	100	مجموع	477	100

نجاح المشاريع:

توزيع عينة البحث وفقا لمتغيري المؤهل العلمي وسنوات الخدمة.

المؤهل العلمي	عدد	%	سنوات الخدمة	عدد	%
ثانوية عامة أو أقل	2	٠.٤	١-٥	٧٤	١.٥
بكالوريوس	191	٤٠	٦-١٠	١١٢	٢.٤
ماجستير	174	٣٠.٤	١١-١٥	١٨٣	٣.٣
دكتوراه	111	٢٣.٢	١٦-٢٠	١٠٩	٢.٨
مجموع	478	١٠٠	مجموع	٤٧٨	١٠٠

المعالجة الاحصائية-

تمت إجراءات المعالجة الإحصائية للبيانات الواردة في الاستبانة باستخدام برنامج الحزم (SPSS)

(Statistical Package for Social Sciences) الاجتماعية للعلوم الاحصائية - تم حساب قيمة كا ٢ لحسن المطابقة لكل مفردة، وذلك للكشف عن الفروق في اختيارات أفراد العينة لبدائل الاستجابة الثلاثة (موافق - غير متأكد - غير موافق) وذلك بتطبيق المعادلة الآتية :

كا ٢ = مج (ت - ت م) / ٢ ت م

حيث أن ت = التكرار الملاحظ أو التجريبي.

ت م = التكرار المتوقع.

- حساب التكرارات ونسبتها لكل مفردة .

-حساب التقدير الرقمي لكل مفردة من خلال المعادلة الآتية:

التقدير الرقمي = ٣ * تكرار موافق + ٢ * تكرار غير متأكد + ١ * تكرار غير موافق

-حساب الوزن النسبي لكل مفردة، من خلال المعادلة الآتية:

الوزن النسبي = التقدير الرقمي X ١٠٠ / ن

ن = عدد العينة

-ترتيب العبارات حسب الوزن النسبي أو الأهمية النسبية لكل منها؛ حيث إن: الأهمية النسبية أو التقدير المئوي = الوزن النسبي / عدد البدائل

نتائج الدراسة

نتائج المحور الأول: المتطلبات الادارية

استهداف البحث قياس الإفصاح عن مخاطر الأمن السيبراني -

من خلال توضيح مخاطر هجمات الأمن السيبراني وأهمية الإفصاح عنها،

وتوضيح وتفسير العوامل المؤثرة في العلاقة بين الإفصاح عن مخاطر الأمن السيبراني وأتعباب المراجعة، حيث تمثل مجتمع الدراسة في الشركات المقيدة في البورصة المصرية والمناحة للتحميل على الموقع الإلكتروني للبورصة المصرية،

وتمثلت عينة الدراسة في عدد من هذه الشركات والتي يتوافر فيها بيانات قياس المتغيرات وعددها (١٥) شركة ، حيث تم الاعتماد على القوائم المالية للشركات عينة الدراسة خلال الفترة من ٢٠١٧ حتى ٢٠٢١.

وتقارير الحوكمة، وتقارير هيكل المساهمين وهيكل مجلس الإدارة ومحاضر اجتماعات لجان المراجعة ومحاضر اجتماع الجمعية العمومية.

وتوصلت نتائج الدراسة النظرية والتطبيقية إلى العديد من النتائج تمثل أهمها في وجود ارتباط إيجابي بين أتعباب عملية المراجعة ومخاطر اختراقات الأمن السيبراني، حيث أن مراجعي الحسابات عندما يجدون مخاطر الأمن السيبراني متزايدة يبذلون المزيد من الجهد أثناء عملية المراجعة الأمر الذي يؤدي إلى فرض أتعباب مرتفعة.

يحتل الأمن والقضاء السيبراني باهتمام العديد من الباحثين خاصة مع ظهور تهديدات قد تصل لحرب إلكترونية. وفي هذا السياق، اهتم علماء السياسة بتفسير هذه القضايا، الأمر الذي خلق ساحة من الجدل والنقاش حول تأثير الأمن السيبراني على شكل النسق الدولي، وما يتضمنه من وحدات ومؤسسات وبنية وتفاعلات وعمليات عالمية تقع في نطاقه.

ويقدم هذا البحث استعراضاً لأهم القضايا الجدلية المطروحة بين علماء السياسة في هذا الشأن. وينقسم البحث بدوره لأربعة مباحث رئيسة المبحث الأول يتناول الوحدات الدولية الفاعلة في النظام الدولي، أما المبحث الثاني فيناقش تأثير الأمن السيبراني على مجموعة المؤسسات الدولية،

في حين أن المبحث الثالث يطرح التغير الذي أحدثه الأمن السيبراني على هيكل النظام الدولي، أما المبحث الرابع يستعرض لأبرز العمليات الدولية الواقعة داخل الفضاء السيبراني بالنسق الدولي.

وتستخدم الورقة اقتراب النسق الدولي (الاقتراب النظمي) للوقوف على هيكل النظام الدولي والفواعل الرئيسية بداخل الفضاء السيبراني

وما أحدثه الأمن السيبراني من تغير على القواعد والعمليات بداخل نسق الدولي.

الخاتمة

أن الأمن السيبراني في الوقت الحاضر أصبح تخصصًا جامعيًا يدرسه الآلاف من الطلبة نظرًا لأهمية هذا التخصص الدقيق، وقدرته على إحداث فرق في مجال أمن المعلومات.

لهذا فإنّ تخصص الأمن السيبراني بوصفه تخصصًا دقيقًا هو تخصص المستقبل الذي تسعى إليه جميع الشركات والمؤسسات الحكومية والخاصة، لذا تعمل الشركات بجد لأجل توسيع قاعدة استخدام الأمن السيبراني

وبشكلٍ عام يمكن اعتبار الأمن السيبراني جزءًا من تخصص هندسة الحاسوب أو تخصص علوم الحاسب الآلي، وفي المجال الشخصي الذي يتعلق بالمعلومات الشخصية فإنّ تخصص الأمن السيبراني يمنع الوصول إلى حسابات الأشخاص سواءً أكانت حسابات التطبيقات الشخصية أم حساباتهم في البنوك والشركات.

كما أن الأمن السيبراني يوسع إمكانية العمل بأمان دون أي مخاطر أمنية لاختراق المعلومات، وقطع الطريق على مستخدمي برامج التجسس واختراق أجهزة الحواسيب وأجهزة الهواتف النقالة، وهذا يترك أثرًا رائعًا في مختلف المجالات لأنه يحافظ على الخصوصية والسرية إلى أقصى درجة.

يجب القول ان الأمن السيبراني ذات أهمية بالغة في عالم تكنولوجيا المعلومات الحالي، فقد تطورت أساليب الهجمات السيبرانية بشكل كبير، مما يشكل تهديدًا جدّيًا على الأفراد والشركات والمؤسسات.

ومن خلال تحقيق الأمن السيبراني، يتم حماية البيانات والشبكات والأنظمة من الاختراق والاستغلال غير القانوني، وتعتبر اتخاذ سياسات أمنية قوية وتوظيف التكنولوجيا المتقدمة مثل تحليل الضوابط وانترنت الأشياء والتعرف على السياق واسعة النطاق، ضرورةً ملحةً لمكافحة التهديدات السيبرانية.

كما تُعزز الوعي والتدريب في مجال الأمان السيبراني قدرة الأفراد والمؤسسات على التعامل مع التحديات الأمنية الرقمية بفعالية

الفصل الأول:

١. كتاب مقدمة في الأمن السيبراني
٢. إحسان الحافظي. السياسات الأمنية في المغرب: في السلطة وأدوار النخب السياسية. المركز العربي للأبحاث ودراسة السياسات، ٢٠٢٠.
٣. منشآت
٤. رحيم، et al. الأمن السيبراني في المنشآت الحكومية. المجلة الجزائرية للدراسات السياسية، ٢٠٢٣، ١، ١٠٩-١٧٩.
٥. نور اون لاين
٦. حمدي، et al. المعالجة الصحفية لظاهرة الاحاد في الصحافة الالكترونية في الجزائر. (٢٠٢٢).
٧. مبتعث
٨. العتيبي، and عبد الرحمن بن بجاد شارع. دور الأمن السيبراني في تعزيز الأمن الإنساني.. Diss. 2017.
٩. الخبير
١٠. الغبيوي، et al. الأمن السيبراني ودوره في الحد من تهديدات الأمن الفكري. Diss. جامعة نايف العربية للعلوم الأمنية، ٢٠٢٠.
١١. RMG

الفصل الثاني:

١. الغبيوي، et al. الأمن السيبراني ودوره في الحد من تهديدات الأمن الفكري. ٢٠٢٠. PhD Thesis. جامعة نايف العربية للعلوم الأمنية.
٢. سراج، شيماء أحمد محمد أحمد and شيماء أحمد محمد أحمد. "التحليل البعدي لدراسات الأمن السيبراني في المجال التربوي". *المجلة العربية للعلوم التربوية والنفسية*. 199-212: (2022)
٣. دياب، إكرام and إكرام عبد الستار محمد. "تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا، وجامعة طوكيو باليابان وإمكان الاستفادة منها في مصر *International Journal of Sustainable Development and Science* 6.3 (2023): 140-205.
٤. محمد صدقي محمد، عماد. "دور لجان المراجعة كأحد آليات الحوكمة لمواجهة مخاطر الهجمات السيبراني في البنوك المصرية: دراسة ميدانية". *مجلة البحوث التجارية*. 248-300: (2023) 45.4

جدول الأشكال

رقم الشكل	عنوان الشكل	رقم الصفحة
١	عدد العاملين بالجامعة	١٣
٢	الموهل العملي	١٤

المشروع نهائي 2

إشراف

د. منى مصطفى العشري

عضو هيئة التدريس - كلية الإدارة - جامعة ميداووشن.

الفصل الدراسي الثاني - ٢٠٢٤ .

" فصل الملاحق "

استبيان

تحية طيبة :

الأمن السيبراني هو مجال حيوي ومتنامي يهدف إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. تزداد أهمية الأمن السيبراني يومًا بعد يوم مع تزايد الاعتماد على التكنولوجيا الرقمية في جميع جوانب الحياة الشخصية والمهنية.

تتطلب الهجمات السيبرانية، مثل البرمجيات الخبيثة، والاحتتيال الإلكتروني، والاختراقات، وجود إجراءات وقائية واستراتيجيات دفاعية فعالة للحفاظ على سرية وسلامة البيانات والمعلومات. ومن هنا، يصبح فهم وتطبيق ممارسات الأمن السيبراني أمرًا ضروريًا للأفراد والمؤسسات على حد سواء.

يهدف هذا الاستبيان إلى جمع المعلومات حول مستوى الوعي والممارسات الأمنية لدى الأفراد والشركات فيما يتعلق بالأمن السيبراني. من خلال هذا الاستبيان، نسعى إلى تحديد الثغرات والاحتياجات التدريبية والتكنولوجية لتحسين التدابير الأمنية وتقليل المخاطر السيبرانية.

نقدر مشاركتكم في هذا الاستبيان، والذي سيساعدنا في تقديم توصيات وتحسينات مستندة إلى البيانات لتطوير بيئة رقمية أكثر أمانًا وموثوقية.

الأسئلة الشخصية :

١. *المعلومات الديموغرافية:*

- ما هو عمرك؟
- ما هو جنسك؟
- ما هو مستوى تعليمك؟
- ما هو مجال عملك؟
- ما هي الدولة التي تقيم فيها؟

٢. *الوعي بالأمن السيبراني:*

- هل سبق لك أن سمعت عن الأمن السيبراني؟
- من خلال أي مصادر تحصل على معلوماتك حول الأمن السيبراني؟ (التلفاز، الإنترنت، العمل، الأصدقاء، إلخ)
- ٣. *السلوكيات الأمنية:*

- هل تستخدم برامج مكافحة الفيروسات على أجهزتك الشخصية؟
- هل تقوم بتحديث برامجك وأنظمة التشغيل بانتظام؟
- كم مرة تقوم بتغيير كلمات المرور الخاصة بحساباتك الإلكترونية؟
- هل تستخدم المصادقة الثنائية (Two-Factor Authentication) لحماية حساباتك؟

٤. *التجارب الشخصية:*

- هل سبق لك أن تعرضت لأي هجوم سيبراني (مثل اختراق الحسابات، البرمجيات الخبيثة، التصيد الاحتيالي)؟
- إذا كانت الإجابة بنعم، فما هو نوع الهجوم وكيف تعاملت معه؟

٥. *الإجراءات الوقائية:*

- ما هي التدابير الأمنية التي تتبعها لحماية معلوماتك الشخصية على الإنترنت؟
- هل تعتقد أن معرفتك الحالية كافية لحمايتك من التهديدات السيبرانية؟

٦. *التعليم والتدريب:*

- هل سبق لك أن تلقيت أي تدريب أو تعليم يتعلق بالأمن السيبراني؟
- إذا كانت الإجابة نعم، ما مدى فعالية هذا التدريب في تحسين معرفتك وممارساتك الأمنية؟

٧. *التصورات والاتجاهات:*

- ما مدى قلقك بشأن الأمان السيبراني؟
- ما هي أبرز المخاوف التي تراودك عند استخدام الإنترنت؟

تساهم هذه الأسئلة في جمع بيانات قيمة تساعد في فهم مستوى الوعي والسلوكيات والاحتياجات المتعلقة بالأمن السيبراني، مما يمكن الجهات المختصة من تطوير برامج تدريبية وإجراءات أمنية فعالة.

المصدر	عدد البيانات	ابعاد المتغير	المتغير
عنوان البحث الوعي بالأمن السيبراني	٤	البعد الأول : الفهم الأساسي لمفاهيم الأمن السيبراني	المتغير الأول
	٤	البعد الثاني : التصورات والاتجاهات نحو الأمن السيبراني	

أسئلة حول الوعي بالأمن السيبراني:

١. * ما مدى معرفتك بالأمن السيبراني؟*

- غير مطلع
- مطلع بشكل قليل
- مطلع بشكل متوسط
- مطلع بشكل جيد
- مطلع بشكل ممتاز

٢. * هل تعلم ما هي البرمجيات الخبيثة (Malware)؟*

- نعم
- لا

٣. * هل سمعت عن التصيد الاحتيالي (Phishing)؟*

- نعم
- لا

٤. * ما هي المصادر التي تعتمد عليها للحصول على معلومات حول الأمن السيبراني؟*

- مواقع الإنترنت
- الكتب والمقالات
- الدورات التدريبية
- الأصدقاء والزملاء
- وسائل الإعلام (التلفاز، الراديو، الصحف)

المصدر	عدد البيانات	ابعاد المتغير	المتغير
عنوان البحث الوعي بسياسات وإجراءات الأمن السيبراني	٥	البعد الاول : تقييم وإدارة المخاطر	المتغير الثاني
	٥	البعد الثاني : الوعي والتدريب	
	٤	البعد الثالث: الحماية التقنية	

اسئله عن الوعي بسياسات وإجراءات الأمن السيبراني

هذا البعد يركز على معرفة الأفراد بالسياسات والإجراءات الأمنية المعمول بها، سواء في مكان العمل أو في حياتهم الشخصية.

أسئلة:

- هل تعرف سياسات الأمان السيبراني في مكان عملك؟
- هل تتبع إرشادات الأمان عند استخدام الإنترنت في العمل؟
- هل تعلم كيفية الإبلاغ عن الحوادث الأمنية في مؤسستك

استبيان عن الوعي بسياسات الأمن السيبراني:
يمكن أن يكون طريقة فعالة لتقييم معرفة الأفراد ومدى التزامهم بالممارسات الآمنة على الإنترنت.

استبيان الوعي بسياسات الأمن السيبراني

القسم الأول: المعلومات الشخصية

١. العمر:

- أقل من ١٨

- ١٨-٢٤

- ٢٥-٣٤

- ٣٥-٤٤

- ٤٥-٥٤

- ٥٥ فأكثر

٢. الجنس:

- ذكر

- أنثى

- آخر

٣. المستوى التعليمي:

- ثانوي

- دبلوم

- بكالوريوس

- ماجستير

- دكتوراه

٤. التخصص (إذا كان ذلك ينطبق):

- تكنولوجيا المعلومات
- الهندسة
- الأعمال
- العلوم الاجتماعية
- آخر

القسم الثاني: الوعي والمعرفة

٥. ما مدى معرفتك بمصطلح "الأمن السيبراني"؟

- لا أعرف
- سمعت به لكن لا أعرف تفاصيله
- لدي معرفة أساسية
- لدي معرفة متوسطة
- لدي معرفة جيدة

٦. هل تعلم ما هي سياسات الأمن السيبراني في مكان عملك أو مؤسستك التعليمية؟

- نعم
- لا

٧. هل تلقيت أي تدريب رسمي على الأمن السيبراني؟

- نعم
- لا

القسم الثالث: السلوك والممارسات

٨. هل تقوم بتغيير كلمات المرور الخاصة بك بانتظام؟

- نعم
- لا

٩. هل تستخدم المصادقة الثنائية لحساباتك على الإنترنت؟

- نعم

- لا

- لا أعرف ما هي المصادقة الثنائية

١٠. هل تتحقق من هوية مرسل البريد الإلكتروني قبل فتح المرفقات أو النقر على الروابط؟

- نعم

- لا

١١. هل تقوم بتحديث برامجك وأنظمة التشغيل بانتظام؟

- نعم

- لا

١٢. هل تستخدم برامج مكافحة الفيروسات وجدار الحماية؟

- نعم

- لا

القسم الرابع: التهديدات والتحديات

١٣. هل تعرضت سابقاً لأي هجوم سيبراني (مثل فيروسات، برمجيات خبيثة، اختراق حسابات)؟

- نعم

- لا

١٤. إذا كانت الإجابة نعم، فما هو نوع الهجوم الذي تعرضت له؟

- فيروسات/برمجيات خبيثة

- اختراق حسابات

- سرقة هوية

- فيشينغ (خداع)

- آخر (يرجى التوضيح)

١٥. ما هي الإجراءات التي تتخذها عند الشك في وجود تهديد سيبراني؟

- تغيير كلمات المرور
- الاتصال بالدعم التقني
- تثبيت/تحديث برامج مكافحة الفيروسات
- تجاهل التهديد
- آخر (يرجى التوضيح)

القسم الخامس: الرأي والتوصيات

١٦. برأيك، ما هو المستوى العام للوعي بسياسات الأمن السيبراني في مجتمعك؟

- منخفض جداً
- منخفض
- متوسط
- عالي
- عالي جداً

١٧. ما هي الوسائل التي تعتقد أنها الأكثر فعالية لزيادة الوعي بسياسات الأمن السيبراني؟

- حملات توعية
- ورش عمل وتدريب
- مواد تعليمية عبر الإنترنت
- برامج تعليمية في المدارس والجامعات

١٨. هل لديك أي اقتراحات لتحسين الوعي بسياسات الأمن السيبراني في مكان عملك أو مجتمعك؟

- (فراغ للنص المفتوح)

القسم الأخير: الملاحظات

جدول أدوات البحث:

موافق بدرجة				العبارة
كبيرة	كبيرة جيدة	متوسط	قليلة جيدة	
				المحور الأول : ابتكار المنتج
				ما مدى معرفتك بمصطلح "الأمن السيبراني"؟
				هل تستخدم برامج مكافحة الفيروسات وجدار الحماية؟
				ما هو المستوى العام للوعي بسياسات الأمن السيبراني في مجتمعك؟
				ما هي الإجراءات التي تتخذها عند الشك في وجود تهديد سيبراني؟
				هل تقوم بتحديث برامجك وأنظمة التشغيل بانتظام؟
				هل تقوم بتغيير كلمات المرور الخاصة بك بانتظام؟