فعالية برنامج تدريبي مقترح لتنمية الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الإنسانية: دراسة تجريبية* "الجزء الأول"

إعداد

مرام خالد يحيى الشريف
طالبة ماجستير في جامعة الملك عبد العزيز
maram22_11@hotmail.com

ليان سعد عوض اللّه الحربي
بكالوريوس علم المعلومات- جامعة طيبة
layanalharbi08@gmail.com

العنود عبد العزيز مصلح الحربي
بكالوريوس علم المعلومات- جامعة طيبة
nooodh741@gmail.com 3

امل عبيد اللّه عبد العزيز السليماني
بكالوريوس علم المعلومات- جامعة طيبة
amool58993@gmail.com

المستخلص:

تتناول هذه الدراسة التعرف على فعالية برنامج تدريبي مقترح لتنمية الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الإنسانية بجامعة طيبة ، ويهدف البحث الحالي إلى بناء برنامج تدريبي لقياس مدى وعي طالبات كلية الآداب والعلوم الإنسانية بجامعة طيبة في الأمن السيبراني، وعلى معرفة درجة وعيهم بالأمن السيبراني، وتحليل وقياس مدى فعالية البرنامج التدريبي المقترح من حيث جوانب القوة وتدعيمها وجوانب الضعف والعمل على تقديم

* الجزء الثاني من المقال ينشر في العدد القادم (المجلد الرابع، العدد الأول يناير 2024) بإذن الله. ويشتمل على الملاحق والمراجع للجزئين معاً.

تاريخ استلام البحث: 2023/5/23 تاريخ إجازة البحث: 2023/8/18

الاقتراحات العلاجية لمعالجتها، وتكمن أهمية الدراسة في أهمية الأمن السيبراني نفسه، وذلك في حماية البيانات والأجهزة وسلامتها من مخاطر الانتهاكات 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 الاعتماد على المنهج التجريبي مستخدماً الاستبانة كأداة لجمع البيانات ، حيث تم إعداد استبانة إلكترونية مكونة من 34 سؤال تضم محورين هما : الوعي بمفهوم الأمن السيبراني والوقاية من مخاطر الاختراق السيبرانية ، وتم تطبيقها على عينة عشوائية بحيث بلغ عدد العينة 192 استمارة قبيلة و189 استمارة 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، وأيضا يستدل أن هناك ضرورة من تعاون جميع جهات وقطاعات الدولة لتشكيل منظومة تتظافر 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 38% وبعد تقديم البرنامج التدريبي بلغت نسبتهم 84.8% كما توصلت الدراسة إلى احتياجهم للدورات التدريبية في مجال الأمن السيبراني حيث بلغت نسبتهم قبل البرنامج 80% وبعد تقديم البرنامج بلغت نسبتهم 84% ، ومن أهم ما توصي به الدراسة ضرورة تقديم برامج تدريبية 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.

المقدمة:

يشهد العالم تطور متسارع في تكنولوجيا المعلومات والاتصالات حيث أصبح الانترنت حلقة الوصل ما بين العالم المترامي الأطراف الذي بات لا يعترف بحدود الزمان والمكان والذي يتبادل 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 ومنافع متعددة ومنها تبادل المعلومات والأفكار على مستوى الأفراد والمؤسسات ودول العالم بصفة عامة حيث أصبح المقياس الذي تقاس به تقدم الدول هو مدى التطور التقني والتكنولوجي ومدى تطبيقها وتبنيها للتقنية وكيفية توجيهها التوجيه الأمثل في سبيل تحقيق مصالحها ومختلف أهدافها، وفي مقابل كل ذلك باتت التقنية يصاحبها العديد من الأخطار والتهديدات السيبرانية التي تقابل مستخدمي الإنترنت ، حيث يسخر البعض جهوده وإمكانياته لاختراق شبكات المعلومات بالإضافة إلى ذلك انتهاك 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 وهيئاتها ،وكما حظي الأمن السيبراني باهتمام بارز لدى جميع الدول أصبحت سياساتها وأنظمتها لا تخلوا من قوانين تختص بمسائل الأمن السيبراني كل ذلك من منطلق تأمين البيانات والمحافظة عليها من مختلف الأخطار والتهديدات التي تواجهها ، وفي سبيل زيادة وعي 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 11/2/1439 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 والمنتسبين لها وتبني مبادرات هادفة لتعزيز الأمن السيبراني لمستخدمي الإنترنت عامة وللطلاب خاصة وضرورة إنشاء إدارات تختص بالأمن السيبراني بالإضافة إلى سعيها إلى إدراجه في مقرراتها وبرامجها التعليمية لتسهم

بذلك في خلق مجتمع واعي سيبرانياً قادراً على ممارسة الأمن السيبراني بشكل تطبيقي ولديه الجاهزية الفعلية لمواجهة مختلف المخاطر السيبرانية.

أهمية الموضوع ومبررات اختياره:

تكمن أهمية الموضوع من أهمية الأمن السيبراني وذلك في حماية البيانات والأجهزة وسلامتها من مخاطر الانتهاكات 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 الاهتمام المتزايد بالأمن السيبراني متزامناً مع رؤية المملكة2030 والتي بدروها تؤكد على دعم استخدام تقنيات المعلومات وتعزيز البيئة الرقمية في جميع مؤسسات المملكة العربية السعودية ومختلف قطاعتها ، 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 تساعد على زيادة الثقافة السيبراني لدى جميع منتسبيها، ولهذا توجهت الباحثات في الدراسة الحالية إلى إعداد برنامج تدريبي 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 والانتهاكات السيبرانية.

الأهداف:

1. تحديد مفهوم الامن السيبراني واهميته
2. رصد أهم الجرائم التي يتعامل معها الأمن السيبراني
3. تحديد درجة وعي طالبات كلية الآداب والعلوم الإنسانية بالأمن السيبراني
4. بناء برنامج تدريبي لقياس مدى وعي طالبات كلية الآداب والعلوم الإنسانية بالأمن السيبراني
5. تحليل قياس مدى فعالية برنامج تدريبي مقترح لتنمية وعي طالبات كلية الآداب والعلوم الإنسانية والوقوف على نقاط القوة وتدعيمها وتقديم المقترحات لمعالجة جوانب الضعف

التساؤلات:

1. ماهية الأمن السيبراني وما أهميته؟
2. ما أهم الجرائم التي يتعامل معها الأمن السيبراني؟
3. هل لدى طالبات كلية الآداب والعلوم الإنسانية وعي بالأمن السيبراني؟
4. كيف تم قياس وعي الطالبات في كلية الآداب والعلوم الإنسانية بالأمن السيبراني؟
5. ما مدى فعالية البرنامج التدريبي المقترح لتنمية وعي طالبات كلية الآداب والعلوم الإنسانية والوقوف على نقاط القوة وتدعيمها وتقديم المقترحات لمعالجة جوانب الضعف؟

حدود الدراسة:

- الحدود الموضوعية: تنمية الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الإنسانية .
- الحدود المكانية: جامعة طيبة كلية الآداب والعلوم الإنسانية لجميع أقسامها وهي كالأتي: الدراسات القرآنية، الدراسات الإسلامية، اللغة العربية، اللغات والترجمة، العلوم الاجتماعية، الاتصال والإعلام، المعلومات ومصادر التعلم.
- الحدود الزمانية: تم إجراء التجربة في عام 1443هـ - 2022م.
- الحدود النوعية: اقتصرت الدراسة على طالبات كلية الآداب والعلوم الإنسانية بجامعة طيبة.

منهج الدراسة وأدوات جمع المادة العلمية:

اتبعت الدراسة المنهج التجريبي لملائمته لطبيعتها وأهدافها من حيث رصد الظاهرة الآنية، وهو يعد أسلوب فعال لاكتساب المعرفة عن طريق الرصد ويتم استخدامه لدراسة الوقائع وتفسيرها، وقامت الباحثات باستخدام تجربة القياس القبلي والبعدي للظاهرة، حيث تم تصميم برنامج تدريبي لقياس وعي الطالبات بالأمن السيبراني والإسهام في رفع درجة الوعي والتحذير من المخاطر والانتهاكات 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 الاعتماد 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 الطبقي فتم التوزيع العشوائي على الأقسام العلمية بالكلية، بلغ حجم العينة القبلية ١٩٨ طالبة والبعدية ١٩٦ طالبة، وتم استبعاد ٤ استمارات من الاستبانة القبلية والبعدية لعدم جديتهم في الإجابة على الأسئلة، وكذلك تم استبعاد ثلاث استمارات من الاستبانة البعدية ، إثنين من تخصص الاتصال والإعلام وواحدة من تخصص الدراسات الإسلامية حيث أنهم أجاوبوا على الاستمارة البعدية ولم يجيبوا على الاستمارة القبلية . وبالتالي بلغ إجمالي حجم العينة بعد استبعاد الاستمارات الغير صالحة إلى ١٩٢ استمارة قبلية و ١٨٩ استمارة بعدية . والجدول التالي يوضح إجمالي حجم العينة موزعا على الأقسام العلمية.

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

القسم العلمي / العدد	عدد الاستجابات القبلية	عدد الاستجابات البعدية	الإجمالي
الدراسات القرآنية	24	24	48
الدراسات الإسلامية	34	34	68
اللغة العربية	25	22	47
اللغات والترجمة	24	24	48
العلوم الاجتماعية	30	30	60
الاتصال والاعلام	33	33	66
المعلومات ومصادر التعلم	22	22	44
الإجمالي	192	189	381

الدراسات السابقة:

أولاً: الدراسات العربية

1- آل مسعود، علي يحيى. (2020). الأمن السيبراني وآلياته في الحد من السلوكيات الإنحرافية للأحداث في المملكة العربية السعودية: دراسة نظرية تحليلية. مجلة كلية التربية، مج20، ع4، 411 - 434 .

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 وتكمن 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 المقترحات 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 2030 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 اكتساب الإحداث في المجتمع السعودي للسلوكيات الإنحرافية السيبرانية.

2- الخضري، جيهان سعد محمد، سلامي، هدى جبريل علي، وكليبي، نعمة ناصر مدبش. (2020). الأمن السيبر اني والذكاء الاصطناعي في الجامعات السعودية: دراسة مقارنة. مجلة تطوير الأداء الجامعي، مج12، ع1 ، 217 – 233

تهدف الدراسة إلى التعرف على مفهوم الأمن السيبراني لدى طلاب الجامعات السعودية وكذلك الوصول لمقترح يساعد على تفعيل الأمن السيبراني داخل الجامعات السعودية . وتكمن أهمية الدراسة في تأكيد دور الجامعات في نشر التوعية بالأمن السيبراني، بالإضافة إلى أنها تفيد 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 اتفاق وتجانس في الآراء بين أفراد عينة البحث بما يتعلق بتعدد 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 الاهتمام بتوعية المؤسسات الجامعية السعودية بتطبيق معايير أمن المعلومات حتى يتسنى 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 .

3- دراسة ابن إبراهيم، منال حسن محمد. (2021). الوعي بجو انب الأمن السيبر اني في التعليم عن بعد. المجلة العلمية لجامعة الملك فيصل - العلوم الإنسانية والإدارية، مج22، ع2 ، 299 – 307

تهدف الدراسة إلى بناء برنامج تدريبي مقترح لتنمية جوانب الوعي بالأمن السيبراني في التعليم عن بعد لدى معلمات العلوم بالمرحلة الابتدائية، والكشف عن فعالية البرنامج التدريبي المقترح في تنمية جوانب الوعي بالأمن السيبراني في التعليم عن بعد لدى معلمات

العلوم بالمرحلة الابتدائية. وتكمن أهمية الدراسة في أنها قدمت برنامج تدريبي برنامج لتنمية جوانب الوعي بالأمن السيبراني في التعليم عن بعد لدى معلمات العلوم بالمرحلة الابتدائية وكذلك توجيه المعلمات إلى أهمية توفير بيئة آمنه خالية من التهديد وخرق المعلومات في الفصول الافتراضية . وتم استخدام المنهج التجريبي 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 المقترح وأوصت الدراسة إلى ضرورة توفير برمجيات وتطبيقات تستطيع المعلمات التعامل معها باحترافية ،وكذلك أوصت إلى تضمين موضوعات متنوعة عن الأمن السيبراني في المناهج الدراسية في مختلف المراحل التعليمية.

4- دراسة البيشي، منير عبدالله مفلح. (2021). الأمن السيبراني في الجامعات السعودية و أثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة. مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، مج29، ع6 ، 353 - 372.

تهدف الدراسة إلى التعرف على واقع الأمن السيبراني من وجهة نظر أعضاء هيئة التدريس، وكذلك التحقق من وجود أثر للأمن السيبراني في تعزيز الثقة الرقمية بالجامعات السعودية من و وجهة نظر أعضاء هيئة التدريس .وتكم أهمية الدراسة في أنها من ضمن الدراسات التي تبحث في ثقافة الأمن السيبراني في البيئة السعودية ،وتربط بين الأمن السيبراني والثقة الرقمية وأنها تبين الإطار الفلسفي للأمن السيبراني والحاجة إليه وإلى تطبيقاته في الجامعات السعودية .وتم استخدام المنهج الوصفي التحليلي ؛ كونه الأنسب لخصائص الدراسة وأهدافها وكما توصلت الدراسة إلى عدة نتائج جاء أهمها أن واقع الأمن السيبراني بالجامعات السعودية من وجهة نظر أعضاء هيئة التدريس مرتفعا بنسبة (73.18%)، كما تبين أن مستوى الثقة الرقمية للجامعات السعودية من وجهة نظر أعضاء هيئة التدريس مرتفعا بنسبة (74.58%)، وتبين أن الأمن السيبراني في الجامعات السعودية يؤثر في تعزيز الثقة الرقمية، حيث بلغت نسبة التأثير (46.70%)، وتبين أنه لا توجد فروق بين استجابات

المبحوثين حول الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية تعزى لمتغيري سنوات الخدمة والدرجة العلمية والتفاعل بينهما واوصت الدراسة إلى ضرورة الايمان بأن الأمن السيبراني من افضل الطرق واقصرها في حماية البيانات والأنظمة وكذلك ضرورة تخصيص قسم لأمن وحماية المعلومات يتولى مهمة تحديث ومتابعة برامج وحماية امن المعلومات والأنظمة الإدارية والأجهزة التقنية.

5- دراسة التيماني، مداخل زيد عبدالرحيم. (2021). و اقع الوعي المعلوماتي بالأمن السيبر اني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبر اني. مجلة الخدمة الاجتماعية، ع67ج ، 1 - 23.

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 وتكمن أهمية الدراسة في الدور الذي تلعبه تقنية المعلومات في حياتنا وتأثيرها على سلوك الفرد والمجتمع ولحداثة موضوع الأمن السيبراني في المجتمع السعودي فظهرت الحاجة لبحث مدى تشكل الوعي الاجتماعي تجاه الأمن السيبراني لدى الافراد في المجتمع السعودي وكذلك تكمن أهميتها في الاسهام المعرفي في مجال الوعي الاجتماعي وربطه بالأمن السيبراني وحيث اتبعت الدراسة المنهج الوصفي التحليلي وتوصلت الدراسة إلى اهم النتائج وهي ان هناك نوعين من الاهتمام بالأمن السيبراني على مستوى المملكة العربية السعودية المستوى الحكومي والشعبي حيث ان 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، واوصت الدراسة إلى انه من ابرز أولويات الفرد عن التعامل مع التقنية لاسيما في مجال الأمن السيبراني هو ان يكون اكثر إدراكاً للمخاطر التي يمكن ان تظهر له في الفضاء السيبراني.

6- دراسة القحطانى، نورة بنت ناصر. (2019). مدى تو افر الوعي بالأمن السيبر انى لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. شؤون اجتماعية، مج36، ع144 ، 85 - 120

تهدف الدراسة إلى التعرف على المفهوم الأقرب إلى للأمن السيبراني لدى طلاب وطالبات الجامعات السعودية والتعرف على اهم الجرائم التي يتعامل معها الأمن السيبراني والتي لها علاقة بالمجتمع من وجهة نظر طلاب وطالبات الجامعات السعودية وتكمن أهمية الدراسة في ندرة البحوث في مجال علم الاجتماع وخاصة كموضوع رئيسي لأحد ميادينه وهو العلم الجنائي التي تناولت مشكلة الأمن السيبراني كونه من المجالات الحديثة حيث ان معظم الدراسات تناولته من منظور امني دون ان تدرسه في اطاره الاجتماعي واهمية 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 تنوع بين نسبة الطلاب والطالبات الذين سمعوا بالأمن السيبراني واوصت الدراسة بالتوعية الإعلامية بمشكلات الأمن السيبراني بكثافة اكثر واطلاع المجتمع السعودي على عمليات الاختراقات الاستهداف لمجتمع المعلومات السعودي من جهات خارجية وطرق تجنب افراد المجتمع كونهم احد اضلاع مجتمع المعلومات السعودي.

7- دراسة أنديجاني، دلال صالح، وفلمبان، فدوى ياسين. (2021). ممارسات تعزيز الوعي بثقافة الأمن السيبر اني وتوصياتها في المملكة العربية السعودية. المجلة العربية للمعلوماتية وأمن المعلومات، ع5 ، 75 - 102.

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 وتكمن 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 تكمن في الارتقاء بثقافة الفرد السيبرانية وحيث اتبعت الدراسة في المنهج الدراسة السبع مراحل لمنهج المراجعة المنهجية للدراسات السابقة وتوصلت الدراسة إلى ان درجات الوعي بالأمن السيبراني متفاوتة لدى طالب وطالبات المرحلة الجامعية بجامعات مختلفة بالمملكة العربية والسعودية، واتضح ان درجة الوعي بالأمن السيبراني لدى الطالب والطالبات تتفاوت من درجة منخفضة إلى درجة عالية واوصت الدراسة إلى تطبيق الدراسات التي تدعم تعزيز الوعي وقياس أثر الاستراتيجيات والتقنيات المتبعة وتوصي بتكثيف الجهود

التربوية بالتعاون مع المركز الوطني الارشـادي التابع للهيئة الوطنية للأمن السـيبراني في المملكة العربيـة السـعوديـة لتوعيـة الافراد والمجتمع بـأهميـة الأمن السـيبراني والتعرف على أخطار الهجمات والتهديدات السيبرانية ووسائل التعامل معها.

8- دراسة فرج، علياء عمركامل إبراهيم. (2022). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي: جامعة الأمير سطام بن عبدالعزيز نموذجا. المجلة التربوية، ج94 ، 509 - 537.

تهدف الدراسـة إلى القاء الضوء على دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سـطام بن عبدالعزيز والكشـف عن الفروقات الفروق بين وجهات النظر لدى أعضـاء هيئة التدريس نحو دواعي تعزيز ثقافة الأمن السـيبراني في ظل التحول الرقمي بجامعة الأمير سـطام بن عبدالعزيز تبعاً لمتغيرات الكلية والمرتبة العلمية وسـنوات الخبرة وتكمن أهمية الدراسـة في انها تتزامن مع رؤية المملكة 2030 والتي تؤكد دعم اسـتخدام تقنيات المعلومات وتعزيز البنية الرقمية مما يتطلب تحقيق الأمن السـيبراني وكذلك توجيه الاهتمام نحو ثقافة الأمن السـيبراني والتحذير من المخاطر والانتهاكات السـيبرانية وتم اسـتخدام المنهج الوصـفي لملائمته لطبيعة الدراسـة وأهدافها وحيث توصـلت الدراسـة إلى اذكاء الوعي بالأمن السـيبراني وعلاقته بالأمن الوطني وبالأمن الشـخصـي وتثقيف الطلبة بالممارسـات التي تحقق الأمن السـيبراني من خلال تصـمينها في المقررات الدراسـية في كافة المراحل التعليمية واوصـت الدراسـة إلى ضـرورة خلق بيئة رقمية آمنه من خلال اتقان المهارات التقنية للأمن السـيبراني واسـتخدام البيانات لاكتشـاف التهديدات والاسـتجابة للحوادث السـيبرانية كما اوصـت كذلك إلى انشاء وحدات تكنولوجية للتأهيل السيبراني لأعضاء هيئة التدريس والطلاب والاداريين .

9- السمحان، منى عبدالله صالح. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية بالمنصورة، ع111، ج1، 2 - 29 .

تهدف الدراسـة إلى معرفة متطلبات تحقيق الأمن السـيبراني لأنظمة المعلومات الإدارية بجامعة الملك سـعود وتكمن أهمية الدراسـة في ان الدراسـات التربوية في مجال الأمن السـيبراني لا زالت محدودة بالإضـافة إلى ان الهجمات الإرهابية ما زالت مسـتمرة وقد تزداد مع التطور

التكنولوجي والثورة المعرفية ومحاولة التوصل إلى توصيات ومقترحات تدعم الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود وتمثلت أداة البحث في استمارة استبيان، تم تطبيقها على عينة مكونة من (478) عامل من العاملين بجامعة الملك سعود بالرياض.

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

10- الصانع، نورة عمر أحمد، عسران، عواطف سعد الدين، السواط، حمد بن حمود بن حميد، أبو عيشة، زاهدة جميل نمر، ومنصور، إيناس محمد سليمان علي. (2020). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. مجلة كلية التربية، مج36، ع6 ، 41 - 90 .

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 وتكمن 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 لمناسبته 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 لتوعية 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.

11- الصحفي، مصباح أحمد حامد. (2019). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. مجلة البحث العلمي في التربية. ع. 20، ج. 10، 2019. ص ص. 493-534

تهدف الدراسة إلى التعرف على مدى وعي معلمات الحاسب بمدينة جدة بماهية الأمن السيبراني والتعرف على مدى وعي معلمات الحاسب الالي بمدينة جدة بطرق المحافظة على نظام الأمن السيبراني وتكمن أهمية الدراسة في انها تتناول قياس مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الالي للمرحلة الثانوية بمدينة جدة وكذلك في انها تسهم في إيجاد حلول عملية من خلال حماية الفرد والمجتمع في ظل تنامي المخاطر والتهديدات التي تعترض هذا المجال الحيوي وتم استخدام المنهج الكمي لمناسبته طبيعة الدراسة وتوصلت الدراسة إلى ان وجود ضعف وقصور لدى معلمات الحاسب الالي في الوعي بمفاهيم الحاسب الالي وكذلك اكدت الدراسة على وجود ضعف لدى معلمات الحاسب الالي في الوعي بمستوى الأمن السيبراني واوصت الدراسة إلى ضرورة توفير برامج تدريبية مجانية متعمقة في الأمن السيبراني للمعلمات الاتي على رأس العمل وكذلك الحاق المعلمات بدبلومات بالأمن السيبراني يرفع مستوى الوعي والفهم والتطبيق لديهن بالإضافة إلى دمج الأمن السيبراني في البرامج التربوية الموجودة محلياً.

12- المنتشرى، فاطمة يوسف. (2020). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للعلوم التربوية والنفسية، ع17 ، 457 – 484

تهدف الدراسة إلى معرفة دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات وكذلك معرفة دور القيادة المدرسية في تعزيز الأمن السيبراني لدى طالبات المدرسة كما تكمن أهمية الدراسة في الدور الهام للأمن السيبراني كأحد المتطلبات الضرورية لحماية المجتمعات من المخاطر السيبراني بالإضافة إلى ذلك تأتي الدراسة إلى استجابة إلى لتوجهات حكومة المملكة العربية السعودية الهادفة إلى تعزيز الوعي بالأمن السيبراني وانشاء 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 الأمن السيبراني لدى المعلمات ولدى طالبات المدرسة يتحقق بدرجة موافقة قليلة من وجهة نظر المعلمات واوصت الدراسة بضورة اجراء تصور مقترح لدور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات والطالبات، وجاءت آليات تطبيقه عبر التنسيق مع الجهات المختصة المعنية بالأمن السيبراني في المملكة العربية السعودية، واشتمل على آليات خاصة بكل من: المعلمات، الطالبات، المعلمات والطالبات معا، 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**

تهدف الدراسة إلى تحليل مشاكل الأمن السيبراني في مدرسة ثانوية عامة واقتراح حلول عملية وتم استخدم منهج دراسة الحالة والدراسة توصلت إلى دراسة حالة عن مدرسة ثانوية حيث تم دراسة اهم نقاط ضعفها امام مجموعة من الهجمات والثغرات الالكترونية وذلك بواسطة الإشارة إلى عواقب واثار الهجمات الالكترونية بالإضافة إلى وسائل الوقاية منها واوصت الدراسة إلى انه من الضروري ان تركز المدرسة الثانوية على توفير مجموعة الأجهزة الخاصة وذات 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 افريقيا ومدارس المملكة المتحدة من خلال مجموعة من المبادرات وتوصلت الدراسة إلى اهم النتائج وهي أن جنوب إفريقيا لديها فهم لمدى ملاءمة وأهمية الوعي بالأمن السيبراني للمتعلمين في المدارس وهناك بعض المؤشرات الواضحة على محاولات لزيادة الوعي بالأمن السيبراني وإرساء ثقافة فعالة للأمن السيبراني في جنوب أفريقيا 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 وتقييمه حيث ركزت الدراسة على العلاقة بين الأمن السيبراني ومستوى وعي طلاب التعليم العالي المرتبطين بالجامعات الوطنية في سريلانكا وتم استخدام المنهج الوصفي التحليلي واختيار عينة الدراسة من جميع الجامعات الحكومية ال15 في سريلانكا كما توصلت الدراسة إلى وجود فرق كبير بين مستوى وعي مستخدمي خدمات الأنترنت من الذكور والاناث حيث ان الذكور تفوقوا على الاناث في مستوى وعيهم بالإضافة إلى ان مستوى الوعي بالأمن السيبراني بين الجامعات السريلانكية للطلبة ليس منخفض بشكل ملحوظ واوصت الدراسة إلى ان هناك حاجة إلى سياسية وتوعية 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 لألمن السيبراني، ولتحقيق ذلك تم إنشاء مقرر يدرس بالمختبرات العلمية وتم تطبيقه وتنفيذه على طلبة البكالوريوس في جامعة نيو ساوث ويلز وكان المقرر بعنوان مقدمة في الأمن السيبراني كما تكمن أهمية الدراسة قي ندرة مهارات الأمن السيبراني لدى المحترفين وحاجة الجامعات إلى توفير هذه المهارات من خلال تحسينات منهجيه وتعليمية في مجال الأمن السيبراني وتوصلت الدراسة إلى معظم الطلاب يتفقون على

ان لديهم فهم افضل للأمن السيبراني من خلال المقرر كما اوصت الدراسة إلى تطوير بعض جوانب مقرر الأمن السيبراني وتحسينها ليعلن جاهزيته في عام 2020 .

❖ **أوجه الاختلاف عن الدراسات السابقة:**

أولا: 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 تدريبي مقترح للطالبات وقياس مدى وعيهم بالأمن السيبراني.

ثانياً: فيما يخص الجانب النظري:

قامت الباحثات بدراسة العناصر التالية في الإطار النظري وهو مالم يتوفر 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 (2020) وابن إبراهيم (2021)

والصحفي (2019) وطرق الحماية من اخطار ضعف الأمن السيبراني الصحفي (2019) واندیجاني (2021) والمنتشري.(2020)

1/1 تعريف الأمن السيبراني:

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

فقد عرفت الهيئة الوطنية الأمن السيبراني في المملكة العربية السعودية "هو حماية الشبكات وأنظمة تقنية 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 كلا 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، لذى 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 (الشايع،2018). ويقصد بالأمن السيبراني القدرة على حماية الشبكات وأنظمة الاتصالات وما تحتويها من معلومات وبيانات هامه من اضرار الاختراق والتلف والهجمات الالكترونية 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).

2/1 الفرق بين الأمن السيبراني وأمن المعلومات:

يعد مفهوم الأمن السيبراني أوسع من أمن المعلومات، حيث يشمل مفهوم الأمن السيبراني حماية وتأمين البيانات والمعلومات التي تتداول 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).

3/1 عناصر الأمن السيبراني :

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

1- السرية والأمان : تعني التأكد من أن المعلومات لا يتم الوصول اليها إلا من قبل الأشخاص المخولين لذلك.
2- استمرارية توفر المعلومات أو الخدمة : تعني التحقق من استمرار عمل النظام المعلوماتي وأيضا استمرار القدرة على التفاعل مع المعلومات ، والتأكد من أن المستخدم لن يمنع من الدخول للنظام.
3- سلامة المحتوى : تعني التأكد من أن محتوى المعلومة صحيح لم يتعرض للحذف أو التعديل أو التغيير (الصحفي وعسكول، 2019).
4- التقنية :تعد التقنية والتكنلوجيا 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

والشـبكات حيث أنها تعتمد في حمايتها على اسـتخدام برامج مضـادة للفيروسـات وبرامج جدران الحماية وغيرها.

5- الأشـخاص: يجب على الأشـخاص الذين يسـتخدمون الأنظمة والبيانات أن يضـعوا كلمات مرور قوية جدا ومن الصـعب تخمينها وتجنب فتح الروابط الخارجية التي تصاحب البريد الالكتروني ولابد من القيام بعمل نسخ احتياطية للبيانات.

6- الأنشـطة والعمليات: حيث يتم توفير التقنيات وتوظيف الأشـخاص المناسـبين من أجل تطبيق الأمن السـيبراني وتفعيله والتعامل معه والتصـدي للهجمات بكفاءة (أبو داسر،2020).

4/1 أهداف الأمن السيبراني :

نشر ثقافة الأمن السيبراني وتوعية الأفراد والمؤسسات جاء للأهداف التالية:

1- محاربة البرمجيات الخبيثة.

2- اتخاذ الإجراءات اللازمة لحماية الأفراد من المخاطر المحتمل حدوثها عند اسـتخدام الإنترنت.

3- مواجهة الهجمات التي تستهدف الأجهزة الحكومية ومؤسسات العامة والخاصة

4- سد الثغرات في نظام أمن المعلومات.

5- التخلص من نقاط الضعف في أنظمة وأجهزة الحاسوب والهواتف بأنواعها.

6- وضـع حد للجرائم الإلكترونية على مسـتوى المؤسـسـات والافراد (السـمحان 2020؛ المنتشري 2020).

5/1 أهمية الأمن السيبراني:

1. حفظ سـلامة وخصـوصـية وسـرية المعلومات من الأخطار الإلكترونية وتوفيرها عند الحاجة لها.
2. توفير بيئة للعمل آمنه إلكترونيًا.
3. تقديم الحماية الكاملة للأجهزة والشبكات والمحافظة عليها .
4. اكتشاف أهم ثغرات الضعف الموجودة في النظام ومعالجتها .

5. إعداد طرق لحماية المعلومات الحساسة والمهمة من الهجمات السيبرانية (سمحان، 2020).

6/1 الجرائم السيبرانية:

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

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

1/6/1 خصائص الجريمة السيبرانية:

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

1- جريمة تعبر الحدود : مما يعني أن الجريمة لم تعد تقتصر على مكان معين او حدود معينة ، ولا تشترط تواجد المجرم في نفس المكان ف باستطاعة المجرم تنفيذ جريمته الالكترونية عن طريق الدخول إلى جهاز الضحية في اي بلد.
2- 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 (نعيم،2013)
3- جريمة ناعمة غير ملاحظة: حيث أن هذا النوع من الجرائم لا يتطلب أي اسلحة أو أدوات حادة كالتي تستخدم في الجرائم التقليدية بالإضافة إلى انها لا تستخدم الأساليب العنيفة حيث انها ترتكب بطريقة هادئة غير ملاحظة وبسرعه هائلة تعتمد بشكلٍ أساسي على قرصنة البيانات وأجهزة الحاسوب (العتيبي،2021).

2/6/1 أنواع وتقسيمات الجرائم السيبرانية:

1- جرائم ضد الأفراد : وتكون بهدف سرقة بيانات فرد بعينه مثل سرقة الهوية او بينات البريد الالكتروني الخاصة بالشخص.
2- جريمة ضد الحكومات : تهدف إلى تدمير البنى التحتية لأجهزة النظام الحكومي والمواقع الرسمية والحاق الضرر بها.
3- جريمة ضد الملكية الفكرية : عبارة عن ادخال برمجيات ضارة بهدف تدمير النظام الخاص بالشركات والبنوك والممتلكات الشخصية .

وتقسم أيضا على أنها:

1. جريمة الدخول أو الولوج غير القانوني:

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

2. جريمة الاعتداء على سلامة البيانات:

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

3. جريمة الاعتراضات غير القانونية:

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

4. جريمة الاعتداء على سلامة النظام:

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

5. جريمة اساءة استخدام الحاسوب:

حيث يتم تطويع واستخدام الحاسوب كأداة لأعمال غير مشروعه بغية ارتكاب أي من الجرائم المعلوماتية (مسلم، 2021).

6. جريمة الاعتداء على الأموال :

تعتبر هذه الجريمة من اخطر انواع الجرائم واكثرها انتشـارا لما يترتب عليها من اضـرار مادية فادحه حيث انها تقوم على سـرقة الأموال عن طريق الانترنت وتسـتهدف المواقع التجارية والضرر بزبائنهم .

7. جريمة الاستغلال الجنسي:

تنطبق هذه الجريمة أيضـا على جرائم الابتزاز حيث يقوم الجاني بهذا النوع من الجرائم عبر منصات التواصل الاجتماعي بهدف الوصول إلى القاصرين والقيام بنشر صور واشارات او كلمات جنسية كما يقوم بالتنصت او استدراج الضحية (العتيبي، 2021).

8. جريمة تفجير البريد الالكتروني:

ان يقوم شخص ما بإرسال الكثير من الرسائل مستهدف شخص بعينه وكمية الرسائل تكون هائلة حتى تقوم بملء البريد الالكتروني للشخص وبالتالي ف الخادم لا يستطيع استقبال الكمية المرسـلة ويتوقف عن العمل ومن الطرق المسـتخدمة في تفجير البريد الالكتروني اسـتخدام الروبوت من اجل ان يقوم بإرسـال الكثير من الرسـائل والملفات الكبيرة الموجهة إلى شخص ما حتى يتعطل بريده.

9. جريمة رفض او حجب الخدمات:DOSS

تعد هذه الجريمة من الجرائم المنتشرة حيث انه يتم ملئ واغراق الموقع بكمية هائلة من البيانات غير اللازمة حتى يتوقف الموقع عن الخدمات بشـكل مؤقت وتعليقه لفترة وجعل اسـتخدامه غير ممكن ويعد هجوم DOS رفض الخدمة هجوم يتم نشـره في نفس الوقت لأكثر من نظام مصاب ويطلق على هذه الهجمات الجماعية هجمات الروبوت.(Goutam, 2015)

3/6/1 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 مستخدم وهي كالتالي:

- ❖ تعتبر أداة اكثر سهولة نظراً لاستخدمهم فقط جهاز حاسب واتصال بالإنترنت وهذا يغنيهم عن الاسلحة والمتفجرات حيث ان الارهاب السيبراني يمثل اكثر قوة ودافعية.
- ❖ الارهاب السيبراني يكون الشخص فيه مجهول الهوية اي يمكنه دخول بأسماء مستعارة وعمل كل ما يريد من تخريب وسرقة في المعلومات دون وجود اي حواج .
- ❖ اختلاف الاهداف المراد القيام بها والممكن ان يكون الهدف أجهزة الحاسوب او شبكات الكمبيوتر الخاصة بالحكومة او الافراد او مختلف القطاعات .
- ❖ يمتلك قدرة هائلة في التأثير والحاق الضرر بشكل مباشر على عدد كبير من المؤسسات والافراد(Weimann.2004).

4/6/1 أصناف المجرم السيبراني:

1. القرصنة: ومنهم

- ❖ الكراكز: هدفهم السرقة أو العبث ويتم ذلك من خلال التسلل لنظام المعالجة والاطلاع على المعلومات المخزنة والحاق الضرر بالنظام.
- ❖ الهاكر: هم هواة هدفهم التسلية أو إثبات الذات أو الفضول ويتم ذلك من خلال التطفل على أمن الشبكات ونظم المعلومات وكسر الحواجز والدخول لأنظمة الحاسبات دون حدوث إي ضرر.

2. المهووسون: يكونون في حالة جنون وهدفهم تحطيم جميع الأنظمة.
3. الحكومات الأجنبية: يستخدمون أجهزة الحاسب للتجسس.
4. الجريمة المنظمة: مثل عصابات المافيا.

5. المتطرفون: يستخدمون الشبكة لنشر أفكارهم وبثها بين الناس(الصحفي،2020).

5/6/1 خصائص المجرم السيبراني:

1. قدرة المجرم على استخدام التقنية الحديثة لأنظمة المعلومات.
2. الذكاء العالي للمجرم السيبراني وقدرته على الابتكار.
3. صعوبة الإمساك بالمجرم السيبراني.
4. المجرم السيبراني شخص اجتماعي.
5. قدرته على إعادة الجريمة السيبرانية عدة مرات.
6. استغلال المجرم السيبراني للأزمات للإيقاع بالضحايا(العتيبي،2021).

7/1 تعريف الهندسة الاجتماعية:

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

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

1/7/1 مراحل هجوم الهندسة الاجتماعية:

1. جمع المعلومات حول الهدف: في هذه المرحلة يقوم المهاجم بجمع معلومات عن الضحية الموجودة على المواقع الالكترونية ، وتعتبر هذه المرحلة اساس نجاح الهندسة الاجتماعية
2. تنمية وتطوير العلاقة مع الهدف: في هذه المرحلة يقوم المهاجم ببناء علاقة مع الضحية والعمل على تطويرها من خلال استغلال نقاط الضعف لدى الضحية ، حتى يستطيع الحصول على المعلومات الشخصية التي يريدها ، مثل ارقام البطاقة الائتمانية ، معلومات الحساب.
3. استغلال العلاقة: يتم استغلال العلاقة عندما يتم بناؤها ، ويتم تطوير العلاقة مع الضحية بشكل تدريجي.
4. 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)

2/7/1 أقسام الهندسة الاجتماعية:

❖ هندسة قائمة على أساس التقنية:

1. 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 فعندما تدخل اسم المستخدم وكلمة المرور تحولك للصفحة الرئيسية وتقوم بسرقة بياناتك.
2. الاحتيال الصوتي: يعتمد على برنامج war Dialler ويقوم هذا البرنامج بالاتصال على أرقام هواتف مختلفة في المنطقة ،ويبدأ الخطر عندما يرد الضحية على الهاكر.
3. الرسائل الاقتحامية المزعجة: هي رسالة إلكترونية تكون إما تأكيد طلبية أو تهنئة من صديق وغيرها وبمجرد الدخول تتم سرقة معلوماتك وتدمير الجهاز.
4. برامج مهمه: يقوم الهكر بنشر روابط لتحميل برامج وعند تحميله يقوم بسرقة المعلومات الحساسة.

❖ هندسة قائمة على أساس بشري أو إنساني:

1. الانتحال: ويتم عن طريق وضع سيناريوهات تستهدف شيئا معين وتكون غالبا عن طريق الاتصال بالهواتف ويقوم المجرم بطلب بعض البيانات مثل:الاسم،التاريخ الميلاد، رقم الهوية وغيرها.
2. سلة المحذوفات: من الأخطاء الشائعة رمي الأقراص أو البريد أو ورقة غير مرغوبه بسلة المهملات لأنها تعتبر جسر الهاكر الأقوى لسرقة الهويات وإقناع الضحايا.
3. التجسس والتنصت: يقوم الهاكر بسرقة كلمات المرور عن طريق مراقبة الضحية والتنصت لمحادثاته الشخصية، لذلك ينصح دائما عدم ترك كلمات المرور على المكتب أو تحت لوحة المفاتيح أو حتى تبادلها(أحمد،2014).

3/7/1 طرق للحد من خطر هجمات الهندسة الاجتماعية:

1. عدم نشر أي معلومات خاصة مع الآخرين على شبكة الإنترنت أو مواقع التواصل والمحافظة على الخصوصية.
2. يجب أن تتحقق من أي رسالة تصلك على البريد الإلكتروني أو مكالمة هاتفية تتطلب معلومات خاصة وحساسة.

3. الحذر من فتح أي روابط أو ملفات مرسلة في البريد الإلكتروني لأنها تكون غالبا مواقع تصيد إلكتروني.
4. تنزيل التطبيقات من مصدرها الصحيح.
5. قيام المؤسسات بتدريب الموظفين والعاملين وتوعيتهم بالأساليب الجديدة للهندسة الاجتماعية.
6. استخدام كلمات مرور مختلفة لكل موقع ويتم تغييره شكل دوري.
7. القيام بتحديث البرامج الموجودة على الأجهزة بشكل دوري.
8. الحرص عندما يتم استخدام الحواسيب العامة مثل الموجودة في مقهى أو مطارات...الخ.
9. التأكد من عناوين المواقع أنها تبدأ ب https وليس http(jain et al ,2016)
10. الحرص على اتلاف المستندات والاوراق المهمة بواسطة اجهزة مخصصة.
11. تجنب استخدام البطاقات الائتمانية الا عند الضرورة .
12. الحرص على عدم الرد على اي مكالمة هاتفية وعدم الثقة بأي بريد الكتروني من اي شخص يطلب معلومات شخصية او بنكية ، ولابد من التأكد من هوية الشخص من خلال الاتصال بالمصدر (الزهراني ، 2014).

8/1 التصيد الإلكتروني:

هجمات التصيد الالكتروني أو الاحتيالي : (Phishing)تندرج هجمات التصيد الالكتروني تحت الجرائم الالكترونية وتسمى بالتصيد بسبب طريقتها في الخداع والإيقاع بالضحية حيث يتم فيها خداع المستخدمين لمشاركة بياناتهم الشخصية والحساسة بكامل إرادتهم مثل ارقام بطاقات الائتمان ، 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 ويعرف التصيد الالكتروني بأنه 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 ويعرف أيضا على انه 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

التصـــيد الاحتيالي هي معرفة المســـتخدمين ل هذا النوع من الجرائم لحماية بياناتهم من إي اختراق او سرقة.

1/8/1 أشكال التصيد الالكتروني:

- ❖ رســـائل التصـــيد عبر البريد الالكتروني (phishing) عبارة عن رســـائل تصـــل إلى المستخدم عن طريق البريد الالكتروني وتظهر على أنها رسالة موثقة (مؤسسة، بنك، شركة) وتحتوي على روابط مزيفة أو ملفات بهدف خداع المستخدم واختراق جهازه والوصول إلى بياناته ، مثل أرقام الدخول ، أرقام البطاقات الائتمانية.
- ❖ رسـائل تصـيد البريد الالكتروني مع تحديد الهدف(spear phishing) يتم هذا النوع بنفس طريقة رســـائل التصـــيد عبر البريد الالكتروني ولكن الفرق هو التركيز على أهداف معينة واستهداف أشخاص معينين .
- ❖ التصيد الصوتي (Voice Phishing) : ويتم هذا النوع عبر الاتصال الهاتفي حيث يقوم المجرم باستخدام الاتصالات الهاتفية وانتحال شخصية معينة مثل البنك أو شركه رسمية ، ويظهر الاتصال على أنه موثوق ويقوم المتصل بتوجيه الضحية للدخول على موقع انترنت بقصد الإيقاع به وسرقة بياناته .
- ❖ تزوير المواقع الالكترونية (Pharming) تقوم هذه الطريقة على إلحاق الضـــرر بخادم نظام أسماء النطاقات DNS والذي يوجه الضحية إلى موقع احتيالي مزور ليصيب جهاز الضحية .
- ❖ التصيد عن طريق (Scareware) للإيقاع بالضحية : برمجيات 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 توهم الضحية بأنه ثبت برنامج لحماية جهازه وف الحقيقة عبارة عن برمجيات .
- ❖ التصـــيد عن طريق تطبيقات الهاتف الذكي : وهي عبارة عن اســـتغلال لتطبيقات التواصـــل الاجتماعي وغيرها من تطبيقات على الهاتف الذكي ، حيث يقوم المجرم ب نشر البرمجيات الخبيثة ، أو دمج تطبيقات خبيثة مع تطبيقات أخرى موثوقة ورفعها إلى متاجر التطبيقات ، استخدام برامج وهمية بأسماء أمنية .

- التصيد بالرمح : يحدث في حالة أن تكون الضحية معروفة مسبقًا من قبل المهندس الاجتماعي.
- التصيد عن طريق الفخ أو الطعم : عبارة عن وضع طعم لإغواء الضحية مقابل إعطاء بيانات حساسة مثل : المواقع التي تقدم روابط تحميل مجانية فعند استخدماها يتم اختراق الجهاز أو وضع البرمجيات الخبيثة في الجهاز، ومن البرمجيات الخبيثة المستخدمة لطريقة الفخ أو الطعم(أحصنة طروادة).

ويجب الأخذ بعين الاعتبار أن أكثر الاساليب المستخدمة في التصيد هي الوسائل التنبيهية ورسائل التحقق من الحساب وتأتي في شكل رسالة من مكان عمل الموظف أو رسالة من البنك(الكندي وآخرون، 2020).

2/8/1 البيئات المستهدفة في التصيد الالكتروني:

تعد الأجهزة الإلكترونية هي البيئة المستهدفة في التصيد الالكتروني وتصنف إلى ثلاث فئات :

- أجهزة الحاسوب الشخصية. (pc)
- الأجهزة الذكية.
- أجهزة الصوت النموذجية (الهواتف المكتبية).

3/8/1 تقنيات الهجوم:

تقنيات الهجوم أو ما تعرف بطرائق الهجوم يمكن تقسيمها إلى ثلاث فئات:

- تقنيات تهيئة الهجوم.
- تقنيات جمع البيانات.
- تقنيات اختراق النظام.(Jakobsson &Soghoian, 2009)

4/8/1 تقنيات التدابير المضادة:

تهدف تقنيات التدابير المضادة إلى حماية المستخدمين في البيئة الرقمية . وتنقسم إلى:

- تقنية التعلم الآلي :تقوم هذه التقنية على تطبيق ما تم تعلمه لاستخراج البيانات ولاكتشاف عمليات التصيد ومن ثم التعامل معها .

- ❖ تقنية التصنيف: تقوم تقنيات التصنيف على تحديد وحصر رسائل البريد الالكتروني المخادعة من خلال خصائص معينة
- ❖ تقنية التجميع: وهي عبارة عن تجميع الحالات المتشابهة قد تكون مجموعات تصيد احتيالي أو مجموعات شرعية ،الهدف منها هو تجميع كل حالة تحت ما يشابهها 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 تندرج ضمن التصيد مثل الاختراقات في النظام أو وجود برمجيات خبيثة.(Sharnoubi& Alaka,2015)

9/1 مجالات استخدام الأمن السيبراني:

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

10/1 أبعاد الأمن السيبراني:

1. 1.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.
2. البعد السياسي: يرتكز البعد السياسي المتعلق بالأمن السيبراني على أساس المحافظة على سياسية الدول وأنظمتها وبنيتها، كما أنه يوجد العديد من التكنولوجيا المتطورة التي من خلالها يمكن نقل المعلومات ونشرها حيث يمكن استخدامها في إحداث العديد من الاضرار التي تؤثر على سلامة الدولة وسيادتها واحداث نوع من الفوضى

والاختلال بين مواطنيها كما أن لهذه التقنيات ميزة الوصـول السـريع لأكبر عدد من المواطنين دون الإشارة إلى دقة المعلومات وصحتها التي تنشر وتصل إليهم.

3. البعد الاقتصـادي: هناك صـلة عميقة ما بين الأمن السـيبراني وبين حماية المصـالح والاحتياجات الاقتصـادية لجميع دول العالم ، وهناك أيضـا علاقة كبيرة ما بين المعرفة والاقتصاد لكون جميع الدول تعتمد في تنمية اقتصادها وانعاشه على إنتاج المعرفة والمعلومات ونشـرها فيما يختص بجميع الأصـعدة المختلفة ، وهذا يوضـح التأثير الكبير للأمن السـيبراني وخطورته فيما يخص الملكية الفكرية والسـرقات والمحافظة على اقتصاد الدولة.
4. البعد القانوني: إن مزاولة كافة الأفراد والعاملين في مختلف المنشـآت والهيئات أعمالهم ومهامهم المختلفة التي ترتبط بلا شـك بجملة من القوانين والأنظمة التي تأطرها وتنظمها ، حيث أنه منذ بروز مجتمع المعلومات نشـأت وتكونت لدينا العديد من الأنظمة والسـياسـات الحديثة بوصـفها الإطار التنظيمي والتشـريعي حيث تعمل على السـعي للمحافظة على المجتمع المعلوماتي بما في ذلك أيضـا حماية الحقوق المتعلقة بذلك المجتمع ،كما أنه يتركز الأمن السـيبراني في البعد القانوني على أهمية المحافظة على المجتمع المعلوماتي بكافة الوسـائل المختلفة والمسـاهمة في إتمام جميع الأنظمة والقوانين والسياسات.
5. البعد الاجتماعي: من سـمات الإنترنت هو الطبيعة المفتوحة وهذا يتضـح من خلال شـبكات التواصـل الاجتماعي كونها تسـمح لجميع الأشـخاص بالتعبير عن الأفكار والقضـايا المختلفة وكذلك الوصـول إلى مختلف الثقافات في جميع أنحاء العالم وأيضـا المعرفة والدراية بمختلف المعلومات في جميع المجالات الموضـوعية وهنا يبرز دور الأمن السيبراني في المحافظة على مبادئ وقيم المجتمع (سمحان،2020).

11/1 المخاطر الناتجة عن ضعف الأمن السيبراني:

هنـاك أنواع عـديـدة من الأخطـار التي تواجـه الأمن السـيبراني وتنقسـم إلى: مخـاطر داخلية– مخاطر خارجية (الصحفي وعسكول،2019):

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

1. أخطاء الافراد (الأخطاء البشرية):

تعتبر الأخطار التي تنتج عن البشـــر من أشـــد أنواع المخاطر التي تشـــكل خطرا كبيرا على نظام المعلومات وقد تكون هذه المخاطر أفعال مقصـــودة من قبل الأفراد وقد تكون أفعال غير مقصـــودة وأيضـــا تشـــتمل على الأفراد الغير مســـموح لهم باســـتخدام النظام أو الدخول إليه وأيضا 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 غير المسموح 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 متعمد لأجهزة الحاسوب والمعدات والبرامج.

2. خلل في المعدات : تتضـــمن هذه المخاطر الخلل في المعدات وعدم توافقها مع أجهزة الحاســـوب وأيضـــا مشـــكلات تتعلق بالكهرباء وطرق ربط المعدات ومشـــكلة الرطوبة والتهوية وأيضا إعطال متعلقة بالحواسيب والطرفيات.
3. أخطاء في البيانات : تعتمد صحة المعلومات التي يتم الحصول عليها على صحة البيانات المدخلة في النظام والتي تم معالجتها.
4. نقاط الضعف : من المحتمل عند وجود نقطة أو عنصر في النظام فهذا يحقق سهولة اختراق النظام من قبل المختصين ويسهل لهم الدخول للنظام فحتى 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 وتتضـمن هذه الأخطار الفيضـانات 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 مسعود،2020).
- 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 .
- التنمر الالكتروني .

12/1 آثار ضعف الأمن السيبراني:

1. 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 تأثيرا كبيرا على البنية التحتية لتلك المنشآت وعلى خدماتها واعمالها.

2. الإرهاب والحرب السيبرانية:

تعتمد الجرائم السيبرانية على تقنيات متقدمة وأجهزة تنصت فائقة الجودة وبرمجيات لفك الشفرات واختراق 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.

3. سرقة الهوية الرقمية والبيانات الخاصة:

تعتبر من أخطر الجرائم التي تهدد المستخدمين لشبكة الإنترنت وقد تتعرض البيانات للسرقة والانتحال والاستيلاء على الممتلكات في مواقع التجارة الإلكترونية مما قد يشكل خطرا كبيرا على المستخدمين وعلى المؤسسات.

4. الحرمان من الخدمة:

ويقصـــد 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 أيضا 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).

13/1 إجراءات تعزيز الأمن السيبراني:

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

- 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 واشارات .
- القيام بتأهيل وتدريب المستخدمين على التعامل واستخدام نظم المعلومات التي تتميز بقوتها وسريتها وأيضا لابد من التوجيهات الي تعمل على توعيتهم وادراكهم لضمان الامن والسرية.
- توعية المستخدمين بالحذر من تحميل أي برامج مجهولة المصدر أو غير موثوقة، وفحص البرمجيات قبل استخدمها 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 وتوافر برمجيات تعمل على التأكد من عدم وجود أي من الفيروسات(المنتشري،2020) (الصانع وآخرون، 2020).
- القيام بدروس متنوعه لطلبة التعليم بمختلف المراحل وتشتمل هذه الدروس 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 فيما يخص مجال الأمن السيبراني وحماية البيانات للاستفادة من تجاربهم(المنتشري،2019).
- عملية التشفير أو ما تسمى بالتعمية وهو ما يعني بتحويل البيانات المقروءة 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).

14/1 الأساليب المناسبة من أجل دعم الأمن السيبراني والتقليل من حدة خطر الاساليب والسلوكيات المنحرفة:

- يجب على الأفراد أنفسهم أن يعملوا على زيادة وعيهم بمخاطر الفضاء السيبراني ويجب عليهم تنمية قدراتهم ومواهبهم 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 زيادة وعيهم 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 الأساليب:

1. تنمية الوعي بالأمن السيبراني وذلك عن طريق :

- تنظيم مجموعة من البرامج والندوات التوعوية التي تهدف للتعريف بالأمن السيبراني والعمل على نشره وتنميته على مستوى الافراد والمؤسسات.
- العمل على التعريف بمخاطر وتهديدات الأمن السيبراني ما بين الطلاب وذلك عن طريق المنصات التعليمية.
- السعي في نشر وبث مفاهيم الأمن السيبراني واهم التهديدات والاخطار الناتجة عنه من خلال ارسال الرسائل النصية للمواطنين .
- تنظيم حملات ودورات توعوية بالأمن السيبراني في الجامعات والمدارس في انحاء المملكة وذلك من اجل تثقيف منتسبي التعليم.
- إنشاء مقررات تعليمية تتضمن مفاهيم الأمن السيبراني واهم المخاطر والتهديدات والأساليب الفعالة لمواجهتها بإشراف الكوادر التعليمية .

2. وضع القوانين والتشريعات المتعلقة بالأمن السيبراني:

- تطبيق الأساليب والأنظمة على مستوى الجامعات والمدارس بغرض 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 وسياسيات 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 الامن السيبراني.

3. الاسهام في استمرار تنمية وفاعلية الأمن السيبراني عن طريق:

- استعمال كلمات المرور القوية المكونة من حروف وأرقام عند انشاء حساب في المواقع الرسمية كما انه لابد ان تكون كلمات المرور تختلف من موقع إلى اخر كمواقع التواصل الاجتماعي او مواقع الشراء الالكتروني .
- 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.

4. المساهمة في تجاوز التحديات والمخاطر التي تقابل تطبيق الأمن السيبراني عن طريق:

- الاسهام في تنمية ونشر الوعي بشأن مخاطر وتهديدات الامن السيبراني.
- نشر الوعي حول المواقع غير الموثوقة وآمنه والحد من الدخول اليها وكذلك الحد من انتشارها.
- زيادة التوعية بقوانين الجرائم المعلوماتية والتعريف بها من خلال الرسائل النصية والندوات والحملات التوعوية.
- أن تتضمن الجامعات والمدارس عدد من الخبراء والمتخصصين في الأمن السيبراني للتعريف به وكذلك المساهمة في مواجهة مخاطره المتنوعة.
- تنظيم البرامج التدريبية التي تستهدف القائمين على العملية التعليمية بحيث تتناول تهديدات واخطار الأمن السيبراني (المطيري،2021).

15/1 أبرز اختراقات الأمن السيبراني خلال عام ٢٠٢٠:

1. تسريب بيانات عملاء شركة مايكروسفت:

مع بدايات عام 2020 ظهرت تقارير عدة تعلن عن تسريب بيانات أكثر من 250 مليون عميل وتسريب بيانات الاتصالات والمعلومات بين خدمة العملاء وبين الشركة لمدة 14 عاما وفي هذه الفترة تصدرت مايكروسفت عناوين الأخبار بسبب المشكلات الأمنية في متصفح الأنترنت Internet Explorerوالذي كان يضم ثغرات أمنية عديدة كما نشرت الولايات المتحدة تحذير أمني متعلق بنظام ويندوز 10 متزامنا مع خبر تسريب بيانات العملاء خلال تلك الفترة.

2. اختراق شركة تويتر:

شهد تويتر عام 2020 اختراقا 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 130 حسابا ولكن الاختراق لم يدم لمدة طويلة لأن الشركة استعادت الحسابات وعلى الرغم من ذلك فأن المخترقين استطاعوا جمع اكثر من 100000 دولار عن طريق التبرعات الوهمية التي قامت بنشرها من خلال حسابات المشاهير .

3. اختراق شركة:zoom

في عام 2020 وفي ظل انتشار جائحة كورونا شهد تطبيق ZOOM انتشارا واسعا 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 500000 مستخدم وفي تلك الفترة لم تكن الشركة مهتمة بشكل كبير في تامين البيانات وتأمين غرف الاجتماعات الخاصة والاكواد الخاصة بها مما جعل عملية الاختراق في غاية السهولة لكن بعد حدوث هذا الاختراق اهتمت الشركة وبشكل كبير في تامين البيانات والمعلومات(البابلي،2021).

4. سرقة 3 ملايين يورو بسبب تبديل شرائح الهاتف:SIM Swapping

استطاع مجموعة مخترقين من أوروبا سرقة حسابات بنكية وذلك من خلال استخدام تقنية للاختراق وهي استبدال شرائح الهاتف لأن رقم الهاتف اصبح ضروريا في وقتنا الحالي ويتم من

خلاله الدخول إلى البنوك وتمكن هؤلاء المخترقين من خداع شركات الهاتف لاستبدال 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 الالكترونية واستطاع المخترقين سرقة 3 ملايين يورو خلال هذه العملية.

16/1 حوادث الأمن السيبراني في المملكة العربية السعودية و انعكاساتها:

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 2012م والذي كان قاصداً ومستهدفا به شركات النفط في المملكة العربية السعودية حيث كان من أضخم الهجمات السيبرانية التي تستهدف الاعمال التجارية الخاصة وتقوم بتسريب جميع المعلومات لها.
- فيروسTrisis حيث أدى إلى اغلاق بعض من مرافق النفط في المملكة العربية السعودية وهو يعمل على نشر برمجيات خبيثة او برامج ضارة تمكنهم من الاستيلاء والحصول على الأنظمة وان يتحكموا بها(الجمل،2020).
- فيروس Mamba Ransomware لقد قام بمهاجمة المملكة العربية السعودية في عام 2017 وكان يسعى إلى الوصول إلى الشبكات التابعة للشركات في المملكة العربية السعودية ويعمل على تشفير الأقراص الصلبة بشكل متكامل لا الملفات فقط (أبو زيد،2019).
- هجوم APT لقد رصدت مراكز الامن الالكتروني هجوماً الهدف منه هو المملكة العربية السعودية ويعد هذا الهجوم متحكم بتواصل مع بروتوكول)HTTP (مركز الأمن الإلكتروني،2017).

17/1 مبادرات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية:

قامت المملكة العربية السعودية في مجال الأمن السيبراني بجهود مستمرة بدءاً من انشائها الهيئة الوطنية للأمن السيبراني وسعيها الحثيث على تقديم مجموعة من التوصيات في هذا الصدد ومنها : تنمية الصمود السيبراني وذلك من اجل 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 وأيضا 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 وايضاً مواجهة مخاطر الأمن السيبراني والعمل على الحد من أثار هذه المخاطر كما انه تم تهيئة المركز الوطني على الإطلاق الاشعارات التي تعلم بأهم وأحدث الثغرات 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 تثقيف 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 وتقنية المعلومات بالشراكة مع صندوق تنمية الموارد البشرية جاءت هذه المبادرة من اجل زيادة الإمكانيات الوطنية الرقمية في جميع المجالات وخاصة التقنية والتكنولوجية المتطورة وذلك بهدف ملاحقة 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 الالكتروني من السرقات والاستعمال غير المجاز 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 تثقيف 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 الأنترنت وأيضا الاستخدام الآمن مع خدمات البريد الالكتروني وشبكات التواصل الاجتماعي
- إدارة هويات صلاحيات الدخول: وذلك عن طريق تطبيق يتم من خلاله التأكد من الهوية متنوعة 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 والأنظمة التابعة للجهة والتي يتم استعمالها للولوج عن بعد بشكل مستمر وكذلك الوقاية من جميع البرمجيات الخبيثة والفيروسات التي تشكل تهديداً على جميع أجهزة العاملين وايضاً حماية الخوادم الخاصة بالجهة والتي يتم من خلالها الدخول عن بعد بواسطة التقنيات وطرق الحماية المتطورة والتحكم فيها بشكل امن وسليم (المطيري،2021).

18/1 نماذج مؤسسات الأمن السيبراني في المملكة:

تماشيا مع رؤية 2030 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 بتدريس طلابها مواد لها علاقة مثل امن المعلومات واتجهت الجهود إلى تأسيس مراكز مخصصة ومعنية بالأمن السيبراني ومن هذه المراكز (القحطاني،2019):

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

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

Maram Alsharif
KAU
maram22_11@hotmail.com

Al Anood Al-harbi
Tibah University
layanalharbi08@gmail.com

Amal Sulaimani
Tibah University
3nooodh741@gmail.com

layan Alharbi
Tibah University
amool58993@gmail.com

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.