



المملكة العربية السعودية

وزارة التعليم

جامعة طيبة

كلية الآداب والعلوم الإنسانية

قسم المعلومات ومصادر التعلم

فعالية برنامج تدريبي مقترن لتنمية الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الإنسانية: دراسة تجريبية

The effectiveness of a proposed training program for developing cybersecurity awareness among female students of the College of Arts and Humanities: an empirical study

مشروع بحثي لنيل درجة البكالوريوس بقسم المعلومات ومصادر التعلم

إشراف الدكتورة: أمل عبدالفتاح

إعداد الطالبات: إعداد الطالبات:

العنود عبدالعزيز الحربي

أمل عبدالله السليماني

ربى سعد المغذوي

سارة عبدالخالق السميري

صفاء ظاهر الجهني

ليان سعد الحربي

مرام خالد الشريف

هندادي مشاري المطيري

ـ 1443 هـ 2022 م

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

شكر وتقدير:

قال رسول الله صلى الله عليه وسلم:(من لم يشكر الناس لم يشكر الله عز وجل).

نحمد الله تعالى حمداً كثيراً طيباً مباركاً مليئاً السماوات والأرض على ما أكرمنا به لإتمام هذه الدراسة التي أرجوا أن تطال على رضاكم.

ونتقدم بجزيل الشكر والتقدير للدكتورة: أمل عبدالفتاح صلاح أحمد على كل ما قدمته لنا من توجيهات ومعلومات قيمة التي ساهمت في إثراء موضوع دراستنا في جوانبها المختلفة ونتقدم أيضاً بالشكر لجميع أعضاء هيئة التدريس في قسم المعلومات ومصادر التعلم في جامعة طيبة على ما قدموه من تحكيم لأدلة البحث.

لكم منا جزيل الشكر والامتنان.

المستخلص :

تتناول هذه الدراسة التعرف على فعالية برنامج تربوي مقترن لتنمية الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الإنسانية بجامعة طيبة ، ويهدف البحث الحالي إلى بناء برنامج تربوي لقياس مدى وعي طالبات كلية الآداب والعلوم الإنسانية بجامعة طيبة في الأمن السيبراني ، وعلى معرفة درجة وعيهم بالأمن السيبراني ، وتحليل وقياس مدى فعالية البرنامج التربوي المقترن من حيث جوانب القوة وتدعمها وجوانب الضعف والعمل على تقديم الاقتراحات العلاجية لمعالجتها ، وتكمّن أهمية الدراسة في أهمية الأمن السيبراني نفسه ، وذلك في حماية البيانات والأجهزة وسلامتها من مخاطر الإنتهاكات السيبرانية والمحافظة على سلامة المعلومات وذلك بالحد من الدخول الغير مصرح به إليها ، وذلك يأتي تبعاً للدور الهام للأمن السيبراني كأحد المتطلبات الضرورية لحماية مجتمعاتنا المعاصرة من مختلف أشكال الجرائم السيبرانية ، ولتحقيق أهداف الدراسة تم الإعتماد على المنهج التجريبي مستخدماً الاستبانة كأداة لجمع البيانات ، حيث تم إعداد استبانة إلكترونية مكونة من ٣٤ سؤال تضم محورين هما : الوعي بمفهوم الأمن السيبراني والوقاية من مخاطر الاختراق السيبرانية ، وتم تطبيقها على عينة عشوائية بحيث بلغ عدد العينة ١٩٢ استثمارة قبيلة و ١٨٩ استثمارة بعدية من طالبات كلية الآداب العلوم الإنسانية بجامعة طيبة، حيث توصلت الدراسة إلى عدد من النتائج من الناحية النظرية وهي أن مفهوم الأمن السيبراني لابد أن يشمل جميع الإجراءات المستخدمة في حماية المعلومات والبيانات والشبكات واختيار الوسيلة المناسبة للحماية من شتى الاختراقات، وأيضاً يستدل أن هناك ضرورة من تعاون جميع جهات وقطاعات الدولة لتشكيل منظومة تتضافر جهودها في توعوية المواطنين والحد من الاختراقات السيبرانية ، ومن الناحية التطبيقية وجد أن الغالبية العظمى من طالبات كلية الآداب والعلوم الإنسانية لم يكن لديهم معرفة سابقة في الأمن السيبراني بنسبة ٣٨٪ وبعد تقديم البرنامج التربوي بلغت نسبتهم ٨٤.٨٪ كما توصلت الدراسة إلى احتياجهم للدورات التدريبية في مجال الأمن السيبراني حيث بلغت نسبتهم قبل البرنامج ٨٠٪ وبعد تقديم البرنامج بلغت نسبتهم ٨٤٪ ، ومن أهم ما توصي به الدراسة ضرورة تقديم برامج تربوية توعوية مكثفة تختص بالأمن السيبراني و كذلك أهمية إضافة مواد ومقررات تعليمية تختص بالأمن السيبراني ، وكذلك تفعيل إدارات الأمن السيبراني في توعية طلبة الجامعة بالأمن السيبراني .

الكلمات المفتاحية:الأمن السيبراني – الهيئة الوطنية للأمن السيبراني – الأمن السيبراني في الجامعات.

Abstract:

This study deals with identifying the effectiveness of a proposed training program to develop cybersecurity awareness among female students of the College of Arts and Humanities at Taibah University. Analyze and measure the effectiveness of the proposed training program in terms of strengths and consolidation and weaknesses and work to present remedial suggestions to address them, and the importance of the study lies in the importance of cybersecurity itself, in protecting data and devices and their safety from the risks of cyber violations and maintaining information integrity by limiting unauthorized access. This comes in accordance with the important role of cybersecurity as one of the necessary requirements to protect our contemporary societies from various forms of cybercrime. With the concept of cyber security and the prevention of the risks of cyber intrusion, It was applied to a random sample so that the sample number reached 192 tribal forms and 189 dimensional forms from the students of the Faculty of Arts and Humanities at Taibah University, where the study reached a number of results in theory, namely that the concept of cybersecurity must include all procedures used to protect information, data and networks. And choosing the appropriate means of protection from various intrusions, and it is also inferred that there is a necessity for the cooperation of all parties and sectors of the state to form a system that combines its efforts in educating citizens and limiting cyber intrusions. Cyber security by 38%, and after presenting the training program, their percentage reached 84.8%. The study also found that they need training courses in the field of cybersecurity, as their percentage before the program reached 80% and after the presentation of the program their percentage reached 84%, and one of the most important recommendations of the study is the need to provide programs Intensive awareness training related to cybersecurity, as well as the importance of adding educational materials and courses related to cybersecurity, as well as activating security departments. For cyber security in educating university students about cyber security.

Keywords: cyber security – the national cyber security authority – cyber security in universities.

قائمة المحتويات:

ت	شكر وتقدير
ث	المستخلص
ج	Abstract
ح	قائمة المحتويات
ذ	قائمة الجداول
ر	قائمة الملحق
الفصل الأول: الإطار العام للدراسة	
١٢	المقدمة
١٣	أهمية الموضوع ومبررات اختياره
١٣	أهداف الدراسة
١٣	تساؤلات الدراسة
١٤	حدود الدراسة
١٤	منهج الدراسة وأدوات جمع المادة العلمية
١٥	عينة الدراسة
١٦	الدراسات السابقة
١٦	أولاً: الدراسات العربية
٢٢	ثانياً: الدراسات الأجنبية
٢٥	فصول الدراسة
الفصل الثاني: الإطار النظري للدراسة	
٢٨	تمهيد
٢٨	١/١ تعريف الأمن السيبراني
٢٩	٢/١ الفرق بين الأمن السيبراني وأمن المعلومات
٢٩	٣/١ عناصر الأمن السيبراني
٣٠	٤/١ أهداف الأمن السيبراني
٣٠	٥/١ أهمية الأمن السيبراني
٣٠	٦/١ المهام الأساسية للأمن السيبراني
٣١	٧/١ تعريف الجرائم السيبرانية

٣١	١/٧/١ خصائص الجرائم السيبرانية
٣٢	٢/٧/١ أنواع وتقسيمات الجرائم السيبرانية
٣٣	٣/٧/١ أنواع التهديدات السيبرانية
٣٤	٤/٧/١ أصناف المجرم السيبراني
٣٤	٥/٧/١ خصائص المجرم السيبراني
٣٥	٨/١ تعريف الهندسة الاجتماعية
٣٥	١/٨/١ مراحل هجوم الهندسة الاجتماعية
٣٦	٢/٨/١ أقسام الهندسة الاجتماعية
٣٧	٣/٨/١ طرق للحد من خطر هجمات الهندسة الاجتماعية
٣٨	٩/١ تعريف التصيد الإلكتروني
٣٨	١٠/٩/١ أشكال التصيد الإلكتروني
٣٩	٢/٩/١ البيئات المستهدفة في التصيد الإلكتروني
٣٩	٣/٩/١ تقنيات الهجوم
٤٠	٤/٩/١ تقنيات التدابير المضادة
٤٠	١٠/١ مجالات استخدام الأمن السيبراني
٤١	١١/١ أبعاد الأمن السيبراني
٤٢	١٢/١ المخاطر الناتجة عن ضعف الأمن السيبراني
٤٤	١٣/١ آثار ضعف الأمن السيبراني
٤٥	١٤/١ إجراءات تعزيز الأمن السيبراني
٤٦	١٥/١ الأساليب المناسبة من أجل دعم الأمن السيبراني والتقليل من حدة خطر الاساليب والسلوكيات المنحرفة
٤٨	١٦/١ أبرز اختراقات الأمن السيبراني خلال عام 2020
٤٩	١٧/١ حوادث الأمن السيبراني في المملكة العربية السعودية وانعكاساتها
٤٩	١٨/١ مبادرات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية
٥١	١٩/١ نماذج مؤسسات الأمن السيبراني في المملكة
٥٢	٢٠/١ نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية
الفصل الثالث: الأمن السيبراني في الجامعات السعودية	
٥٩	تمهيد

٥٩	١/٢ دور وزارة التعليم والجامعات في تنمية الوعي السيبراني
٦٠	٢/٢ أساليب تفعيل الوعي السيبراني في الجامعات
٦١	٣/٢ مراحل تعزيز قيم المواطنة الرقمية لدى طلبة الجامعات
٦٢	٤/٢ البرامج التربوية في الجامعات السعودية
٦٥	٥/٢ نماذج من إدارات الأمن السيبراني في الجامعات السعودية
٦٨	٦/٢ دور الأمن السيبراني في الجامعات السعودية ٢٠٣٠
٦٩	٧/٢ دور الممارسة التطبيقية للأمن السيبراني في تنمية دقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة

الفصل الرابع: الإطار العلمي

٧١	إجراءات تطبيق التجربة
٧٢	تحليل نتائج الاستبيان القبلي والبعدي

الفصل الخامس

٨٧	الخاتمة
٨٨	أولاً: النتائج
٩١	ثانياً: التوصيات
٩٢	المراجع العربية
٩٦	المراجع الأجنبية

قائمة الجداول:

١٥	جدول رقم (١) يوضح التوزيع لعدد أفراد عينة الدراسة مع الأقسام العلمية
٧٢	جدول رقم (٢) يوضح توزيع أفراد العينة على الفئات العمرية
٧٣	الجدول رقم (٣) المستوى الدراسي لأفراد العينة
٧٤	الجدول (٤)وعي طالبات كلية الآداب والعلوم الإنسانية بمفهوم الأمن السيبراني
٧٦	الجدول رقم (٥) مدى احتياج طالبات كلية الآداب والعلوم الإنسانية لدورات تدريبية تختص بالأمن السيبراني
٧٧	جدول رقم (٦) مدى قدرة طالبات كلية الآداب والعلوم الإنسانية على التقرير بين أمن المعلومات والامن السيبراني
٧٨	جدول رقم (٧) وعي طالبات كلية الآداب والعلوم الإنسانية بالجرائم السيبرانية
٨١	الجدول رقم (٨) مدى معرفة طالبات كلية الآداب والعلوم الإنسانية لحماية أنفسهم من الاختراقات السيبرانية

قائمة الملاحق:

٩٧	الملحق رقم (١) الاستبانة في صورتها النهائية
١٠١	الملحق رقم (٢) الدورة التدريبية

الفصل الأول: الإطار العام للدراسة

يشتمل على:

- المقدمة.
- أهمية الموضوع ومبررات اختياره.
- أهداف الدراسة.
- تساؤلات الدراسة.
- حدود الدراسة.
- منهج الدراسة وأدوات جمع المادة العلمية.
- عينة الدراسة.
- الدراسات السابقة.

-أولاً: الدراسات العربية.

-ثانياً: الدراسات الأجنبية.

- فصول الدراسة.

المقدمة:

يشهد العالم تطور متسرع في تكنولوجيا المعلومات والاتصالات حيث أصبح الانترنت حلقة الوصل ما بين العالم المتزامي الأطراف الذي بات لا يعترف بحدود الزمان والمكان والذي يتداول المعلومات والأفكار في شتى المجالات والأصعدة لمختلف الأهداف والغايات، ولا سيما في ظل انتشار الهواتف الذكية والأجهزة المحمولة، ولاشك أن التطور التقني الملحوظ له إسهامات ومتعددة ومنها تبادل المعلومات والأفكار على مستوى الأفراد والمؤسسات ودول العالم بصفة عامة حيث أصبح المقياس الذي تقام به تقدم الدول هو مدى التطور التقني والتكنولوجي ومدى تطبيقها وتبنيها للتقنية وكيفية توجيهها الأمثل في سبيل تحقيق مصالحها ومختلف أهدافها، وفي مقابل كل ذلك بانت التقنية يصاحبها العديد من الأخطار والتهديدات السيبرانية التي تقابل مستخدمي الإنترت ، حيث يسرخ البعض جهوده وإمكانياته لاختراق شبكات المعلومات بالإضافة إلى ذلك انتهاء خصوصية المستفيدين والعبث بالمعلومات وتزويرها ونشر المعلومات المسيئة والإشاعات الضالة وغيرها من أشكال الجرائم السيبرانية التي تعود بالعديد من الأضرار الاقتصادية والسياسية والاجتماعية ، ومن هذا المنطلق حرصت الدول على تكريس جهودها في سبيل تحقيق الأمن السيبراني لمواطنيها ومؤسساتها وهيئتها ، وكما حظي الأمن السيبراني باهتمام بارز لدى جميع الدول أصبحت سياساتها وأنظمتها لا تخوا من قوانين تختص بمسائل الأمن السيبراني كل ذلك من منطلق تأمين البيانات والمحافظة عليها من مختلف الأخطار والتهديدات التي تواجهها ، وفي سبيل زيادةوعي المجتمعات حوله للحد من مخاطره والقدرة على التصدي لها وعملت العديد من الدول النامية على تحقيق هذا الهدف ومنها المملكة العربية السعودية حيث قامت بتاريخ ١٤٣٩/٢/١١ بإنشاء الهيئة الوطنية للأمن السيبراني لتكون الهيئة هي الجهة المختصة في المملكة بالأمن السيبراني، تتولى مسؤولية تعزيز الأمن السيبراني وحماية البنية التحتية والمحافظة على مصالحها الوطنية وجميع قطاعاتها من مختلف المخاطر والتهديدات التي تواجهها في الفضاء السيبراني ، وبجانب هذا الاهتمام يلاحظ الدور الفعال الذي يقع على عاتق المؤسسات الجامعية في المملكة العربية السعودية في تحقيق الوعي بهذا النوع من الأمن لدى طلابها والمتسببن لها وتبني مبادرات هادفة لتعزيز الأمن السيبراني لمستخدمي الإنترت عامه وللطلاب خاصة وضرورة إنشاء إدارات تختص بالأمن السيبراني بالإضافة إلى سعيها إلى إدراجه في مقرراتها وبرامجها التعليمية لتسهم بذلك في خلق مجتمع واعي سبيرانياً قادراً على ممارسة الأمن السيبراني بشكل تطبيقي ولديه الجاهزية الفعلية لمواجهة مختلف المخاطر السيبرانية .

أهمية الموضوع ومبررات اختياره:

تكمّن أهمية الموضوع من أهمية الأمن السيبراني، وذلك في حماية البيانات والأجهزة وسلامتها من مخاطر الإنتهاكات السيبرانية والمحافظة على سلامة المعلومات وذلك بالحد من الدخول الغير مصرح به إليها ، وذلك يأتي تبعاً للدور الهام للأمن السيبراني كأحد المتطلبات الضرورية لحماية مجتمعاتنا المعاصرة من مختلف أشكال الجرائم السيبرانية ، حيث يأتي الإهتمام المتزايد بالأمن السيبراني متزامناً مع رؤية المملكة 2030 والتي بدورها تؤكد على دعم استخدام تقنيات المعلومات وتعزيز البيئة الرقمية في جميع مؤسسات المملكة العربية السعودية ومختلف قطاعاتها ، وهنا تأتي أهمية المؤسسات التعليمية كونها أحد المؤسسات التي تنشط في تعزيز الوعي بالأمن السيبراني والعمل بفاعلية على حث جميع منتسبيها على الممارسة التطبيقية للأمن السيبراني من خلال ما تقدمه من برامجها ومبادراتها وكذلك مقرراتها التعليمية التي تساعده على زيادة الثقافة السيبراني لدى جميع منتسبيها ، ولهذا توجهت الباحثات في الدراسة الحالية إلى إعداد برنامج تدريسي يوجه الاهتمام نحو تعزيز ثقافة الأمن السيبراني وقياس مدى وعي طالبات كلية الآداب والعلوم الإنسانية بكافة أقسامها بالأمن السيبراني والإسهام في رفع درجة الوعي والتحذير من المخاطر والإنتهاكات السيبرانية.

الأهداف:

١. التعرف على الأمن السيبراني مفهومه وأهميته.
٢. الوقوف على أهم الجرائم التي يتعامل معها الأمن السيبراني.
٣. معرفة درجة وعي طالبات كلية الآداب والعلوم الإنسانية بالأمن السيبراني.
٤. بناء برنامج تدريسي لقياس مدى وعي طالبات كلية الآداب والعلوم الإنسانية بالأمن السيبراني.
٥. تحليل قياس مدى فعالية برنامج تدريسي المقترن لتتميمه وعي طالبات كلية الآداب والعلوم الإنسانية والوقوف على نقاط القوة وتدعمها وتقديم المقترنات لمعالجة جوانب الضعف.

التساؤلات:

١. ما هو الأمن السيبراني وما أهميته؟
٢. ماهي أهم الجرائم التي يتعامل معها الأمن السيبراني؟
٣. ماهي درجة وعي طالبات كلية الآداب والعلوم الإنسانية بالأمن السيبراني؟
٤. كيف تم قياس وعي الطالبات في كلية الآداب والعلوم الإنسانية بالأمن السيبراني؟
٥. ما مدى فعالية البرنامج التدريسي المقترن لتتميمه وعي طالبات كلية الآداب والعلوم الإنسانية والوقوف على نقاط القوة وتدعمها وتقديم المقترنات لمعالجة جوانب الضعف؟

حدود الدراسة:

الحدود الموضوعية : تتميم الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الإنسانية.

الحدود المكانية : جامعة طيبة كلية الآداب والعلوم الإنسانية لجميع أقسامها وهي كالأتي: الدراسات القرانية، الدراسات الإسلامية، اللغة العربية، اللغات والترجمة، العلوم الاجتماعية، الاتصال والإعلام، المعلومات ومصادر التعلم.

الحدود الزمانية : تم إجراء التجربة في الفصل الدراسي الثاني لعام ١٤٤٣ هـ - ٢٠٢٢ م.

الحدود النوعية : اقتصرت الدراسة على طالبات كلية الآداب والعلوم الإنسانية بجامعة طيبة.

منهج الدراسة وأدوات جمع المادة العلمية:

اتبعت الدراسة المنهج التجريبي لملائمة طبيعتها وأهدافها من حيث رصد الظاهرة الآتية، وهو يعد أسلوب فعال لإكتساب المعرفة عن طريق الرصد ويتم استخدامه لدراسة الواقع وتفسيرها، وقامت الباحثات بإستخدام تجربة القياس القبلي والبعدي للظاهرة، حيث تم تصميم برنامج تدريبي لقياس وعي الطالبات بالأمن السيبراني والإسهام في رفع درجة الوعي والتحذير من المخاطر والإنهاكات السيبرانية، حيث تضمن البرنامج التدريبي المحاور التالية:

- تعريف الأمن السيبراني والفرق بين الأمن السيبراني وأمن المعلومات.
- أهمية وأهداف وعناصر الأمن السيبراني.
- آثار ضعف الأمن السيبراني.
- الهجمات الإلكترونية، وأنواع البرمجيات الخبيثة.
- الجرائم السيبرانية وأنواعها، وأصناف المجرمين.
- التصيد الإلكتروني وأشكاله.
- الهندسة الاجتماعية ومراحل الهجوم وطرق الحماية والوقاية من الهجمات السيبرانية.
- قانون الجرائم في المملكة.
- جهود المملكة في الأمن السيبراني.
- الأمن السيبراني في الجامعات السعودية.

وإثر ذلك تم تصميم استبيان قبلي وبعدي يضم الأسئلة نفسها لقياس مدى وعي طالبات كلية الآداب والعلوم الإنسانية بالأمن السيبراني قبل وبعد التجربة.

عينة الدراسة:

بلغ إجمالي أفراد مجتمع الدراسة ٨٢٧١ طالبة بجميع أقسام الكلية ، وتم الإعتماد على برنامج sample size لحساب حجم العينة بمستوى الثقة ٩٥ % وهامش خطأ ٥ % وبالتالي فإن عدد أفراد العينة ١٩٢ طالبة .

تم توزيع العدد بطريقة طبقية على أعداد الطالبات بكل قسم، ولكن كان معدل الاستجابة ضعيف ولم تستطع الباحثات من الالتزام بالتوزيع الطبيعي فتم التوزيع العشوائي على الأقسام العلمية بالكلية، بلغ حجم العينة القبلية ١٩٨ طالبة والبعدية ١٩٦ طالبة، وتم إستبعاد ٤ إستمارات من الإستبانة القبلية والبعدية لعدم جديتهم في الإجابة على الأسئلة، وكذلك تم إستبعاد ثلاثة إستمارات من الاستبانة البعدية ، إثنين من تخصص الاتصال والإعلام وواحدة من تخصص الدراسات الإسلامية حيث أنهم أجاوبوا على الإستمارة البعدية ولم يجيبوا على الإستمارة القبلية . وبالتالي بلغ إجمالي حجم العينة بعد استبعاد الإستمارات الغير صالحة إلى ١٩٢ استماراة قبلية و ١٨٩ استماراة بعدية . والجدول التالي يوضح إجمالي حجم العينة موزعاً على الأقسام العلمية.

جدول رقم (١) يوضح التوزيع لعدد أفراد عينة الدراسة مع الأقسام العلمية:

القسم العلمي العدد	الإجمالي	عدد الاستجابات القبلية	عدد الاستجابات البعدية	
				الإجمالي
الدراسات القرانية	٤٨	٢٤	٢٤	
الدراسات الإسلامية	٦٨	٣٤	٣٤	
اللغة العربية	٤٧	٢٥	٢٢	
اللغات والترجمة	٤٨	٢٤	٢٤	
العلوم الاجتماعية	٦٠	٣٠	٣٠	
الاتصال والإعلام	٦٦	٣٣	٣٣	
المعلومات ومصادر التعلم	٤٤	٢٢	٢٢	
الإجمالي	٣٨١	١٩٢	١٨٩	

أولاً: الدراسات العربية

١) آل مسعود، علي يحيى. (٢٠٢٠). الأمن السيبراني وآلياته في الحد من السلوكيات الإنحرافية للأحداث في المملكة العربية السعودية: دراسة نظرية تحليلية. مجلة كلية التربية، مج ٢٠، ع ٤، ٤١١ - ٤٣٤.

تهدف الدراسة إلى التعرف على طبيعة المخاطر السيبرانية المهددة للأحداث والمعززة لسلوكياتهم الانحرافية وكذلك الوقوف على جهود المملكة وما تضمنته الأنظمة السعودية لتعزيز الأمن السيبراني ووقاية الأحداث والمجتمع من السلوكيات الإنحرافية السيبرانية وتكمّن أهمية الدراسة في إلقاء الضوء على واقع المخاطر السيبرانية المهددة للأحداث والذين لا تزال خبرتهم محدودة مقارنة بغيرهم من فئات عمرية أخرى وتحاول تقديم بعض المقترنات العلمية لتعزيز الأمن السيبراني في المجتمع السعودي وتم استخدام المنهج الوصفي التحليلي في الدراسة وتوصلت الدراسة إلى أن المخاطر السيبرانية تتخذ العديد من الأشكال التي تستهدف إلحاق الضرر بالإحداث وتلك المخاطر تطال العديد من مكونات وقيم المجتمع السعودي بالإضافة إلى أن أحد مستهدفات رؤية ٢٠٣٠ التحول نحو العالم الرقمي وهذا التحول يستوجب المحافظة على الأمن السيبراني ودعمه. وفي هذا الإطار فقد تم تأسيس الهيئة الوطنية للأمن السيبراني، كما تم تأسيس عدد من المؤسسات الأخرى المعنية بقضية الأمن السيبراني في المملكة وخلصت الدراسة إلى : تحديد عدد من الأساليب التي يمكن من خلالها دعم الأمن السيبراني والحد من إكتساب الإحداث في المجتمع السعودي للسلوكيات الإنحرافية السيبرانية.

٢) الخضري، جيهان سعد محمد، سلامي، هدى جبريل علي، و كليبي، نعمة ناصر مدش. (٢٠٢٠). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية: دراسة مقارنة. مجلة تطوير الأداء الجامعي، مج ١٢ ، ع ١٧ - ٢١٧

٢٣٣

تهدف الدراسة إلى التعرف على مفهوم الأمن السيبراني لدى طلاب الجامعات السعودية وكذلك الوصول لمقترح يساعد على تفعيل الأمن السيبراني داخل الجامعات السعودية . وتكمّن أهمية الدراسة في تأكيد دور الجامعات في نشر التوعية بالأمن السيبراني، بالإضافة إلى أنها تقيد القائمين على المؤسسات التعليمية في تطوير منهج علمي يتناول كيفية التعامل مع قضية الأمن السيبراني وقد تم استخدام المنهج الوصفي التحليلي في الدراسة وتوصلت الدراسة إلى : وجود إتفاق وتجانس في الآراء بين أفراد عينة البحث بما يتعلق بتنوع المخاطر التي تتعرض لها الجامعات السعودية، متمثلة في البرامج الخبيثة، وتدمير البيانات، وكذلك ندرة التدريب على برامج الذكاء الاصطناعي ، بالنسبة للقيادات الجامعية والطلاب كما أوصت الدراسة إلى زيادة الإهتمام بتوعية المؤسسات الجامعية السعودية بتطبيق معايير أمن المعلومات حتى يتسعى لها مواجهة أي هجوم أو دخول غير مصرح به على أنظمة المعلومات، وكذلك تنظيم دورات تدريبية للطلاب وأعضاء هيئة التدريس والإداريون لتدريبهم على تطبيق أمن المعلومات.

٣) دراسة ابن إبراهيم، منال حسن محمد. (٢٠٢١). الوعي بجوانب الأمان السيبراني في التعليم عن بعد. *المجلة العلمية لجامعة الملك فيصل - العلوم الإنسانية والإدارية*, مج ٢٢ ، ع ٢٩٩ - ٣٠٧ .

تهدف الدراسة إلى بناء برنامج تدريبي مقتراح لتنمية جوانب الوعي بالأمان السيبراني في التعليم عن بعد لدى معلمات العلوم بالمرحلة الابتدائية ، والكشف عن فعالية البرنامج التدريبي المقترن في تنمية جوانب الوعي بالأمان السيبراني في التعليم عن بعد لدى معلمات العلوم بالمرحلة الابتدائية. وتكمن أهمية الدراسة في أنها قدمت برنامج تدريبي ببرنامج لتنمية جوانب الوعي بالأمان السيبراني في التعليم عن بعد لدى معلمات العلوم بالمرحلة الابتدائية وكذلك توجيه المعلمات إلى أهمية توفير بيئة آمنة خالية من التهديد وخرق المعلومات في الفصول الافتراضية . وتم استخدام المنهج التجاري حيث أنه الأنسب لأهداف الدراسة كما توصلت الدراسة إلى أهم النتائج: وهي البحث عن وجود فرق ذي دلالة إحصائية عند مستوى ($\alpha \leq 0.05$)، بين متوسطي درجات المعلمات في التطبيقين القبلي والبعدي لمقياس الوعي؛ لصالح التطبيق البعدي؛ ويدل هذا على فاعلية البرنامج التدريبي المقترن وأوصت الدراسة إلى ضرورة توفير برمجيات وتطبيقات تستطيع المعلمات التعامل معها باحترافية وكذلك أوصت إلى تضمين موضوعات متنوعة عن الأمان السيبراني في المناهج الدراسية في مختلف المراحل التعليمية .

٤) دراسة البيشي، منير عبدالله مفاح. (٢٠٢١). الأمان السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة. *مجلة الجامعة الإسلامية للدراسات التربوية والنفسية*، مج ٢٩ ، ع ٦ ، ٣٥٣ - ٣٧٢ .

تهدف الدراسة إلى التعرف على واقع الأمان السيبراني من وجهة نظر أعضاء هيئة التدريس، وكذلك التحقق من وجود أثر للأمان السيبراني في تعزيز الثقة الرقمية بالجامعات السعودية من وجهة نظر أعضاء هيئة التدريس . وتكم أهمية الدراسة في أنها من ضمن الدراسات التي تبحث في ثقافة الأمان السيبراني في البيئة السعودية، وترتبط بين الأمان السيبراني والثقة الرقمية وأنها تبين الإطار الفلسفى للأمان السيبراني والحاجة إليه وإلى تطبيقاته في الجامعات السعودية . وتم استخدام المنهج الوصفي التحاليلي ؛ كونه الأنسب لخصائص الدراسة وأهدافها وكما توصلت الدراسة إلى عدة نتائج جاء أهمها أن واقع الأمان السيبراني بالجامعات السعودية من وجهة نظر أعضاء هيئة التدريس مرتفعا بنسبة (٧٣.١٨٪)، كما تبين أن مستوى الثقة الرقمية للجامعات السعودية من وجهة نظر أعضاء هيئة التدريس مرتفعا بنسبة (٧٤.٥٨٪)، وتبيّن أن الأمان السيبراني في الجامعات السعودية يؤثر في تعزيز الثقة الرقمية، حيث بلغت نسبة التأثير (٤٦.٧٠٪)، وتبيّن أنه لا توجد فروق بين استجابات المبحوثين حول الأمان السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية تعزى لمتغيري سنوات الخدمة والدرجة العلمية والتفاعل بينهما وأوصت الدراسة إلى ضرورة الإيمان بأن الأمان السيبراني من افضل الطرق واقتصرها في حماية البيانات والأنظمة وكذلك ضرورة تحصيص قسم لأمن وحماية المعلومات يتولى مهمة تحديث ومتابعة برامج وحماية من المعلومات والأنظمة الإدارية والأجهزة التقنية.

٥) دراسة التيمياني، مداخل زيد عبدالرحيم. (٢٠٢١). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني. مجلة الخدمة الاجتماعية، ع٦٧ ج١ ، ٢٣ - ١.

تهدف الدراسة إلى التعرف بداية الاهتمام بمفهوم الأمن السيبراني في المجتمع السعودي و كذلك التعرف على دور القطاع التعليمي والمصرفي في صناعة الأمن السيبراني في المجتمع السعودي وتكون أهمية الدراسة في الدور الذي تلعبه تقنية المعلومات في حياتنا وتأثيرها على سلوك الفرد والمجتمع وحداثة موضوع الأمن السيبراني في المجتمع السعودي فظهرت الحاجة لبحث مدى تشكل الوعي الاجتماعي تجاه الأمن السيبراني لدى الأفراد في المجتمع السعودي وكذلك تكون أهميتها في الاتساع المعرفي في مجال الوعي الاجتماعي وربطه بالأمن السيبراني وحيث اتبعت الدراسة المنهج الوصفي التحليلي وتوصلت الدراسة إلى أهم النتائج وهي أن هناك نوعين من الاهتمام بالأمن السيبراني على مستوى المملكة العربية السعودية المستوى الحكومي والشعبي حيث أن الاهتمام الحكومي بموضوع الأمن السيبراني بدأ بشكل مبكر قبل أن يدرك الأفراد في المجتمع هذا المفهوم، كما توصلت الدراسة إلى أن أكثر أنماط الجرائم السيبرانية انتشاراً بين الأفراد في المجتمع السعودي هي جريمة الاحتيال الإلكتروني، وأوصت الدراسة إلى أنه من أبرز أولويات الفرد عن التعامل مع التقنية لاسيما في مجال الأمن السيبراني هو أن يكون أكثر إدراكاً للمخاطر التي يمكن أن تظهر له في الفضاء السيبراني.

٦) دراسة القحطاني، نورة بنت ناصر. (٢٠١٩). مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. شؤون اجتماعية، مج٣٦، ع١٤٤ ، ٨٥ - ١٢٠

تهدف الدراسة إلى التعرف على المفهوم الأقرب إلى للأمن السيبراني لدى طلاب وطالبات الجامعات السعودية والتعرف على أهم الجرائم التي يتعامل معها الأمن السيبراني والتي لها علاقة بالمجتمع من وجهة نظر طلاب وطالبات الجامعات السعودية وتكون أهمية الدراسة في ندرة البحث في مجال علم الاجتماع وخاصة كموضوع رئيسي لأحد ميادينه وهو العلم الجنائي التي تتناول مشكلة الأمن السيبراني كونه من المجالات الحديثة حيث أن معظم الدراسات تتناوله من منظور امني دون ان تدرس في اطاره الاجتماعي وأهمية الفئة المستهدفة وهي طلاب وطالبات الجامعات السعودية الذين يمكن ان يشكلوا على المستوى المنظور الأداة الفعالة لتحقيق الأمن السيبراني وتم استخدام المنهج الوصفي التحليلي وتوصلت الدراسة إلى ان انه يوجد تنويع بين نسبة الطلاب والطالبات الذين سمعوا بالأمن السيبراني وأوصت الدراسة بالتوعية الإعلامية بمشكلات الأمن السيبراني بكثافة اكبر واطلاع المجتمع السعودي على عمليات الاختراقات الاستهداف لمجتمع المعلومات السعودي من جهات خارجية وطرق تجنب افراد المجتمع كونهم احد اضلاع مجتمع المعلومات السعودي.

٧) دراسة أندیجانی، دلال صالح، و فلمنان، فدوی یاسین. (٢٠٢١). ممارسات تعزیز الوعی بثقافة الأمن السيبراني وتوصياتها في المملكة العربية السعودية. *المجلة العربية للمعلوماتية وأمن المعلومات*, ع ٥ ، ٧٥ - ١٠٢ .

تهدف الدراسة إلى التعرف على الممارسات المتبعة لتعزيز الوعي بثقافة الأمن السيبراني لدى افراد المجتمع بالمملكة العربية السعودية و كذلك التعرف على الفئات المستهدفة بتعزيز الوعي بثقافة الأمن السيبراني وتکمن أهمية الدراسة من عدة نواحي منها اجتماعية في المساهمة في بناء مجتمع واعي بأهمية الأمن السيبراني ومن ناحية بيئية المشاركة في تأمين بيئة تعليمية امنه مستدامه وأخرى ثقافية تکمن في الارتقاء بثقافة الفرد السيبرانية وحيث اتبعت الدراسة في المنهج الدراسه السبع مراحل لمنهج المراجعة المنهجية للدراسات السابقة وتوصلت الدراسه إلى ان درجات الوعي بالأمن السيبراني متباينة لدى طالب وطالبات المرحلة الجامعية بجامعات مختلفة بالمملكة العربية وال سعودية، واتضح ان درجة الوعي بالأمن السيبراني لدى الطالب والطالبات تتباين من درجة منخفضة إلى درجة عالية واوصت الدراسه إلى تطبيق الدراسات التي تدعم تعزيز الوعي وقياس أثر الاستراتيجيات والتقييمات المتبعة وتوصي بتکثيف الجهود التربوية بالتعاون مع المركز الوطني الارشادي التابع للهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية لتوعية الافراد والمجتمع بأهمية الأمن السيبراني والتعرف على أخطار الهجمات والتهديدات السيبرانية ووسائل التعامل معها.

٨) دراسة فرج، علياء عمر كامل إبراهيم. (٢٠٢٢). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي: جامعة الأمير سطام بن عبدالعزيز نموذجا. *المجلة التربوية*, ج ٩٤ ، ٥٠٩ - ٥٣٧ .

تهدف الدراسة إلى القاء الضوء على دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطام بن عبدالعزيز والكشف عن الفروقات الفروق بين وجهات النظر لدى أعضاء هيئة التدريس نحو دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطام بن عبدالعزيز تبعاً لمتغيرات الكلية والمدرسة العلمية وسنوات الخبرة وتکمن أهمية الدراسة في انها تتنازم مع رؤية المملكة ٢٠٣٠ والتي تؤكد دعم استخدام تكنولوجيات المعلومات وتعزيز البنية الرقمية مما يتطلب تحقيق الأمن السيبراني وكذلك توجيه الاهتمام نحو ثقافة الأمن السيبراني والتحذير من المخاطر والانتهاكات السيبرانية وتم استخدام المنهج الوصفي لملائمة طبيعة الدراسة وأهدافها وحيث توصلت الدراسه إلى اذكاء الوعي بالأمن السيبراني وعلاقته بالأمن الوطني وبالأمن الشخصي وتنقify الطلبة بالممارسات التي تحقق الأمن السيبراني من خلال تصميمنها في المقررات الدراسية في كافة المراحل التعليمية واوصت الدراسه إلى ضرورة خلق بيئه رقمية آمنه من خلال اتقان المهارات التقنية للأمن السيبراني واستخدام البيانات لاكتشاف التهديدات والاستجابة للحوادث السيبرانية كما اوصت كذلك إلى انشاء وحدات تكنولوجية للتأهيل السيبراني لأعضاء هيئة التدريس والطلاب والاداريين .

٩) السمحان، منى عبدالله صالح. (٢٠٢٠). مطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية بالمنصورة، ع١١١، ج١، ٢ - ٢٩.

تهدف الدراسة إلى معرفة متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود وتكمّن أهمية الدراسة في أن الدراسات التربوية في مجال الأمن السيبراني لا زالت محدودة بالإضافة إلى أن الهجمات الإرهابية ما زالت مستمرة وقد تزداد مع التطور التكنولوجي والثورة المعرفية ومحاولة التوصل إلى توصيات ومقترنات تدعم الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود وتمثل أدلة البحث في استماره استبيان، تم تطبيقها على عينة مكونة من (٤٧٨) عامل من العاملين بجامعة الملك سعود بالرياض.

وتوصلت الدراسة إلى أنه يتواجد سياسات امنية لأنظمة المعلومات الإدارية بالجامعة وكذلك أن هناك تطبيق للإجراءات الإدارية الضرورية لتحقيق الأمن السيبراني داخل أنظمة المعلومات الإدارية بالجامعة واوصت الدراسة إلى التأكيد إلى ضرورة اهتمام جامعة الملك سعود بمتطلبات حماية أنظمة المعلومات الإدارية بالجامعة وكذلك ادراج مجال الأمن السيبراني ضمن مناهج التعليم في المملكة.

١٠) الصانع، نورة عمر أحمد، عسaran، عواطف سعد الدين، السواط، حمد بن حمود بن حميد، أبو عيشة، زاهدة جميل نمر، ومنصور، إيناس محمد سليمان علي. (٢٠٢٠). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. مجلة كلية التربية، مج٣٦، ع٦ ، ٤١ - ٩٠ .

تهدف الدراسة إلى تحديد درجة وعي المعلمين بالأمن السيبراني من وجهة نظرهم وكذلك تحديد درجة استخدام المعلمين لأساليب واستراتيجيات حماية الطلبة من مخاطر الانترنت من وجهة نظرهم هذا وتكمّن أهمية الدراسة في لف انتباه المعلمين لأهمية الوعي بالأمن السيبراني نظراً للدور المؤثر الذي يلعبونه في حياة الطلبة وتزويد المعلمين بأساليب واستراتيجيات ابتكارية يستخدمها زملاؤهم في حماية الطلبة من مخاطر الانترنت وتعزيز القيم والهوية الوطنية لديهم وتم استخدام المنهج الوصفي الارتباطي ل المناسبة طبيعة الدراسة وتوصلت الدراسة إلى ارتفاع درجة وعي المعلمين بالأمن السيبراني في مجال حماية الأجهزة الخاصة والمحمولة من الهجمات السيبرانية كما توصلت الدراسة إلى وجود علاقة ارتباطية موجبة ومتوسطة بين وعي المعلمين بالأمن السيبراني واستخدامهم لأساليب حماية الطلبة من مخاطر الانترنت واستخدامهم لأساليب تعزيز القيم والهوية الوطنية واوصت الدراسة إلى أهمية نشر ثقافة الوعي بالأمن السيبراني بين معلمي جميع المراحل الدراسية العامة لتنمية الطلبة بمخاطر الانترنت بمختلف أنواعها بالإضافة إلى اعداد برامج تقنية توعوية تهدف إلى تدريب المعلمين على أساليب حماية الطلبة من مخاطر الانترنت واتخاذ التدابير والاحتياطات الأمنية من مخاطر الهجمات الالكترونية.

١١) الصيفي، مصباح أحمد حامد. (٢٠١٩). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسوب الآلي للمرحلة

الثانوية بمدينة جدة. مجلة البحث العلمي في التربية. ع. ٢٠، ج. ٢٠١٩، ص. ٤٩٣ - ٥٣٤.

تهدف الدراسة إلى التعرف على مدى وعي معلمات الحاسوب بمدينة جدة بماهية الأمن السيبراني والتعرف على مدى وعي معلمات الحاسوب الآلي بمدينة جدة بطرق المحافظة على نظام الأمان السيبراني وتكمّن أهمية الدراسة في أنها تتناول قياس مستوى الوعي بالأمن السيبراني لدى معلمات الحاسوب الآلي للمرحلة الثانوية بمدينة جدة وكذلك في أنها تسهم في إيجاد حلول عملية من خلال حماية الفرد والمجتمع في ظل تناامي المخاطر والتهديدات التي تعرّض هذا المجال الحيوي وتم استخدام المنهج الكمي ل المناسبته طبيعة الدراسة وتوصلت الدراسة إلى أن وجود ضعف وقصور لدى معلمات الحاسوب الآلي في الوعي بمفاهيم الحاسوب الآلي وكذلك أكدت الدراسة على وجود ضعف لدى معلمات الحاسوب الآلي في الوعي بمستوى الأمان السيبراني وأوصت الدراسة إلى ضرورة توفير برامج تدريبية مجانية متعمقة في الأمان السيبراني للمعلمات التي على رأس العمل وكذلك الحق المعلمات بديبلومات بالأمن السيبراني يرفع مستوى الوعي والفهم والتطبيق لديهن بالإضافة إلى دمج الأمان السيبراني في البرامج التربوية الموجودة محلياً.

١٢) المنشري، فاطمة يوسف. (٢٠٢٠). دور القيادة المدرسية في تعزيز الأمان السيبراني في المدارس الحكومية للبنات

بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للعلوم التربوية والنفسية، ع ١٧ ، ٤٥٧ - ٤٨٤

تهدف الدراسة إلى معرفة دور القيادة المدرسية في تعزيز الأمان السيبراني لدى المعلمات وكذلك معرفة دور القيادة المدرسية في تعزيز الأمان السيبراني لدى طالبات المدرسة كما تكمّن أهمية الدراسة في الدور الهام للأمن السيبراني كأحد المتطلبات الضرورية لحماية المجتمعات من المخاطر السيبراني بالإضافة إلى ذلك تأتي الدراسة إلى استجابة إلى لتجهات حكومة المملكة العربية السعودية الهدافة إلى تعزيز الوعي بالأمن السيبراني وإنشاء العديد من الهيئات المختصة العاملة في هذا المجال وتم استخدام المنهج الوصفي التحليلي في الدراسة كما توصلت الدراسة إلى اهم النتائج وهي أن دور القيادة المدرسية في تعزيز الأمان السيبراني لدى المعلمات ولدى طالبات المدرسة يتحقق بدرجة موافقة قليلة من وجهة نظر المعلمات وأوصت الدراسة ب بصورة اجراء تصور مقترن لدور القيادة المدرسية في تعزيز الأمان السيبراني لدى المعلمات والطالبات، وجاءت آليات تطبيقه عبر التنسيق مع الجهات المختصة المعنية بالأمان السيبراني في المملكة العربية السعودية، وتشتمل على آليات خاصة بكل من: المعلمات، الطالبات، المعلمات والطالبات معاً، بالإضافة إلى آليات حماية البيئة المادية لشبكة الانترنت.

ثانياً: الدراسات الأجنبية:

1. Goran, Ion, "Cyber Security Risks in Public High Schools" (2017). CUNY Academic Works

وتم استخدام منهج دراسة تهدف الدراسة إلى تحليل مشاكل الأمن السيبراني في مدرسة ثانوية عامة واقتراح حلول عملية الحاله والدراسة توصلت إلى دراسة حالة عن مدرسة ثانوية حيث تم دراسة اهم نقاط ضعفها امام مجموعة من الهجمات والثغرات الالكترونية وذلك بواسطة الإشارة إلى عاقب واثار الهجمات الالكترونية بالإضافة إلى وسائل الوقاية منها واوصت الدراسة إلى انه من الضروري ان تتركز المدرسة الثانوية على توفير مجموعة الأجهزة الخاصة ذات الأمان العالي

2. Kritzinger, Elmarie and Bada, Maria and Nurse, Jason R. C. (2017) A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK

تهدف الدراسة إلى رفع مستوى الوعي بالأمن السيبراني لدى الطلبة في مدارس جنوب إفريقيا ومدارس المملكة المتحدة من خلال مجموعة من المبادرات وتوصلت الدراسة إلى اهم النتائج وهي أن جنوب إفريقيا لديها فهم لمدى ملائمة وأهمية الوعي بالأمن السيبراني للمتعلمين في المدارس وهناك بعض المؤشرات الواضحة على محاولات لزيادة الوعي بالأمن السيبراني وإرساء ثقافة فعالة للأمن السيبراني في جنوب إفريقيا وفيما يتعلق بالمملكة المتحدة، يجري حاليا تنظيم العديد من المبادرات والبرامج لزيادة الوعي بالأمن السيبراني واوصت الدراسة إلى ضرورة انشاء وحدات إلزامية للأمن السيبراني للطلاب والمعلمين وإنشاء خطة مدرسية وطنية تصف كيفية معالجة الأمن السيبراني لتحسين جهود التوعية لجميع المتعلمين والمعلمين في المدارس.

3. Nagahawatta, R., Warren, M., & Yeoh, W. (2020). A Study of Cyber Security Issues in Sri Lanka. International Journal of Cyber Warfare and Terrorism (IJCWT)

تهدف الدراسة إلى مدى توفر الوعي بالأمن السيبراني لدى طلاب جامعات سيريلانكا وتقديره حيث ركزت الدراسة على العلاقة بين الأمن السيبراني ومستوى وعي طلاب التعليم العالي المرتبطين بالجامعات الوطنية في سيريلانكا وتم استخدام المنهج الوصفي التحليلي و اختيار عينة الدراسة من جميع الجامعات الحكومية الـ 15 في سيريلانكا كما توصلت الدراسة إلى وجود فرق كبير بين مستوى وعي مستخدمي خدمات الانترنت من الذكور والإناث حيث ان الذكور تفوقوا على الإناث في مستوى وعيهم بالإضافة إلى ان مستوى الوعي بالأمن السيبراني بين الجامعات السيريلانكية للطلبة ليس منخفض بشكل ملحوظ واوصت الدراسة إلى ان هناك حاجة إلى سياسية وترويجية وطنية للأمن السيبراني تركز على الطلاب كأصحاب مصلحة رئيسية في قطاع التعليم.

4. Redman, S. Yaxley, K. and Joiner, K. (2020) Improving General Undergraduate Cyber Security Education: A Responsibility for All Universities

تهدف الدراسة إلى تحسين التعليم العام للأمن السيبراني، ولتحقيق ذلك تم إنشاء مقرر يدرس بالمخترابات العلمية وتم تطبيقه وتنفيذها على طلبة البكالوريوس في جامعة نيو ساوث ويلز وكان المقرر بعنوان مقدمة في الأمن السيبراني كما تكمن أهمية الدراسة في ندرة مهارات الأمن السيبراني لدى المحترفين وخاصة الجامعات إلى توفير هذه المهارات من خلال تحسينات منهجية وتعليمية في مجال الأمن السيبراني وتوصلت الدراسة إلى معظم الطلاب يتفقون على أن لديهم فهم أفضل للأمن السيبراني من خلال المقرر كما اوصت الدراسة إلى تطوير بعض جوانب مقرر الأمن السيبراني وتحسينها ليعلن جاهزيته في عام 2020 .

﴿ أوجه الإختلاف عن الدراسات السابقة: ﴾

أولاً: فيما يخص الجانب التطبيقي:

- اختلفت الدراسة الحالية عن الدراسات السابقة في استخدامها للمنهج التجريبي وتطبيقه على عينة من طالبات كلية الآداب والعلوم الإنسانية بجامعة طيبة، وذلك عن طريق إعداد برنامج تربيري مقترن للطالبات وقياس مدى وعيهم بالأمن السيبراني.

ثانياً: فيما يخص الجانب النظري:

قامت الباحثات بدراسة العناصر التالية في الإطار النظري وهو مالم يتتوفر في الدراسات السابقة:

- تناول إدارات الأمن السيبراني المتواجدة في جامعات المملكة العربية السعودية وتوضيح أبرز الأساليب والإستراتيجيات التي من خلالها يتم تفعيل الأمن السيبراني فيها.
- عرض البرامج التدريبية التي أعدتها الجامعات السعودية المتعلقة بتعزيز الأمن السيبراني.
- الكشف عن أبرز حوادث الأمن السيبراني وعرض أهم مبادرات الهيئة الوطنية للأمن السيبراني في المملكة وكذلك نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية.

﴿ أوجه الاتفاق مع الدراسات السابقة: ﴾

اتفقت الدراسة الحالية مع الدراسات السابقة في الإطار النظري من حيث:

- تناول مفهوم الأمن السيبراني والمفاهيم المرتبطة به وكذلك أهدافه وأهميته وتوضيح الفرق بين الأمن السيبراني وأمن المعلومات وأبعاد الأمن السيبراني وكذلك أنواع الجرائم السيبرانية مثل ما جاء دراسة الخضري (٢٠٢٠) وابن إبراهيم (٢٠٢١) والصحفي (٢٠١٩) وطرق الحماية من اخطار ضعف الأمن السيبراني الصحفي (٢٠١٩) وانديجانى (٢٠٢١) والمنتشرى (٢٠٢٠).

فصول الدراسة:

الفصل الأول :

تناول في هذا الفصل الإطار المنهجي للدراسة والتي تشمل على:

- المقدمة.
- أهمية الموضوع ومبررات اختياره.
- أهداف الدراسة.
- تساؤلات الدراسة.
- حدود الدراسة.
- منهج الدراسة وأدوات جمع المادة العلمية.
- عينة الدراسة.
- الدراسات السابقة العربية/الأجنبية.
- فصول الدراسة.

الفصل الثاني :

تناول في هذا الفصل الإطار النظري للدراسة والتي تشمل على:

- تمهيد.
- تعريف الأمن السيبراني.
- الفرق بين الأمن السيبراني وأمن المعلومات.
- عناصر وأهداف وأهمية الأمن السيبراني.
- المهام الأساسية للأمن السيبراني.
- الجرائم السيبرانيةتعريف، وخصائصها، أنواعها وتقسيماتها، أنواع التهديدات، أصناف المجرم، خصائصهم.
- الهندسة الاجتماعيةتعريف، مراحل هجومها، أقسامها، طرق الحد منها.
- التصيد الإلكترونيتعريف، أشكالها، البيئات المستهدفة، تقنيات الهجوم، تقنيات التدابير المضادة.
- مجالات استخدام الأمن السيبراني.
- أبعاد الأمن السيبراني.
- المخاطر الناتجة عن ضعف الأمن السيبراني.
- آثار ضعف الأمن السيبراني.

- إجراءات تعزيز الأمن السيبراني.
- الأساليب المناسبة من أجل دعم الأمن السيبراني والتقليل من حدة خطر الاساليب والسلوكيات المنحرفة.
- أبرز اخترافات الأمن السيبراني خلال عام ٢٠٢٠.
- حوادث الأمن السيبراني في المملكة العربية السعودية وانعكاساتها.
- مبادرات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية.
- نماذج مؤسسات الأمن السيبراني في المملكة العربية السعودية.
- نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية.

الفصل الثالث :

تناول في هذا الفصل الأمن السيبراني في الجامعات السعودية:

- تمهيد.
- دور وزارة التعليم والجامعات في تنمية الوعي بالأمن السيبراني .
- أساليب تعليم الأمن السيبراني في الجامعات.
- مراحل تعزيز قيم المواطنة الرقمية لدى طلبة الجامعات.
- البرامج التدريبية في الجامعات السعودية.
- نماذج من إدارات الأمن السيبراني في الجامعات السعودية.
- دور الأمن السيبراني في الجامعات السعودية ٢٠٣٠ .
- دور الممارسة التطبيقية للأمن السيبراني في تنمية دقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة.

الفصل الرابع :

تناول في هذا الفصل الإطار العملي:

- إجراءات تطبيق التجربة.
- تحليل الاستبيان القبلي والبعدي.

الفصل الخامس:

• الخاتمة.

• أولاً: النتائج.

• ثانياً: التوصيات.

• المراجع العربية/الأجنبية.

الفصل الثاني: الإطار النظري للدراسة

يشتمل على:

- تمهيد.
- تعريف الأمن السيبراني.
- الفرق بين الأمن السيبراني وأمن المعلومات.
- عناصر وأهداف وأهمية الأمن السيبراني.
- المهام الأساسية للأمن السيبراني.
- الجرائم السيبرانية تعريف، وخصائصها، أنواعها وتقسيماتها، أنواع التهديدات، أصناف المجرم، خصائصهم.
- الهندسة الاجتماعية تعريف، مراحل هجومها، أقسامها، طرق الحد منها.
- التصيد الإلكتروني تعريف، أشكالها، البيئات المستهدفة، تقنيات الهجوم، تقنيات التدابير المضادة.
- مجالات استخدام الأمن السيبراني.
- أبعاد الأمن السيبراني.
- المخاطر الناتجة عن ضعف الأمن السيبراني.
- وأشار ضعف الأمن السيبراني.
- إجراءات تعزيز الأمن السيبراني.
- الأساليب المناسبة من أجل دعم الأمن السيبراني والتقليل من حدة خطر الاساليب والسلوكيات المنحرفة.
- أبرز اختراقات الأمن السيبراني خلال عام ٢٠٢٠.
- حوادث الأمن السيبراني في المملكة العربية السعودية وانعكاساتها .
- مبادرات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية .
- نماذج مؤسسات الأمن السيبراني في المملكة العربية السعودية.
- نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية.

تمهيد:

تناول الفصل مفهوم كل ما يتعلق بالأمن السيبراني والجريمة السيبرانية وخصائصها وأنواعها و مجالات استخدام الأمن السيبراني وأبعاده. وكذلك تناول الفصل أبرز اختراقات الأمن السيبراني والمخاطر الناتجة عن ضعف الأمن السيبراني ومبادرات الهيئة الوطنية للأمن السيبراني مع عرض نماذج عن مؤسسات الأمن السيبراني بالمملكة.

١/١ تعريف الأمن السيبراني:

التعريف بالأمن السيبراني يختلف باختلاف طريقة الكتابة فيه ومنهجها ونهج دراسة من تكلم عنه، ويأتي الأمن السيبراني من كلمتين Cyber security، هي بالأصل كلمة لاتينية، ومعناها الفضاء المعلوماتي فالمعنى بالأمن السيبراني هو أمن الفضاء المعلوماتي، وظهر الأمن السيبراني بسبب الثورة الرقمية والتكنولوجيا المعاصرة وهو يعتبر من المفاهيم الحديثة المعاصرة نسبياً (الطيار، 2020).

فقد عرفت الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية "هو حماية الشبكات وأنظمة المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل أمن المعلومات والأمن الإلكتروني والأمن الرقمي".

الأمن السيبراني: هي التدابير التي تقوم بحماية كلاً من الموارد المالية والبشرية التي ترتبط بالاتصالات، ويقوم الأمن السيبراني بتخفيف وإصلاح الخسائر الناجمة في حال حدوث تهديدات أو قرصنة (جبور، 2016)

الأمن السيبراني: يعرف بأنه أمن للمعلومات والبيانات والشبكات وأنظمة المعلومات وأي جهاز متصل بالإنترنت، لذا لابد من الالتزام بمعايير وإجراءات للحماية لمواجهة أو منع أو الحد من أي تهديد أو اختراق (أبو حسين، 2021).

الأمن السيبراني: يعرف بأنه مجموعة من الأدوات التنظيمية والإجرائية والتقنية والأنشطة التي تهدف لحماية أصول المعلومات من أي تهديد داخلي أو خارجي أو تلف أو تغيير أو تعديل أو تعطل من أجل الوصول للمعلومات والخدمات (الشائع، 2018). ويقصد بالأمن السيبراني القدرة على حماية الشبكات وأنظمة الاتصالات وما تحتويها من معلومات وبيانات هامة من اضرار الاختراق والتلف والهجمات الإلكترونية والاستخدام الاجرامي غير المصرح وللحد من مخاطرها والعمل على إيقاف الفيروسات وحظر الوصول الضار وفرض المصادقة وما غير ذلك من المخاطر التي تؤدي إلى الاضرار بأجهزة الكمبيوتر والشبكات المحيطة بها وذلك لضمان استمرارية مجتمع المعلومات وحماية البنية التحتية في الفضاء السيبراني .(Craigen et al,2014)

٢/١ الفرق بين الأمن السيبراني وأمن المعلومات:

يعد مفهوم الأمن السيبراني أوسع من أمن المعلومات، حيث يشمل مفهوم الأمن السيبراني حماية وتأمين البيانات والمعلومات التي تداول عبر مختلف الشبكات والتي يتم تخزينها في خوادم لحمايتها من الاختراقات ومن الوصول غير المشرع، ويقصد بالأمن السيبراني مجموع الوسائل التقنية والتنظيمية التي يتم استخدامها لمنع الاستخدام غير المصرح وذلك بهدف حماية سرية وخصوصية البيانات الشخصية.

أما بالنسبة لمفهوم أمن المعلومات فهو العلم المختص بتأمين المعلومات المتداولة عبر شبكة الانترنت عن طريق الوسائل الضرورية لاكتشاف ورصد التهديدات وحماية المعلومات التي تكون في نظام حاسوبي (صائغ، 2018).

٣/١ عناصر الأمن السيبراني:

لا بد من تواجد مجموعة من العناصر في الأمن السيبراني لضمان الحماية الكاملة للمعلومات :

١. السرية والأمان : تعني التأكيد من أن المعلومات لا يتم الوصول إليها إلا من قبل الأشخاص المخولين لذلك.
٢. استمرارية توفر المعلومات أو الخدمة : تعني التتحقق من استمرار عمل النظام المعلوماتي وأيضاً استمرار القدرة على التفاعل مع المعلومات ، والتأكد من أن المستخدم لن يمنع من الدخول للنظام.
٣. سلامة المحتوى : تعني التأكيد من أن محتوى المعلومة صحيح لم يتعرض للحذف أو التعديل أو التغيير (الصيفي وعسكري ، ٢٠١٩).
٤. التقنية : تعد التقنية والتكنولوجيا الحديثة عنصر هام بالنسبة للأشخاص والمؤسسات حيث أنها تعمل على حماية خصوصية الأفراد ضد أي هجمات تواجههم في الفضاء السيبراني وتعمل على حماية جميع أنواع الأجهزة منها الهواتف والحواسيب والشبكات حيث أنها تعتمد في حمايتها على استخدام برامج مضادة للفيروسات وبرامج جدران الحماية وغيرها.
٥. الأشخاص: يجب على الأشخاص الذين يستخدمون الأنظمة والبيانات أن يضعوا كلمات مرور قوية جداً ومن الصعب تخمينها وتجنب فتح الروابط الخارجية التي تصاحب البريد الإلكتروني ولابد من القيام بعمل نسخ احتياطية للبيانات.
٦. الأنشطة والعمليات: حيث يتم توفير التقنيات وتوظيف الأشخاص المناسبين من أجل تطبيق الأمن السيبراني وتفعيله والتعامل معه والتصدي للهجمات بكفاءة (أبو داسر، 2020).

٤/١ أهداف الأمن السيبراني:

نشر ثقافة الأمن السيبراني ووعية الأفراد والمؤسسات جاء للأهداف التالية:

١. محاربة البرمجيات الخبيثة.
٢. اتخاذ الإجراءات اللازمة لحماية الأفراد من المخاطر المحتمل حدوثها عند استخدام الإنترن特.
٣. مواجهة الهجمات التي تستهدف الأجهزة الحكومية ومؤسسات العامة والخاصة
٤. سد الثغرات في نظام أمن المعلومات.
٥. التخلص من نقاط الضعف في أنظمة وأجهزة الحاسوب والهواتف بأنواعها.
٦. وضع حد للجرائم الإلكترونية على مستوى المؤسسات والأفراد (السمحان 2020؛ المنتشيри 2020).

٥/١ أهمية الأمن السيبراني:

١. حفظ سلامة وخصوصية وسرية المعلومات من الأخطار الإلكترونية وتوفيرها عند الحاجة لها.
٢. توفير بيئة للعمل آمنه إلكترونياً.
٣. تقديم الحماية الكاملة للأجهزة والشبكات والمحافظة عليها.
٤. اكتشاف أهم ثغرات الضعف الموجودة في النظام ومعالجتها.
٥. إعداد طرق لحماية المعلومات الحساسة والمهمة من الهجمات السيبرانية (سمحان، 2020).

٦ المهام الأساسية للأمن السيبراني:

١. الأخذ بجميع التدابير لحماية المواطنين والمستهلكين من أي خطر وتهديد.
٢. المحافظة على حماية وخصوصية وسرية البيانات الشخصية.
٣. ضمان استمرارية عمل نظم المعلومات.
٤. إنشاء صناعة وطنية في مجال الأمن السيبراني لتحقيق الريادة.
٥. تعزيز حماية أنظمة تقنية المعلومات لتصبح مرجعية وطنية لشؤونها المتخصصة بهدف حماية الدولة والمصالح الحيوية وأمن بنيتها التحتية الحساسة.
٦. محاولة حماية الأنظمة التكنولوجيا التشغيلية ومكوناتها والخدمات التي تقدمها ،والبيانات التي تحتويها.
٧. تعزيز حماية الشبكات(وريدة،2021).

٧/١ الجرائم السيبرانية:

إن الجرائم السيبرانية تعتبر من أشد وأقوى أنواع الجرائم التي يتم إرتكابها في البيئة الرقمية والتي تمثل خطورة على المعلومات لما تسببه من خسائر فادحة .

تعريف الجريمة السيبرانية: هي الاستخدام غير المشروع للتكنولوجيا بقصد التدمير والتعدي على ممتلكات الغير من خلال الأجهزة وما تحويه من معلومات ، وتعرف أيضاً بأنها طريقة للهجوم عبر شبكة الانترنت ويقوم الشخص بالتسلل لموقع الإلكترونية غير مصرح له بالدخول إليها. ويمكن تعريفها أيضاً، بأنها فعل محضور يعاقب عليه القانون يرتكبه الجاني ويترتب على ذلك عقوبة جنائية (رباعية، 2016).

١/٧/١ خصائص الجريمة السيبرانية:

الجرائم التي تحدث في الفضاء السيبراني تختلف عن الجرائم التقليدية، ولها خصائص تميزها منها:

١. جريمة تعبر الحدود : مما يعني أن الجريمة لم تعد تقصر على مكان معين أو حدود معينة ، ولا تشترط تواجد المجرم في نفس المكان ف باستطاعة المجرم تنفيذ جريمته الالكترونية عن طريق الدخول إلى جهاز الضحية في اي بلد .
٢. جريمة صعبة الاكتشاف والإثبات : تتميز الجريمة السيبرانية بصعوبة اكتشافها واثباتها على الفاعل حيث أن المجرم من السهل أن يخفي آثار فعلته وبالتالي لن يترك اي آثار خلفه لذا يصعب اكتشافها وعادة ما يتم الكشف عن الجريمة بالصدفة (نعم، 2013)
٣. جريمة ناعمة غير ملاحظة: حيث أن هذا النوع من الجرائم لا يتطلب أي أسلحة أو أدوات حادة كالتي تستخدم في الجرائم التقليدية بالإضافة إلى أنها لا تستخدم الأساليب العنيفة حيث أنها ترتكب بطريقة هادئة غير ملاحظة وبسرعه هائلة تعتمد بشكلٍ أساسي على قرصنة البيانات وأجهزة الحاسوب (العتيبي، 2021).

٢/٧/١ أنواع وتقسيمات الجرائم السيبرانية:

١. جرائم ضد الأفراد : وتكون بهدف سرقة بيانات فرد بعينه مثل سرقة الهوية او بيانات البريد الالكتروني الخاصة بالشخص .
٢. جريمة ضد الحكومات : تهدف إلى تدمير البنى التحتية لأجهزة النظام الحكومي والموقع الرسمية والحادق الضرر بها .
٣. جريمة ضد الملكية الفكرية : عبارة عن ادخال برمجيات ضارة بهدف تدمير النظام الخاص بالشركات والبنوك والممتلكات الشخصية .

وتقسم أيضا على انها :

١. جريمة الدخول أو الولوج الغير قانوني:

حيث يقوم مرتكب الجريمة بانتهاك امن الموقع بغية الحصول على معلومات وتدرج تحتها عدة مسميات منها (السطو غير المشروع ، القرصنة) .

٢. جريمة الاعتداء على سلامة البيانات:

وتكون عن طريق إتلاف البيانات او اجراء تعديل او طمس للبيانات .

٣. جريمة الاعترضات غير القانونية:

وتكون هذه الجريمة عن طريق التجسس او التنصت غير القانوني وتكون غالبا لأهداف سياسية

٤. جريمة الاعتداء على سلامة النظام:

وتكون هذه الجريمة عن طريق تعمد الإضرار بنظام الحاسوب وملحقاته بقصد التخريب والتعطيل .

٥. جريمة اساءة استخدام الحاسوب:

حيث يتم تطوير واستخدام الحاسوب كأداة لأعمال غير مشروعه بغية ارتكاب أي من الجرائم المعلوماتية (مسلم ، ٢٠٢١) .

٦. جريمة الاعتداء على الأموال :

تعتبر هذه الجريمة من اخطر انواع الجرائم واكثرها انتشارا لما يتربى عليها من اضرار مادية فادحة حيث انها تقوم على سرقة الأموال عن طريق الانترنت وتستهدف المواقع التجارية والضرر بزيائدهم .

٧. جريمة الاستغلال الجنسي :

تطبق هذه الجريمة أيضا على جرائم الابتزاز حيث يقوم الجاني بهذا النوع من الجرائم عبر منصات التواصل الاجتماعي بهدف الوصول إلى القاصرين والقيام بنشر صور واسارات او كلمات جنسية كما يقوم بالتنصت او استدراج الضحية (العتيبي ، ٢٠٢١) .

٨. جريمة تفجير البريد الالكتروني:

ان يقوم شخص ما بإرسال الكثير من الرسائل مستهدف شخص بعينه وكمية الرسائل تكون هائلة حتى تقوم بملئ البريد الالكتروني للشخص وبالتالي فالخادم لا يستطيع استقبال الكمية المرسلة ويتوقف عن العمل ومن الطرق المستخدمة في تفجير البريد الالكتروني استخدام الروبوت من اجل ان يقوم بإرسال الكثير من الرسائل والملفات الكبيرة الموجهة إلى شخص ما حتى يتتعطل بريده.

٩. جريمة رفض او حجب الخدمات DOSS:

تعد هذه الجريمة من الجرائم المنتشرة حيث انه يتم مليء واغراق الموقع بكمية هائلة من البيانات الغير لازمة حتى يتوقف الموقع عن الخدمات بشكل مؤقت وتعليقه لفترة وجعل استخدامه غير ممكن ويعود هجوم DOS رفض الخدمة هجوم يتم نشره في نفس الوقت لأكثر من نظام مصاب ويطلق على هذه الهجمات الجماعية هجمات الروبوت (Goutam, 2015).

٣/٧/١ أنواع التهديدات السيبرانية:

تشتمل على عدة انواع ومن ضمنها كالتالي:

- الجرائم الالكترونية وتستهدف فيها جهات فاعلة من اجل تحقيق مكاسب مادية او حدوث خلل فيها.
- هجمات الالكترونية يكون الغاية منها جمع معلومات ذات سرية من اجل دوافع سياسية
- الارهاب السيبراني الذي يعمل أحداث اضطرابات في النظام(Kaspersky,2010).

ومن أسباب استخدام الارهاب السيبراني:

هناك عدة اسباب تؤدي الي ان يكون الارهاب السيبراني خياراً مستخدماً وهي كالتالي:

- تعتبر أداة اكثراً سهولة نظراً لاستخدامهم فقط جهاز حاسب واتصال بالإنترنت وهذا يغنينهم عن الأسلحة والمتفجرات حيث ان الارهاب السيبراني يمثل اكثراً قوة ودافعة.
- الارهاب السيبراني يكون الشخص فيه مجحول الهوية اي يمكنه دخول بأسماء مستعارة وعمل كل ما يريد من تخريب وسرقة في المعلومات دون وجود اي حواجز.
- اختلاف الاهداف المراد القيام بها والممكن ان يكون الهدف أجهزة الكمبيوتر او شبكات الكمبيوتر الخاصة بالحكومة او الأفراد او مختلف القطاعات.
- يمتلك قدرة هائلة في التأثير والحادق الضرر بشكل مباشر على عدد كبير من المؤسسات والافراد(Weimann.2004).

٤/٧/١ أصناف المجرم السيبراني:

١. القرصنة: ومنهم
 - الكراکز: هدفهم السرقة أو العبث ويتم ذلك من خلال التسلل لنظام المعالجة والإطلاع على المعلومات المخزنة، والحادق على الضرر بالنظام.
 - الهاكر: هم هواة هدفهم التسللية أو إثبات الذات أو الفضول ويتم ذلك من خلال التطفل على أمن الشبكات ونظم المعلومات وكسر الحاجز والدخول لأنظمة الحاسوب، دون حدوث أي ضرر.
٢. المهووسون: يكونون في حالة جنون وهدفهم تحطيم جميع الأنظمة.
٣. الحكومات الأجنبية: يستخدمون أجهزة الحاسوب للتجسس.
٤. الجريمة المنظمة: مثل عصابات المافيا.
٥. المتطرفون: يستخدمون الشبكة لنشر أفكارهم وبثها بين الناس (الصافي، 2020).

٤/٧/٢ خصائص المجرم السيبراني:

١. قدرة المجرم على استخدام التقنية الحديثة لأنظمة المعلومات.
٢. الذكاء العالي للمجرم السيبراني وقدرته على الابتكار.
٣. صعوبة الإمساك بالمجرم السيبراني.
٤. المجرم السيبراني شخص اجتماعي.
٥. قدرته على إعادة الجريمة السيبرانية عدة مرات.
٦. استغلال المجرم السيبراني للأزمات للايقاع بالضحايا (العتبي، 2021).

٨/١ تعريف الهندسة الاجتماعية:

الهندسة الاجتماعية: هي عملية يتم من خلالها خداع الناس وحصول المتسلل على معلومات خاصة وسرية تقييد المتسلل بطريقة ما (Rusch,n.d).

وأيضا هي عبارة عن مجموعة من الممارسات والأنشطة الضارة التي تؤدي بالضرر للضحية(Bisson,2015).

١/٨/١ مراحل هجوم الهندسة الاجتماعية:

١. جمع المعلومات حول الهدف: في هذه المرحلة يقوم المهاجم بجمع معلومات عن الضحية الموجوده على الموقع الالكتروني ، وتعتبر هذه المرحلة اساس نجاح الهندسة الاجتماعية
٢. تنمية وتطوير العلاقة مع الهدف: في هذه المرحلة يقوم المهاجم ببناء علاقة مع الضحية والعمل على تطوريها من خلال استغلال نقاط الضعف لدى الضحية ، حتى يستطيع الحصول على المعلومات الشخصية التي يريدها ، مثل ارقام البطاقة الائتمانية ، معلومات الحساب.
٣. استغلال العلاقة: يتم استغلال العلاقة عندما يتم بناؤها ، ويتم تطوير العلاقة مع الضحية بشكل تدريجي.
٤. التنفيذ والوصول إلى الهدف: يقوم المهاجم بالتنفيذ الفعلي في هذه المرحلة لما خطط له ، مع محاولة الوصول للهدف النهائي ، واذا لم يتوصل إلى النتائج المرجوة ، يعيد تكرار الخطوات السابقة (كمال و عبدالرؤوف ، 2018) .(Mouton et al,2016)

٢/٨/١ أقسام الهندسة الاجتماعية:

هندسة قائمة على أساس التقنية:

١. الاحتيال الإلكتروني: مثل رسالة تصلك على بريدك الإلكتروني من البنك للتحقق من معلوماتك، وتحتوي على رابط وعند دخولك تفتح لك صفحة مشابه تمام لصفحة البنك وهي صفحه احتياله فعندها تدخل اسم المستخدم وكلمة المرور تحولك للصفحة الرئيسية وتقوم بسرقة بياناتك.
٢. الاحتيال الصوتي: يعتمد على برنامج war Dialler ويقوم هذا البرنامج بالاتصال على أرقام هواتف مختلفة في المنطقة، ويببدأ الخطر عندما يرد الضحية على الهاكر.
٣. الرسائل الاقتحامية المزعجة: هي رسالة إلكترونية تكون إما تأكيد طلبية أو تهنئة من صديق وغيرها وب مجرد الدخول تتم سرقة معلوماتك وتدمر الجهاز.
٤. برامج مهمة: يقوم الهاكر بنشر روابط لتحميل برامج وعند تحميله يقوم بسرقة المعلومات الحساسة.

هندسة قائمة على أساس بشري أو إنساني:

١. الانتهاك: ويتم عن طريق وضع سيناريوهات تستهدف شيئاً معيناً وتكون غالباً عن طريق الاتصال بالهواتف، ويقوم المجرم بطلب بعض البيانات مثل: الاسم، التاريخ الميلاد، رقم الهوية وغيرها.
٢. سلة المحنوفات: من الأخطاء الشائعة رمي الأقراص أو البريد أو ورقة غير مرغوبه بسلة المهملات لأنها تعتبر جسر الهاكر الأقوى لسرقة الهويات وإقناع الضحايا.
٣. التجسس والتنصت: يقوم الهاكر بسرقة كلمات المرور عن طريق مراقبة الضحية والتنصت لمحادثاته الشخصية، لذلك ينصح دائماً عدم ترك كلمات المرور على المكتب أو تحت لوحة المفاتيح أو حتى تبادلها (أحمد، 2014).

٣/٨/١ طرق للحد من خطر هجمات الهندسة الاجتماعية:

١. عدم نشر أي معلومات خاصة مع الآخرين على شبكة الإنترت أو موقع التواصل والمحافظة على الخصوصية.
٢. يجب أن تتحقق من أي رسالة تصلك على البريد الإلكتروني أو مكالمة هاتفية تتطلب معلومات خاصة وحساسة.
٣. الحذر من فتح أي روابط أو ملفات مرسلة في البريد الإلكتروني لأنها تكون غالباً موقع تصيد إلكتروني.
٤. تنزيل التطبيقات من مصدرها الصحيح.
٥. قيام المؤسسات بتدريب الموظفين والعاملين وتوعيتهم بالأساليب الجديدة للهندسة الاجتماعية.
٦. استخدام كلمات مرور مختلفة لكل موقع ويتم تغييره بشكل دوري.
٧. القيام بتحديث البرامج الموجودة على الأجهزة بشكل دوري.
٨. الحرص عندما يتم استخدام الحواسيب العامة مثل الموجودة في مقهى أو مطارات... الخ.
٩. التأكد من عناوين المواقع أنها تبدأ ب [https](https://) وليس [http](http://) (jain et al, 2016).
١٠. الحرص على اتلاف المستندات والأوراق المهمة بواسطة أجهزة مخصصة.
١١. تجنب استخدام البطاقات الائتمانية إلا عند الضرورة.
١٢. الحرص على عدم الرد على أي مكالمة هاتفية وعدم الثقة بأي بريد الكتروني من أي شخص يطلب معلومات شخصية أو بنكية ، ولابد من التأكد من هوية الشخص من خلال الاتصال بالمصدر (الزهراني ، 2014) .

٩/١ التصيد الإلكتروني:

هجمات التصيد الإلكتروني أو الإحتيالي (Phishing) : تدرج هجمات التصيد الإلكتروني تحت الجرائم الإلكترونية وتسمى بالتصيد بسبب طريقتها في الخداع والإيقاع بالضحية حيث يتم فيها خداع المستخدمين لمشاركة بياناتهم الشخصية والحساسة بكامل إرادتهم مثل أرقام بطاقات الإنتمان ، وكلمات المرور وغيرها ، مما يسمح للمخترق بالوصول إلى أجهزتهم دون علمهم ب هذا ولكن اذا كان لديك علم بهذه الحيل وأساليب التصيد فمن السهل تجنبها .

تعريف التصيد الإلكتروني: عبارة عن أسلوب لخداع المستخدم بالنقر على روابط أو مرفقات ضارة ، بهدف إختراق أجهزة الضحايا للتجسس عليها أو إلحاق الضرر بها أو سرقة المعلومات وغيرها من التهديدات الإلكترونية . وتعرف أيضا على انها عبارة عن : رسائل مزيفة تبدو في ظاهر الأمر أنها موثوقة ، ولكن يمكن لهذه الرسائل إلحاق الضرر بجهازك او معلوماتك الشخصية وأشهر هذه الطرق هي رسائل البريد الإلكتروني . إن أولى الطرق للوقاية من هجمات التصيد الإحتيالي هي معرفة المستخدمين ل هذا النوع من الجرائم لحماية بياناتهم من اي إختراق او سرقة .

١/٩/١ أشكال التصيد الإلكتروني:

- رسائل التصيد عبر البريد الإلكتروني (phishing) عبارة عن رسائل تصل إلى المستخدم عن طريق البريد الإلكتروني وتحتوي على أنها رسالة موثقة (مؤسسة، بنك، شركة) وتحتوي على روابط مزيفة أو ملفات بهدف خداع المستخدم وإختراق جهازه والوصول إلى بياناته ، مثل أرقام الدخول ، أرقام البطاقات الإنتمانية .
- رسائل تصيد البريد الإلكتروني مع تحديد الهدف (spear phishing) يتم هذا النوع بنفس طريقة رسائل التصيد عبر البريد الإلكتروني ولكن الفرق هو التركيز على أهداف معينة وإستهداف أشخاص معينين .
- التصيد الصوتي : (Voice Phishing) ويتم هذا النوع عبر الإتصال الهاتفي حيث يقوم المجرم بإستخدام الإتصالات الهاتفية وإنتحال شخصية معينة مثل البنك أو شركه رسمية ، ويظهر الإتصال على أنه موثوق ويقوم المتصل بتوجيه الضحية للدخول على موقع انترنت بقصد الإيقاع به وسرقة بياناته .
- تزوير الموقع الإلكترونية (Pharming) تقوم هذه الطريقة على إلحاق الضرر بخادم نظام أسماء النطاقات DNS والذي يوجه الضحية إلى موقع إحتيالي مزور ليصيب جهاز الضحية .
- التصيد عن طريق (Scareware) للإيقاع بالضحية : برامجيات خبيثة تظهر على شكل إعلانات أو نوافذ منبثقة ويكون ظاهر عليها عبارات تحذير تخبر الضحية أن جهازه مصاب بفيروسات حتى يقوم بالضغط على النافذة لتحميل برنامج الفيروسات وكل هذه عبارة عن نوافذ وهمية توهם الضحية بأنه ثبت برنامج لحماية جهازه وف الحقيقة عبارة عن برامجيات.

- التصيد عن طريق تطبيقات الهاتف الذكي : وهي عبارة عن إستغلال لتطبيقات التواصل الاجتماعي وغيرها من تطبيقات على الهاتف الذكي ، حيث يقوم المجرم بنشر البرمجيات الخبيثة ، أو دمج تطبيقات خبيثة مع تطبيقات أخرى موثوقة ورفعها إلى متاجر التطبيقات ، إستخدام برامج وهمية بأسماء أمنية .
 - التصيد بالرمح : يحدث في حالة أن تكون الضحية معروفة مسبقاً من قبل المهندس الاجتماعي.
 - التصيد عن طريق الفخ أو الطعم : عبارة عن وضع طعم لإغواء الضحية مقابل إعطاء بيانات حساسة مثل : الموقع التي تقدم روابط تحميل مجانية فعند استخدامها يتم اختراق الجهاز أو وضع البرمجيات الخبيثة في الجهاز ، ومن البرمجيات الخبيثة المستخدمة لطريقة الفخ أو الطعم (أحسناء طروادة).
- ويجب الأخذ بعين الاعتبار أن أكثر الأساليب المستخدمة في التصيد هي الوسائل التنبهية ورسائل التحقق من الحساب وتأتي في في شكل رسالة من مكان عمل الموظف أو رسالة من البنك(الكندي وأخرون، 2020).

٢/٩/١ البيئات المستهدفة في التصيد الإلكتروني:

- تعد الأجهزة الإلكترونية هي البيئة المستهدفة في التصيد الإلكتروني وتصنف إلى ثلاث فئات :
- أجهزة الكمبيوتر الشخصية (pc) .
 - الأجهزة الذكية .
 - أجهزة الصوت النموذجية (الهواتف المكتبة) .

٣/٩/١ تقنيات الهجوم:

- تقنيات الهجوم أو ما تعرف بطرائق الهجوم يمكن تقسيمها إلى ثلاثة فئات:
- تقنيات تهيئة الهجوم .
 - تقنيات جمع البيانات .
 - تقنيات إختراق النظام(Jakobsson & Soghoian, 2009)

٤/٩١ تقييات التدابير المضادة:

تهدف تقييات التدابير المضادة إلى حماية المستخدمين في البيئة الرقمية.

وتتقسم إلى:

- تقنية التعلم الآلي: تقوم هذه التقنية على تطبيق ماتم تعلمه لاستخراج البيانات لاكتشاف عمليات التصيد ومن ثم التعامل معها.
- تقنية التصنيف: تقوم تقييات التصنيف على تحديد وحصر رسائل البريد الإلكتروني المخادعة من خلال خصائص معينة
- تقنية التجميع: وهي عبارة عن تجميع الحالات المشابهة قد تكون مجموعات تصيد إحتيالي أو مجموعات شرعية ،الهدف منها هو تجميع كل حالة تحت ما يشبهها لتسهيل طريقة التعامل معها.
- تقنيات كشف الشذوذ : الشذوذ عبارة عن نمط أو نوع من البيانات لا يتوافق مع الحالة الطبيعية للنظام ، تقوم هذه التقنية على كشف أي سلوكيات غريبة في النظام وتعاملها على أنها حالات شاذة تدرج ضمن التصيد مثل الإختراقات في النظام أو وجود برمجيات خبيثة(Sharnoubi & Alaka, 2015).

١٠/١ مجالات استخدام الأمن السيبراني:

١. حماية الأجهزة ووسائل التخزين: أي حماية جميع أنواع الأجهزة والمعدات التقنية من المخاطر والهجمات والاختراقات والقدرة على التعامل معها.
٢. التعامل الآمن مع خدمات تصفح الإنترن特: المقصود به توعية الأفراد بالمخاطر الناتجة عن الهجمات والجرائم الإلكترونية والعمل على نشر المعلومات والإجراءات التي تساعد على حماية المعلومات(السواط، 2020)

١١/١ أبعاد الأمن السيبراني:

١. البعد العسكري: ينبع الاهتمام بالأمن السيبراني بما يتعلق من الناحية العسكرية من إمكانية وقدرة الجرائم والتهديدات السيبرانية والهجمات والتجاوزات المتتالية على إحداث الحروب وخلق نوع من المنازعات المسلحة المستمرة كما أنها تؤدي بذلك إلى تجاوزات على المؤسسات النووية وأنظمتها وبالتالي يتشكل نوع من التهديدات لأمن الدولة ويساهم في إحداث الأزمات المتعددة.
٢. البعد السياسي: يرتكز البعد السياسي المتعلق بالأمن السيبراني على أساس المحافظة على سياسية الدول وأنظمتها وبنيتها، كما أنه يوجد العديد من التكنولوجيا المتطرفة التي من خلالها يمكن نقل المعلومات ونشرها حيث يمكن استخدامها في إحداث العديد من الاضرار التي تؤثر على سلامة الدولة وسيادتها واحادات نوع من الفوضى والاختلال بين مواطنها كما أن لهذه التقنيات ميزة الوصول السريع لأكبر عدد من المواطنين دون الإشارة إلى دقة المعلومات وصحتها التي تنشر وتصل إليهم.
٣. البعد الاقتصادي: هناك صلة عميقة ما بين الأمن السيبراني وبين حماية المصالح والاحتياجات الاقتصادية لجميع دول العالم ، وهناك أيضاً علاقة كبيرة ما بين المعرفة والاقتصاد لكون جميع الدول تعتمد في تنمية اقتصادها و انعашه على إنتاج المعرفة والمعلومات ونشرها فيما يختص بجميع الأصنعة المختلفة ، وهذا يوضح التأثير الكبير للأمن السيبراني وخطورته فيما يخص الملكية الفكرية والسرقات والمحافظة على اقتصاد الدولة.
٤. البعد القانوني: إن مزاولة كافة الأفراد والعاملين في مختلف المنشآت والهيئات أعمالهم ومهامهم المختلفة التي ترتبط بلا شك بجملة من القوانين والأنظمة التي تأطراها وتنظمها ، حيث أنه منذ بروز مجتمع المعلومات نشأت وتكونت لدينا العديد من الأنظمة والسياسات الحديثة بوصفها الإطار التنظيمي والتشريعي حيث تعمل على السعي للمحافظة على المجتمع المعلوماتي بما في ذلك أيضاً حماية الحقوق المتعلقة بذلك المجتمع ، كما أنه يرتكز الأمن السيبراني في البعد القانوني على أهمية المحافظة على المجتمع المعلوماتي بكل الوسائل المختلفة والمساهمة في إتمام جميع الأنظمة والقوانين والسياسات.
٥. البعد الاجتماعي: من سمات الإنترن트 هو الطبيعة المفتوحة وهذا يتضح من خلال شبكات التواصل الاجتماعي كونها تسمح لجميع الأشخاص بالتعبير عن الأفكار والقضايا المختلفة وكذلك الوصول إلى مختلف الثقافات في جميع أنحاء العالم وأيضاً المعرفة والدرية بمختلف المعلومات في جميع المجالات الموضوعية وهنا يبرز دور الأمن السيبراني في المحافظة على مبادئ وقيم المجتمع (سمحان، 2020).

١٢/١ المخاطر الناتجة عن ضعف الأمان السيبراني:

هناك أنواع عديدة من الأخطار التي تواجه الأمان السيبراني وتنقسم إلى: مخاطر داخلية - مخاطر خارجية (الصحي وعسكري، 2019):

- المخاطر الداخلية هي التي تكون ناتجة من نظام المعلومات نفسه وهي متعددة منها:

١. أخطاء الأفراد (الأخطاء البشرية) :

تعتبر الأخطار التي تنتج عن البشر من أشد أنواع المخاطر التي تشكل خطراً كبيراً على نظام المعلومات وقد تكون هذه المخاطر أفعال مقصودة من قبل الأفراد وقد تكون أفعال غير مقصودة وأيضاً تشمل على الأفراد الغير مسموح لهم باستخدام النظام أو الدخول إليه وأيضاً تشمل الأشخاص المسموح لهم ومن أجل ذلك لابد على الجهة الأمنية وضع سياسات وقوانين أمنية وبذل قصارى جهدهم من أجل الحد من هذه المخاطر ومن هذه المخاطر:

• أخطاء في إدارة النظام أو تشغيله أو في تركيب الحاسوب.

• ترك المعلومات في أيدي الجميع.

• استخدام النظام من قبل الأشخاص الغير مسموح لهم استخدامها.

• الإهمال والإفصاح عن المعلومات السرية التي تخص العميل.

• عدم الاحتفاظ بنسخ احتياطية من الملفات.

• سرقة المعدات والبرمجيات بما فيها من بيانات ومعلومات.

• تخريب متعذر لأجهزة الحاسوب والمعدات والبرامج.

٢. خلل في المعدات : تتضمن هذه المخاطر الخلل في المعدات وعدم توافقها مع أجهزة الحاسوب وأيضاً مشكلات تتعلق بالكهرباء وطرق ربط المعدات ومشكلة الرطوبة والتهوية وأيضاً إعطال متعلقة بالحواسيب والطرفيات.

٣. أخطاء في البيانات : تعتمد صحة المعلومات التي يتم الحصول عليها على صحة البيانات المدخلة في النظام والتي تم معالجتها.

٤. نقاط الضعف : من المحتمل عند وجود نقطة أو عنصر في النظام فهذا يحقق سهولة اختراق النظام من قبل المختصين ويسهل لهم الدخول للنظام حتى الأشخاص الذين ليس لديهم الخبرة الكافية للاختراق يستطيعون اختراق النظام من خلال نقاط الضعف.

المخاطر الخارجية هي التي تأتي من خارج النظام ونذكر منها :

- أخطار الكوارث وتتضمن هذه الأخطار الفيضانات والبراكين والحرائق والبيئة الغير مجهزة والهزة الأرضية التي تسبب خلل في المعدات ووسائل الاتصال.
- مخاطر سلوكية أخلاقية في محتوى صفحات الانترنت تؤثر على القيم والأخلاق السلوكية والدينية وتؤدي إلى تغيير بعض الثوابت الدينية والمعتقدات وبالتالي الابتعاد عن الجانب الديني (ال سعود، ٢٠٢٠).
- مخاطر إلكترونية ومن أهمها الابتزاز الإلكتروني والاختراق والتجسس وهناك دوافع عديدة تؤدي إلى القيام بهذه السلوكيات التي تؤدي إلى الانحراف الأخلاقي.
- مخاطر نفسية واجتماعية حيث يوجد لدى الفرد اختلال في نفسيته وعلاقاته الاجتماعية مما يؤدي به للقيام بمثل هذه السلوكيات الخاطئة وبالتالي لا يرى الفرد الأخطار الناتجة عن تصرفاته.
- التمر الإلكتروني.

١٣/ آثار ضعف الأمان السيبراني:

١. اختراق وتخريب البنية التحتية للاتصالات وتكنولوجيا المعلومات:

الهدف من الهجمات السيبرانية هو الإعاقة للخدمات الحيوية ونشر البرامج الخبيثة كالفيروسات والعمل على تعطيل البنية التحتية ونظم التحكم وخاصة في المرافق الهامة كالخدمات الحكومية مما يؤثر تأثيراً كبيراً على البنية التحتية لتلك المنشآت وعلى خدماتها وأعمالها.

٢. الإرهاب وال الحرب السيبرانية:

تعتمد الجرائم السيبرانية على تقنيات متقدمة وأجهزة تتصل فائقة الجودة وبرمجيات لفك الشفرات واحتراق أنظمة أمن الشبكات وتسعى إلى هجمات متنوعة مثل الهجمات الموزعة لإعاقة الخدمات على الشبكات ولأغراض إجرامية كالتخريب والإرهاب ولأغراض الحروب السيبرانية وتستخدم الهجمات في العمليات الإرهابية وتعطيل البنية التحتية.

٣. سرقة الهوية الرقمية والبيانات الخاصة:

تعتبر من أخطر الجرائم التي تهدد المستخدمين لشبكة الإنترنت وقد تتعرض البيانات للسرقة والاحتلال والاستيلاء على الممتلكات في موقع التجارة الإلكترونية مما قد يشكل خطراً كبيراً على المستخدمين وعلى المؤسسات.

٤. الحرمان من الخدمة:

ويقصد به إيقاف القدرة على تقديم الخدمات المعتادة وذلك يتم من خلال إغراق الجهاز المقدم للخدمة بمجموعة كبيرة من الأوامر التي تؤدي إلى توقفه عن العمل كما قد ينتج عن هذه الهجمات أيضاً إيقاف الاتصال ما بين جهازين أو منع شخص معين من الوصول إلى خدمة أو نظام كما يستخدم هذا النوع من الهجمات كجزء لهجمات أكبر أخرى فالهدف الرئيسي لهذا النوع من الهجمات هو إجبار النظام المستهدف على الاستجابة للأوامر بشكل يفوق قدرته وبذلك يتم إعاقة تقديم الخدمات (البابلي، 2021).

١٤/١ إجراءات تعزيز الأمن السيبراني:

يوجد العديد من الإجراءات والطرق المتبعة لتعزيز والحد من مخاطر الأمن السيبراني وسوف نذكر منها بالتفصيل كالتالي:

- التأكد من سلامة وصحة البنية التحتية والحفاظ على تحديث جدران الحماية ومتابعتها بشكل منتظم.
- اعداد كلمات مرور قوية وان تكون غير معتادة ولابد من تحتوي على حروف وأرقام واسارات.
- القيام بتأهيل وتدريب المستخدمين على التعامل واستخدام نظم المعلومات التي تتميز بقوتها وسريتها وأيضا لابد من التوجيهات التي تعمل على توعيتهم وادراكمهم لضمان الامن والسرية.
- توعية المستخدمين بالحذر من تحميل أي برامج مجهولة المصدر أو غير موثوقة، وفحص البرمجيات قبل استخدامها بشكل فعلي.
- الامكانية من تحديد الدخول وتأمين الوصول إلى النظام وهنا لابد من وضع بعض الأسس والتعليمات للأشخاص المخولين لهم بدخول والتعامل مع النظام بكل موثوقية.
- النسخ الاحتياطي المقصود به هو العمل على نسخ احتياطية للبيانات والملفات من اجل ضمان الحصول عليها عند حدوث مشكلة ما وهي تكون محددة مسبقا من اجل ضمان التوحيد في معايير الحفظ والحماية.
- الوقاية والامن من الفيروسات وهي تتضمن توفر اشخاص لديهم خبرة في الحماية من الفيروسات وطرق تعامل معها وتتوفر برمجيات تعمل على التأكد من عدم وجود أي من الفيروسات(المنتشرى، ٢٠٢٠) (الصانع وآخرون، 2020).
- القيام بدورات متعددة لطلبة التعليم بمختلف المراحل وتشتمل هذه الدورات على تعريفهم بأهمية الأمن السيبراني وحماية البيانات والحفاظ عليها من أخطار الجرائم الالكترونية.
- السعي إلى تحقيق التكامل بين مختلف القطاعات الحكومية والخاصة فيما يخص تعزيز أهمية الأمن السيبراني لدى تلك القطاعات وتعريف العاملين لديها بأهمية الأمن السيبراني ووضع دورات تدريبية فيما يخص هذا المجال.
- عقد الشراكات مع الدول المتقدمة في ما يخص مجال الأمن السيبراني وحماية البيانات للاستفادة من تجاربهم(المنتشرى،2019).
- عملية التشفير أو ما تسمى بالتعمية وهو ما يعني بتحويل البيانات المقرؤة إلى شكل غير قابل للقراءة بحيث يضمن عدم قراءته إلا عن طريق الشخص الذي يملك مفتاح التشفير او الرمز السري ، فلا يمكن معالجتها أو فهمها إلى بعد فك التشفير ، ويعد من أهم الطرق البسيطة لحماية المعلومات .
- التحقق الدائم من حماية الأمان الخاص بالشبكة التي يتم الارسال والاستقبال منها وذلك بشكل دوري (أبو داسر، 2020).

١٥/١ الأسلوب المناسب من أجل دعم الأمن السيبراني والتقليل من حدة خطر الاساليب والسلوكيات المنحرفة:

- يجب على الأفراد أنفسهم أن يعملا على زيادةوعيهم بمخاطر القضاء السيبراني ويجب عليهم تعمية قدراتهم وموهبتهم حتى يتمكنوا من التعامل مع المخاطر ومواجهتها بالشكل المطلوب مع مراعاة الأنظمة العقابية القانونية لتصرفاتهم الالكترونية.
 - يجب على الجهات المعنية أن تقوم بعملية التوعية بأهمية الأمن السيبراني للمجتمع كامل من أجل السعي في مواجهة مخاطر ضعف الأمن السيبراني والحد من خطرها.
 - العمل على القيام ببرامج توعوية وهادفة تستهدف الوالدين من أجل زيادةوعيهم بمخاطر الأمن السيبراني من أجل المساهمة في الحماية من المخاطر وتعزيز الأمن السيبراني.
 - طلب المساعدة من الخبراء في مجال الأمن السيبراني من أجل توعية فئة الشباب بمخاطر شبكات التواصل الاجتماعية والتي تأتي من خلالها التصرفات والسلوكيات المنحرفة والخاطئة(ال مسعود،2020).
- وأيضا من الأسلوب:

١. تنمية الوعي بالأمن السيبراني وذلك عن طريق:
 - تنظيم مجموعة من البرامج والندوات التوعوية التي تهدف للتعریف بالأمن السيبراني والعمل على نشره وتنميته على مستوى الأفراد والمؤسسات.
 - العمل على التعریف بمخاطر وتهديدات الأمن السيبراني ما بين الطلاب وذلك عن طريق المنصات التعليمية.
 - السعي في نشر وبيث مفاهيم الأمن السيبراني واهم التهديدات والاخطر الناتجة عنه من خلال ارسال الرسائل النصية للمواطنين.
 - تنظيم حملات ودورات توعوية بالأمن السيبراني في الجامعات والمدارس في انحاء المملكة وذلك من اجل تقييف منتسبي التعليم.
 - إنشاء مقررات تعليمية تتضمن مفاهيم الأمن السيبراني واهم المخاطر والتهديدات والأسلوب الفعاله لمواجهتها بإشراف الكوادر التعليمية.
٢. وضع القوانين والتشريعات المتعلقة بالأمن السيبراني:
 - تطبيق الأساليب والأنظمة على مستوى الجامعات والمدارس بغض حماية الأمن السيبراني بالتزامن مع التشريعات التي نصت عليها قوانين الهيئة الوطنية للأمن السيبراني.
 - ضرورة توافر عدد من الخبراء والمتخصصين في مجال الأمن السيبراني في الجامعات والمدارس.
 - تطبيق أنظمة وسياسات الأمن السيبراني التي أصدرت من قبل الهيئة الوطنية للأمن السيبراني.

- توفير ميزانية خاصة للأمن السيبراني بحيث تتلاءم مع الميزانية التي تم تخصيصها للخدمات الإلكترونية والتقنية وذلك بهدف استمرار تفعيل أنشطة وحملات الأمن السيبراني.
- ٣. الالسهام في استمرار تنمية وفاعلية الأمن السيبراني عن طريق:
 - استعمال كلمات المرور القوية المكونة من حروف وأرقام عند انشاء حساب في الموقع الرسمية كما انه لابد ان تكون كلمات المرور تختلف من موقع إلى اخر كموقع التواصل الاجتماعي او موقع الشراء الإلكتروني.
 - ضمان الحفاظ على الوثائق والملفات الهامة وعمل نسخ احتياطية لها وذلك لحمايتها من مخاطر السرقة والانتهاكات.
 - استعمال التشفير للملفات الهامة ووضع كلمات المرور الخاصة بها بحيث يتم ارسالها وتبادلها بشكل امن عن طريق الانترنت.
 - الحرص عند استخدام التطبيقات والبرامج تطبيق خاصية الوصول بشكل مؤقت عند استعمالها.
- ٤. المساهمة في تجاوز التحديات والمخاطر التي تقابل تطبيق الأمن السيبراني عن طريق:
 - الالسهام في تنمية ونشر الوعي بشأن مخاطر وتهديدات الامن السيبراني.
 - نشر الوعي حول المواقع الغير موثوقة وآمنه والحد من الدخول اليها وكذلك الحد من انتشارها.
 - زيادة التوعية بقوانين الجرائم المعلوماتية والتعریف بها من خلال الرسائل النصية والندوات والحملات التوعوية.
 - أن تتضمن الجامعات والمدارس عدد من الخبراء والمتخصصين في الأمن السيبراني للتعریف به وكذلك المساهمة في مواجهة مخاطر المتنوعة.
 - تنظيم البرامج التدريبية التي تستهدف القائمين على العملية التعليمية بحيث تتناول تهديدات ومخاطر الأمن السيبراني (المطيري، 2021).

١٦/١ أبرز اختراقات الأمن السيبراني خلال عام ٢٠٢٠:

١. تسريب بيانات عملاء شركة ميكروسوفت:

مع بدايات عام ٢٠٢٠ ظهرت تقارير عدّة تعلن عن تسريب بيانات أكثر من ٢٥٠ مليون عميل وتسريب بيانات الاتصالات والمعلومات بين خدمة العملاء وبين الشركة لمدة ١٤ عاماً وفي هذه الفترة تصدرت ميكروسوفت عنوانين الأخبار بسبب المشكلات الأمنية في متصفح الانترنت Internet Explorer والذي كان يضم ثغرات أمنية عديدة كما نشرت الولايات المتحدة تحذير أمني متعلق بنظام ويندوز ١٠ متزامناً مع خبر تسريب بيانات العملاء خلال تلك الفترة.

٢. اختراق شركة توينتر:

شهد توينتر عام ٢٠٢٠ اختراقاً استهدف حسابات المشاهير حيث قاموا المخترقين بالدخول على حساب أحد الموظفين في الشركة والذي يمتلك صلاحية التحكم في الدعم الفني للحسابات بشكل مباشر حيث كان هدف المخترقون من استخدام تلك الحسابات هو جمع تبرعات عن طريق عملة Bitcoin وتم اختراق حوالي ١٣٠ حساباً ولكن الاختراق لم يتم لمدة طويلة لأن الشركة استعادت الحسابات وعلى الرغم من ذلك فإن المخترقين استطاعوا جمع أكثر من ١٠٠٠٠٠ دولار عن طريق التبرعات الوهمية التي قامت بنشرها من خلال حسابات المشاهير.

٣. اختراق شركة ZOOM:

في عام ٢٠٢٠ وفي ظل انتشار جائحة كورونا شهد تطبيق ZOOM انتشاراً واسعاً لأنه يسهل عملية التواصل والعمل وتم استخدامه في التعليم عن بعد ومع الانتشار المتزايد للتطبيق وبشكل كبير حصل اختراق في خوادم الشركة وقاموا المخترقين بتسريب معلومات أكثر من ٥٠٠٠٠ مستخدم وفي تلك الفترة لم تكن الشركة مهتمة بشكل كبير في تأمين البيانات وتؤمن غرف الاجتماعات الخاصة والأكواد الخاصة بها مما جعل عملية الاختراق في غاية السهولة لكن بعد حدوث هذا الاختراق اهتممت الشركة وبشكل كبير في تأمين البيانات والمعلومات (البابلي، ٢٠٢١).

٤. سرقة ٣ ملايين يورو بسبب تبديل شرائح الموبايل: SIM Swapping:

استطاع مجموعة مخترقين من أوروبا سرقة حسابات بنكية وذلك من خلال استخدام تقنية للاختراق وهي استبدال شرائح الموبايل لأن رقم الهاتف أصبح ضرورياً في وقتنا الحالي ويتم من خلاله الدخول إلى البنوك وتمكن هؤلاء المخترقين من خداع شركات الهاتف لأستبدال شرائح المحمول الخاصة بشخصيات عامة لديها حسابات بنكية وتم سحب الأموال من الصراف الآلي دون الحاجة إلى بطاقة ائتمانية وذلك عن طريق PIN CODE بالإضافة إلى رقم الهاتف والمحفظة الإلكترونية واستطاع المخترقين سرقة ٣ ملايين يورو خلال هذه العملية.

١٧/١ حوادث الأمن السيبراني في المملكة العربية السعودية وانعكاساتها:

واجهت المملكة العربية السعودية العديد من الحوادث التي تتعلق بالأمن السيبراني حيث تشير التقارير التي تم العمل بها بأن منطقة الشرق الأوسط تعتبر مبتغى وهدف ينجذب لها العديد من الذين يعملون بالهجمات السيبرانية وسوف نذكر بعض من الهجمات:

- هجوم فيروس شامون في عام ٢٠١٢م والذي كان قاصداً ومستهدفاً به شركات النفط في المملكة العربية السعودية حيث كان من أضخم الهجمات السيبرانية التي تستهدف الاعمال التجارية الخاصة وتقوم بتسريب جميع المعلومات لها.
- فيروس Trisis حيث أدى إلى إغلاق بعض من مراقب النفط في المملكة العربية السعودية وهو يعمل على نشر برمجيات خبيثة أو برامج ضارة تمكنهم من الاستيلاء والحصول على الأنظمة وان يتحكموا بها (الجمل، 2020).
- فيروس Mamba Ransomware لقد قام بمحاجمة المملكة العربية السعودية في عام ٢٠١٧ وكان يسعى إلى الوصول إلى الشبكات التابعة للشركات في المملكة العربية السعودية ويعمل على تشفير الأقراص الصلبة بشكل متكملاً لا الملفات فقط (أبو زيد، 2019).
- هجوم APT لقد رصدت مراكز الامن الإلكتروني هجوماً الهدف منه هو المملكة العربية السعودية ويعد هذا الهجوم متحكم بتواصل مع بروتوكول HTTP (مركز الأمن الإلكتروني، 2017).

١٨/١ مبادرات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية:

قامت المملكة العربية السعودية في مجال الأمن السيبراني بجهود مستمرة بدءاً من إنشائها الهيئة الوطنية للأمن السيبراني وسعيها الحثيث على تقديم مجموعة من التوصيات في هذا الصدد ومنها : تنمية الصمود السيبراني وذلك من أجل جعل العاملين والموظفين لديهم القدرة على تأدية جميع المهام والاعمال عن بعد وبالتالي لا يستلزم حضورهم إلى أماكن العمل وفي هذا المجال عملت الهيئة الوطنية للأمن السيبراني على اصدار جملة من الضوابط والقيود للأمن السيبراني خاصة للعمل عن بعد حيث انها اشتملت على: زيادة الوعي بالأمن السيبراني والمحافظة على جميع أنظمة المعلومات وأجهزتها وبرمجياتها وكذلك إدارة صلاحيات الدخول والهوية وإدارة امن وسلامة الشبكات والتشفير وأيضاً إدارة جميع المخاطر والتصدي لها ومواجهتها ومتابعة الأمن السيبراني وضمان المراقبة المستمرة له ، كما انها عملت على تقديم مجموعة من الحملات والمبادرات على المستوى الوطني التي من شأنها ان تسهم في زيادة الوعي بالأمن السيبراني على مستوى المجتمع وتحقيقه ونشره في جميع انحاء المجتمع ومن هذه المبادرات :

- **المركز الوطني الارشادي للأمن السيبراني:** من مهام المركز السعي لزيادة الوعي بالأمن السيبراني وأيضاً مواجهة مخاطر الأمن السيبراني والعمل على الحد من أثار هذه المخاطر كما انه تم تهيئة المركز الوطني على الإطلاق الاشعارات التي تعلم بأهم وأحدث التغرات الأمنية
- **الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز:** تم انشاء هذا الاتحاد من اجل تكوين الطاقات البشرية المحلية المحترفة في مجال الأمن السيبراني والعمل على تحسين وتطوير البرمجيات والدرونز كما ان الاتحاد يندرج تحت اللجنة الأولمبية السعودية التي من شأنها تنفيذ افراد المجتمع وزيادة الوعي بالأمن السيبراني والبرمجة والدرونز من خلال مجموعة من الحملات والمبادرات وكذلك تشجيع افراد المجتمع للدخول في هذه المجال والتعرف عليه والاحتراف فيه.
- **الاكاديمية الوطنية للأمن السيبراني:** وهي عبارة عن حملة تابعة لوزارة الاتصالات وتكنولوجيا المعلومات بالشراكة مع صندوق تنمية الموارد البشرية جاءت هذه المبادرة من اجل زيادة الإمكانيات الوطنية الرقمية في جميع المجالات وخاصة التقنية والتكنولوجية المتطرفة وذلك بهدف ملائحة احتياجات التحول الرقمي وتتضمن عدد من المسارات ومنها: تحليل البيانات والذكاء الاصطناعي والحوسبة السحابية وكذلك تحسين التطبيقات والويب وأيضا تصميم البرامج التنفيذية والتخطيط لتصميم الألعاب.
- **مبادرة حصين:** تم انشاء هذه المبادرة واطلاقها تعزيز الأمن السيبراني وذلك على الصعيد الوطني، كما ان المبادرة تتولى مهمة حماية البريد الإلكتروني من السرقات والاستعمال الغير مجاز به، ومن خلال مبادرة حصين يمكن معرفة مستوى تفعيل مبادرة حصين في الجهات الحكومية وأيضا العمل على سجلات أسماء النطاق وانشائها واستكشاف لهذه السجلات والمساهمة في تنفيذ الجهات الوطنية بضرورة توثيق أسماء للنطاقات وكيفية انشائها.
- وفي ظل جائحة كورونا (COVID-19) عملت الهيئة الوطنية للأمن السيبراني على مستوى المملكة بإصدار مجموعة من القيود للعمل عن بعد وذلك في سبيل الاستعداد والتأهب لمواجهة هذه الجائحة وتخطيها ومنها:
 - **زيادة الوعي والتثقيف بالأمن السيبراني:** وذلك عن طريق الاستخدام الامن اثناء تصفح الانترنت وأيضا الاستخدام الآمن مع خدمات البريد الإلكتروني وشبكات التواصل الاجتماعي
 - **إدارة هويات صلاحيات الدخول:** وذلك عن طريق تطبيق يتم من خلاله التأكد من الهوية متعددة العناصر لعمليات الدخول عن بعد والمراقبة المستمرة لجميع هويات الدخول والصلاحيات التي يتم من خلالها نفي وإنجاز العمل عن بعد
 - **وقاية الأنظمة وأجهزة معالجة المعلومات :** وذلك عن طريق تقييد الأصول التقنية وحصرها وأنظمة التابعة للجهة والتي يتم استعمالها للولوج عن بعد بشكل مستمر وكذلك الوقاية من جميع البرمجيات الخبيثة والفيروسات التي تشكل

تهديدًا على جميع أجهزة العاملين وأيضًا حماية الخوادم الخاصة بالجهة والتي يتم من خلالها الدخول عن بعد بواسطة التقنيات وطرق الحماية المتطرفة والتحكم فيها بشكل امن وسلامي (المطيري، 2021).

١٩/١ نماذج مؤسسات الأمن السيبراني في المملكة:

تماشيا مع رؤية ٢٠٣٠ وفي ظل التحديات والعقبات التي تظهر ادركت المملكة ضرورة تكامل جهودها المبذولة من اجل ان يتم تحقيق الاهداف المرجوة والمستهدفة وذلك من خلال البدء بحماية البنية التحتية وحماية الانظمة المستخدمة فقد اظهرت جهودها في التوعية بالأمن السيبراني والعمل على تحقيقه في المجتمع حيث جعلت التعليم نقطة البداية لهذه الجهود حيث ان معظم الجامعات بدأت بالاهتمام بتثقيف طلابها مواد لها علاقة مثل امن المعلومات واتجهت الجهود إلى تأسيس مراكز مخصصة ومعنية بالأمن السيبراني ومن هذه المراكز (القطانى، 2019):

- المركز الوطني للعمليات الامنية في وزارة الداخلية.
- المركز الوطني لتقنية امن المعلومات بمدينة الملك عبدالعزيز للعلوم والتقنية.
- الاتحاد السعودي للأمن السيبراني والبرمجة وهو مؤسسة وطنية تأسست تحت مظلة اللجنة الاولمبية السعودية.
- مركز التميز لامن المعلومات بجامعة الملك سعود .
- وحدة الأمن السيبراني بجامعة الامير سلطان.

٢٠ نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية:

١٤٢٨ هـ

بسم الله الرحمن الرحيم

مرسوم ملكي رقم م ١٧ / ٣ / ١٤٢٨

بعون الله تعالى

نَحْنُ عَبْدُ اللَّهِ بْنِ عَبْدِ الْعَزِيزِ آلِ سَعْوَدِ

مَلِكُ الْمُمْلَكَةِ الْعَرَبِيَّةِ السُّعُودِيَّةِ

هـ. بناء على المادة (السبعين) من النظام الأساسي للحكم، الصادر بالأمر الملكي رقم (٩٠/أ) وتاريخ ٢٧ / ٨ / ١٤١٢هـ وبناء على المادة (العشرين) من نظام مجلس الوزراء، الصادر بالأمر الملكي رقم (١٣/أ) وتاريخ ٣ / ٣ / ١٤١٤هـ.

هـ. وبناء على المادة (الثامنة عشرة) من نظام مجلس الشورى، الصادر بالأمر الملكي رقم (٩١/أ) وتاريخ ٢٧ / ٨ / ١٤١٢هـ.

هـ. وبعد الاطلاع على قرار مجلس الشورى رقم (٦٨/٤٣) وتاريخ ١٦ / ٩ / ١٤٢٧هـ وبعد الاطلاع على قرار مجلس الوزراء رقم (٧٩) وتاريخ ٧ / ٣ / ١٤٢٨هـ.

رسمنا بما هو آت:

أولاً: الموافقة على نظام مكافحة جرائم المعلوماتية، بالصيغة المرافقة.

ثانياً: على سمو نائب رئيس مجلس الوزراء والوزراء - كل فيما يخصه - تنفيذ مرسومنا هذا.

عبد الله بن عبد العزيز

بسم الله الرحمن الرحيم

قرار مجلس الوزراء رقم ٧٩ بتاريخ ٧ / ٣ / ١٤٢٨

إن مجلس الوزراء

بعد الاطلاع على المعاملة الواردة من ديوان رئاسة مجلس الوزراء برقم ٤٧٦٧٥/ب وتاريخ ٢٤ / ١٠ / ١٤٢٧هـ، المشتملة على هـ، في شأن مشروع نظام مكافحة جرائم خطاب معالي وزير الاتصالات وتقنية المعلومات رقم ٢٣٠ وتاريخ ٢٢ / ٤ / ١٤٢٦هـ المعلوماتية.

هـ، المعدين هـ، ورقم (٥٠٩) وتاريخ ٢٧ / ١٢ / ١٤٢٧هـ وبعد الاطلاع على المحضرين رقم (٤١١) وتاريخ ٢٩ / ١١ / ١٤٢٦هـ في هيئة الخبراء.

هـ. وبعد النظر في قرار مجلس الشورى رقم (٦٨ / ٤٣) و تاريخ ١٦ / ٩ / ١٤٢٧
هـ. وبعد الاطلاع على توصية اللجنة العامة لمجلس الوزراء رقم (٥٠) و تاريخ ١٧ / ١ / ١٤٢٨

يقر

الموافقة على نظام مكافحة جرائم المعلوماتية، بالصيغة المرفقة.

وقد أعد مشروع مرسوم ملكي بذلك، صيغته مرافقة لهذا.

رئيس مجلس الوزراء

نظام مكافحة جرائم المعلوماتية

المادة الأولى

يقصد بالألفاظ والعبارات الآتية - أيّها وردت في هذا النظام - المعاني المبينة أمامها ما لم يقتضي السياق خلاف ذلك:

- الشخص : أي شخص ذي صفة طبيعية أو اعتبارية ، عامة أو خاصة .
- النظام المعلوماتي : مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسيبات الآلية.
- الشبكة المعلوماتية : ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت) .
- البيانات : المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسوب الآلي ، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسوب الآلي ، كالأرقام والحراف والرموز وغيرها.
- برامج الحاسوب الآلي : مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسوب الآلي ، أو شبكات الحاسوب الآلي ، وتقوم بأداء الوظيفة المطلوبة.
- الحاسوب الآلي : أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها ، يؤدي وظائف محددة بحسب البرنامج ، والأوامر المعطاة له.
- الدخول غير المشروع : دخول شخص بطريقة متعددة إلى حاسب آلي ، أو موقع إلكتروني أو نظام معلوماتي ، أو شبكة حاسوب آلية غير مصرح لذلك الشخص بالدخول إليها.
- الجريمة المعلوماتية : أي فعل يرتكب متضمناً استخدام الحاسوب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.
- الموقع الإلكتروني : مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.

- الالتقط : مشاهدة البيانات ، أو الحصول عليها دون مسوغ نظامي صحيح .

المادة الثانية

يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية ، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها ، وبما يؤدي إلى ما يأتي :

١. المساعدة على تحقيق الأمن المعلوماتي.
٢. حفظ الحقوق المترتبة على الاستخدام المشروع للحواسيب الآلية والشبكات المعلوماتية .
٣. حماية المصلحة العامة ، والأخلاق ، والأدب العامة .
٤. حماية الاقتصاد الوطني.

المادة الثالثة

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمئة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كل شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية:

١. التنصت على ما هو مرسى عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسوب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه.
٢. الدخول غير المشروع لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا .
٣. الدخول غير المشروع إلى موقع الكتروني ، أو الدخول إلى موقع الكتروني لتعديل تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.
٤. المساس بالحياة الخاصة عن طريق إساءة استخدام الهاتف النقالة المزودة بالكاميرا، أو ما في حكمها .
٥. التشهير بالآخرين ، وإلحاق الضرر بهم ، عبر وسائل تقنيات المعلومات المختلفة .

المادة الرابعة

يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية:

- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند ، أو توقيع هذا السند ، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتهاك صفة غير صحيحة .
- الوصول - دون مسوغ نظامي صحيح - إلى بيانات بنكية ، أو إئتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات ، أو معلومات ، أو أموال، أو ما تتيحه من خدمات.

المادة الخامسة

يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية:

- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.
- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.
- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

المادة السادسة

يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية:

- إنتاج ما من شأنه المساس بالنظام العام ، او القيم الدينية، او الآداب العامة ، او حرمة الحياة الخاصة، او إعداده ، او إرساله، أو تخزينه عن طريق الشبكة المعلوماتية ، أو أحد أجهزة الحاسوب الآلي .
- إنشاء موقع على الشبكة المعلوماتية ، أو أحد أجهزة الحاسوب الآلي أو نشره ، للاتجار في الجنس البشري، أو تسهيل التعامل به.
- إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالأدب العامة أو نشرها أو ترويجها.
- إنشاء موقع على الشبكة المعلوماتية ، أو أحد أجهزة الحاسوب الآلي أو نشره ، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها.

المادة السابعة

يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية :

١. إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية .
٢. الدخول غير المشروع إلى موقع إلكتروني ، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني .

المادة الثامنة

لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنَت الجريمة بأي من الحالات الآتية:

١. ارتكاب الجاني الجريمة من خلال عصابة منظمة .
٢. شغل الجاني وظيفة عامة ، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه.
٣. التغريب بال欺ْسُر ومن في حكمهم، واستغلالهم .
٤. صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.

المادة التاسعة

يعاقب كل من حرض غيره، أو ساعده، أو اتفق معه على ارتكاب أيٍّ من الجرائم المنصوص عليها في هذا النظام ؛ إذا وقعت الجريمة بناء على هذا التحرير، أو المساعدة، أو الإنفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ، ويُعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية.

المادة العاشرة

يعاقب كل من شرع في القيام بأيٍّ من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة .

المادة الحادية عشرة

للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وإن كان الإبلاغ بعد العلم بالجريمة تعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة.

المادة الثانية عشرة

لا يخل تطبيق هذا النظام بالأحكام الواردة في الأنظمة ذات العلاقة وخاصة ما يتعلق بحقوق الملكية الفكرية ، والاتفاقيات الدولية ذات الصلة التي تكون المملكة طرفا فيها.

المادة الثالثة عشرة

مع عدم الإخلال بحقوق حسي النية ، يجوز الحكم بمصادر الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها . كما يجوز الحكم بإغلاق الموقع الإلكتروني ، أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لارتكاب أي من هذه الجرائم ، وكانت الجريمة قد ارتكبت بعلم مالكه.

المادة الرابعة عشرة

تتولى هيئة الاتصالات وتكنولوجيا المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة .

المادة الخامسة عشرة

تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام.

المادة السادسة عشرة

ينشر هذا النظام في الجريدة الرسمية ويعمل به بعد (مائة وعشرين) يوماً من تاريخ نشره.

الفصل الثالث:الأمن السيبراني في الجامعات

يشتمل على:

- تمهيد.
- دور وزارة التعليم والجامعات في تنمية الوعي بالأمن السيبراني .
- أساليب تعزيز الأمان السيبراني في الجامعات.
- مراحل تعزيز قيم المواطنة الرقمية لدى طلبة الجامعات.
- البرامج التدريبية في الجامعات السعودية.
- نماذج من إدارات الأمن السيبراني في الجامعات السعودية.
- دور الأمن السيبراني في الجامعات السعودية .٢٠٣٠
- دور الممارسة التطبيقية للأمن السيبراني في تنمية دقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة.

تمهيد:

تناول الفصل كل ما يخص الأمن السيبراني في الجامعات السعودية بالطرق الى دور وزارة التعليم و الجامعات في تنمية الوعي بالأمن السيبراني مع ذكر أهم الأساليب المتبعة في تفعيل الأمن السيبراني ، وكذلك استعراض البرامج التدريبية في الجامعات السعودية وأهدافها ، كما تناول الفصل ايضا عرض أبرز نماذج إدارات الأمن السيبراني في الجامعات السعودية ودور الأمن السيبراني في الجامعات السعودية وفقاً لرؤية ٢٠٣٠ بالإضافة الى دور الممارسة التطبيقية للأمن السيبراني في تنمية دقة التطبيق العلمي للأمن المعلوماتي لدى طالبات الجامعة.

١/٢ دور وزارة التعليم والجامعات في تنمية الوعي بالأمن السيبراني :

تلعب المدارس والجامعات دورا هاما في المجتمع. حيث انه لديهم مكانة رفيعة في السلم التعليمي ، وبالتالي يقع على عانقهما العديد من المهام والمسؤوليات والقيام بمعالجة المشكلات الظاهرة وتسلیط الضوء على المشكلات الظاهرة في المجتمع، ولاشك أن المدارس والجامعات لم يعد يتقصّر دورهم على الدراسة والتعليم ، وإنما ينظر إليهم على أنهم بيت الخبرة ، لأنها تجمع العديد من الطاقات البشرية ذوي الخبرة والمستوى العلمي والفكري المتقدم ؛ أصبحت مرتبطة بالمجتمع إرتباطا وثيقا ومتينا ، لا سيما أنها أصبحت تتولى مهمة توعية الشباب وحمايتهم حيال المخاطر والهجمات التي قد يتعرضون إليها لا سيما الهجمات التي تتعلق بالناحية المعلوماتية والثقافية . حيث أنها برزت في عصرنا وأصبحت سمة من سماته الواضحة ، فاستعمالهم للتطبيقات التكنولوجية قد يسهم في تعرضهم لنوع من الهجمات أو الجرائم الإلكترونية ، وكذلك قد تؤدي بهم إلى الإنحرافات الأخلاقية . وهذا يتعاظم دور المدارس والجامعات تجاه تلك المعضلات ، حيث يعدّ أمن المعلومات والجرائم الإلكترونية من أهمها، لا سيما في ظل تنامي استخدام التقنيات والأجهزة الإلكترونية المتقدّرة.

ونذكر بعض من الوسائل التي تؤديها وزارة التعليم في مواجهة الجرائم المعلوماتية وتنمية الوعي بالأمن السيبراني :

١. وضع الوزارة خطط عمل للتعامل مع المخاطر وتضمينها للجهات و المؤسسات المعنية التي تساعدها على مواجهة المخاطر السيبرانية.
٢. تنظيم دورات تدريبية خاصة للمعلمين في المجالات الآتية: الوعي بالأمن السيبراني من جهة المعلمين وما هي الإجراءات التي يستطيعون إتباعها لمواجهة مخاطر الفضاء السيبراني.
٣. إشراك أولياء الأمور في الخطط والبرامج المتعلقة بالأمن السيبراني.
٤. نشر الوعي بأهمية الأمن السيبراني بشكل واسع والإستعانة بالوسائل المعينة على ذلك مثل الندوات وورش العمل ونشر الوعي في موقع التواصل والنشرات التوعوية.
٥. تضمين موضوع الأمن السيبراني في الأدلة الخاصة بالمعلمين.
٦. التثقيف بأن الأمن السيبراني يعد إحدى مهارات الحياة المهمة التي لابد من اكتسابها وتدريسه والتوعية بأهميته.

٧. التنظيم مع المؤسسات المهتمة والمساندة على نشر الوعي بالأمن السيبراني كالمؤسسات الأكاديمية والاقتصادية، والمؤسسات المجتمعية على التخطيط وتقديم الدعم المناسب وعمل الندوات والتدريبات المستفاد منها في زيادةوعي وأهمية الأمن السيبراني (المنتوري وحريري، ٢٠٢٠).

كما يتمثل دور الجامعات في تنمية المهارات المتعلقة في الأمن السيبراني فيما يلي:

١. التعرف على المخاطر وأوجه القصور المحتملة عند مشاركة الطالبات في الأنشطة الموجودة على شبكة الإنترت .
٢. العمل على توعية الطالبات فيما يتعلق بحماية البيانات الشخصية.
٣. استخدام التقنيات المختلفة والحديثة التي تساعده على التأمين والحماية.
٤. زيادة الوعي حول مخاطر الإنترت المتعددة كالاتمر الإلكتروني وموقع الإنترت ذات المحتوى غير الملائم.
٥. السعي إلى نشر سياسات وإجراءات الأمن الرقمي وتحديثها بكل جديد (الجندى، ٢٠١٩).

٢/٢ أسلوب تفعيل الأمن السيبراني في الجامعات:

١. إنشاء مركز خاص بالأمن السيبراني ويترعرع من المركز وحدة خاصة بكل كلية من كليات الجامعة.
٢. تقديم برامج تدريبية بشكل مستمر للتوعية بمخاطر الجرائم والسعى إلى مكافحتها.
٣. عقد مؤتمر سنوي في الجامعة يتم التحدث فيه عن أمن المعلومات للتوعية الطلبة وجميع العاملين في الجامعة.
٤. عقد شراكة بين الجامعة ووزارة الإعلام وذلك لعمل حملات إعلامية لوقاية الطلبة من مشكلات الأمن السيبراني.
٥. العمل على توفير البرامج الأكademie في الأمن السيبراني لطلبة الدراسات العليا.
٦. ضرورة دعم وتشجيع أعضاء هيئة التدريس للقيام بالابحاث في تخصص الأمن السيبراني.
٧. ضرورة توعية الطلبة باستخدام الذاكرة الخارجية من أجل النسخ الاحتياطي للرسائل العلمية ولابد أن يتم الحق من دقة وصحة المعلومات التي يتلقاها الطلبة من الشبكات الإجتماعية .
٨. إضافة بعض من المصطلحات والمفاهيم بما يتعلق بالأمن السيبراني في المقررات التي يتم دراستها.
٩. لابد من وجود مناهج دراسية تتعلق بالأمن السيبراني في مختلف القطاعات التعليمية .
١٠. توفير وسائل وبرامج الجامعات من أجل التطبيق العملي والنظري للأمن السيبراني.
١١. تحديث الخطط الدراسية بما يتواافق مع التطورات المعلوماتية والتكنولوجية (الهندى، ٢٠٢١).

٣/٢ مراحل تعزيز قيم المواطنة الرقمية لدى طلبة الجامعات:

- مرحلة الوعي :**

في هذه المرحلة يتم توعية الطلبة حول كيفية الإستخدام الأنسب والأمثل للتكنولوجيا والبرمجيات والتقنيات الرقمية ، مع إعطاء أمثلة حول كيفية الإستخدام غير المناسب والخاطئ من أجل أن يتم تعليمهم ما هو مناسب وما هو غير مناسب.

- مرحلة الممارسة الموجهة:**

تعتبر بأنها الإستعمال الأمثل للتكنولوجيا من خلال القيام بتدريب ومعرفة الطلاب بإستخدام التقنية والحرص على التعرف على الأمان السيبراني من خلال التوجيه والإرشاد عن طريق التطبيق والممارسة العملية بالتوجيه إلى الواقع والصفحات الإلكترونية بطريقة آمنة .

- مرحلة النمذجة وإعطاء المثل والقدوة:**

ويتم ذلك من خلال تقديم أنشطة تدعم الحوار بين الطلبة والمعلمين عن المواطنة الرقمية وتقديم نماذج إيجابية للطلبة للأقتداء بها.

- مرحلة التغذية الراجعة والتحليل:**

وفي هذه المرحلة تتم المتابعة المستمرة للطلاب وتقديم التغذية الراجعة والتزيد بالمهارات كالتميز والتحليل عند إستخدام التقنيات الحديثة (محمد، ٢٠٢٠).

٤/ البرامج التدريبية في الجامعات السعودية :

ونظراً لأهمية الأمن السيبراني قامت الجامعات بتقديم العديد من البرامج التدريبية لتعزيز مفهوم الأمن السيبراني وذلك لعدة أسباب:

- تزايد المخاطر السيبرانية التي تهدد الأمن الوطني في ظل النقص الحاد في الكوادر البشرية المؤهلة.
- مواكبة رؤية ٢٠٣٠ والإستجابة لمتطلبات سوق العمل .
- الحاجة إلى متخصصين في مجال مكافحة الجرائم الإلكترونية .
- الحاجة إلى أشخاص من ذوي الخبرة لديهم القدرة على معرفة وإكتشاف نقاط الضعف الأمنية.

ومن يعرض أبرز البرامج التدريبية في الجامعات السعودية الخاصة بالأمن السيبراني :

جامعة الإمام عبد الرحمن بن فيصل : تقدم الجامعة برنامج بكالوريوس الأمن السيبراني والتحري الرقمي في كلية علوم الحاسوب وتقنية المعلومات وهو إنتاج مهنيين ومتخصصين بارعين يهدف إلى فهم العمليات التي تؤثر على أمن المعلومات، حماية أصول المعلومات ، جمع وحفظ الأدلة الرقمية، تحليل البيانات، تحديد وإصلاح الثغرات الأمنية.

الرؤية : وصول برنامج الأمن السيبراني والتحري الرقمي على مستوى وطني وإقليمي وعالمي.

الرسالة : حصول المتربين على تعليم عالي الجودة في مجال الأمن السيبراني والتحري الرقمي ، ودعم عملية التعليم مدى الحياة .

أهداف البرنامج التعليمية : قدرة البرنامج على إخراج مؤهلين قادرين على :

- تحليل المشاكل المعقدة في الحوسنة .
- تطبيق الحلول والمقترحات لتلبية احتياجات الحوسنة .
- تطبيق الممارسات الأمنية للمحافظة على العمليات في بيئة مليئة بالأخطار والتهديدات .
- معرفة المسؤوليات المهنية والحكم في الحوسنة بالإعتماد على المبادئ القانونية والأخلاقية.
- العمل بشكل فعال كعضو أو قائد فريق .

جامعة الملك سعود : تقدم الجامعة برنامج بكالوريوس في الحوسنة التطبيقية (مجال الأمن السيبراني) .

وذلك بتنفيذ معايير عاليه لدعم التعليم التطبيقي حتى يتسعى لها إعداد الكوادر البشرية المؤهلة لسوق العمل والمؤهلين لمواجهة التهديدات داخل الفضاء الإلكتروني.

أهداف البرنامج التعليمية :

- القدرة على الممارسة في مهن تقنية المعلومات والاتصالات.
- القدرة على إجراء البحوث في مجالات الحوسنة بالإضافة إلى متابعة الدراسات العليا.
- القدرة على تفعيل دور التعلم مدى الحياة .
- القدرة على الخوض في المراكز القيادية والالتزام بالأخلاقيات المهنية .

جامعة الأمير سلطان : تقدم الجامعة برنامج مسار الأمن السيبراني ضمن كلية علوم الحاسوب والمعلومات بجامعة الأمير سلطان ، وذلك إستجابة لأهمية الأمن السيبراني وتزايد الطلب للمتخصصين في هذا المجال في الوقت الراهن .

أهداف البرنامج التعليمية :

تمكين الطلاب من تطبيق المبادئ والممارسات الأساسية في الأمن السيبراني وإخراج طلاب قادرين على التعامل مع كافة التحديات الأمنية التي تواجههم من أجل ضمان المحافظة على المعلومات واستمرار العمل في ظل وجود التهديدات والمخاطر الأمنية .

جامعة دار الحكمة: أطلقت الجامعة برنامج البكالوريوس في الأمن السيبراني والذي يعد من أول البرامج المتخصصة في الأمن السيبراني على مستوى المملكة الذي يختص بتكوين المعرفة اللازمة وتزويد الملحقات لحماية المعلومات و الأنظمة الحاسوبية والتكنولوجية بالمؤسسات والمنظمات العامة والخاصة من الهجمات والإختراقات الإلكترونية .

أهداف البرنامج التعليمية:

تلبية إحتياجات سوق العمل على المستوى المحلي والعالمي .

توائم مخرجات البرنامج مع معايير مجلس الإعتماد الأكاديمي الدولي للهندسة والتكنولوجيا (ABET) .

جامعة الأمير مقرن بن عبد العزيز: تقدم الجامعة برنامج الريادة في تعليم الحاسوب الآلي الذي يهدف إلى تدريب الطالب على إجراء أبحاث مبتكرة في أحدث مجالات الحاسوب الآلي والعلوم السيبرانية لمساهمة في تنمية وحماية المجتمع.

أهداف البرنامج التعليمية:

- القدرة على توفير برامج ذات جودة عالية في جميع التخصصات المتعلقة بالحاسب الآلي والأمن السيبراني والحوسبة الجنائية ، هندسة البرمجيات ، الذكاء الاصطناعي .
- تلبية متطلبات التنمية الوطنية وسوق العمل وإخراج إداريين قادرين على التعامل مع إحتياجات المجتمع التقنية .
- توفير بيئة اكاديمية آمنة تشجع على جودة التعليم والتميز
- إعداد خريجين قادرين على إيجاد بيئات تتسم بأعلى درجات الأمن وحماية نظم المعلومات .

كلية الأمن السيبراني في الرياض : أقر رئيس مجلس إدارة الاتحاد السعودي للأمن السيبراني والبرمجة بالقيام بعمل مقر خاص بكل من المجالات الآتية ، الأمن السيبراني والبرمجة والذكاء الاصطناعي في مدينة الرياض وذلك تزامناً مع رؤية ٢٠٣٠ للسعي نحو الأفضل وبناء مجتمعات تميز بالمعرفة وتقنية وتنافس مع الدول المتقدمة . وتهدف الكلية إلى تعليم الطلاب بالوسائل الحديثة والمبتكرة وفقاً للتحقيق رؤية المملكة العربية السعودية، وتمكّن الكلية الشهادات الاحترافية والجامعة المتوسطة والبكالوريوس وما بعد البكالوريوس في ٨ تخصصات مختلفة :

- بكالوريوس العمليات السيبرانية .
- بكالوريوس الجرائم السيبرانية.
- بكالوريوس الذكاء الاصطناعي.
- دبلوم التحقيق في الجرائم السيبرانية .
- دبلوم الدفاع السيبراني .
- دبلوم البيانات الضخمة .
- دبلوم حوكمة أمن المعلومات .
- دبلوم الإستجابة للحوادث السيبرانية.

جامعة الأميرة نورة بنت عبدالرحمن: تقدم الجامعة برنامج بكالوريوس في الأمن السيبراني تماشياً مع المتطلبات والأهداف التعليمية المذكورة سابقاً ، كما أطلقت الجامعة برنامج معكسر الأمن السيبراني بالتعاون مع كلية علوم الحاسوب والمعلومات للتدريب التقني ويكون البرنامج من ٧٠ ساعه تدريبيه (٤ دورات متخصصة في الأمن السيبراني) بتدريب مكثف خلال أسبوعين .

- دورة الأمن السيبراني والاختراق الأخلاقي .
- دورة CWC اختراق وحماية المواقع .
- دورة cyber linux أنظمة التشغيل .
- دورة cyber python برمجة .

٥/٢ نماذج من إدارات الأمن السيبراني في الجامعات السعودية:

إدارة الأمن السيبراني في جامعة طيبة :

أنشئت إدارة الأمن السيبراني في جامعة طيبة بشكل مستقل عن عمادة تقنية المعلومات، بتاريخ ١٤٣٨/٨/١٤ رقم (٣٧٢٤٠) ومديرها المهندس حاتم عبدالله العمري، وتقوم الإدارة بتوعية منسوبيها وتقديم إرشادات لهم في م مواضيع مختلفة مثل: الجرائم المعلوماتية، كيف تصاب أجهزتنا بالبرامج الخبيثة، وكيف تكون مسؤولة عن حماية شبكتك، حماية البريد الإلكتروني، البرمجيات الضارة، أمن الأجهزة، حماية خصوصيتك أثناء تعلمك أو عملك عن بعد... الخ من خلال نصوص وصور وفيديوهات قصيرة ومفيدة. وتستقبل الإدارة الاستفسارات والبلاغات الأمنية السيبرانية من خلال تعبئة نموذج أو مراسلتهم عبر بريد الكتروني خاص بالإدارة، وتحتكر إدارة أمن المعلومات وحماية أجهزتها وأنظمتها وشبكاتها وفقاً لإجراءات وسياسات المحافظة على سلامة الأصول المعلوماتية والتقنية في جامعة طيبة، وأن تكون هناك إدارة لجميع التهديدات والمخاطر المحتملة ووضع الحلول .

رؤية الإدارة: أن تصل إلى فضاء سيراني آمن وموثوق يمكنها من النمو والازدهار.

رسالة الإدارة: تهدف الإدارة لرفع مستوىوعي منسوبيها بالأمن السيبراني وأن ترسخ مبدأ المسؤولية المشتركة في حماية الفضاء السيبراني في الجامعة.

أهداف الإدارة:

- حماية الأصول المعلوماتية والتقنية في الجامعة ووضع الحلول التقنية لحمايتها.
- دعم استراتيجية أعمال الجامعة.
- تعزيز سلوك أفضل الممارسات في مجال الأمن السيبراني.

إدارة الأمن السيبراني في جامعة أم القرى:

أنشئت الإدارة بتاريخ ١٤٤١/٦/١٧ لتكون إدارة مستقلة تابعة لمعالي رئيس جامعة أم القرى، وتسعى الإدارة لتطبيق أفضل المعايير الدولية ورفع مستوى الأمان والحماية داخل الجامعة، وتحقيق إمكانية الإبلاغ عن الحوادث السيبرانية.

رؤية الإدارة: الوصول لفضاء سيراني آمن وموثوق.

رسالة الإدارة: تسعى بأن تحافظ على الأصول التقنية في الجامعة وحمايتها من أي مخاطر سيرانيه داخلية أو خارجية ، وأيضا تحسين مستويات الالتزام بمعايير الأمن السيبراني الدولية والوطنية، وحماية سرية البيانات وسلامتها وتوافرها المستفيد بشكل مستدام.

الأهداف الاستراتيجية:

- رفع مستوىوعي منسوبتها وتعريفهم بالممارسات الصحيحة لاستخدام مصادر الجامعة التقنية.
- تعريف منسوبتها بالإجراءات والسياسات التي يجب تطبيقها داخل الجامعة فيما يتعلق بالأمن السيبراني.
- إستمرار عمل منظومة التقنية في الجامعة وحماية سرية المعلومات المرتبطة بها.
- العمل على بناء إطار عمل تستطيع الجامعة أن تتعاون مع منسوبتها لحماية أصولها المعلوماتية من أي مخاطر داخلية أو خارجية.

إدارة الأمن السيبراني جامعة الجوف :

أنشئت إدارة الأمن السيبراني في جامعة الجوف بتاريخ ١٤٣٩/١١/١٠ والتي تعد إحدى إدارات الجامعة الأساسية التي تم إنشاؤها بشكل مستقل، وترتبط الإدارة إرتباطاً إدارياً بوكالة الجامعة. وهي الجسر الرابط بين الجامعة والهيئة الوطنية للأمن السيبراني .

تتألف الإدارة من قسمين رئيسيين القسم الأول هو قسم الحكومة والإلتزام و تقوم الوحدات الخاصة بهذا القسم بدورها لتحقيق متطلبات وإحتياجات الهيئة الوطنية للأمن السيبراني وذلك من خلال ضمان الإلتزام بجميع السياسات والمعايير الوطنية الخاصة بالأمن السيبراني. أما القسم الثاني فهو قسم الثبات والصمود السيبراني حيث من مهام الوحدات تحت هذا القسم مراقبة الأصول المعلوماتية من التهديدات السيبرانية، إكتشاف التغيرات والعمل على حلها، والتصدي للهجمات السيبرانية ، وتحليل المخاطر السيبرانية.

رؤية الإدارة : وصول جامعة الجوف إلى فضاء سيراني آمن وموثوق.

رسالة الإدارة : تعزيز وتحسين مستويات الالتزام بمعايير الأمن السيبراني الوطنية والدولية بالإضافة إلى المحافظة على الأصول التقنية في جامعة الجوف وحمايتها من المخاطر السيبرانية الداخلية والخارجية، ومواجهة التهديدات وتقليل المخاطر السيبرانية، والمحافظة على سرية البيانات وسلامتها من التلاعب و التأكيد على توافرها للمستفيدين بشكل دائم .

أهداف الإدارة :

- دعم استراتيجية أعمال جامعة الجوف: ضمان إسهام خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع داخل جامعة الجوف.
- حماية الأصول المعلوماتية والتقنية في جامعة الجوف.
- توفير الحلول التقنية الالزمة لحماية الأصول المعلوماتية والتقنية في جامعة الجوف.
- تنمية سلوك أفضل الممارسات في مجال الأمن السيبراني.
- تطوير العاملين بالمهارات والمؤهلات في مجال الأمن السيبراني، وتعزيز الوعي بالأمن السيبراني من خلال قنوات متعددة، وبناء ثقافة إيجابية للأمن السيبراني.

إدارة الأمن السيبراني في جامعة جدة :

أنشئت الإدارة في الجامعة في تاريخ ١٤٣٨/١١٤ هـ ، تهتم الإدارة بتعزيز الأمن السيبراني وحماية أصول الجامعة التقنية وإدارة المخاطر المحتمل حدوثها ضد المخاطر السيبرانية لضمان استمرارية أعمال الجامعة البحثية والعلمية والإدارية. رؤية الإدارة : الوصول إلى فضاء سيراني آمن وموثوق.

رسالة الإدارة : تقديم خدمات كاملة لتقوية وتعزيز الأمن السيبراني للجامعة.

أهداف الإدارة :

- الحفاظ على الأصول التقنية والمعلوماتية في الجامعة.
- دعم استمرارية أعمال الجامعة.
- تحقيق التقييد والإلتزام بأنظمة الهيئة الوطنية للأمن السيبراني.
- تعزيز إتباع أحسن الممارسات في الأمن السيبراني.

إدارة الأمن السيبراني في جامعة الملك عبدالعزيز :

ستعمل الجامعة على متابعة وإصدار المعايير والسياسات ومتابعة مستوى التقدم في تطبيق الأهداف والتمسك بأنظمة الهيئة الوطنية للأمن السيبراني مع تنفيذ المشاريع التقنية الضرورية لحماية أصول الجامعة.

رؤية الإدارة : توفير بيئة تعليمية آمنة في الجامعة تساعد على النمو وتحقيق رؤية ٢٠٣٠ .

رسالة الإدارة : تقديم بيئة آمنة لحماية أنظمة تقنية المعلومات والتقنيات التشغيلية ضد المخاطر السيبرانية ، والحفاظ على المعلومات عن طريق أنظمة أمنية للمراقبة وسياسات للاستخدام ، والتوعية بالمخاطر ووسائل الحماية من هذه المخاطر.

إدارة الأمن السيبراني في جامعة الملك خالد : تضم الجامعة إدارة خاصة بالأمن السيبراني وقد حصلت إدارة الأمن السيبراني في جامعة الملك خالد على شهادة الايزو ٢٠١٣ في نظام إدارة امن المعلومات من قبل المنظمة الدولية للمعايير وذلك نتيجة لتطبيقها أعلى مستويات التميز في مجال حماية أمن المعلومات وتضم الإدارة العديد من البرامج والندوات التوعوية تحت عنوان الأمن السيبراني.

٦/٢ دور الأمن السيبراني في الجامعات السعودية :

١. تقديم خدمات إستشارية مختصة بدور الأمن السيبراني في الجامعات والمؤسسات التعليمية في المملكة.
٢. تعزيز ورش العمل المختصة بالأمن السيبراني.
٣. التوعية بدور الأمن السيبراني.
٤. وضع حلول تساعد في تفادي الإختراقات والثغرات الأمنية.
٥. توفير خدمات التدريب لمنسوبي الجامعات.
٦. حماية وحفظ حقوق الملكية الفكرية وبراءات الإختراع الخاصة بأصحابها (الخضري، 2020) .

يرى بعض العلماء أن تطبيق الممارسة التطبيقية للأمن السيبراني له دوره الواضح في تنمية التطبيق العملي للأمن المعلوماتي لدى طلاب وطالبات المرحلة الجامعية . وذلك من خلال تنمية القدرات والمهارات وفقاً للمستويات المختلفة بينهم، وتعمل هذه المستويات على تحديد طبيعة أمن المعلومات للبنية المؤسسية وذلك من أجل أن يتتوفر كامل الدعم المطلوب في جميع حالات التقصير التي قد تحصل وتقدم المساعدة ووضع المقترنات المتاحة من أجل أن يتم تعديل بعض المناطق الأمنية ووضع بعض الاحترازات والإلتزام بها فيما يخص جدران الحماية الأمنية، وبالتالي تتمكن الطالبات من فهم النطاق المحيط بهم وفهم نطاق المعايير والوثائق الارشادية ويصبح لديهم فهم كامل بكافة المخاطر والتهديدات التي ممكن أن تواجههم سواءً الآن أو في المستقبل ، ولابد للمؤسسة أن تقوم بوضع السياسات والمعايير الأمنية وتقوي بنيتها التحتية ، وبإمكان الطلاب أن يحددو نفاطن الضعف والقوة ويعملوا على تقييم المخاطر والتهديدات ويصبح لديهم إدراك كامل بالأمن الوطني وتصنيفاته وحمايته للوثائق والمعلومات والبيانات.

يوجد كذلك المزيد من الدراسات المتعلقة بالمارسات التطبيقية للأمن السيبراني، وأيضاً تناولت دقة تطبيق الأمن المعلوماتي وهناك عدد من الدراسات التي تهدف للقيام بالتعرف على الشبكات ، وكيف تتم عملية الربط والأداء بينهم والأنواع الرئيسية التابعة منها وذكر منها، الشبكة المحلية ،والشبكات الواسعة ، والعنكبوتية، وقياس أهميتها بالنسبة للأشخاص و المؤسسات والطرق التي يتم اتباعها من أجل الحماية والوقاية من الأخطار. وتناول الدراسة التي تمت في الكليات التقنية وكان الغاية من هذه الدراسة هو تحديد الغاية من التعرف على واقع إدارة أمن نظم المعلومات وتم خلال هذه الدراسة التوصل إلى أن الكليات التقنية لابد عليها من المعرفة والإدراك بالقيمة والأهمية الناتجة من سياسيات الأمن المعلوماتي ، إلا أنها تقسم بعض القصور في السياسات وأيضاً يعتبر مفهوم الوعي الأمني واسع جداً ولا بد توعية الجميع به كما في دراسة أخرى كان الهدف منها هو وضع بعض السياسات التي تعمل على ضمان والتأكد من سرية المعلومات بتوفير الوقت والجهد لكافة المستخدمين.

إن الممارسة بشكل دائم للأمن السيبراني تعمل على التنمية العلمية لطالبات الجامعة . والتي تتمثل في المعرفة المعمقة والتطبيقات الواقعية لتجارب العلمية وخطوات الإدارات كأدارة الوقت ولتقييم الذاتي كما يلي:

١. إدراك الطالبات لأهمية برامج الحماية وإمكانية التعرف على مواطن الضعف.
٢. مقدرة الطالبات على تحسين إمكانيات الحماية الأمنية المتوقعة وجميع المخاطر الأمنية الأخرى. (الجندى، ٢٠١٩).

الفصل الرابع: الإطار العملي

يشتمل على:

- إجراءات تطبيق التجربة.
- تحليل الاستبيان القبلي والبعدي.

إجراءات تطبيق التجربة:

قامت الباحثات بما يلي:

- قمنا باختيار أداة الدراسة وهي الاستبانة الإلكترونية.
- تحديد المجالات الرئيسية التي اشتملتها الاستبانة.
- صياغة الفقرات التي تقع تحت كل مجال.
- إعداد الاستبانة في صورتها الأولية والتي تشمل على (٤٢) سؤال وعرض الأسئلة على دكتورة المقرر.
- القيام بتحكيم الاستبيان من قبل بعض من أساتذة القسم وعددهم ٨ أساتذة وتم إرسال إليهم نسخه عن طريق الواتساب بصيغة .word و pdf.
- بعد الإطلاع على آراء المحكمين تم إجراء التعديلات التي أوصوا بها وبناء على ذلك تم تعديل الإستبانة حيث تم تعديل سؤال الفئة العمرية حيث كانت الخيارات تضم العمر ٤٠ فما فوق وتم تعديله إلى الفئة ٢٩ ، بالإضافة إلى إلغاء سؤال (١٢) وهو مستوى تعاملك مع الهجمات الإلكترونية ، وكما إجراء تعديل على الأسئلة المتكررة والمتتشابهة التي تحمل نفس المعنى مثل سؤال (١٣) و(١٥) الخاصة بكلمات المرور ودمجها في سؤال واحد، هذا وقد تم تعديل المصطلحات وتوحيدتها مثل الكمبيوتر إلى الحاسب الآلي ، بالإضافة إلى إلغاء الأسئلة التي تختص بمتطلبات تحقيق الأمن السيبراني وهي عبارة عن ٤ أسئلة للتقليل من طول الإستبانة ، كما تم إضافة سؤال: هل لدى معرفة سابقة بمفهوم التصيد الإلكتروني وإضافة سؤال هل لدى معرفة سابقة بالهندسة الاجتماعية ، وتعديل سؤال المستوى إلى المستوى الدراسي ، وأخيراً تغير كلمة القسم إلى التخصص.
- بعد إجراء التعديلات النهائية للإستبانة بلغ عدد الأسئلة (٣٤) سؤال وفق التقدير (موافق ، موافق بشدة ، محайд ، غير موافق ، غير موافق بشدة) . حيث تتضمن العناصر التالية:
 ١. الوعي بمفهوم الأمن السيبراني.
 ٢. الوقاية من مخاطر الاختراق.رابط أداة الدراسة القبلي: https://docs.google.com/forms/d/1RDuZiajEhCuDioTEjoDxG8pAujhzBuVWi-f4nFwG6MU/viewform?edit_requested=true رابط أداة الدراسة البعدي: https://docs.google.com/forms/d/15JwPxfvRoq_7TrALmldosjoq7cP1jYA6dTF2Wkw5yGQ/viewform?edit_requested=true
- الاتفاق مع أساتذة الأقسام لأخذ جزء من المحاضرة وشرح الدورة للطلاب.
- توجيه الإستبانة الإلكترونية للطلابات عينة الدراسة للإجابة عليها قبل خضوعهم للتدريب وثم توزيعها بشكل الكتروني وتم تجميعها ثم تقديم البرنامج التدريبي الخاص بتوعيتهم بالأمن السيبراني وبعد الانتهاء تم توزيع الاستبانة البعدية بشكل الكتروني وتجميعها.
- تحليل الاستبيان القبلي والبعدي لقياس مدى وعي الطالبات.

تحليل نتائج الاستبيان القبلي والبعدي:

جدول رقم (٢) يوضح توزيع أفراد العينة على الفئة العمرية:

النسبة المئوية	المجموع	النسبة	من ٢١ إلى ٣٠	النسبة	أقل من ٢٠	القسم العلمي الفئة العمرية
%١٢.٥	٢٤	%١٧	٢٠	%٥.٤	٤	الدراسات القرانية
%١٧.٧	٣٤	%٧.٦	٩	%٣٣.٨	٢٥	الدراسات الإسلامية
%١٣	٢٥	%١٨.٦	٢٢	%٤.١	٣	اللغة العربية
%١٢.٥	٢٤	%٢٠.٣	٢٤	%٠.٠٠	٠	اللغات والترجمة
%١٥.٦	٣٠	%١٥.٣	١٨	%١٦.٢	١٢	العلوم الاجتماعية
%١٧.٢	٣٣	%٨.٥	١٠	%٣١.١	٢٣	الإتصال والإعلام
%١١.٥	٢٢	%١٢.٧	١٥	%٩.٥	٧	المعلومات ومصادر التعلم
%١٠.٠	١٩٢	%٦١.٥	١١٨	%٢٨	٧٤	الإجمالي

في الجدول (٢) أظهرت النتائج أن الغالبية العظمى من أعمار طلابات بين عمر ٢١ إلى ٣٠ بنسبة ٦١.٥٪ وهو العمر المناسب لدخول طلابات للجامعة ثم يليه عمر طلابات أقل من ٢٠ بنسبة ٢٨٪، وأظهرت النتائج تجاوب الأقسام العلمية في تعبئة الإستبيان أن طلابات في قسم الدراسات الإسلامية كانوا الأكثر وبنسبة ١٧.٧٪، ثم قسم الإتصال والإعلام وبنسبة ١٧.٢٪، ثم قسم العلوم الاجتماعية وبنسبة ١٥.٦٪، ثم قسم اللغة العربية وبنسبة ١٣٪، ثم قسم الدراسات القرانية وقسم اللغات والترجمة المتشاربين في العدد وبنسبة ١٢.٥٪، وثم كان القسم الأقل عدداً المعلومات ومصادر التعلم ١١.٥٪.

الجدول رقم (٣) يوضح المستوى الدراسي لأفراد العينة:

النسبة	العدد	المستوى الدراسي
% ٤٥.٨	٨٨	الثاني
% ٣٣.٤	٤٥	الرابع
% ١٥.٦	٣٠	السادس
% ١٥.١	٢٩	الثامن
% ١٠٠	١٩٢	المجموع

في الجدول رقم (٣) يوضح أن الغالبية العظمى من طلابات بالمستوى الثاني وبنسبة ٤٥.٨٪، ثم المستوى الرابع وبنسبة ٣٣.٤٪، ثم المستوى السادس وبنسبة ١٥.٦٪، ثم المستوى الثامن وبنسبة ١٥.١٪.

يوضح الجدول مدى وعي طالبات كلية الآداب والعلوم الإنسانية عينة الدراسة بمفهوم الأمن السيبراني وذلك قبل إجراء التجربة وبعدها.

الجدول (٤) وعي طالبات كلية الآداب والعلوم الإنسانية بمفهوم الأمن السيبراني:

الاستجابة البعدية					الاستجابة القبلية					
غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	
٣	١١	١٦	١١٤	٤٥	١٨	٥٥	٤٢	٦٦	١١	لدي معرفة سابقة بمفهوم الأمن السيبراني؟
%١.٦	%٥.٨	%٨.٥	%٦٠.٣	%٢٣.٨	%٩.٤	%٢٨.٦	%٢١.٩	%٣٤.٤	%٥.٧	
٥	١١	١٨	٩٤	٦١	٥	١٤	٣٩	١١٤	٢٠	الأمن السيبراني: هو أمن المعلومات على أجهزة وشبكات الحاسب الآلي والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو اختلف قد يحدث.
%٢.٧	%٥.٨	%٩.٥	%٤٩.٧	%٣٢.٣	%٢.٦	%٧.٤	%٢٠.٥	%٦٠	%١٠.٥	
١	٢	١١	١٠٣	٧٢	٥	٦	٣٣	١١٥	٣٣	الأمن السيبراني: هو استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به ، ومنع سوء الاستغلال واستعادة المعاملات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها.
%٠.٥	%١.١	%٥.٨	%٥٤.٥	%٣٨.١	%٢.٦	%٣.١	%١٧.٢	%٥٩.٩	%١٧.٢	
٠	١	٨	١١١	٦٩	٥	٥	٣٣	١١٤	٣٥	الأمن السيبراني: هو حماية المستخدمين من أي مخاطر تواجههم.
%٠.٠	%٠.٥	%٤.٢	%٥٨.٧	%٣٦.٥	%٢.٦	%٢.٦	%١٧.٢	%٥٩.٤	%١٨.٢	

- حسب النتائج الموضحة بالجدول رقم (٤) تبين لنا أن عينة الدراسة إنقسمت إلى قسمين قبل بدء التجربة حيث أن جزء من عينة الدراسة كان لديهم وعي سابق بمفهوم الأمان السيبراني قبل تطبيق التجربة عليهم والنصف الآخر لم يكن لديهم الوعي بمفهوم الأمان السيبراني، ولكن بعد قيامنا بتطبيق التجربة كان هناك ارتفاع في نسب الوعي بمفهوم الأمان السيبراني وذلك إستناداً على الإستجابات القبلية والبعدية للإستبيان حيث بلغت نسبة موافق بشدة وموافق للسؤال الأول ٤٠.١٪ وهذه نسبة جيدة إلى حد ما ، بينما بلغت نسبة غير موافق وغير موافق بشدة ٣٨٪ ومحايد ٢١.٩٪، أما بعد إجراء التجربة فقد ارتفعت نسبة الوعي لديهم بمفهوم الأمان السيبراني حيث بلغت الإستجابات البعدية النسب التالية موافق بشدة وموافق ٨٤.١٪ ونستنتج من خلال هذه النسب أن الوعي لدى أفراد العينة قد زاد بشكل ملحوظ وفي المقابل بلغت نسبة غير موافق وغير موافق بشدة ٧٠.٤٪ ومحايد ٨.٥٪ مما يؤكد نجاح التجربة في جانب زيادة الوعي بمفهوم الأمان السيبراني ، وتتأثرها المباشر على وعيهم بهذا المفهوم وذلك إستناداً على إجابتهم من خلال الاستبانة ، وعند إنتقالنا للسؤال الثاني الخاص بمفاهيم الأمان السيبراني التي كانت عبارة عن ثلاثة مفاهيم يركز كل مفهوم منها على جزء حيث كان المفهوم الأول يركز على الأجهزة والشبكات بينما المفهوم الثاني كان يركز على الوسائل التقنية والتنظيمية ، والمفهوم الثالث الذي ركز على المستخدم ، ومن خلال النتائج الموضحة أعلاه نستنتج انه قبل تطبيق التجربة كان هناك اتفاق نسبة كبيرة من أفراد العينة على المفاهيم الثلاثة بنسب متساوية وذلك إستناداً على الإستبانة القبلية ، وكانت النسب تتركز في موافق بشدة وموافق بنسبة ٧٠٪ في المفاهيم الثلاثة وهي النسب الأعلى بالمقارنة لغير موافق ومحايد وذلك يدل على الاتفاق حول هذه المفاهيم ، وعند إجراء التجربة كان هناك ارتفاع ملحوظ في نسب الموافقة وإنخفاض نسب عدم الموافقة وذلك إستناداً على النتائج الموضحة ، ولكن لوحظ بعد التجربة أن المفهومين الخاصة بالوسائل التقنية والمستخدمين حصلت على أعلى نسب موافقه من أفراد العينة حيث تراوحت نسب الموافقه بين ٩٠٪ و ٩٥٪ .

يركز الجدول التالي على مدى احتياج طالبات كلية الآداب والعلوم الإنسانية لدورات تدريبية تختص بالأمن السيبراني، قبل وبعد التجربة لمعرفة مدى إهتمامهم وإستجابتهم لما يختص بالأمن السيبراني وقياس مدى تأثير التجربة على مدى احتياجاتهم لدورات تدريبية في مجال الأمن السيبراني.

الجدول رقم (٥) مدى احتياج طالبات كلية الآداب والعلوم الإنسانية لدورات تدريبية تختص بالأمن السيبراني:

الاستجابة البعدية					الاستجابة القبلية					احتاج إلى دورات تدريبية في الأمن السيبراني ؟
غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	
١	١١	١٨	١٠٨	٥١	٦	١٠	٢٢	١٠٣	٥١	
%٠٠.٥	%٥٠.٨	%٩٠.٥	%٥٧.١	%٢٧	%٣٠.١	%٥٠.٢	%١١٠.٥	%٥٣.٧	%٢٦.٦	

- توضح النتائج السابقة من خلال الجدول رقم (٥) لسؤال أحتاج إلى دورات تدريبية في الأمن السيبراني، مدى حاجة أفراد العينة إلى دورات تدريبية خاصة بالأمن السيبراني قبل تطبيق التجربة وبعد تطبيق التجربة . فمن خلال الإستجابات القبلية للإستبانة كان هناك إرتفاع في نسب الموافقة حيث بلغت نسبة موافق بشدة وموافق %٨٠ وغير موافق وموافق بشدة %٨٠.٣ مما يؤكد مدى حاجتهم وإهتمامهم في الحصول على الدورات التدريبية . وعند تطبيق التجربة فقد كانت نسب الموافقة أعلى وذلك إستناداً على الإستجابات البعدية للإستبانة حيث إرتفعت نسبة موافق بشدة وموافق إلى %٨٤.١ بينما إنخفضت نسبة غير موافق وغير موافق بشدة إلى %٦٠.٣ ، فقد لوحظ زيادة عدد الراغبين في الحصول على الدورات التدريبية في الأمن السيبراني ونستنتج من ذلك دور تطبيق التجربة في التوعية بأهمية موضوع الأمن السيبراني وضرورة الحصول على مزيد من الدورات التدريبية في هذا المجال.

يوضح الجدول التالي مدى قدرة طالبات كلية الآداب والعلوم الإنسانية عينة الدراسة على التفريق بين أمن المعلومات والأمن السيبراني قبل وبعد إجراء التجربة.

جدول رقم (٦) مدى قدرة طالبات كلية الآداب والعلوم الإنسانية على التفريق بين أمن المعلومات والأمن السيبراني:

الاستجابة البعدية					الاستجابة القبلية					استطيع التفريق بين الأمن السيبراني وأمن المعلومات؟
غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	
١	٥	١٣	١٠٦	٦٤	٢٧	٦٥	٤٥	٤٦	٩	
%٠٥	%٢.٧	%٦.٨	%٥٦.١	%٣٣.٩	%١٤.١	%٣٣.٩	%٢٣.٤	%٢٤	%٤.٧	

- تبين لنا من خلال النتائج الجدول رقم(٦) أن التجربة كان لها تأثير واضح و مباشر في إجابات أفراد العينة و حل مشكلة اللبس بين المفهومين فكانت النتائج تبين أن هناك ٩٠٪ من أفراد العينة أصبحوا قادرين على التفريق بين مفهومي الأمن السيبراني وأمن المعلومات ، فقد وضحت الإستجابات القبلية للإستبانة أن هناك فئة كبيرة من العينة لا تستطيع التفريق بين مفهومي الأمن السيبراني وأمن المعلومات وذلك بحسب النتائج القبلية التالية : حيث بلغت نسبة موافق بشدة و موافق ٢٨.٧٪ وهذه نسبة منخفضة بالنسبة لغير موافق حيث بلغت نسبة غير موافق و غير موافق بشدة ٤٨٪ وهذا يعني أن هناك ٤٨٪ من أفراد العينة ليست لديهم القدرة على التفريق بين هذين المفهومين ولكن الأمر اختلف بعد تطبيق التجربة، فعندما نأتي لقياس استجابتهم البعدية (بعد تطبيق التجربة). فنجد الفارق الواضح في النسب فقد ارتفعت نسبة موافق بينما انخفضت نسبة عدم الموافقة فقد بلغت نسبة موافق بشدة و موافق بعد التجربة ٩٠٪ وهذه نسبة كبيرة جدا ، بينما انخفضت نسبة غير موافق و غير موافق بشدة إلى ٣٠.٣٪ . وذلك يدل على دور التجربة الفعال في زيادة الوعي بمفهوم الأمن السيبراني وأمن المعلومات حيث تبين لهم بأمن المفهومين يتقنون بالاهتمامهما بالمعلومات الرقمية بينما الاختلاف أن الأمن السيبراني يتعلق بتتأمين الأشياء المعرضة للخطر من خلال تكنولوجيا المعلومات والاتصالات، وأمن المعلومات هو كل شيء عن حماية المعلومات التي تتركز بشكل عام على سرية وسلامة وتوافر المعلومات.

يوضح الجدول مدى وعي طالبات كلية الآداب والعلوم الإنسانية عينة الدراسة بالجرائم السيبرانية التي تحدث في الفضاء السيبراني.

جدول رقم (٧) وعي طالبات كلية الآداب والعلوم الإنسانية بالجرائم السيبرانية:

الاستجابة البعدية					الاستجابة القلبية					
غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	
١	٣	١٢	٨٦	٨٧	١٧	٥٩	٣٩	٦٢	١٥	لدي معرفة بالجرائم السيبرانية؟
%٠.٥	%١.٦	%٦.٤	%٤٥.٥	%٤٦	%٨.٩	%٣٠.٧	%٢٠.٣	%٣٢.٣	%٧.٨	
٢	٤	٧	١٠٦	٧٠	٢٣	٦٧	٣٣	٥٤	١٥	لدي معرفة بمفهوم التصيد الالكتروني؟
%١.١	%٢.١	%٣.٧	%٥٦.١	%٣٧	%١٢	%٣٥	%١٧.٢	%٢٨.١	%٧.٨	
٢	٥	١٧	١٠١	٦٤	٣٥	٨٣	٣٠	٣٤	١٠	لدي معرفة بمفهوم الهندسة الاجتماعية؟
%١.١	%٢.٧	%٩	%٥٣.٤	%٣٣.٩	%١٨.٢	%٤٣	%١٥	%١٨.٧	%٥.٢	
١	٣	٤	٩٠	٩١	١٣	١٥	١٧	٩٤	٥٣	لدي معرفة بمخاطر فتح روابط ومرافق البريد الالكتروني؟
%٠.٥	%١.٦	%٢.١	%٤٧.٦	%٤٨.١	%٦.٧	%٧.٨	%٨.٩	%٤٩	%٢٧.٦	
٢	٣	٥	٩٧	٨٢	١٤	٢٢	٣٨	٧٤	٢٢	لدي معرفة بالإجراءات اللازمة لحماية حاسبي من الاختراق؟
%١.١	%١.٦	%٤.٧	%٥١.٣	%٤٣.٤	%٨.٢	%١٢.٩	%٢٢.٤	%٤٣.٥	%١٢.٩	
٣	٠	٧	٩١	٨٨	٣	١٥	٢٤	١٠٨	٤٢	تح تقافة الأمن السيبراني من التجسس والتخريب الالكتروني على مستوى المجتمع؟
%١.٦	%٠.٠	%٣.٧	%٤٨.٢	%٤٦.٦	%١.٦	%٧.٨	%١٢.٥	%٥٦.٣	%٢١.٩	
١	٣	١١	٨٧	٨٧	١٠	٣٠	٢٨	٨٧	٣٧	لدي معرفة تامة بمخاطر تنزيل البرامج من الانترنت؟
%٠.٥	%١.٦	%٥.٨	%٤٦	%٤٦	%٥.٢	%١٥.٦	%١٤.٦	%٤٥.٣	%١٩.٣	

- حسب النتائج الموضحة في الجدول (٧) تبين لنا أن عينة الدراسة لمن يكن لديها الوعي الكافي بالجرائم السيبرانية حيث أن جزء بسيط من العينة القبلية لديها وعي لا يأس به حيث بلغت موافق بشدة وموافق بنسبة ٤٠.١٪ ومحايد بنسبة ٢٠.٣٪ وغير موافق وغير موافق بشدة ٣٩.٦٪، والنتائج البعدية تظهر لنا ازيداد وعي عينة الدراسة بمفهوم الجرائم السيبرانية حيث بلغت موافق موافق بشدة وموافق ٩١.٥٪ ومحايد بنسبة ٦.٤٪ وغير موافق وغير موافق بشدة بنسبة ١.٥٪ وذلك يدل على نجاح التجربة بعد أن تم تعريفهم بأن الجرائم السيبرانية هي الاستخدام غير المشروع للتكنولوجيا بقصد التدمير والتعدى على ممتلكات الغير من خلال الأجهزة وما تحتويه من معلومات، وتعريفهم بأنواعها، وأصناف المجرمين في الفضاء السيبراني.
- أظهرت النتائج القبلية بالنسبة لسؤال لدى معرفة بمفهوم التصيد الإلكتروني أن جزء بسيط من العينة لديها معرفة بمفهوم التصيد الإلكتروني حيث بلغت نسبة موافق بشدة وموافق ٣٩.٩٪ ومحايد ١٧.٢٪ وغير موافق وغير موافق بشدة ٤٧٪، وتظهر النتائج البعدية أن جزء كبير من عينة الدراسة أصبح لديهم وعي كافي بمفهوم التصيد الإلكتروني حيث بلغت موافق بشدة وموافق بنسبة ٩٣.١٪ ومحايد بنسبة ٣.٧٪ وغير موافق وغير موافق بشدة ٣.٢٪، وذلك بعد أن تم تعريفهم بأن التصيد الإلكتروني هو أسلوب لخداع المستخدم بالنقر على روابط أو مرفقات ضارة، بهدف اختراق أجهزة الضحايا للتجسس عليها أو إلحاق الضرر بها أو سرقة المعلومات وغيرها من التهديدات الإلكترونية وتعريفهم أيضاً بأشكالها.
- بينت النتائج القبلية الخاصة بسؤال لدى معرفة بمفهوم الهندسة الاجتماعية بأن عينة الدراسة ليس لديها وعي كافية بهذا المفهوم حيث بلغت موافق بشدة وموافق بنسبة ٢٣.٩٪ ومحايد بنسبة ١٥٪ وغير موافق وغير موافق بشدة بنسبة ٦١.٢٪، والنتائج البعدية تظهر لنا مدى نجاح التجربة في زيادة وعيهم بمفهوم الهندسة الاجتماعية حيث بلغت موافق بشدة وموافق ٨٧.٣٪ ومحايد بنسبة ٩٪ وغير موافق وغير موافق بشدة ٣.٨٪، وذلك بعد أن تم تعريفهم بأن الهندسة الاجتماعية عملية يتم من خلالها خداع الناس وحصول المتسلل على معلومات خاصة وسرية تقييد المتسلل بطريقة ما، وتعريفهم بمراحل الهجوم، وطرق الحماية.
- أوضحت النتائج القبلية لسؤال لدى معرفة بمخاطر فتح روابط ومرفقات البريد الإلكتروني بأن عينة الدراسة لديها وعي كافي بمخاطر فتح الروابط ومرفقات البريد الإلكتروني وذلك بسبب التوعية من قبل البنوك وشركات الاتصال والجامعات وسائل التوعية المتداولة من قبل الأشخاص الذين وقعوا ضحية فتح روابط غير آمنه أو قريب لهم عبر موقع التواصل الاجتماعي وقيامهم بتتبّع الآخرين وتحذيرهم من خلال صوت أو مقطع فيديو أو رسالة نصية عن خطورة فتح أي روابط غير آمنه حيث بلغت موافق بشدة وموافق ٧٦.٦٪ ومحايد بنسبة ٨٠.٩٪ وغير موافق وغير موافق بشدة بنسبة ١٤٠.٥٪، وفي النتائج البعدية تم توعية الجزء المتبقى من العينة التي لم يكن لديها الوعي الكافي حيث بلغت موافق بشدة وموافق بنسبة ٩٥.٧٪ ومحايد بنسبة ٢٠.١٪ وغير موافق وغير موافق بشدة ٢٠.١٪.

- أظهرت النتائج القبلية لسؤال لدي معرفة بالإجراءات الازمة لحماية حاسبي من الاختراق أن أكثر من نصف العينة لديها وعي جيد بحماية حاسباتهم من الاختراقات حيث بلغت موافق بشدة وموافق نسبة ٥٦.٤٪ ومحايد بنسبة ٢٢.٤٪ وغير موافق وغير موافق بشدة ٢١.١٪، وفي النتائج البعدية زاد وعيهم بعد تعريفهم بالبرمجيات التي تساعدهم على حماية أجهزتهم من الاختراقات حيث بلغت موافق بشدة وموافق نسبة ٩٤.٧٪ ومحايد ٢٠.٧٪ وغير موافق وغير موافق بشدة ٢٠.٧٪.
- وضحت النتائج القبلية بالنسبة لسؤال تحد ثقافة الأمن السيبراني من التجسس والتخريب الإلكتروني على مستوى المجتمع بأن عينة الدراسة تتوافق مع هذه العبارة حيث بلغت موافق بشدة وموافق ٧٨.٢٪ ومحايد ١٢.٥٪ وغير موافق وغير موافق بشدة ٩٠.٤٪، وبعد القيام بالتجربة وضحت النتائج البعدية ازيداد إتفاقهم على هذه العبارة حيث بلغت موافق بشدة ٩٤.٨٪ ومحايد ٣٠.٧٪ وغير موافق وغير موافق بشدة ٣٠.٧٪.
- بينت النتائج القبلية الخاصة لسؤال لدى معرفة تامه بمخاطر تنزيل البرامج من الإنترنط أن عينة الدراسة لديها وعي جيد بمخاطر تنزيل البرامج من الإنترنط حيث بلغت موافق بشدة وموافق نسبة ٦٤.٦٪ ومحايد ١٤.٦٪ وغير موافق وغير موافق بشدة ٢٠.٨٪، وفي النتائج البعدية زاد وعيهم أكثر بالمخاطر حيث بلغت نسبة موافق بشدة وموافق بنسبة ٩٢٪ ومحايد ٥.٨٪ وغير موافق وغير موافق بشدة ٢٠.١٪.

يوضح الجدول التالي مدى معرفة طالبات كلية الآداب والعلوم الإنسانية عينة الدراسة حماية أنفسهم من الاختراقات السiberانية التي تحدث في الفضاء السiberاني.

الجدول رقم (٨) مدى معرفة طالبات كلية الآداب والعلوم الإنسانية لحماية أنفسهم من الاختراقات السiberانية:

الاستجابة البعدية						الاستجابة القبلية						
غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة			
١	٤	٦	٧٤	١٠٤	٦	١٤	٢٦	٨٧	٥٩			تجنب وضع البيانات والصور الشخصية على موقع التواصل الاجتماعي الا للضرورة؟
% .٦	% ٢.٤	% ٣.٧	% ٢٩	% ٦٤.٢	% ٣.١	% ٧.٣	% ١٣.٥	% ٤٥.٣	% ٣٠.٧			
٥٠	٥٠	١٦	٤٥	٢٨	٢٠	٤٥	٣٣	٧٤	٢٠			احفظ بأرقامي السرية في المتصفح؟
% ٢٦.٥	% ٢٦.٥	% ٨.٥	% ٢٣.٨	% ١٤.٨	% ١٠.٤	% ٢٣.٤	% ١٧.٢	% ٣٨.٥	% ١٠.٤			
٥٣	٥٦	١٧	٤٤	١٩	٣١	٤٨	٢٦	٦٥	٢٢			استخدم نفس كلمة المرور لجميع مواقع التواصل الاجتماعي والبريد الإلكتروني؟
% ٢٨	% ٢٩.٦	% ٩	% ٢٣.٣	% ١٠.١	% ١٦.٢	% ٢٥	% ١٣.٥	% ٣٣.٩	% ١١.٥			
١	٢	١٣	٨٠	٩٣	١٢	٣٧	٢٨	٨٥	٣٠			أقوم بقراءة شروط وتعليمات المستخدم لبرنامج مجاني قبل الضغط على موافق؟
% .٥	% ١.١	% ٧.٩	% ٤٢.٣	% ٤٩.٢	% ٦.٣	% ١٩.٨	% ١٤.٦	% ٤٤.٣	% ١٥.٦			
٤	٣	١٢	٨٤	٨٦	١٣	٤٠	٣٧	٧٥	٢٧			استخدم برنامج الحماية من الفيروسات بصورة مستمرة؟
% ٢.١	% ١.٦	% ٦.٤	% ٤٤.٥	% ٤٦	% ٦.٨	% ٢٠.٨	% ١٩.٣	% ٣٩.١	% ١٤.١			
٨٧	٥٠	١٠	٢٧	١٥	٥٣	٦٨	٢٦	٣٥	١٠			افتح رسالة الكترونية غير معروفة لدي؟
% ٤٦	% ٢٦.٥	% ٥.٢	% ١٤.٣	% ٧.٩	% ٢٧.٦	% ٣٥.٤	% ١٣.٥	% ١٨.٢	% ٥.٢			
٣	٤	١٤	٧٨	٩٠	٦	٢٦	٣٥	٨٥	٤٠			أقوم بالتخلص من رسائل البريد مجهولة المصدر دون فتحها؟
% ١.٦	% ٢.١	% ٧.٤	% ٤١.٣	% ٤٧.٦	% ٣.١	% ١٣.٥	% ١٨.٢	% ٤٤.٣	% ٢٠.٨			
٢	١	٤	٧٧	١٠٥	٤	٩	٢٤	٩٦	٥٩			أحرص على استخدام متصفح امن لإنترنت؟
% ١.١	% ٠.٥	% ٢.١	% ٤٠.٧	% ٥٥.٦	% ٢.١	% ٤.٧	% ١٢.٥	% ٥.٠	% ٣٠.٧			
١	٤	٦	٧٨	١٠٠	٥	٢٥	٣١	٨٧	٤٤			احذر كثيرا عند الاتصال بال شبكات العامة؟
% .٥	% ٢.١	% ٣.٢	% ٤١.٣	% ٥٢.٩	% ٢.٦	% ١٣	% ١٦.٢	% ٤٥.٣	% ٢٢.٩			
.	١	٤	٦٤	١٢٠	٦	٣	١٩	٧٧	٨٧			ابعد عن مشاركة معلوماتي الشخصية مع الغرباء على الانترنت
% .٠	% ٠.٥	% ٢.١	% ٣٣.٩	% ٦٣.٥	% ٣.١	% ١.٦	% ٩.٩	% ٤٠.١	% ٤٥.٣			
.	٤	١٠	٧٦	٩٩	٨	٢٥	٤٦	٨٢	٣١			افحص جهازي الآلي بصورة مستمرة؟
% .٠	% ٢.١	% ٥.٣	% ٤٠.٢	% ٥٢.٤	% ٤.٢	% ١٣	% ٢٤	% ٤٢.٧	% ١٦.٢			

٢	٢	٩	٧٩	٩٧	٢٥	٥١	٢٥	٦٥	٢٦	اعرف بمن اتصل في حال حدوث اختراق؟
%١.١	%١.١	%٤٠.٨	%٤١.٨	%٥١.٣	%١٣	%٢٦.٦	%١٣	%٣٣.٩	%١٣٠.٥	
٠	٣	٧	٨٨	٩١	١٣	٢٥	٣٩	٨٧	٢٨	أقوم بتحديث نظام التشغيل بصورة دورية؟
%٠٠	%١.٦	%٣٠.٧	%٤٦.٦	%٤٨.٢	%٦.٨	%١٣	%٢٠.٣	%٤٥.٣	%١٤.٦	
١	٣	٧	٦٤	١١٤	٦	١٣	١٧	٨٣	٧٣	اختار كلمة مرور مكونة من أرقام وحروف ورموز؟
%٠٠.٥	%١.٦	%٣٠.٧	%٣٣.٩	%٦٠.٣	%٣.١	%٦.٨	%٨.٩	%٤٣.٢	%٣٨	
٨٢	٤٦	٨	٣٣	٢٠	٤٤	٦٦	٢٥	٤٥	١٢	أترك الحساب او النظام مفتوح بدون تسجيل خروج عند المغادرة؟
%٤٣.٤	%٢٤.٣	%٤٠.٢	%١٧.٥	%١٠.٦	%٢٢.٩	%٣٤.٤	%١٣	%٢٣.٤	%٦.٣	
١	٢	٨	٩٦	٨٢	٨	١٧	٤٥	٩٤	٢٨	اهتم بتطوير مهاراتي وزيادة معارفي بالآليات المناسبة لتحقيق الأمان السيبراني وطرق الوقاية من المشاكل السيبرانية
%٠٠.٥	%١.١	%٤٠.٢	%٥٠.٨	%٤٣.٤	%٤.٢	%٨.٩	%٢٣.٤	%٤٩	%١٤.٦	

من خلال الجدول رقم (٨) أردنا معرفة مدى وعي عينة الدراسة طالبات كلية الآداب والعلوم الإنسانية في حماية أنفسهم من الاختراقات السيبرانية عبر مجموعة من الأسئلة:

- وضحت النتائج القبلية لسؤال أتجنب وضع البيانات والصور الشخصية على موقع التواصل الاجتماعي إلا للضرورة، وعي جزء كبير من عينة الدراسة في عدم وضع بياناتهم وصورهم على موقع التواصل الاجتماعي إلا للضرورة حيث بلغت موافق بشدة وموافق نسبة ٧٦٪ ومحايد نسبة ١٣٠.٥٪ وغير موافق وغير موافق بشدة ١٠٠.٤٪، ووضحت النتائج البعدية إزدياد وعيهم حيث بلغت موافق بشدة وموافق نسبة ٩٣.٢٪ ومحايد نسبة ٣٠.٧٪ وغير موافق وغير موافق بشدة ٣٪.
- بيّنت النتائج القبلية لسؤال احتفظ بأرقامي السرية في المتصفح على أن نسبة كبيرة تقوم بحفظ أرقامها السرية على المتصفح وجدهم بالمخاطر التي قد يتعرضون لها حيث بلغت نسبة موافق بشدة وموافق ٤٨.٩٪ ومحايد ١٧٠.٢٪ وغير موافق موافق بشدة ٣٣٪، وبيّنت النتائج البعدية إزدياد وعي البعض والبعض الآخر أصر على أن يحتفظ بأرقامه السرية في المتصفح رغم تعريفهم بالمخاطر حيث بلغت موافق بشدة وموافق نسبة ٣٨.٦٪ ومحايد نسبة ٨٠.٥٪ وغير موافق وغير موافق بشدة بنسبة ٥٣٪.

- أظهرت النتائج القبلية لسؤال استخدم نفس كلمة المرور لجميع موقع التواصل الاجتماعي والبريد الإلكتروني بأن نصف عينة الدراسة تقريباً تقوم بالاختبار كلمة سر واحدة لجميع مواقعها حيث بلغت موافق بشدة وموافق نسبة ٤٥.٤٪ ومحايد بنسبة ١٣.٥٪ وغير موافق بشدة ٤١.٢٪، وأظهرت النتائج البعدية بإزديادوعي البعض حيث أنهم سوف يقومون بالاختيار كلمات مرور مختلفة لكل موقع والبعض الآخر أصرروا على استخدام نفس كلمة السر لجميع الموقع رغم المخاطر التي قد تصبهم فقد بلغت نسبة موافق وموافق ٣٣.٤٪ ومحايد بنسبة ٩٪ وغير موافق وغير موافق بشدة ٥٧.٦٪.
- وضحت النتائج القبلية لسؤال أقوم بقراءة شروط وتعليمات المستخدم لبرنامج مجاني قبل الضغط على موافق بأن نسبة كبيرة من عينة الدراسة تقوم بقراءتها وهذا يدل على وعيهم حيث بلغت موافق بشدة وموافق بنسبة ٥٩.٩٪ ومحايد بنسبة ٦٤.٦٪ وغير موافق وغير موافق بشدة ٢٦.١٪، ووضحت النتائج البعدية ازديادوعي البقية حيث بلغت نسبة موافق بشدة وموافق بنسبة ٩١.٥٪ ومحايد بنسبة ٧٨.٩٪ وغير موافق وغير موافق بشدة بنسبة ١٠.٦٪.
- بينت النتائج القبلية لسؤال استخدم برنامج الحماية من الفيروسات بصورة مستمرة بأن نصف العينة تقريباً لديها وعي واهتمام باستخدام برامج حماية حيث بلغت موافق بشدة وموافق نسبة ٥٣.٢٪ ومحايد نسبة ١٩.٣٪ وغير موافق وغير موافق بشدة ٢٧.٦٪، وبينت النتائج البعدية بإزدياد وعيهم أكثر بضرورة استخدام برنامج للحماية ضد الفيروسات حيث زادت نسبة موافق بشدة وموافق بنسبة ٩٠.٥٪ وانخفضت كلا من محايد بنسبة ٦.٤٪ وغير موافق وغير موافق بشدة ٣.٧٪.
- أظهرت النتائج القبلية لسؤال افتح رسائل إلكترونية غير معروفة بأن عينة الدراسة لديهم وعي حيث بلغت موافق بشدة وموافق بنسبة ٢٣.٤٪ ومحايد بنسبة ١٣.٥٪ وغير موافق وغير موافق بشدة ٦٣٪، وأظهرت النتائج البعدية زيادة وعي العينة حيث بلغت موافق بشدة وموافق ٢٢.٢٪ ومحايد بنسبة ٥.٢٪ وغير موافق وغير موافق بشدة ارتفعت بنسبة ٧٢.٥٪.
- وضحت النتائج القبلية لسؤال أقوم بالتخلص من رسائل البريد مجهولة المصدر دون فتحها إلى أن هناك جزء من أفراد العينة كان لديهم وعي مسبق حيث بلغت نسبة موافق بشدة وموافق قبل إجراء التجربة ٦٥.١٪ وغير موافق وغير موافق بشدة ١٦.٦٪ ومحايد بنسبة ١٨.٢٪، ولكن بعد إجراء التجربة لوحظ ارتفاع نسبة وعي أفراد العينة حيث بلغت النتائج البعدية موافق بشدة وموافق ٨٨.٩٪ وغير موافق وغير موافق بشدة ٣.٧٪ ومحايد بنسبة ٧.٤٪.
- توصلت النتائج القبلية لسؤال أحضرت على استخدام متصفح للإنترنت إلى أن هناك وعي مسبق لدى أفراد العينة بضرورة استخدام المتصفحات الآمنة حيث كان هناك وعي حيث بلغت موافق بشدة وموافق ٨٠.٧٪ وغير موافق وغير موافق بشدة بنسبة ضئيلة بلغت ٦.٨٪ ومحايد بنسبة ١٢.٥٪، وبعد تطبيق التجربة إرتفعت نسبة الوعي لدى أفراد العينة حيث بلغت نسبة موافق بشدة وموافق ٩٦.٣٪ وغير موافق وغير موافق بشدة انخفضت إلى ١.٦٪ ومحايد بنسبة ٢.١٪.

- توضح نتائج سؤال احذر كثيرا عند الإتصال بالشبكات العامة إلى أن هنا زيادة في وعي أفراد العينة بعد التجربة ، وهذا ماؤضحته النتائج التالية قبل التجربة بلغت نسبة موافق بشدة وموافق ٦٨.٢٪ وغير موافق وغير موافق بشدة نسبة ١٥٪ ومحايد بنسبة ١٦.٢٪ ، وكما هو متوقع بعد إجراء التجربة إرتفعت نسبة الوعي حيث بلغت موافق بشدة وموافق ٩٤.٢٪ وغير موافق وغير موافق بشدة ٢٠.٦٪ ومحايد بنسبة ٣.٢٪ .
- وضحت النتائج القبلية لسؤال أبتعد عن مشاركة معلوماتي الشخصية مع الغرباء على الإنترن特 أن جزء كبير من أفراد العينة كان لديهم وعي مسبق وذلك قبل تطبيق التجربة حيث بلغت موافق بشدة وموافق بنسبة ٨٥.٤٪ بينما غير موافق وغير موافق بشدة بلغت ٤.٧٪ ومحايد بنسبة ٩.٩٪ ، وبعد تطبيق التجربة قد زاد الوعي لدى أفراد العينة بنسبة ٩٧.٤٪.
- توضح النتائج القبلية لسؤال أ Finch جهازي الآلي بصورة مستمرة أنه كانت هناك نسبة وعي متوسطة إلى حد ما حيث بلغت نسبة موافق بشدة وموافق ٥٨.٩٪ وغير موافق وغير موافق بشدة ١٧.٢٪ ومحايد بنسبة ٢٤٪ ومن خلال هذا نستنتج وجود فئة بحاجة إلى التوعية ، وبعد إجراء التجربة إزدادت نسبة الوعي بشكل كبير حيث بلغت موافق بشدة وموافق ٩٢.٦٪ وغير موافق وغير موافق بشدة بنسبة ٢٠.١٪ ومحايد بنسبة ٥.٣٪ .
- توضح النتائج لسؤال أعرف بمن أتصل في حال حدوث إنترانق أن هناك تقاويم في درجة الوعي لدى أفراد العينة قبل التجربة حيث بلغت نسبة موافق بشدة وموافق قبل التجربة ٤٧.٤٪ وغير موافق وغير موافق بشدة ٣٩.٦٪ ومحايد بنسبة ١٣٪ وهذه نسب تحتاج إلى التوعية، وبعد تطبيق التجربة إرتفعت نسبة الوعي بشكل كبير لتصل إلى ٩٣.١٪ وغير موافق وغير موافق بشدة إنخفضت لتصل إلى ٢٠.٢٪ ومحايد بنسبة ٤.٨٪ .
- توضح النتائج القبلية لسؤال أقوم بتحديث نظام التشغيل بصورة دورية إلى وجود نسبة وعي جيدة قبل بدء التجربة وزيادة نسبة هذا الوعي بعد التجربة ، حيث بلغت نسبة موافق بشدة وموافق قبل إجراء التجربة ٥٩.٩٪ وغير موافق وغير موافق بشدة ١٩.٨٪ ومحايد بنسبة ٢٠.٤٪ . وبعد إجراء التجربة زادت نسبة الوعي لدى أفراد العينة ، حيث بلغت النتائج البعيدة للتجربة موافق بشدة وموافق ٩٤.٨٪ وهذا يوضح مدى إرتفاع نسبة الوعي بينما إنخفضت نسب عدم الموافقة لتصل إلى ١٠.٦٪ ومحايد بنسبة ٣.٧٪ .
- توضح النتائج القبلية لسؤال أختار كلمة مرور مكونة من أرقام وأحرف ورموز أن نسبة كبيرة من أفراد العينة كانت لديهم المعرفة بكلمة المرور المناسبة فقد كانت نسبة الوعي قبل التجربة تصل إلى ٨١.٢٪ ونسبة ضئيلة ليس لديهم الوعي بكلمة المرور المناسبة حيث بلغت نسبة غير موافق ٩.٩٪ ومحايد بنسبة ٨.٩٪ ، وبعد إجراء التجربة إرتفعت نسبة الوعي حيث بلغت موافق بشدة وموافق ٩٤.٢٪ وإنخفضت نسبة غير موافق وغير موافق بشدة لتصل إلى ٢٠.١٪ ومحايد بنسبة ٣.٧٪ .
- توضح النتائج لسؤال أترك النظام مفتوح بدون تسجيل خروج عند المغادرة أن هناك زيادة في الوعي بعد إجراء التجربة مقارنة بقبل بدء التجربة حيث بلغت النتائج القبلية موافق بشدة وموافق ٢٩.٧٪ وغير موافق وغير موافق بشدة ٥٧.٤٪ ومحايد بنسبة ١٣٪ ، وبعد تطبيق التجربة بلغت النتائج كالتالي موافق وموافق بشدة ٢٨.٢٪ وغير موافق وغير موافق بشدة إرتفعت لتصل إلى ٦٧.٧٪ وهذه النسب تدل على زيادة الوعي لدى أفراد العينة بعد التجربة .

- توضح النتائج القبلية لسؤال أهتم بتطوير مهاراتي وزيادة معارفي بالآليات المناسبة لتحقيق الأمان السيبراني وطرق الوقاية أن هناك نسبة جيدة في إهتمامهم (أفراد العينية) بتطوير مهاراتهم حيث بلغت النتائج القليلة موافق بشدة وموافق ٦٣.٦٪ وغير موافق وغير موافق بشدة ١٣.١٪ وبلغت نسبة محاید نسبة لابأس بها حيث كانت ٢٣.٤٪، وبعد تطبيق التجربة إرتفعت نسبة إهتمامهم بتطوير مهاراتهم لتصل إلى ٩٣.٢٪ بينما إنخفضت نسب عدم الموافقة بشكل كبير ومحاید لتصل إلى ٤٠.٢٪.

الفصل الخامس

يشتمل على:

- الخاتمة.
 - أولاً: النتائج.
 - ثانياً: التوصيات.
 - المراجع.
- المراجع العربية. -المراجع الأجنبية.

الخاتمة:

الحمد لله رب العالمين ب توفيق من الله عز وجل أتممنا خاتم بحثنا هذا الذي تحدثنا فيه باستفاضة عن فعالية برنامج تدريبي مقترن لتنمية الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الإنسانية حيث يعد من الأسس التي ينبغي أن يتم معرفتها والعمل على توعية المؤسسات التعليمية بها والتعرف على الأمور التي يجب أن يتم إدراكتها لتجنب الوقوع بالمخاطر وذلك يكون عبر تعزيز الوعي لجميع الأشخاص في المؤسسات التعليمية من أجل التركيز على هذا المجال وتقديم كافة الوسائل بمختلف أشكالها التي من شأنها أن تعمل على نشر أهمية ودور الأمن السيبراني بشكل أفضل حيث تم الاستشهاد بالعديد من مصادر المعلومات التي من شأنها أن تكون دليلاً لمن يبحث عن هذا الموضوع وسائل رب العالمين أن يجعل هذا البحث سبيلاً لنا للخروج من الجامعة وسائل الله أن نكون قد وفقنا في انتقاء الموضوع والحديث عنه وبيان كل ما يتعلق به وسائله أن يكون هذا البحث نافعاً لكل الباحثين والمهتمين بهذا المجال الواسع.

النتائج:

ـ فيما يخص الجانب النظري :

١. كشفت نتائج الدراسة أن مفهوم الأمن السيبراني لابد أن يغطي جميع الاجراءات المستخدمة في حماية المعلومات والبيانات والشبكات واختيار أفضل وسائل الحماية المناسبة من أي احتراق أو تعديل أو تعطيل أو الاستخدام غير المشروع كما تتمثل أهمية الأمن السيبراني في حماية الموارد البشرية والمادية من الانتهاكات والاستخدام الإجرامي غير المصرح التي قد تتعرض إليها والعمل على تخفيف وإصلاح الخسائر الناجمة في حال حدوث تهديدات أو قرصنة وتوفير بيئة عمل إلكترونية آمنة.
٢. يستدل من نتائج الدراسة ضرورة تعاون مختلف الجهات والمؤسسات في الدوله للعمل في منظومة وطنية متكاملة للحد من مخاطر الجرائم ومواجهتها والعمل على نشر التوعية والتصرف الصحيح عند مواجهة إحدى أنواع الجرائم والسعى إلى تقليل أثرها لأنها تشكل خطوره كبيره على المعلومات و تعرض الأنظمة للمشاكل التقنية كما أن الهدف الأساسي من تلك الجرائم هو تحقيق الربح المادي واستخدام البيانات الشخصية بصورة غير قانونية والحصول على المعلومات السرية والمهمة.
٣. توضح لنا من نتائج الدراسة أن بعض الجامعات السعودية قامت بتوفير إدارات للأمن السيبراني حيث تسعى الجامعة إلى توفير بيئة آمنه وموثقة من خلال العمل على توعية جميع المنسوبين من أعضاء هيئة التدريس والطلبة والعاملين بالمخاطر والوسائل التي ينبغي اتباعها من أجل عدم الوقوع فيها وضرورة المحافظة على الأصول المعلوماتية التي تزدهر بها الجامعة والتأكد من ضمان استمرار توفر المعلومات للمستفيدين بشكل سليم، وتعمل الإدارات على تعزيز مبدأ الحماية المشتركة وتعريف جميع العاملين بالسياسات التي لابد أن يتم اتباعها في مجال الأمن السيبراني.

ـ فيما يخص الجانب العملي :

١. كشف البرنامج التدريبي المقدم إلى طالبات كلية الآداب والعلوم الإنسانية أن عينة الدراسة كانت ١٩٢ طالبة في الاستبيان القبلي و ١٨٩ طالبه في الاستبيان البعدى .
٢. كشفت النتائج أن أعلى استجابة من قسم الاتصال والاعلام بنسبة ١٧.٧٪، وأقل استجابة من قسم المعلومات ومصادر التعلم بنسبة ١١.٥٪.
٣. كشفت النتائج أن الغالبية العظمى للاستجابات من الطالبات بالمستوى الثاني بنسبة ٤٥.٨٪، كما تراوحت الأعمار الأكثر استجابة من عمر ٢١ إلى ٣٠ بنسبة ٦١.٥٪ .
٤. يستدل من نتائج البرنامج التدريبي أن الغالبية العظمى من طالبات كلية الآداب والعلوم الإنسانية لم يكن لديهم معرفة سابقة بالأمن السيبراني حيث بلغت النسبة ٣٨٪ وبعد تقديم البرنامج التدريبي تبين لنا مدى استفادة عينة الدراسة منها حيث بلغت النسبة ٨٤.٨٪.
٥. كشفت النتائج أن التعريف الأكثر اتفاقاً من قبل عينة الدراسة في الاستبيان القبلي كان هناك إتفاق نسبة كبيرة من عينة الدراسة على المفاهيم الثلاثة وبعد تقديم البرنامج التدريبي لوحظ أن المفهومين الخاصه بالوسائل التقنية والمستخدمين حصلت على نسبة بين ٩٠٪ و ٩٥٪.
٦. يستدل من النتائج أن عينة الدراسة اتفقت على احتياجهم لدورات تدريبية في مجال الأمن السيبراني بنسبة ٨٠٪ في الاستبيان القبلي أما بالنسبة لمدى احتياجهم للدورات التدريبية في الاستبيان البعدى بلغت النسبة ٨٤.١٪ مما يوضح زيادةوعي الطالبات وحرصهم على الإلتحاق بالدورات والبرامج التدريبية.
٧. كشفت نتائج الدراسة فيما يخص الفرق بين الأمن السيبراني وأمن المعلومات أن عينة الدراسة في الاستبيان القبلي لم يكن لديها المعرفة الكافية حول الفرق حيث بلغت النسبة ٤٨٪ أما بعد تقديم البرنامج التدريبي وتوضيح الفرق بين المصطلحين تمكنت عينة الدراسة من التفريق بين أمن المعلومات والأمن السيبراني حيث بلغت النسبة ٩٠٪ مما يدل على فعالية البرنامج التدريبي في زيادة الوعي لدى الطالبات وتوضيح الفرق بين المفهومين.
٨. تبين لنا من نتائج البرنامج التدريبي أن عينة الدراسة لم تكن لديها المعرفة الكافية بمفهوم الجرائم المعلوماتية حيث بلغت النسبة في الاستبيان القبلي ٣٩.٦٪ أما بعد تقديم الدورة التدريبية بلغت النسبة في الاستبيان البعدى ٩١.٥٪ مما يدل على زيادة الوعي لدى عينة الدراسة.
٩. يستدل من النتائج أن عينة الدراسة لم يكن لديها الوعي الكافي بمفهوم التصييد الإلكتروني حيث بلغت النسبة ٣٩.٩٪ في الاستبيان القبلي، وبعد تقديم الدورة زاد وعيهم وبلغت النسبة ٩٣.١٪ في الاستبيان البعدى.

١٠. كشفت نتائج الدراسة فيما يخص مفهوم الهندسة الاجتماعية بأن عينة الدراسة لم يكن لديها الوعي الكافي بالمفهوم حيث بلغت النسبة ٢٣.٩٪ في الاستبيان القبلي، وأما في الاستبيان البعدى بلغت النسبة ٨٧.٣٪ مما يدل على زيادة وعيهم بهذا المفهوم.
١١. كشفت لنا نتائج البرنامج التربى فيما يخص المعرفة بخطورة تنزيل البرامج من الإنترنط أن عينة الدراسة لديهم وعي لا بأس به حيث بلغت النسبة في الاستبيان القبلي ٧٦.٦٪ ، ولكن في الاستبيان البعدى تزايد وعي العينة بشكل كبير وأصبح لديهم وعي كافى حيث أصبحت النسبة ٩٥.٧٪.
١٢. أوضحت نتائج الدراسة في ما يتعلق بسؤال عينة الدراسة حول المعرفه الكافيه بمخاطر فتح روابط ومرفقات البريد الإلكتروني أن عينة الدراسة لديهم وعي كافى حول هذه المخاطر الناتجة وما تؤدى إليه من أضرار حيث بلغت النسبة في الاستبيان القبلي ٧٦.٦٪ ، وبعد تقديم البرنامج التربى ارتفعت نسبة الوعي إلى ٩٥.٧٪.
١٣. استعرضنا في البرنامج التربى أرقام التواصل مع الهيئات المختصة في حين التعرض إلى أي هجوم أو اختراق كما تم سؤال عينة الدراسة عن مدى معرفتهم بالأرقام الخاصة في حال تعرضهم للاختراق وتبين لنا أن هناك اختلاف متقاوت في مدى الوعي حيث بلغت النسبة في الاستبيان القبلي وقبل إجراء التجربة ٤٧.٤٪ وبعد تقديم البرنامج التربى ارتفعت نسبة الوعي إلى ٩٣.١٪.
١٤. كشفت النتائج في ما يتعلق بسؤال أحذر كثيرا عند الاتصال بالشبكات العامة أن نسبة كبيرة من عينة الدراسة كان لديها وعي حيث بلغت ٦٨.٢٪ في الاستبيان القبلي، وبعد تقديم البرنامج التربى زاد وعي البقية حيث بلغت النسبة ٩٤.٢٪ في الاستبيان البعدى.
١٥. يستدل من النتائج فيما يخص سؤال استخدم برنامج الحماية من الفيروسات بأن نصف عينة الدراسة لديها وعي حيث بلغت النسبة ٥٣.٢٪ في الاستبيان القبلي، وبعد تقديم الدوره وتعريفهم على برامج الحماية زادت نسبة الوعي بنسبة ٩٠.٥٪.

الوصيات:

١. تقديم برامج تربوية للطلاب لتوسيعهم بالأمن السيبراني.
٢. إضافة مواد تعليمية متعلقة بالأمن السيبراني .
٣. تقديم الدعم والتحفيز لزيادة إعداد البحوث والدراسات المتعلقة بالأمن السيبراني.
٤. تحسين وعي الطالبات لتهيئتهم على مقاومة الجرائم في الفضاء السيبراني بكافة أنواعها عن طريق عقد الدورات والبرامج التربوية.
٥. إقامة وورش عمل داخل الجامعة لتوسيعه الطالبات وأعضاء هيئة التدريس حول كيفية مواجهة مخاطر الأمن السيبراني .
٦. نشر ثقافة الوعي بأهمية الأمن السيبراني وانه افضل الطرق لحماية الاجهزه والبيانات.
٧. إنشاء مراكز إبلاغ واستجابة لحالات الطوارئ الخاصة بالأجهزة الإلكترونية.
٨. تطوير أنظمة الجامعات التقنية، التي تمنع وصول العابثين والمختفين لأنظمة الجامعات وحمايتها.
٩. متابعة التطوير في البنية التحتية داخل الجامعات ومواكبة التكنولوجيا الجديدة.
١٠. ضرورة قيام إدارة الجامعات بعقد مناقشات وحوارات مع المختصين بالأمن السيبراني لمعرفة أحدث التطورات.
١١. الاهتمام بالدمج بين الجانب النظري والجانب العملي في إعداد البرامج التربوية.
١٢. استقطاب مؤهلين ومختصين في مجال الأمن السيبراني في الجامعات.
١٣. تفعيل دور الإدارات بالأمن السيبراني وتفعيل دورها في توعية طلبة الجامعة بالأمن السيبراني.
١٤. ضرورة إدراج مقرر الأمن السيبراني ضمن الخطط التدريسية لبرامج علم المعلومات.
١٥. تشجيع مجالات البحث العلمي والابتكار في مجال الأمن السيبراني.
١٦. تشجيع المؤسسات الغير الحكومية العاملة في هذا المجال وتشجيع الاستثمار في تخصصات الأمن السيبراني.
١٧. تطوير المهارات وإعداد الكادر البشري لمواجهة أخطار الفضاء السيبراني وتوفير الأمن الكافي له لسد الفجوة بين القدرات الحالية والمستقبلية.
١٨. تطوير سبل تفعيل وتحسين أداء الوسائل الدفاعية الموجودة لحماية الفضاء السيبراني حالياً والتحقق من أدائها بشكل متقن .
١٩. الاعتماد على سياسات مرنة يمكن تغييرها وتطويرها لتحقيق الأمن وحماية الأجهزة والتقنيات والشبكات في الجامعات.

المراجع:

المراجع العربية:

- ال مسعود، علي يحيى (٢٠٢٠). الأمن السيبراني والياته في الحد من السلوكات الانحرافية للاحداث في المملكة العربية السعودية: دراسة نظرية تحليلية.
- أبو حسين، حنين جميل، و الحنيطي، مأمون أحمد راشد (٢٠٢١). الإطار القانوني لخدمات الأمن السيبراني: دراسة مقارنة (رسالة ماجستير غير منشورة). جامعة الشرق الأوسط، عمان. مسترجع من <http://search.mandumah.com.sdl.idm.oclc.org/Record/1208936>
- أبو داسر، عبدالله سعيد (٢٠٢٠). حماية الملكية الفكرية. روح القوانين.
- أبو زيد، عاطف. (٢٠١٩). الأمن السيبراني في الوطن العربي. المركز العربي للبحوث والدراسات. متاح على الرابط التالي: <http://www.acrseg.org/41356>
- أبو منصور، حسين يوسف. (٢٠١٧). توظيف تقنية التصنيف الربطي للكشف عن موقع التصيد الإلكتروني . المجلة العربية الدولية للمعلوماتية ، مج ٥ ، ع ٩.
- أحمد، عبدالخالق محمد. (٢٠١٤). الهندسة الاجتماعية. المال والاقتصاد: بنك فيصل الاسلامي السوداني، ع ٧٥ - ٢٣ . مسترجع من <http://search.mandumah.com.sdl.idm.oclc.org/Record/630305>
- البابلي. عمار ياسر محمد زهير (٢٠٢١). التحديات الأمنية المعاصرة للهجمات السيبراني.
- بيومي، عبدالفتاح (٢٠٠٧). مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مصر: دار الكتب القانونية.
- جبور، منى الأشقر (٢٠١٦). السيبرانية هاجس العصر. لبنان:جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية.
- الجمل، حازم (٢٠٢٠). الحماية الجنائية للأمن السيبراني في ضوء رؤية ٢٠٣٠. مجلة البحث الأمنية.
- الجندي، علياء بنت عبدالله إبراهيم (٢٠١٩). دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة.
- الخضري، جيهان سعد محمد، سلامي، هدى جبريل علي، و كليبي، نعمة ناصر مدش. (٢٠٢٠). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية: دراسة مقارنة. مجلة تطوير الأداء الجامعي: جامعة المنصورة - مركز

- رباعية ، عبداللطيف محمود (٢٠١٦) . الجرائم الإلكترونية ، التجريم والملاحقة والإثبات ، مقدم إلى المؤتمر الأول للجرائم الإلكترونية في فلسطين ، جامعة النجاح الوطنية .
- الزهراني ، احمد (٢٠١٤) ، الهندسة الاجتماعية . الأكاديميون السعوديون . تم الاسترجاع من :
<https://www.saudiacademics.com/article/computer-tech/item/1120>
- سمحان، منى عبدالله صالح (٢٠٢٠). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية بالمنصورة: جامعة المنصورة - كلية التربية، ع ١١١، ج ٢ ، ٢٩ - ٢ . مسترجع
- السواط. حمد بن حمود بن حميد (٢٠٢٠). العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية.
- الشايع، خالد سعد (٢٠١٨) الأمن السيبراني مفهومه وخصائصه وسياساتها الدار العالمية للنشر،الرياض.
- الصانع، نوره عمر أحمد، عسaran، عواطف سعد الدين، السواط، حمد بن حمود بن حميد، أبو عيشة، زاهدة جميل نمر، و منصور، إيناس محمد سليمان علي. (٢٠٢٠). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترن特 وتعزيز القيم والهوية الوطنية لديهم. مجلة كلية التربية: جامعة أسيوط - كلية التربية، مج ٣٦ ، ع ٤١ - ٩٠ . مسترجع من <http://search.mandumah.com.sdl.idm.oclc.org/Record/1085483>
- صائغ، وفاء بنت حسن عبدالوهاب (٢٠١٨) . وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية.
- الصحفي، روان عطية الله (٢٠٢٠). الجرائم السيبرانية.المجلة الإلكترونية متعددة التخصصات. ع ٢٤ ، ١-٥٣ ، مسترجع من : <https://www.eimj.org/upload/images/photo/pdf/>
- الصحفي، مصباح أحمد حامد، و عسکول، سناء بنت صالح. (٢٠١٩) . مستوى الوعي بالأمن السيبراني لدى معلمات الحاسوب الآلي للمرحلة الثانوية بمدينة جدة. مجلة البحث العلمي في التربية: جامعة عين شمس - كلية البنات للآداب والعلوم والتربية، ع ٢٠ ، ج ١٠ ، ٤٩٣ - ٥٣٤ . مسترجع من
<http://search.mandumah.com.sdl.idm.oclc.org/Record/1029923>

- الطيار، حسين بن سليمان بن راشد (٢٠٢٠). الأُمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية. مجلة جامعة الطائف للعلوم الإنسانية: جامعة الطائف، مجل ٦ ، ع ٢١ ، ٢٥٥ - ٢٩٨ . مسترجع من <http://search.mandumah.com.sdl.idm.oclc.org/Record/1061557>
- العتيبي ، زياد بن محمد عادي (٢٠٢١) ، جرائم السيبرانية المرتكبة عبر الوسائل الرقمية وبيان مفهومها من حيث أشكالها، خصائصها، أركانها والدافع من إرتكابها . المجلة الأكاديمية العالمية للدراسات القانونية ، ٣ (١) .
<http://iajour.com/index.php/Ir/article/download/168/106>
- العريشي، جبريل حسن، و الدوسي، سلمى بنت عبدالرحمن بن محمد. (٢٠١٨). دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع. مجلة مكتبة الملك فهد الوطنية: مكتبة الملك فهد الوطنية، مجل ٢٤ ، ع ٢٤ ، ٣٠٢ - ٣٧٣ . مسترجع من <http://search.mandumah.com/Record/947870>
- الفلاوي ، أحمد عبيس نعمة (٢٠١٨) . الهجمات السيبرانية ، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر (ط) . بيروت منشورات زين الحقوقية .
- القحطاني، نورة بنت ناصر. (٢٠١٩) . مدى توفر الوعي بالأُمن السيبراني لدى طلاب وطالبات الجامعات السعودية.
- كمال، بن شايب ، و عبد الرؤوف بن قيدة . (٢٠١٨) أخطار الهندسة الاجتماعية على المجتمع الإلكتروني . المركز الجامعي بوالصوف – ميلة الملتقى الوطني الثالث حول المستهلك والإقتصاد الرقمي : ضرورة الإنقال وتحديات الحماية ٢٣ و ٢٤ فبراير. مسترجع من <http://dspace.centre-univ-mila.dz/jspui/bitstream/123456789/129/1/81.pdf>
- الكندي، سالم سعيد علي، و البلوشي، حليمه سليمان. (٢٠٢٠) . الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان: دراسة حالة لطلبة الكلية التقنية بالمصنعة. مجلة الآداب والعلوم الاجتماعية: جامعة السلطان قابوس - كلية الآداب والعلوم الاجتماعية، مجل ١١ ، ع ٧١ ، ٨٤ - ٨٤ . مسترجع من <http://search.mandumah.com.sdl.idm.oclc.org/Record/1164982>
- محمد، هبه هاشم. (٢٠٢٠) . برنامج مقترن على جغرافية الحروب السيبرانية لتنمية الوعي بمخاطرها وتعزيز قيم المواطنة الرقمية.
- مركز الأمن الإلكتروني [NCSC_SA] (٢٠١٧، نوفمبر ، ٢٠) . رصد مركز الأمان الإلكتروني هجوماً إلكترونياً جديداً متقدماً APT يستهدف المملكة العربية السعودية تعتمد انشطة الهجوم التي تم ملاحظتها على استخدام [نص] [تغريدة] تويتر.
- مسلم، نيراس إبراهيم (٢٠٢١) . الجرائم السيبرانية وأثرها على الأمان السيبراني ، مجلة القادسية ، ١٢ ، (١) .
<https://www.iasj.net/iasj/download/a03a424a67ab7588>

- المطيري ،مشاعل شبيب مطيران الظفيري. (٢٠٢١). و اقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية.

- المنتشري، فاطمة يوسف، و حريري، رندة (٢٠٢٠). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للتربية النوعية: المؤسسة العربية للتربية والعلوم والآداب*، ع ٩٥ ، ١٤٠ - ١٤٠ . مسترجع من

<http://search.mandumah.com.sdl.idm.oclc.org/Record/1056594>

- المنتشري،حليمة يوسف (٢٠١٩). *الأمن السيبراني والمواطنة الرقمية*.معهد الإدارة العامة. متاح على الرابط التالي:
[file:///C:/Users/acer/OneDrive/%D8%B3%D8%B7%D8%AD%20%D8%A7%D9%84%D9%85%D9%83%D8%AA%D8%A8/0302-041-157-007%20\(1\).pdf](file:///C:/Users/acer/OneDrive/%D8%B3%D8%B7%D8%AD%20%D8%A7%D9%84%D9%85%D9%83%D8%AA%D8%A8/0302-041-157-007%20(1).pdf)

- نعيم ، سعيد علي (٢٠١٣) . آليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري ، مذكرة ماستر ،كلية الحقوق ، جامعة العقيد الحاج الحضر .

- الهندي، رشا عبدالقادر محمد (٢٠٢١). تصور مقترن لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني.

- هيئة الخبراء بمجلس الوزراء:
<https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1>

- الهيئة الوطنية للأمن السيبراني [@NCA_KSA] (@NCA_KSA [@NCA_KSA]) (٢٠١٨ ، ٣٠ يوليو). الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من [نص] [تعريدة].تويتر. استرجع [https://twitter.com/nca_ksa/status/1023917241870557184?s=12://:https://](https://twitter.com/nca_ksa/status/1023917241870557184?s=12://:https://twitter.com/nca_ksa/status/1023917241870557184?s=12://:https://) في نوفمبر ٥ ، ٢٠٢٢ ، من:

- وريدة،خليلة (٢٠٢١).إشكالية المواطننة في ظل قيم التكنولوجيا الحديثة بين حرية المواطن والأمن السيبراني. *حوليات جامعة الجزائر*، ع ٣٥ ، ٨٠٦. (٢) (٣٥).
<https://www.asjp.cerist.dz/en/downArticle/18/35/2/154429>

المراجع الأجنبية:

- Al-Sharnoubi, Muhammad, Alaka, Furqan, Chisasoun, Sonya (2015). Why Phishing Still Works: User Anti-Phishing Strategies. College of Computer Science, Carleton University, Ottawa, Canada.
- Bisson D (2015) .Social engineering attacks to watch out for. The state of security.
<http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/>. Accessed 23 March 2015.
- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10).
- El-Aroud, Ahmed Lina Zou, (2017). Phishing Environments, Techniques and Countermeasures: Yarmouk University, Jordan, University of Maryland, Timor County.
- Goutan,R. K (2015). importance of cyber security. Retrieved from:
<https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.9225&rep=rep1&type=pdf>
- Jain A, Goswami H, Singh M, Sankhla R. Kumar (2016). Social Engineering: Hacking a Human Being through Technology.
- Kaspersky.(2010).Types of cyber threats.Retrieved from:
<https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>
- Mouton, F.; Leenen, L.; Venter, H (2016). Social engineering attack examples, templates and scenarios. Comput.Secur.59, 186–209. [CrossRef]
- Rusch, Jonathan J. “The ‘Social Engineering’ of Internet Fraud.” United States Department of Justice (no date).
http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm.
- Weimann,gabriel(2004). Cyberterrorism. Retrieved from:
<https://www.usip.org/sites/default/files/sr119.pdf>

الملاحق:

ملحق رقم (١) الاستبانة في صورتها النهائية:

استبيان بالأمن السيبراني والإسلام بأساسيات الأمن السيبراني وتنمية طالبات كلية الآداب والعلوم الإنسانية بخطورة الهجمات عند استخدام شبكة الانترنت وموقع التواصل الاجتماعي ومعرفة العقوبات المترتبة عند حدوث الجرائم وأنواع المجرمين المرتكبين لها.

البيانات الشخصية للطالبة:

اسم الطالبة الثلاثي:			
<input type="radio"/> من ٢٠ - ٣٠	<input type="radio"/> اقل من ٢٠	<input type="radio"/> من ٢١ - ٣٠	العمر:
<input type="radio"/> اللغات والترجمة	<input type="radio"/> اللغة العربية	<input type="radio"/> الاتصال والاعلام	<input type="radio"/> الدراسات القرآنية
<input type="radio"/> الدراسات الاسلامية	<input type="radio"/> المعلومات ومصادر التعلم	<input type="radio"/> العلوم الاجتماعية	التخصص :
<input type="radio"/> الثامن	<input type="radio"/> السادس	<input type="radio"/> الرابع	<input type="radio"/> الثاني
			المستوى الجامعي وفقا لخطتها
			الدراسية:

الوعي بمفهوم الأمن السيبراني:

١-لدي معرفة سابقة بالأمن السيبراني؟

غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
٢- مفهوم الأمن السيبراني :				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
				هو أمن المعلومات على أجهزة وشبكات الحاسب الآلي والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو اختلاف قد يحدث .
				هو استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به ، ومنع سوء الاستغلال واستعادة المعاملات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها .
				هو حماية المستخدمين من أي مخاطر تواجههم.
٣- أحتاج إلى دورات تدريبية في الأمن السيبراني؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق

٤- أستطيع التفريق بين الأمان السيبراني وأمن المعلومات؟

غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
لدي معرفة بمفهوم الهندسة الاجتماعية؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
لدي معرفة بمفهوم التصييد الالكتروني؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
٥- لدى معرفة بكيفية التصرف في حال التعرض للاختراق؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
٦- لدى معرفة بمخاطر فتح روابط ومرفقات البريد الالكتروني؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
٧- لدى معرفة بالإجراءات الازمة لحماية حاسبي الشخصي من الإختراق؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
٨- لدى معرفة تامة بمخاطر تنزيل البرامج والملفات من الإنترن特؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
٩- لدى معرفة بالجرائم السيبرانية؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
١٠- اهتم بتغيير كلمات المرور الخاصة بدخول خدمات الإنترن特 كل فترة؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
١١- تحد ثقافة الأمان السيبراني من التجسس والتخريب الإلكتروني على مستوى المجتمع؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
١٢- أحرص على الإبلاغ عن الرسائل المشكوك فيها للجهات المختصة؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق
١٣- أحرص على تحميل التحديثات والبرامج الآمنة؟				
غير موافق بشدة	غير موافق	محايد	موافق بشدة	موافق

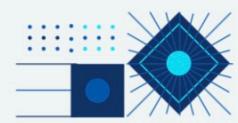
١- اتجنب وضع البيانات والصور الشخصية على موقع التواصل الاجتماعي الا لضرورة؟			
موافق	ممايز	غير موافق	موافق بشدة
٢- احتفظ بأرقامي السرية في المتصفح؟			
موافق	ممايز	غير موافق	موافق بشدة
٣- استخدم نفس كلمة المرور لجميع مواقع التواصل الاجتماعي والبريد الإلكتروني؟			
موافق	ممايز	غير موافق	موافق بشدة
٤- أقوم بقراءة شروط وتعليمات المستخدم لبرنامج مجاني قبل الضغط على أوافق؟			
موافق	ممايز	غير موافق	موافق بشدة
٥- افتح رسالة الكترونية غير معروفة لدى؟			
موافق	ممايز	غير موافق	موافق بشدة
٦- أقوم بعمل نسخة احتياطية للملفات المهمة؟			
موافق	ممايز	غير موافق	موافق بشدة
٧- أعرف بمن اتصل في حال حدوث اختراق؟			
موافق	ممايز	غير موافق	موافق بشدة
٨- أقوم بتحديث نظام التشغيل بصورة دورية؟			
موافق	ممايز	غير موافق	موافق بشدة
٩- اهتم بتغيير كلمة المرور بشكل منتظم؟			
موافق	ممايز	غير موافق	موافق بشدة
١٠- اختار كلمة مرور مكونة من حروف وأرقام ورموز؟			
موافق	ممايز	غير موافق	موافق بشدة
١١- اترك الحساب أو النظام مفتوح بدون تسجيل خروج عند المغادرة؟			
موافق	ممايز	غير موافق	موافق بشدة
١٢- اهتم بتطوير مهاراتي وزيادة معارفي بالآليات المناسبة لتحقيق الأمان السيبراني وطرق الوقاية من المشاكل السيبرانية؟			
موافق	ممايز	غير موافق	موافق بشدة
١٣- أقوم بالتخلص من رسائل البريد الإلكتروني مجهولة المصدر دون فتحها؟			
موافق	ممايز	غير موافق	موافق بشدة
١٤- احذر كثيرا عند الاتصال بالشبكات العامة؟			
موافق	ممايز	غير موافق	موافق بشدة
١٥- افحص جهازي الآلي بصورة مستمرة؟			
موافق	ممايز	غير موافق	موافق بشدة
١٦- ابتعد عن مشاركة معلوماتي الشخصية مع الغرباء على الإنترن特؟			
موافق	ممايز	غير موافق	موافق بشدة
١٧- استخدم برنامج الحماية من الفيروسات بصورة مستمرة؟			
موافق	ممايز	غير موافق	موافق بشدة



دورة الامن السيبراني

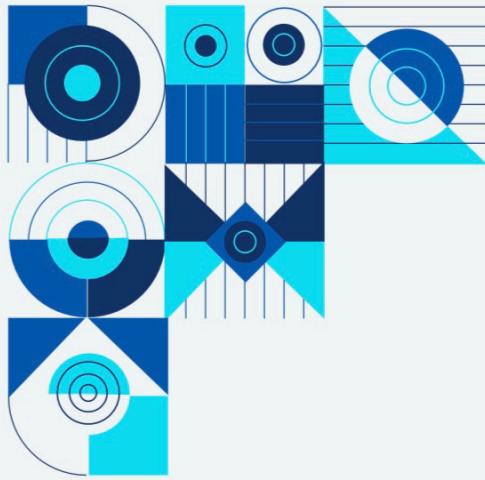


SLIDESMANIA.CC



SLIDESMANIA.CC





محاور الدورة

- الهدف من الدورة.
- تعريف الامن السيبراني.
- الفرق بين الامن السيبراني وامن المعلومات.
- اهداف وأهمية الامن السيبراني.
- عناصر الامن السيبراني.
- آثار ضعف الامن السيبراني.
- الهجمات الالكترونية وأنواع البرمجيات الخبيثة.
- الجرائم السيبرانية، وأنواعها، وأصناف المجرمين.
- التصييد الالكتروني وأشكاله.
- الهندسة الاجتماعية ومراحل الهجوم وطرق الحماية والوقاية من الهجمات السيبرانية.
- قانون الجرائم في المملكة.
- جهود المملكة في الامن السيبراني.
- الامن السيبراني في الجامعات السعودية



الهدف من الدورة:

الالمام بأساسيات الامن السيبراني وتنمية طالبات كلية الأداب
والعلوم الإنسانية بخطة الهجمات عند استخدام شبكة الانترنت
ومواقع التواصل الاجتماعي ومعرفة العقوبات المترتبة عند
حدوث الجرائم وأنواع المجرمين المرتكبين لها





مفهوم الامن السيبراني :

حماية الشبكات وأنظمة تقنية المعلومات والبرمجيات والأجهزة وما تقدمه من خدمات وما تحويه من البيانات من أي اختراق او تخريب او تعديل او استغلال او دخول غير مشروع ويشمل امن المعلومات والامن الالكتروني



الفرق بين الامن السيبراني وأمن المعلومات

الأمن السيبراني:
يتعلق بتتأمين
الأشياء المعرضة
للخطر من خلال
التكنولوجيا
المعلومات
والاتصالات.

يهتمون
 بالمعلومات
 الرقمية

أمن المعلومات: هو
كل شيء عن حماية
المعلومات التي
تركز بشكل عام
على سرية وسلامة
وتوافر المعلومات.

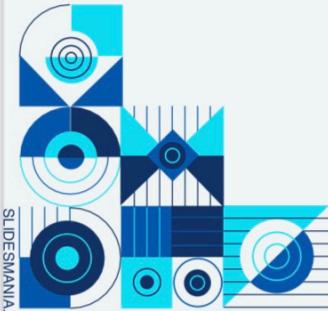


“

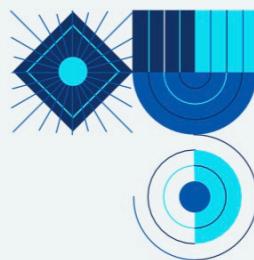
اهداف الامن السيبراني :



- ❖ محاربة البرامج الخبيثة.
- ❖ اتخاذ الإجراءات والتدابير الازمة من اجل توفير الحماية للأفراد من المخاطر المحتمل حدوثها عند استخدام الانترنت.
- ❖ مواجهة الهجمات التي تستهدف المؤسسات والجهات الحكومية.
- ❖ سد الثغرات في أنظمة المعلومات.
- ❖ وضع حد للجرائم الالكترونية.

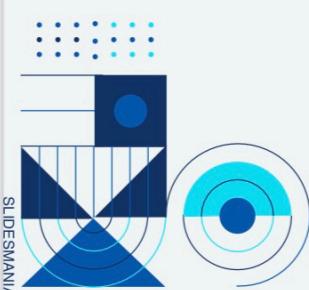


SLIDESMANIA.CC



أهمية الامن السيبراني :

- ❖ حفظ سلامة وسرية المعلومات والبيانات
- ❖ توفير بيئة آمنة للكترونيا
- ❖ تقديم الحماية الكاملة للأجهزة والشبكات
- ❖ اكتشاف الثغرات والعمل على إصلاحها
- ❖ وضع قوانين وتشريعات لحماية الجميع
- ❖ حماية المجتمع من الهجمات السيبرانية



SLIDESMANIA.CC





عناصر الامن السيبراني:

- ❖ السرية والأمان : التأكد من أن المعلومات لا يصل لها الا الأشخاص المخولين
- ❖ استمرارية توفر المعلومات أو الخدمة: التأكد من استمرارية عمل النظام وعدم منع المستفيد من الدخول إلى النظام
- ❖ سلامة المحتوى : التأكد من أن المحتوى صحيح ولم يتعرض للحذف والتغيير
- ❖ التقنية : تعتمد في حمايتها على البرامج المضادة للفيروسات والجدران الناريه
- ❖ الأشخاص : يجب على مستخدمين النظام وضع كلمات مرور قوية وصعب تخمينها وتجنب فتح الروابط الخارجية
- ❖ الأنشطة والعمليات : توفير التقنيات والأشخاص المناسبين من أجل تطبيق



آثار ضعف الامن السيبراني :

- ❖ اختراق وتخریب البنية التحتية للاتصالات وتكنولوجيا المعلومات: الهدف من الهجمات السيبرانية هو الإعاقة للخدمات الحيوية ونشر البرامج الخبيثة كالفيروسات والعمل على تعطيل البنية التحتية ونظم التحكم مما يؤثر تأثيراً كبيراً على البنية التحتية لتلك المنشآت وعلى خدماتها وأعمالها.
- ❖ الإرهاب وال الحرب السيبرانية: تعتمد الجرائم السيبرانية على تقنيات متقدمة وأجهزة تنصت وبرمجيات لفك الشفرات واحتراق أنظمة أمن الشبكات وتسعي إلى هجمات متنوعة ولأغراض الحروب السيبرانية وتستخدم الهجمات في العمليات الإرهابية وتعطيل البنية التحتية
- ❖ سرقة الهوية الرقمية والبيانات الخاصة: تعتبر من أخطر الجرائم التي تهدد المستخدمين لشبكة الإنترنت وقد تتعرض البيانات للسرقة والانتهال
- ❖ الحرمان من الخدمة: يقصد به إيقاف القدرة على تقديم الخدمات المعتادة وذلك يتم من خلال إغراق الجهاز المقدم للخدمة بمجموعة كبيرة من الأوامر التي تؤدي إلى توقفه عن العمل



SLIDESMANIA.C



تعريف الجريمة السيبرانية :

هي الاستخدام غير المشروع للتكنولوجيا بقصد التدمير والتعدي على ممتلكات الغير من خلال الأجهزة وما تحتويه من معلومات

أنواع الجرائم السيبرانية :

- ❖ جريمة الدخول أو الولوج الغير قانوني
- ❖ جريمة الاعتداء على سلامة البيانات
- ❖ جريمة الاعتراضات غير القانونية
- ❖ جريمة الاعتداء على سلامة النظام
- ❖ جريمة اساءة استخدام الحاسوب
- ❖ جريمة الاعتداء على الأموال
- ❖ جريمة الاستغلال الجنسي

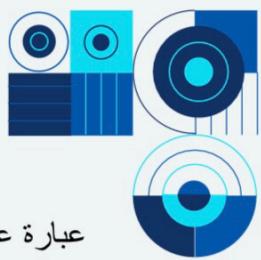


SLIDESMANIA.C



أصناف المجرم السيبراني:

- ❖ القرصنة ومنهم
- الكرacker : هدفهم السرقة أو العبث
- الهاكر : هدفهم إثبات الذات أو الفضول
- ❖ المهووسون : يكونون في حالة جنون و هدفهم تحطيم جميع الأنظمة
- ❖ الحكومات الأجنبية : يستخدمون أجهزة الحاسوب للتجسس الجريمة المنظمة : مثل عصابات المافيا
- ❖ المتطرفون : يستخدمون الشبكة لنشر أفكارهم وبثها بين الناس



تعريف التصيد الإلكتروني:

عبارة عن أسلوب لخداع المستخدم بالنقر على روابط أو مرفقات ضارة ، بهدف اختراق أجهزة الضحايا للتجسس عليها او إلحاق الضرر بها أو سرقة المعلومات وغيرها من التهديدات الإلكترونية .

أشكال التصيد :

- ❖ رسائل التصيد عبر البريد الإلكتروني ورسائل تصيد البريد الإلكتروني مع تحديد الهدف.
- ❖ التصيد الصوتي.
- ❖ تزوير الواقع الإلكترونية .
- ❖ التصيد عن طريق الإيقاع بالضحية.
- ❖ التصيد عن طريق تطبيقات الهاتف الذكي .



الهندسة الاجتماعية:

الهندسة الاجتماعية: هي عملية يتم من خلالها خداع الناس وحصول المتسلل على معلومات خاصة وسرية تفيد المتسلل بطريقة ما.

مراحل هجوم الهندسة الاجتماعية:

- ❖ جمع المعلومات حول الهدف.
- ❖ تنمية وتطوير العلاقة مع الهدف.
- ❖ التنفيذ والوصول إلى الهدف.

طرق الحماية من الهجمات السيبرانية والوقاية من الهندسة الاجتماعية :

- ❖ عمل نسخ احتياطية بشكل مستمر للبيانات.
- ❖ استخدام محرك بحث يركز على الخصوصية وحماية كلمة المرور.
- ❖ الحذر من التواذف المبنية عند تصفح الويب.
- ❖ عدم نشر أي معلومات خاصة مع الآخرين على شبكة الإنترن特 أو موقع التواصل والمحافظة على الخصوصية.
- ❖ يجب أن تتحقق من أي رسالة تصلك على البريد الإلكتروني أو مكالمة هاتفية تتطلب معلومات خاصة وحساسة.
- ❖ الحذر من فتح أي روابط أو ملفات مرسلة في البريد الإلكتروني لأنها تكون غالباً موقع تصيد إلكتروني.
- ❖ تنزيل التطبيقات من مصدرها الصحيح.
- ❖ قيام المؤسسات بتدريب الموظفين والعاملين وتوعيتهم بالأساليب الجديدة للهندسة الاجتماعية.
- ❖ استخدام كلمات مرور مختلفة لكل موقع ويتم تغييره شكل دوري.
- ❖ القيام بتحديث البرامج الموجودة على الأجهزة بشكل دوري.
- ❖ الحرص عندما يتم استخدام الحواسيب العامة مثل الموجودة في مقهى أو مطارات... الخ.
- ❖ الحرص على اتلاف المستندات والأوراق المهمة بواسطة أجهزة مخصصة.

برمجيات تساعدك على مكافحة الفيروسات في حاسبك:

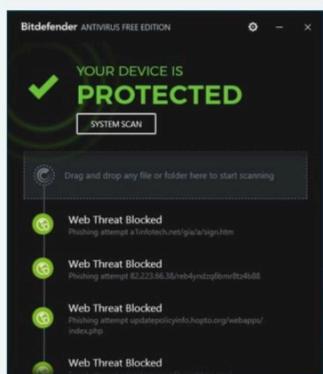
Kaspersky Free



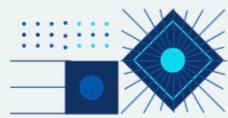
Avast Free Antivirus



Bitdefender Antivirus Free Edition



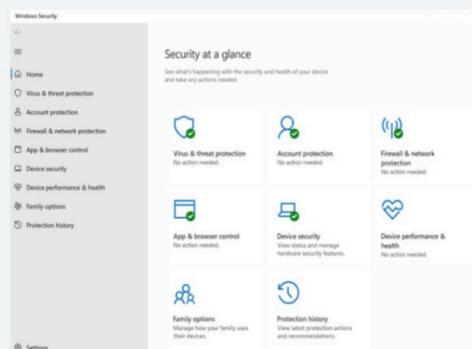
برمجيات تساعدك على مكافحة الفيروسات في حاسبك:



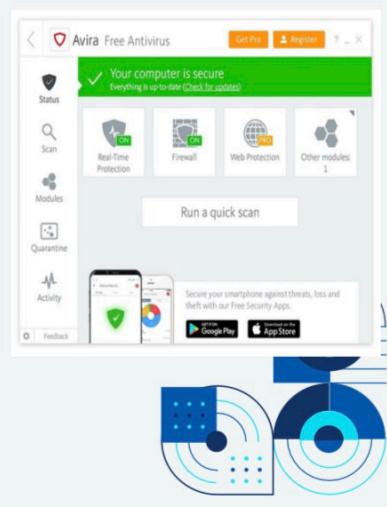
ZoneAlarm Free Antivirus



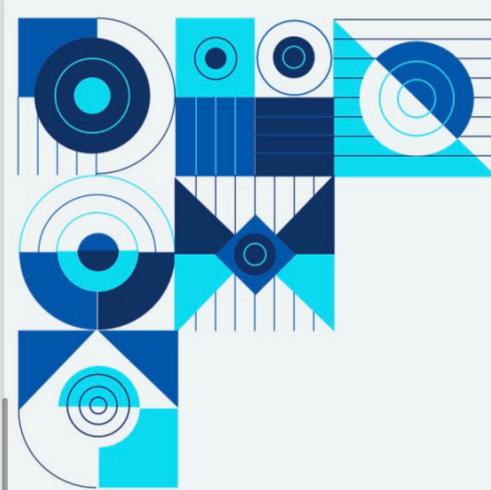
Microsoft Defender



Avira Free Antivirus



SLIDESMANIA.C



خدمة الإبلاغ عن رسائل الاحتيال

قد تصلك رسالة احتيال (SMS) تدعى أنها من أحد البنوك،
أو تبلغك بالفوز بجائزة مالية.. ماذا تفعل؟



رسالة احتيال!

عزيزي العميل
تم حذف بطاقة الترخيص التي الخاصة
بكم، لذلك تم إيقاف حسابكم في
البنك. للتأكد من صحة المعلومات
ماهيل هذه الرسالة على الفور
05...23-05...39

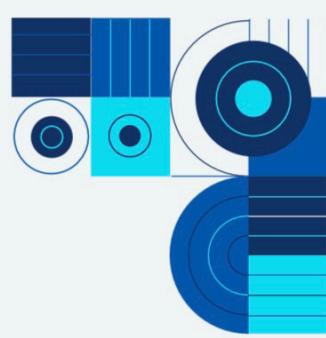
سارع بالإبلاغ عنها
 بإعادة إرسال الرسالة
 النصية إلى الرقم

330330

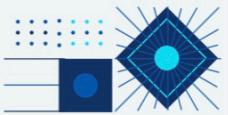
* الخدمة مجانية لجميع عملاء
 مقدمي خدمات الاتصالات المتنقلة

زين **موبايلي** **STC**

مدينة إتصالات وتقنية المعلومات
Communication and Information Technology Commission

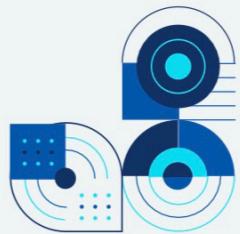


SLIDESMANIA.C



رقم الجرائم الإلكترونية في السعودية:
يمكنكم الإبلاغ في حالة تعرضكم لأحد الجرائم الإلكترونية من خلال أحد الوسائل التالية:

- ١-الاتصال على رقم الأمن العام "الجرائم الإلكترونية" ...
00966114419688
- ٢-الاتصال على الرقم الموحد ... 1909 .
- ٣-الاتصال على الرقم الدولي للإبلاغ عن الجرائم الإلكترونية ... +966114908666
- ٤-التواصل عن طريق تطبيق كلنا أمن لخدمات مواجهة الجرائم الإلكترونية .
- ٥-التواصل إلكترونياً من خلال الموقع الإلكتروني لوزارة الداخلية السعودية "خدمة أبشر"



قانون الجرائم الرقمية في المملكة العربية السعودية:

- ١-يعاقب بالسجن مدة لا تزيد عن سنه وغرامة مالية لا تزيد على خمسين ألف ريال عند ارتكاب ما يلي:
 - ❖ التنصت على ما هو مرسى عن طريق الشبكة العنكبوتية
 - ❖ الدخول غير المشروع لغرض التهديد والابتزاز او التلف والتعديل
 - ❖ التشهير بالأخرين والحقن بالضرر بهم
- ٢-يعاقب بالسجن مدة لا تزيد عن ثلاثة سنوات وغرامة مالية لا تزيد عن مليوني ريال :
 - ❖ الوصول دون مسوغ نظامي صحيح الى بيانات بنكية او ائتمانية
- ٣-يعاقب بالسجن مدة لا تزيد عن اربع سنوات وغرامة مالية لا تزيد على ثلاثة ملايين ريال:
 - ❖ الدخول غير المشروع لاغاء البيانات او حذفها
 - ❖ إعاقة الوصول الى الخدمات التقنية





جهود المملكة في الامن السيبراني



إنشاء المركز الوطني الإرشادي للأمن السيبراني وذلك بهدف تعزيز مستوىوعي بالسيبراني والحد من المخاطر والتهديدات السيبراني ووجهة .



إنشاء الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز في عام 2017 وذلك بهدف تنمية قدرات وامكانيات وطنية احترافية رائدة في مجال الامن .



تم انشاء الهيئة الوطنية للأمن السيبراني من منطلق أهمية البيانات والأنظمة التقنية بالإضافة الى البنية التحتية والتي لها صلة وثيقة بالشؤون الوطنية والتي لابد من توفير الحماية اللازمة لها من مخاطر وتهديدات الفضاء السيبراني



جهود المملكة في الامن السيبراني:

- ❖ إطلاق العديد من برامج التعليم والتدريب للأشخاص والمؤسسات في مجال الأمن السيبراني.
- ❖ اتجاه العديد من الجهات الحكومية إلى إبرام شراكات تعاون في مجال الأمن السيبراني.
- ❖ اطلاق العديد من البرامج وأاليات العمل لمعالجة النقص في مهارات تكنولوجيا المعلومات والأمن السيبراني.
- ❖ إعطاء ما يقارب 231 منحة دراسية للطلبة الذين يقررون دراسة تخصص الأمن السيبراني.
- ❖ تدريب ما يقارب 751 موظفًا من 113 شركة، و 288 طالبًا على بروتوكولات الأمن السيبراني.





الامن السيبراني في الجامعات السعودية:

كما انه يوجد مجموعة من الادوار التي تسهم في تنمية المهارات المتعلقة بالامن السيبراني في المحيط الجامعي وهي كالتالي:

1. القيام بتوعية الطالبات بكيفية حماية البيانات الشخصية من المخاطر التي قد تعرّضها

2. القيام بتوعية وتنقيف الطالبات بمختلف المخاطر المحتملة وذلك عند قيام الطالبات في عمليات البحث ومشاركة البيانات في شبكة الانترنت

3. استخدام التقنيات المختلفة والمتقدمة التي تساهم في حماية البيانات والملفات وتأمينها من شتى المخاطر السيبرانية

4. القيام بزيارة التوعية فيما يتعلق بمخاطر الانترنت المختلفة من امثالها التنمـر الالكتروني وموقع الانترنت التي تتضمن المحتوى السلبي

5. الاسهام في نشر وبث مختلف سياسيات وأنظمة الامن السيبراني والتربية الى كل ما هو حديث وجيد وذلك بشكل دوري

