فعالية برنامج تدريبي مقترح لتنمية الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الإنسانية: دراسة تجريبية[1] "الجزء الثاني"

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

أمل عبيد اللّه عبد العزيز السليماني

بكالوريوس علم المعلومات- جامعة طيبة

amool58993@gmail.com

19/1 نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية:

بسم الله الرحمن الرحيم

مرسوم ملكي رقم م/17 بتاريخ 8 / 3 / 1428

بعون الله تعالى

نحن عبد الله بن عبد العزيز آل سعود

ملك المملكة العربية السعودية

بناء على المادة (السبعين) من النظام الأساسي للحكم، الصادر بالأمر الملكي رقم (أ/٩٠) وتاريخ ٢٧ / ٨ / ١٤١٢ هـ

[1] تم نشر الجزء الجزء الأول من المقال في (المجلد الثالث، العدد الرابع أكتوبر - ديسمبر 2023)

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

وبناء على المادة (العشـــرين) من نظام مجلس الوزراء، الصـــادر بالأمر الملكي رقم (أ/١٣) وتاريخ ٣/٣ / ١٤١٤ هـ.

وبناء على المادة (الثامنة عشـرة) من نظام مجلس الشـــورى، الصـــادر بالأمر الملكي رقم (أ/٩١) وتاريخ ٢٧ / ٨ / ١٤١٢ هـ.

وبعد الاطلاع على قرار مجلس الشورى رقم (٦٨ /٤٣) وتاريخ ١٦ / ٩ / ١٤٢٧ هـ.

وبعد الاطلاع على قرار مجلس الوزراء رقم (٧٩) وتاريخ ٧ / ٣ / ١٤٢٨ هـ.

رسمنا بما هو آت:

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

ثانيًا: 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 79 بتاريخ 7 / 3 / 1428

إن مجلس الوزراء

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

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

وبعد النظر في قرار مجلس الشورى رقم (٦٨ / ٤٣) وتاريخ ١٦ / ٩ / ١٤٢٧ هـ.

وبعد الاطلاع على توصية اللجنة العامة لمجلس الوزراء رقم (٥٠) وتاريخ ١٧ / ١ / ١٤٢٨ هـ.

يقرر

الموافقة على نظام مكافحة جرائم المعلوماتية، بالصيغة المرافقة.

وقد أعد مشروع مرسوم ملكي بذلك، صيغته مرافقة لهذا.

رئيس مجلس الوزراء

نظام مكافحة جرائم المعلوماتية

المادة الأولى

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

- الشخص: أي شخص ذي صفة طبيعية أو اعتبارية، عامة أو خاصة .

- النظام المعلوماتي: مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات 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 الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها.
- برامج الحاسب الآلي: مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي، وتقوم بأداء الوظيفة المطلوبة.
- الحاسب 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 البرامج، والأوامر المعطاة له.
- الدخول غير المشروع: دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها.
- الجريمة المعلوماتية: أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.
- الموقع الإلكتروني: مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.
- الالتقاط: 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:

1. المساعدة على تحقيق الأمن المعلوماتي.
2. حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية .
3. حماية المصلحة العامة، والأخلاق، والآداب العامة .
4. حماية الاقتصاد الوطني.

المادة الثالثة

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1. التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه.
2. الدخول غير المشروع لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا .
3. الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.
4. المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها .
5. 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 أيًا من الجرائم المعلوماتية الآتية:

1. الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة .
2. الوصول - دون مسوغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، 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 أيًا من الجرائم المعلوماتية الآتية:

1. الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.
2. 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.
3. 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 كلُّ شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية:

1. إنتاج ما من شأنه المساس بالنظام العام، او القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي .
2. إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار في الجنس البشري، أو تسهيل التعامل به.
3. إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها.
4. إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب 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 كلُّ شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية:

1. 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 .
2. 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 اقترنت الجريمة بأي من الحالات الآتية:

1. ارتكاب الجاني الجريمة من خلال عصابة منظمة .
2. شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلًا سلطاته أو نفوذه.
3. التغرير بالقُصَّر ومن في حكمهم، واستغلالهم .
4. صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.

المادة التاسعة

يعاقب كل من حرَّض غيره، أو ســاعده، أو اتفق معه على ارتكاب أيٍّ من الجرائم المنصــوص عليها في هذا النظام ؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويعاقب بما لا يتجاوز نصــف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية.

المادة العاشرة

يعاقب كل من شــرع في القيام بأي من الجرائم المنصــوص 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 وخاصــة ما يتعلق بحقوق الملكية الفكرية، والاتفاقيات الدولية ذات الصلة التي تكون المملكة طرفًا فيها.

المادة الثالثة عشرة

مع عدم الإخلال بحقوق حسـني النية، يجوز الحكم بمصـادرة الأجهزة، أو البرامج، أو الوسـائل 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 إغلاقًا نهائيًا أو مؤقتًا متى كان مصدرًا لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكه.

المادة الرابعة عشرة

تتولى هيئة الاتصــالات وتقنية المعلومات وفقًا لاختصــاصــها تقديم الدعم والمســاندة 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) يومًا من تاريخ نشره.

1/2 دوروزارة 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 عاتقهما العديد من المهام والمسؤوليات والقيام بمعالجة المشكلات الظاهرة وتسليط الضوء على المشكلات الظاهرة في المجتمع، ولاشك أن المدارس والجامعات لم يعد يقتصر 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 ارتباطا وثيقا ومتينا، لا سميا 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 الى الانحرافات الأخلاقية . وهنا يتعاظم دور المدارس والجامعات تجاه تلك المعضلات، حيث يعد أمن المعلومات والجرائم الإلكترونية من أهمها، لا سيما في ظل تنامي استخدام التقنيات والأجهزة الإلكترونية المتطورة.

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

1. وضع الوزارة خطط عمل للتعامل مع المخاطر وتضمينها للجهات والمؤسسات المعنية التي تساعد على مواجهة المخاطر السيبرانية.
2. تنظيم دورات تدريبة خاصة للمعلمين في المجالات الآتية: الوعي بالأمن السيبراني من جهة المعلمين وماهي الإجراءات التي يستطيعون إتباعها لمواجهة مخاطر الفضاء السيبراني.
3. إشراك أولياء الأمور في الخطط والبرامج المتعلقة بالأمن السيبراني.
4. نشر الوعي بأهمية الأمن السيبراني بشكل واسع والاستعانة بالوسائل المعينة على ذلك مثل الندوات وورش العمل ونشر الوعي في مواقع التواصل والنشرات التوعوية.
5. تضمين موضوع الأمن السيبراني في الأدلة الخاصة بالمعلمين.
6. التثقيف بأن الأمن السيبراني يعد إحدى مهارات الحياة المهمة التي لابد من اكتسابها وتدريسه والتوعية بأهميته.

7. 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 زيادة وعي وأهمية الأمن السيبراني (المنتشري وحريري، 2020).

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

1. التعرف على المخاطر وأوجه القصور المحتملة عند مشاركة الطالبات في الأنشطة الموجودة على شبكة الإنترنت .
2. العمل على توعية الطالبات فيما يتعلق بحماية البيانات الشخصية.
3. استخدام التقنيات المختلقة والحديثة التي تساعد على التأمين والحماية.
4. زيادة الوعي حول مخاطر الإنترنت المتعددة كالتنمر الإلكتروني ومواقع الإنترنت ذات المحتوى غير الملائم.
5. السعي إلى نشر سياسات وإجراءات الأمن الرقمي وتحديثها بكل جديد (الجندي، 2019).

2/2 أساليب تفعيل الأمن السيبراني في الجامعات:

1. إنشاء مركز خاص بالأمن السيبراني ويتفرع من المركز وحدة خاصة بكل كلية من كليات الجامعة.
2. تقديم برامج تدريبية بشكل مستمر للتوعية بمخاطر الجرائم والسعي إلى مكافحتها.
3. عقد مؤتمر سنوي في الجامعة يتم التحدث فيه عن أمن المعلومات لتوعية الطلبة وجميع العاملين في الجامعة.
4. عقد شراكة بين الجامعة ووزارة الإعلام وذلك لعمل حملات إعلامية لوقاية الطلبة من مشكلات الأمن السيبراني.
5. العمل على توفير البرامج الاكاديمية في الأمن السيبراني لطلبة الدراسات العليا.
6. ضرورة دعم وتشجيع أعضاء هيئة التدريس للقيام بالأبحاث في تخصص الأمن السيبراني.
7. ضرورة توعية الطلبة باستخدام الذاكرة الخارجية من أجل النسخ الاحتياطي للرسائل العلمية ولابد أن يتم التحقق من دقة وصحة المعلومات التي يتلقاها الطلبة من الشبكات الاجتماعية.

8. إضافة بعض من المصطلحات والمفاهيم بما يتعلق بالأمن السيبراني في المقررات التي يتم دراستها.
9. لابد من وجود مناهج دراسية تتعلق بالأمن السيبراني في مختلف القطاعات التعليمية.
10. توفير وسائل وبرامج الجامعات من أجل التطبيق العملي والنظري للأمن السيبراني.
11. تحديث الخطط الدراسية بما يتوافق مع التطورات المعلوماتية والتقنية (الهندي، 2021).

3/2 مراحل تعزيز قيم المواطنة الرقمية لدى طلبة الجامعات:

- مرحلة الوعي:

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

- مرحلة الممارسة الموجهة:

تعتبر بأنها الاستعمال الأمثل للتكنولوجيا من خلال القيام بتدريب ومعرفة الطلاب باستخدام التقنية والحرص على التعرف على الأمن السيبراني من خلال التوجيه والإرشاد عن طريق التطبيق والممارسة العملية بالتوجيه إلى المواقع والصفحات الإلكترونية بطريقة آمنه .

- مرحلة النمذجة وإعطاء المثل والقدوة:

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

- مرحلة التغذية الراجعة والتحليل:

وفي هذه المرحلة تتم المتابعة المستمرة للطلاب وتقديم التغذية الراجعة والتزيد بالمهارات كالتمييز والتحليل عند استخدام التقنيات الحديثة (محمد، 2020).

4/2 البرامج التدريبية في الجامعات السعودية:

ونظرا 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 والاستجابة لمتطلبات سوق العمل .
- الحاجة إلى متخصصين في مجال مكافحة الجرائم الالكترونية .
- الحاجة إلى أشخاص من ذوي الخبرة لديهم القدرة على معرفة واكتشاف نقاط الضعف الأمنية.

وسنستعرض أبرز البرامج التدريبية في الجامعات السعودية الخاصة بالأمن السيبراني:

جامعة الإمام عبدالرحمن بن فيصل:

تقدم الجامعة برنامج بكالوريوس الأمن السيبراني والتحري الرقمي في كلية علوم الحاسب 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، وتحديد وإصلاح الثغرات الأمنية.

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

الرسالة: حصول المتدربين 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 الحوسبة .
- تطبيق الحلول والمقترحات لتلبية احتياجات الحوسبة .
- تطبيق الممارسات الأمنية للمحافظة على العمليات في بيئة مليئة بالأخطار والتهديدات.
- معرفة المسؤوليات المهنية والحكم في الحوسبة بالاعتماد على المبادئ القانونية والأخلاقية.
- العمل بشكل فعال كعضو أو قائد فريق .

جامعة الملك سعود:

تقدم الجامعة برنامج بكالوريوس في الحوسبة التطبيقية (مجال الأمن السيبراني) . وذلك بتنفيذ معايير عالية لدعم التعليم التطبيقي حتى يتسنى لها إعداد الكوادر البشرية المؤهلة لسوق العمل والمؤهلين لمواجهة التهديدات داخل الفضاء الالكتروني.

أهداف البرنامج التعليمية:

- القدرة على الممارسة في مهن تقنية المعلومات والاتصالات.
- القدرة على إجراء البحوث في مجالات الحوسبة بالإضافة الى 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 الحاسب والمعلومات بجامعة الأمير سلطان، وذلك استجابة 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 والأنظمة الحاسوبية والتكنولوجية بالمؤسسات والمنظمات العامة والخاصة من الهجمات والاختراقات الإلكترونية .

أهداف البرنامج التعليمية:

- تلبية احتياجات سوق العمل على المستوى المحلي والعالمي .
- توائم مخرجات البرنامج مع معايير مجلس الاعتماد الأكاديمي الدولي للهندسة والتكنولوجيا (ABET) .

جامعة الأمير مقرن بن عبدالعزيز:

تقدم الجامعة برنامج الريادة في تعليم الحاسب الآلي الذي يهدف إلى تدريب الطلاب على إجراء أبحاث مبتكره في أحدث مجالات الحاسب الآلي والعلوم السيبرانية للمساهمة 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 احتياجات المجتمع التقنية.
- توفير بيئة اكاديمية آمنه 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 الأتية، الأمن السيبراني والبرمجة والذكاء الاصطناعي في مدينة الرياض وذلك تزامنا مع رؤية 2030 للسعي نحو الأفضل وبناء مجتمعات تتميز بالمعرفة وتقنية وتتنافس مع الدول المتقدمة. وتهدف الكلية إلى تعليم الطلاب بالوسائل الحديثة والمبتكرة وفقاُ للتحقيق رؤية المملكة العربية السعودية، وتمنح الكلية الشهادات الاحترافية والجامعية المتوسطة والبكالوريوس وما بعد البكالوريوس في 8 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 الاستجابة للحوادث السيبرانية.

جامعة الأميرة نورة بنت عبدالرحمن:

تقدم الجامعة برنامج بكالوريوس في الأمن السيبراني تماشيا مع المتطلبات والأهداف التعليمية المذكورة سابقا، كما أطلقت الجامعة برنامج معسكر الأمن السيبراني بالتعاون مع كلية علوم الحاسب والمعلومات للتدريب التقني ويتكون البرنامج من ٧٠ ساعه تدريبية (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 .

5/2 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 مواضيع مختلفة مثل: الجرائم المعلوماتية، كيف تصاب أجهزتنا بالبرامج الخبيثة وكيف تكون مسؤول عن حماية شبكتك، حماية البريد الإلكتروني، البرمجيات الضارة أمن الأجهزة، حماية خصوصيتك أثناء تعلمك أو عملك عن بعد...الخ من خلال نصوص وصور وفيديوهات قصيره ومفيدة. وتستقبل الإدارة الاستفسارات والبلاغات الأمنية السيبرانية من خلال تعبئة نموذج أو مراسلتهم عبر بريد الكتروني خاص بالإدارة، وتختص الإدارة بحوكمة وإدارة أمن المعلومات وحماية أجهزتها وأنظمتها وشبكاتها وفقا لإجراءات وسياسات للمحافظة على سلامة الأصول المعلوماتية والتقنية في جامعة طيبة، وأن تكون هناك إدارة لجميع التهديدات والمخاطر المحتملة ووضع الحلول .

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

رسالة الإدارة: تهدف الإدارة لرفع مستوى وعي 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 تابعه لمعالي رئيس جامعة أم القرى وتسعى الإدارة لتطبيق أفضل المعايير الدولية ورفع مستوى الأمان والحماية داخل الجامعة وتتيح إمكانية الإبلاغ عن الحوادث السيبرانية.

رؤية الإدارة: الوصول لفضاء سيبراني أمن وموثوق.

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

الأهداف الاستراتيجية:

- رفع مستوى وعي منسوبيها وتعريفهم بالممارسات الصحيحة لاستخدام مصادر الجامعة التقنية.
- تعريف منسوبيها بالإجراءات والسياسات التي يجب تطبيقها داخل الجامعة فيما يتعلق بالأمن السيبراني.
- استمرار عمل منظومة التقنية في الجامعة وحماية سرية المعلومات المرتبطة بها.
- العمل على بناء إطار عمل تستطيع الجامعة أن تتعاون مع منسوبيها 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 ارتباطا إداريا بوكالة الجامعة. وهي الجسر الرابط بين الجامعة والهيئة الوطنية للأمن السيبراني .

تتألف الإدارة من قسمين رئيسين القسم الأول هو قسم الحوكمة والالتزام وتقوم الوحدات الخاصة بهذا القسم بدورها لتحقيق متطلبات واحتياجات الهيئة الوطنية للأمن السيبراني وذلك من خلال ضمان الالتزام 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، اكتشاف الثغرات والعمل على حلها، والتصدي للهجمات السيبرانية، وتحليل المخاطر السيبرانية.

رؤية الإدارة: وصول جامعة الجوف إلى فضاء سيبراني 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 والتأكيد 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 اللازمة 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 14\8\1438هـ، تهتم الإدارة بتعزيز الأمن السيبراني وحماية أصول الجامعة التقنية وإدارة المخاطر المحتمل حدوثها ضد المخاطر السيبرانية لضمان استمرارية أعمال الجامعة البحثية والتعليمية والإدارية.

رؤية الإدارة: الوصول إلى فضاء سيبراني 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 التقيد والالتزام بأنظمة الهيئة الوطنية للأمن السيبراني.
- تعزيز إتباع أحسن الممارسات في الأمن السيبراني.

- **إدارة الأمن السيبراني في جامعة الملك عبد العزيز:**

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 تعليمة آمنه في الجامعة تساعد على النمو وتحقيق رؤية 2030.

رسالة الإدارة: تقديم بيئة آمنه 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.

6/2 دور الأمن السيبراني في الجامعات السعودية 2030:

1. تقديم خدمات استشارية مختصة بدور الأمن السيبراني في الجامعات والمؤسسات التعليمية في المملكة.
2. تفعيل ورش العمل المختصة بالأمن السيبراني.

3. التوعية بدور الأمن السيبراني.
4. وضع حلول تساعد في تفادي الاختراقات والثغرات الأمنية.
5. توفير خدمات التدريب لمنسوبي الجامعات.
6. حماية وحفظ حقوق الملكية الفكرية وبراءات الاختراع الخاصة بأصحابها (الخضري، 2020) .

7/2 دور الممارسة التطبيقية للأمن السيبراني في تنمية دقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة:

يرى بعض العلماء أن تطبيق الممارسة التطبيقية للأمن السيبراني له دوره الواضح في تنمية التطبيق العملي لأمن المعلومات لدى طلاب وطالبات المرحلة الجامعية . وذلك من خلال تنمية القدرات والمهارات وفقا للمستويات المختلفة بينهم، وتعمل هذه المستويات على تحديد طبيعة أمن المعلومات للبنية المؤسسية وذلك من أجل أن يتوفر كامل الدعم المطلوب في جميع حالات التقصير التي قد تحصل وتقديم المساعدة ووضع المقترحات المتاحة من أجل أن يتم تفعيل بعض المناطق الأمنية ووضع بعض الاحترازات والالتزام 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 سواء الآن أو في المستقبل، ولابد للمؤسسة أن تقوم بوضع السياسات والمعايير الأمنية وتقوي بنيتها التحتية، وبإمكان الطلاب أن يحددوا نقاط الضعف والقوة ويعملوا على تقييم المخاطر والتهديدات ويصبح لديهم إدراك كامل بالأمن الوطني وتصنيفاته وحمايته للوثائق والمعلومات والبيانات.

يوجد كذلك المزيد من الدراسات المتعلقة بالممارسات 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 ونذكر منها، الشبكة المحلية،والشبكات الواسعة، والعنكبوتية، وقياس أهميتها بالنسبة للأشخاص و المؤسسات والطرق التي يتم اتباعها من اجل الحماية والوقاية من الأخطار. و نتناول 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 و الأهمية الناتجة من سياسيات الأمن المعلوماتي، إلا أنها تتسم ببعض القصور في السياسيات وأيضا يعتبر مفهوم الوعي الأمني واسع جدا ولابد توعية الجميع به كما في دراسة أخرى كان الهدف منها هو وضع بعض السياسيات 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 كإدارة الوقت ولتقويم الذاتي كما يلي:

1. إدراك الطالبات لأهمية برامج الحماية وإمكانية التعرف على مواطن الضعف.
2. مقدرة الطالبات على تحسين إمكانيات الحماية الأمنية المتوقعة وجميع المخاطر الأمنية الأخرى. (الجندي، 2019).

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 تشتمل 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 pdf و word.
- بعد الاطلاع على آراء المحكمين تم إجراء التعديلات التي أوصوا بها وبناء على ذلك تم تعديل الاستبانة 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 والمتشابهة التي تحمل نفس المعنى مثل سؤال (١٣) و(١٥) الخاصة بكلمات المرور

ودمجها في سؤال واحد، هذا وقد تم تعديل المصطلحات وتوحيدها مثل الكمبيوتر إلى الحاسب الآلي ، بالإضافة إلى إلغاء الأسئلة التي تختص بمتطلبات تحقيق الأمن السيبراني وهي عبارة عن ٤ أسئلة للتقليل من طول الاستبانة، كما تم إضافة سؤال: هل لدي معرفة سابقة بمفهوم التصيد الإلكتروني وإضافة سؤال هل لدي معرفة سابقة بالهندسة الاجتماعية، و تعديل سؤال المستوى إلى المستوى الدراسي ، وأخيرا تغير كلمة القسم إلى التخصص.

- بعد إجراء التعديلات النهائية للاستبانة بلغ عدد الأسئلة (٣٤) سؤال وفق التقدير (موافق، موافق بشدة، محايد، غير موافق، غير موافق بشدة). حيث تتضمن العناصر التالية:

1. الوعي بمفهوم الأمن السيبراني.
2. 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 للطالبات.
- توجيه الاستبانة الإلكترونية للطالبات 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 (1) يوضح توزيع أفراد العينة على الفئة العمرية

القسم العلمي / الفئة العمرية	أقل من 20	النسبة	من 21 إلى 30	النسبة	المجموع	النسبة المئوية
الدراسات القرآنية	4	%5.4	20	٪17	24	٪12.5
الدراسات الإسلامية	25	٪ 33.8	9	٪ 7.6	34	٪17.7
اللغة العربية	3	٪4.1	22	%18.6	25	٪13
اللغات والترجمة	0	%0.00	24	%20.3	24	٪12.5
العلوم الاجتماعية	12	%16.2	18	٪15.3	30	٪15.6
الاتصال والاعلام	23	٪31.1	10	٪8.5	33	٪17.2
المعلومات ومصادر التعلم	7	٪9.5	15	%12.7	22	٪11.5
الإجمالي	74	٪28	118	٪61.5	192	٪100

في الجدول (2) أظهرت النتائج أن الغالبية العظمى من أعمار الطالبات بين عمر 21 إلى 30 بنسبة 61.5٪ وهو العمر المناسب لدخول الطالبات للجامعة ثم يليه عمر الطالبات أقل من 20 بنسبة 28٪، وأظهرت النتائج تجاوب الأقسام العلمية في تعبئة الاستبيان أن الطالبات في قسم الدراسات الإسلامية كانوا الأكثر و بنسبة 17.7٪،ثم قسم الاتصال والإعلام وبنسبة 17.2٪، ثم قسم العلوم الاجتماعية وبنسبة 15.6٪، ثم قسم اللغة العربية وبنسبة 13٪، ثم قسم الدراسات القرآنية وقسم اللغات والترجمة المتشابهين في العدد وبنسبة 12.5٪، وثم كان القسم الأقل عددا المعلومات ومصادر التعلم11.5 ٪.

الجدول رقم (3) يوضح المستوى الدراسي لأفراد العينة

المستوى الدراسي	العدد	النسبة
الثاني	88	٪45.8
الرابع	45	٪33.4
السادس	30	٪15.6
الثامن	29	٪15.1
المجموع	192	٪100

في الجدول رقم (3) يوضح أن الغالبية العظمى من الطالبات بالمستوى الثاني وبنسبة 45.8٪، ثم المستوى الرابع وبنسبة 33.4٪، ثم المستوى السادس وبنسبة 15.6٪، ثم المستوى الثامن وبنسبة 15.1٪.

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

الجدول (4) وعي طالبات كلية الآداب والعلوم الإنسانية بمفهوم الأمن السيبراني

	الاستجابة القبلية					الاستجابة البعدية				
	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
لدي معرفة سابقة بمفهوم الأمن السيبراني؟	11	66	42	55	18	45	114	16	11	3
	٪5.7	٪34.4	٪21.9	٪28.6	٪9.4	٪23.8	%60.3	%8.5	%5.8	%1.6
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 اختلاف قد يحدث.	20	114	39	14	5	61	94	18	11	5
	%10.5	%60	%20.5	%7.4	%2.6	٪32.3	%49.7	%9.5	%5.8	٪2.7
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.	33	115	33	6	5	72	103	11	2	1
	%17.2	%59.9	%17.2	%3.1	٪2.6	%38.1	%54.5	%5.8	%1.1	%0.5
الأمن السيبراني: هو حماية المستخدمين من أي مخاطر تواجههم.	35	114	33	5	5	69	111	8	1	0
	%18.2	%59.4	%17.2	%2.6	%2.6	%36.5	%58.7	%4.2	%0.5	٪0.0

حسب النتائج الموضحة بالجدول رقم (4) تبين لنا أن عينة الدراسة انقسمت إلى قسمين قبل بدء التجربة حيث أن جزء من عينة الدراسة كان لديهم وعي سابق بمفهوم الأمن السيبراني قبل تطبيق التجربة عليهم والنصف الآخر لم يكن لديهم الوعي بمفهوم الأمن السيبراني، ولكن بعد قيامنا بتطبيق التجربة كان هناك ارتفاع في نسب الوعي بمفهوم الأمن السيبراني وذلك استنادا على الاستجابات القبلية والبعدية للاستبيان حيث بلغت نسبة موافق بشدة وموافق للسؤال الأول 40.1٪ وهذه نسبة جيدة إلى حد ما، بينما بلغت نسبة غير موافق وغير موافق بشدة 38٪ ومحايد 21.9٪، أما بعد إجراء التجربة فقد ارتفعت نسبة الوعي لديهم بمفهوم الأمن السيبراني حيث بلغت الاستجابات البعدية النسب التالية موافق بشدة وموافق 84.1٪ ونستنتج من خلال هذه النسب أن الوعي لدى أفراد العينية قد زاد بشكل ملحوظ وفي المقابل بلغت نسبة غير موافق وغير موافق بشدة 7.4٪ ومحايد 8.5 ٪ مما يؤكد نجاح التجربة في جانب زيادة الوعي بمفهوم الأمن السيبراني، وتأثيرها المباشر على وعيهم بهذا المفهوم وذلك استنادا على إجابتهم من خلال الاستبانة، وعند انتقالنا للسؤال الثاني الخاص بمفاهيم الأمن السيبراني التي كانت عبارة عن ثلاث 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 استنادا على الاستبانة القبلية ، وكانت النسب تتركز في موافق بشدة وموافق بنسبة70٪ 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 وانخفاض نسب عدم الموافقة وذلك استنادا على النتائج الموضحة، ولكن لوحظ بعد التجربة أن المفهومين الخاصة بالوسائل التقنية والمستخدمين حصلت على أعلى نسب موافقه من أفراد العينة حيث تراوحت نسب الموافقة بين 90٪ و95٪ .

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

الجدول رقم (5) مدى احتياج طالبات كلية الآداب والعلوم الإنسانية لدورات تدريبية تختص بالأمن السيبراني

	الاستجابة القبلية					الاستجابة البعدية				
	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
احتاج إلى دورات تدريبية في الأمن السيبراني ؟	51	103	22	10	6	51	108	18	11	1
	٪26.6	٪53.7	٪11.5	%5.2	٪3.1	٪27	٪57.1	%9.5	٪5.8	٪0.5

توضح النتائج السابقة من خلال الجدول رقم (5) 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 الاستجابات القبلية للاستبانة كان هناك ارتفاع في نسب الموافقة حيث بلغت نسبة موافق بشدة وموافق 80٪ وغير موافق وغير موافق بشدة 8.3٪ مما يؤكد مدى حاجتهم واهتمامهم في الحصول على الدورات التدريبية . وعند تطبيق التجربة فقد كانت نسب الموافقة أعلى وذلك استنادا على الاستجابات البعدية للاستبانة حيث ارتفعت نسبة موافق بشدة وموافق إلى 84.1٪ بينما انخفضت نسبة غير موافق وغير موافق بشدة إلى 6.3 ٪، 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 (6) مدى قدرة طالبات كلية الآداب والعلوم الإنسانية على التفريق بين أمن المعلومات والامن السيبراني

	الاستجابة القبلية					الاستجابة البعدية				
	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
استطيع التفريق بين الأمن السيبراني وامن المعلومات؟	9	46	45	65	27	64	106	13	5	1
	٪4.7	٪24	٪23.4	٪33.9	٪14.1	٪33.9	%56.1	%6.8	%2.7	%0.5

تبين لنا من خلال النتائج الجدول رقم(5) أن التجربة كان لها تأثير واضح ومباشر في إجابات أفراد العينة وحل مشكلة اللبس بين المفهومين فكانت النتائج تبين أن هناك 90٪ من أفراد العينية أصبحوا قادرين على التفريق بين مفهومي الأمن السيبراني وأمن المعلومات، فقد وضحت الاستجابات القبلية للاستبانة أن هناك فئة كبيرة من العينة لا تستطيع التفريق بين مفهومي الأمن السيبراني وامن المعلومات وذلك بحسب النتائج القبلية التالية: حيث بلغت نسبة موافق بشدة وموافق 28.7٪ وهذه نسبة منخفضة بالنسبة لغير موافق حيث بلغت نسبة غير موافق وغير موافق بشدة 48٪ وهذا يعني أن هناك 48٪ من أفراد العينية 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 نسب عدم الموافقة فقد بلغت نسبة موافق بشدة وموافق بعد التجربة 90٪ وهذه نسبة كبيرة جدا، بينما انخفضت نسبة غير موافق وغير موافق بشدة إلى 3.3٪ . وذلك يدل على دور التجربة الفعال في زيادة الوعي بمفهوم الأمن السيبراني وأمن المعلومات حيث تبين لهم بأمن المفهومين يتقفان باهتمامهما بالمعلومات الرقمية بينما الاختلاف أن الأمن السيبراني يتعلق بتأمين الأشياء المعرضة للخطر من خلال تكنولوجيا المعلومات والاتصالات وأمن المعلومات هو كل شيء عن حماية المعلومات التي تركز 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 القبلية					الاستجابة البعدية				
	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
لدي معرفة بالجرائم السيبرانية ؟	15	62	39	59	17	87	86	12	3	1
	%7.8	%32.3	%20.3	%30.7	%8.9	%46	%45.5	%6.4	%1.6	%0.5
لدي معرفة بمفهوم التصيد الالكترونية؟	15	54	33	67	23	70	106	7	4	2
	%7.8	%28.1	%17.2	%35	%12	%37	%56.1	%3.7	%2.1	%1.1

	الاستجابة القبلية					الاستجابة البعدية				
	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
لدي معرفة بمفهوم الهندسة الاجتماعية؟	10	34	30	83	35	64	101	17	5	2
	%5.2	%18.7	%15	% 43	%18.2	%33.9	%53.4	%9	%2.7	%1.1
لدي معرفة بمخاطر فتح روابط ومرفقات البريد الالكتروني؟	53	94	17	15	13	91	90	4	3	1
	%27.6	%49	%8.9	%7.8	%6.7	%48.1	%47.6	%2.1	%1.6	%0.5
لدي معرفة بالإجراءات اللازمة لحماية حاسبي من الاختراق؟	22	74	38	22	14	82	97	5	3	2
	%12.9	%43.5	%22.4	%12.9	%8.2	%43.4	%51.3	%2.7	%1.6	٪1.1
تحد ثقافة الأمن السيبراني من التجسس والتخريب الالكتروني على مستوى المجتمع؟	42	108	24	15	3	88	91	7	0	3
	%21.9	%56.3	%12.5	%7.8	%1.6	%46.6	%48.2	%3.7	٪٠,٠	٪1.6
لدي معرفة تامة بمخاطر تنزيل البرامج من الإنترنت؟	37	87	28	30	10	87	87	11	3	1
	%19.3	%45.3	%14.6	%15.6	%5.2	%46	%46	%5.8	%1.6	%0.5

- حسب النتائج الموضحة في الجدول (7) تبين لنا أن عينة الدراسة لمن يكن لديها الوعي الكافي بالجرائم السيبرانية حيث أن جزء بسيط من العينة القبلية لديها وعي لابأس به حيث بلغت موافق بشدة وموافق بنسبة 40.1 ٪ ومحايد بنسبة 20.3٪ وغير موافق وغير موافق بشدة 39.6٪، والنتائج البعدية تظهر لنا ازدياد وعي عينة الدراسة بمفهوم الجرائم السيبرانية حيث بلغت موافق بشدة وموافق 91.5٪ ومحايد بنسبة 6.4٪ وغير موافق وغير موافق بشدة بنسبة 1.5٪ وذلك يدل على نجاح التجربة بعد أن تم تعريفهم بأن الجرائم السيبرانية هي الاستخدام غير المشروع للتكنولوجيا بقصد التدمير والتعدي على ممتلكات الغير من خلال الأجهزة وما تحتويه من معلومات، وتعريفهم بأنواعها، وأصناف المجرمين في الفضاء السيبراني.
- أظهرت النتائج القبلية بالنسبة لسؤال لدي معرفة بمفهوم التصيد الإلكتروني أن جزء بسيط من العينة لديها معرفة بمفهوم التصيد الإلكتروني حيث بلغت نسبة موافق بشدة وموافق 39.9٪ ومحايد 17.2٪ وغير موافق وغير موافق بشدة 47٪،وتظهر النتائج البعدية

أن جزء كبير من عينة الدراسة أصبح لديهم وعي كافي بمفهوم التصيد الإلكتروني حيث بلغت موافق بشدة وموافق بنسبة 93.1٪ ومحايد بنسبة 3.7٪ وغير موافق وغير موافق بشدة 3.2٪،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 أيضا بأشكالها.

- بينت النتائج القبلية الخاصة بسؤال لدي معرفة بمفهوم الهندسة الاجتماعية بأن عينة الدراسة ليس لديها وعي كافة بهذا المفهوم حيث بلغت موافق بشدة وموافق بنسبة 23.9٪ ومحايد بنسبة 15٪ وغير موافق وغير موافق بشدة بنسبة 61.2٪،والنتائج البعدية تظهر لنا مدى نجاح التجربة في زيادة وعيهم بمفهوم الهندسة الاجتماعية حيث بلغت موافق بشدة وموافق 87.3٪ ومحايد بنسبة 9٪ وغير موافق وغير موافق بشدة 3.8٪ ؛وذلك بعد أن تم تعريفهم بأن الهندسة الاجتماعية عملية يتم من خلالها خداع الناس وحصول المتسلل على معلومات خاصة وسرية تفيد المتسلل بطريقة ما، وتعريفهم بمراحل الهجوم،وطرق الحماية.
- أوضحت النتائج القبلية لسؤال لدي معرفة بمخاطر فتح روابط ومرفقات البريد الإلكتروني بأن عينة الدراسة لديها وعي كافي بمخاطر فتح الروابط ومرفقات البريد الالكتروني وذلك بسبب التوعية من قبل البنوك وشركات الاتصال والجامعات ورسائل التوعية المتداولة من قبل الأشخاص الذين وقعوا ضحية فتح روابط غير أمنه أو قريب لهم عبر مواقع التواصل الاجتماعي وقيامهم بتنبيه الأخرين وتحذيرهم من خلال صوت أو مقطع فيديو أو رسالة نصية عن خطورة فتح أي روابط غير أمنه حيث بلغت موافق بشدة وموافق 76.6٪ ومحايد بنسبة8.9٪ وغير موافق وغير موافق بشدة بنسبة 14.5٪،وفي النتائج البعدية تم توعية الجزء المتبقي من العينة التي لم يكن لديها الوعي الكافي حيث بلغت موافق بشدة وموافق بنسبة 95.7٪ ومحايد بنسبة 2.1٪ وغير موافق وغير موافق بشدة 2.1٪.
- أظهرت النتائج القبيلة لسؤال لدي معرفة بالإجراءات اللازمة لحماية حاسبي من الاختراق أن أكثر من نصف العينة لديها وعي جيد بحماية حاسباتهم من الاختراقات حيث بلغت

موافق بشدة وموافق نسبة 56.4٪ ومحايد بنسبة 22.4٪ وغير موافق وغير موافق بشدة 21.1٪ ،وفي النتائج البعدية زاد وعيهم بعد تعريفهم بالبرمجيات التي تساعدهم على حماية أجهزتهم من الاختراقات حيث بلغت موافق بشدة وموافق نسبة 94.7٪ ومحايد 2.7٪ وغير موافق وغير موافق بشدة 2.7٪.

- 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 78.2٪ ومحايد 12.5٪ وغير موافق وغير موافق بشدة 9.4٪ ،وبعد القيام بالتجربة وضحت النتائج البعدية ازدياد اتفاقهم على هذه العبارة حيث بلغت موافق بشدة موافق 94.8٪ ومحايد 3.7٪ وغير موافق وغير موافق بشدة 3.7٪.
- بينت النتائج القبلية الخاصة لسؤال لدي معرفة تامه بمخاطر تنزيل البرامج من الإنترنت أن عينة الدراسة لديها وعي جيد بمخاطر تنزيل البرامج من الإنترنت حيث بلغت موافق بشدة وموافق نسبة 64.6٪ ومحايد 14.6٪ وغير موافق وغير موافق بشدة 20.8٪ ،وفي النتائج البعدية زاد وعيهم أكثر بالمخاطر حيث بلغت نسبة موافق بشدة وموافق بنسبة 92٪ ومحايد 5.8٪ وغير موافق وغير موافق بشدة 2.1٪.

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

الجدول رقم (8) مدى معرفة طالبات كلية الآداب والعلوم الإنسانية لحماية أنفسهم من الاختراقات السيبرانية

	الاستجابة القبلية					الاستجابة البعدية				
	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
اتجنب وضع البيانات والصور الشخصية على مواقع التواصل الاجتماعي الا للضرورة؟	59	87	26	14	6	104	74	6	4	1
	%30.7	%45.3	%13.5	%7.3	%3.1	%64.2	%29	%3.7	%2.4	%0.6

	الاستجابة القبلية					الاستجابة البعدية				
	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
احتفظ بأرقامي السرية في المتصفح؟	20	74	33	45	20	28	45	16	50	50
	%10.4	%38.5	%17.2	%23.4	%10.4	%14.8	%23.8	%8.5	%26.5	%26.5
استخدم نفس كلمة المرور لجميع مواقع التواصل الاجتماعي والبريد الالكتروني؟	22	65	26	48	31	19	44	17	56	53
	%11.5	%33.9	%13.5	%25	%16.2	%10.1	%23.3	%9	%29.6	%28
أقوم بقراءة شروط وتعليمات المستخدم لبرنامج مجاني قبل الضغط على موافق؟	30	85	28	37	12	93	80	13	2	1
	%15.6	%44.3	%14.6	%19.8	%6.3	%49.2	%42.3	%7.9	%1.1	%0.5
استخدم برنامج الحماية من الفيروسات بصورة مستمرة؟	27	75	37	40	13	86	84	12	3	4
	%14.1	%39.1	%19.3	%20.8	%6.8	%46	%44.5	%6.4	%1.6	%2.1
افتح رسالة الكترونية غير معروفة لدي؟	10	35	26	68	53	15	27	10	50	87
	%5.2	%18.2	%13.5	%35.4	%27.6	%7.9	%14.3	%5.2	%26.5	%46
أقوم بالتخلص من رسائل البريد مجهولة المصدر دون فتحها؟	40	85	35	26	6	90	78	14	4	3
	%20.8	%44.3	%18.2	%13.5	%3.1	%47.6	%41.3	%7.4	%2.1	%1.6
أحرص على استخدام متصفح امن للإنترنت؟	59	96	24	9	4	105	77	4	1	2
	%30.7	%50	%12.5	%4.7	%2.1	%55.6	%40.7	%2.1	%0.5	%1.1
احذر كثيرا عند الاتصال بالشبكات العامة؟	44	87	31	25	5	100	78	6	4	1
	%22.9	%45.3	%16.2	%13	%2.6	%52.9	%41.3	%3.2	%2.1	%0.5
ابتعد عن مشاركة معلوماتي الشخصية مع الغرباء على الانترنت	87	77	19	3	6	120	64	4	1	0
	%45.3	%40.1	%9.9	%1.6	%3.1	%63.5	%33.9	%2.1	%0.5	٪0.0

	الاستجابة القبلية					الاستجابة البعدية				
	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
افحص جهازي الآلي بصورة مستمرة؟	31	82	46	25	8	99	76	10	4	0
	%16.2	%42.7	%24	%13	%4.2	%52.4	%40.2	%5.3	%2.1	٪0.0
اعرف بمن اتصل في حال حدوث اختراق؟	26	65	25	51	25	97	79	9	2	2
	%13.5	%33.9	%13	%26.6	%13	%51.3	%41.8	%4.8	%1.1	%1.1
أقوم بتحديث نظام التشغيل بصورة دورية؟	28	87	39	25	13	91	88	7	3	0
	%14.6	%45.3	%20.3	%13	%6.8	%48.2	%46.6	%3.7	%1.6	٪0.0
اختار كلمة مرور مكونة من ارقام وحروف ورموز؟	73	83	17	13	6	114	64	7	3	1
	%38	%43.2	%8.9	%6.8	%3.1	%60.3	%33.9	%3.7	%1.6	%0.5
أترك الحساب او النظام مفتوح بدون تسجيل خروج عند المغادرة؟	12	45	25	66	44	20	33	8	46	82
	%6.3	%23.4	%13	%34.4	%22.9	%10.6	%17.5	%4.2	%24.3	%43.4
اهتم بتطوير مهاراتي وزيادة معارفي بالآليات المناسبة لتحقيق الأمن السيبراني وطرق الوقاية من المشاكل السيبرانية	28	94	45	17	8	82	96	8	2	1
	%14.6	%49	%23.4	%8.9	%4.2	%43.4	%50.8	%4.2	%1.1	%0.5

من خلال الجدول رقم (8) 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 مواقع التواصل الاجتماعية إلا للضرورة، وعي جزء كبير من عينة الدراسة في عدم وضع بياناتهم وصورهم على مواقع التواصل الاجتماعي إلا للضرورة حيث بلغت موافق بشدة وموافق نسبة 76٪ ومحايد نسبة 13.5٪ وغير موافق وغير موافق بشدة 10.4٪،ووضحت النتائج

البعدية ازدياد وعيهم حيث بلغت موافق بشدة وموافق نسبة 93.2٪ ومحايد نسبة 3.7٪ وغير موافق وغير موافق بشدة 3٪.

- بينت النتائج القبلية لسؤال احتفظ بأرقامي السرية في المتصفح على أن نسبة كبيرة تقوم بحفظ أرقامها السرية على المتصفح وجهلهم بالمخاطر التي قد يتعرضون لها حيث بلغت نسبة موافق بشدة وموافق 48.9٪ ومحايد 17.2٪ وغير موافق وغير موافق بشدة 33٪، وبينت النتائج البعدية ازدياد وعي البعض والبعض الأخر أصر على أن يحتفظ بأرقامه السرية في المتصفح رغم تعريفهم بالمخاطر حيث بلغت موافق بشدة وموافق نسبة 38.6٪ ومحايد نسبة 8.5٪ وغير موافق وغير موافق بشدة بنسبة 53٪.
- أظهرت النتائج القبلية لسؤال استخدم نفس كلمة المرور لجميع مواقع التواصل الاجتماعي والبريد الإلكتروني بأن نصف عينة الدراسة تقريبا تقوم باختبار كلمة سر واحده لجميع مواقعها حيث بلغت موافق بشدة وموافق نسبة 45.4٪ ومحايد بنسبة 13.5٪ وغير موافق وغير موافق بشدة 41.2٪،وأظهرت النتائج البعدية بازدياد وعي البعض حيث أنهم سوف يقومون باختيار كلمات مرور مختلفة لكل موقع والبعض الأخر أصروا على استخدام نفس كلمة السر لجميع المواقع رغم المخاطر التي قد تصيبهم فقد بلغت نسبة موافق بشدة وموافق 33.4٪ ومحايد بنسبة 9٪ وغير موافق وغير موافق بشدة 57.6٪.
- 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 59.9٪ ومحايد بنسبة 14.6٪ وغير موافق وغير موافق بشدة 26.1٪، ووضحت النتائج البعدية ازدياد وعي البقية حيث بلغت نسبة موافق بشدة وموافق بنسبة 91.5٪ ومحايد بنسبة 7.9٪ وغير موافق وغير موافق بشدة بنسبة 1.6٪.
- بينت النتائج القبلية لسؤال استخدم برنامج الحماية من الفيروسات بصورة مستمرة بأن نصف العينة تقريبا لديها وعي واهتمام باستخدام برامج حماية حيث بلغت موافق بشدة وموافق نسبة 53.2٪ ومحايد نسبة 19.3٪ وغير موافق وغير موافق بشدة 27.6٪، وبينت النتائج البعدية بازدياد وعيهم أكثر بضرورة استخدام برنامج للحماية ضد الفيروسات

حيث زادت نسبة موافق بشدة وموافق بنسبة 90.5٪ وانخفضت كلا من محايد بنسبة 6.4٪ وغير موافق وغير موافق بشدة 3.7٪.

- أظهرت النتائج القبلية لسؤال افتح رسائل إلكترونية غير معروفة بأن عينة الدراسة لديهم وعي حيث بلغت موافق بشدة وموافق بنسبة 23.4٪ ومحايد بنسبة 13.5٪ وغير موافق وغير موافق بشدة 63٪، وأظهرت النتائج البعدية زيادة وعي العينة حيث بلغت موافق بشدة وموافق 22.2٪ ومحايد بنسبة 5.2٪ وغير موافق وغير موافق بشدة ارتفعت بنسبة 72.5٪.
- 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 65.1٪ وغير موافق وغير موافق بشدة 16.6٪ ومحايد بنسبة 18.2٪، ولكن بعد إجراء التجربة لوحظ ارتفاع نسبة وعي أفراد العينة حيث بلغت النتائج البعدية موافق بشدة وموافق 88.9٪ وغير موافق وغير موافق بشدة 3.7٪ ومحايد بنسبة 7.4٪ .
- توصلت النتائج القبلية لسؤال أحرص 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 80.7٪ وغير موافق وغير موافق بشدة بنسبة ضئيلة بلغت 6.8٪ ومحايد بنسبة 12.5٪، وبعد تطبيق التجربة ارتفعت نسبة الوعي لدى أفراد العينية حيث بلغت نسبة موافق بشدة وموافق 96.3٪ وغير موافق وغير موافق بشدة انخفضت إلى 1.6٪ ومحايد بنسبة 2.1٪ .
- توضح نتائج سؤال احذر كثيرا عند الاتصال بالشبكات العامة إلى أن هنا زيادة في وعي أفراد العينة بعد التجربة، وهذا ما وضحته النتائج التالية قبل التجربة بلغت نسبة موافق بشدة وموافق 68.2٪ وغير موافق وغير موافق بشدة نسبة 15٪ ومحايد بنسبة 16.2٪، وكما هو متوقع بعد إجراء التجربة ارتفعت نسبة الوعي حيث بلغت موافق بشدة وموافق 94.2٪ وغير موافق وغير موافق بشدة 2.6٪ ومحايد بنسبة 3.2٪ .
- وضحت النتائج القبيلة لسؤال أبتعد عن مشاركة معلوماتي الشخصية مع الغرباء على الإنترنت أن جزء كبير من أفراد العينة كان لديهم وعي مسبق وذلك قبل تطبيق التجربة

حيث بلغت موافق بشدة وموافق بنسبة 85.4٪ بينما غير موافق وغير موافق بشدة بلغت 4.7٪ ومحايد بنسبة 9.9٪، وبعد تطبيق التجربة قد زاد الوعي لدى أفراد العينة بنسبة 97.4٪.

- توضح النتائج القبلية لسؤال أفحص جهازي الآلي بصورة مستمرة أنه كانت هناك نسبة وعي متوسطة إلى حد ما حيث بلغت نسبة موافق بشدة وموافق 58.9٪ وغير موافق وغير موافق بشدة 17.2٪ ومحايد بنسبة 24٪ ومن خلال هذا نستنتج وجود فئة بحاجة إلى التوعية، وبعد إجراء التجربة ازدادت نسبة الوعي بشكل كبير حيث بلغت موافق بشدة وموافق 92.6٪ وغير موافق وغير موافق بشدة بنسبة 2.1٪ ومحايد بنسبة 5.3٪.
- توضح النتائج لسؤال أعرف بمن أتصل في حال حدوث اختراق أن هناك تفاوت في درجة الوعي لدى أفراد العينة قبل التجربة حيث بلغت نسبة موافق بشدة وموافق قبل التجربة 47.4٪ وغير موافق وغير موافق بشدة 39.6٪ ومحايد بنسبة 13٪ وهذه نسب تحتاج إلى التوعية، وبعد تطبيق التجربة ارتفعت نسبة الوعي بشكل كبير لتصل إلى 93.1٪ وغير موافق وغير موافق بشدة انخفضت لتصل إلى 2.2٪ ومحايد بنسبة 4.8٪.
- 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 59.9٪ وغير موافق وغير موافق بشدة 19.8٪ ومحايد بنسبة 20.4٪ . وبعد إجراء التجربة زادت نسبة الوعي لدى أفراد العينة، حيث بلغت النتائج البعدية للتجربة موافق بشدة وموافق 94.8٪ وهذا يوضح مدى ارتفاع نسبة الوعي بينما انخفضت نسب عدم الموافقة لتصل إلى 1.6٪ ومحايد بنسبة 3.7٪.
- 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 81.2٪ ونسبة ضئيلة ليس لديهم الوعي بكلمة المرور المناسبة حيث بلغت نسبة غير موافق 9.9٪ ومحايد بنسبة 8.9٪، وبعد إجراء التجربة ارتفعت نسبة الوعي حيث بلغت موافق بشدة وموافق 94.2٪ وانخفضت نسبة غير موافق وغير موافق بشدة لتصل إلى 2.1٪ ومحايد بنسبة 3.7٪ .

- توضـح النتائج لسـؤال أترك النظام مفتوح بدون تسـجيل خروج عند المغادرة أن هناك زيادة في الوعي بعد إجراء التجربة مقارنة بقبل بدء التجربة حيث بلغت النتائج القبلية موافق بشـدة وموافق 29.7٪ وغير موافق وغير موافق بشـدة 57.4٪ ومحايد بنسـبة 13٪، وبعد تطبيق التجربة بلغت النتائج كالتالي موافق وموافق بشـدة 28.2٪ وغير موافق وغير موافق بشـدة ارتفعت لتصـل إلى67.7٪ وهذه النسـب تدل على زيادة الوعي لدى أفراد العينة بعد التجربة .
- توضـح النتائج القبلية لسـؤال أهتم بتطوير مهاراتي وزيادة معارفي بالآليات المناسـبة لتحقيق الأمن السيبراني وطرق الوقاية أن هناك نسبة جيدة في اهتمامهم (أفراد العينية) بتطوير مهاراتهم حيث بلغت النتائج القليلة موافق بشدة وموافق 63.6٪ وغير موافق وغير موافق بشـدة 13.1٪ وبلغت نسبة محايد نسبة لابأس بها حيث كانت 23.4٪، وبعد تطبيق التجربة ارتفعت نسبة اهتمامهم بتطوير مهاراتهم لتصل إلى 93.2٪ بينما انخفضت نسب عدم الموافقة بشكل كبير ومحايد لتصل إلى 4.2٪ .

الخاتمة:

الحمدالله رب العالمين بتوفيق من الله عز وجل أتممنا ختام بحثنا هذا الذي تحدثنا فيه باسـتفاضـة عن فعالية برنامج تدريبي مقترح لتنمية الوعي بالأمن السـيبراني لدى طالبات كلية الآداب والعلوم الإنسـانية حيث يعد من الأسـس التي ينبغي أن يتم معرفتها والعمل على توعية المؤسسات التعليمية بها والتعرف على الأمور التي يجب أن يتم إدراكها لتجنب الوقوع بالمخاطر وذلك يكون عبر تعزيز الوعي لجميع الاشـخاص في المؤسـسـات التعليمية من أجل التركيز على هذا المجال وتقديم كافة الوسـائل بمختلف أشـكالها التي من شـأنها أن تعمل على نشـر أهمية ودور الأمن السيبراني بشكل أفضل حيث تم الاستشهاد بالعديد من مصادر المعلومات التي من شـأنها أن تكون دليلاً لمن يبحث عن هذا الموضـوع و نسـأل رب العالمين أن يجعل هذا البحث سـبيلًا لنا للتخرج من الجامعة ونسـأل الله أن نكون قد وفقنا في انتقاء الموضـوع والحديث عنه وبيان كل ما يتعلق به ونسـأله أن يكون هذا البحث نافعا لكل الباحثين والمهتمين بهذا المجال الواسع.

النتائج:

- **فيما يخص الجانب النظري:**

1. 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 اختراق 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 آمنه.
2. يستدل من نتائج الدراسة ضرورة تعاون مختلف الجهات والمؤسسات في الدولة للعمل في منظومة وطنية متكاملة للحد من مخاطر الجرائم ومواجهتها والعمل على نشر التوعية والتصرف الصحيح عند مواجهة إحدى أنواع الجرائم والسعي إلى تقليل أثرها لأنها تشكل خطورة كبيره على المعلومات وتعرض الأنظمة للمشاكل التقنية كما أن الهدف الأساسي من تلك الجرائم هو تحقيق الربح المادي واستخدام البيانات الشخصية بصوره غير قانونية والحصول على المعلومات السرية والمهمة.
3. توضح لنا من نتائج الدراسة أن بعض الجامعات السعودية قامت بتوفير إدارات للأمن السيبراني حيث تسعى الجامعة إلى توفير بيئة آمنه وموثوقة 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.

- **فيما يخص الجانب العملي:**

1. كشفت النتائج أن أعلى استجابة من قسم الاتصال والاعلام بنسبة 17.7٪، وأقل استجابة من قسم المعلومات ومصادر التعلم بنسبة 11.5٪.
2. كشفت النتائج أن الغالبية العظمى للاستجابات من الطالبات بالمستوى الثاني بنسبة 45.8٪، كما تراوحت الأعمار الأكثر استجابة من عمر 21 إلى 30 بنسبة 61.5٪ .

3. يستدل من نتائج البرنامج التدريبي أن الغالبية العظمى من طالبات كلية الآداب والعلوم الإنسانية لم يكن لديهم معرفة سابقة بالأمن السيبراني حيث بلغت النسبة 38٪ وبعد تقديم البرنامج التدريبي تبين لنا مدى استفادة عينة الدراسة منها حيث بلغت النسبة 84.8٪.
4. كشفت النتائج أن التعريف الأكثر اتفاقا من قبل عينة الدراسة في الاستبيان القبلي كان هناك اتفاق نسبة كبيره من عينة الدراسة على المفاهيم الثلاثة وبعد تقديم البرنامج التدريبي لوحظ أن المفهومين الخاصة بالوسائل التقنية والمستخدمين حصلت على نسبة بين 90٪ و 95٪.
5. يستدل من النتائج أن عينة الدراسة اتفقت على احتياجهم لدورات تدريبية في مجال الأمن السيبراني بنسبة 80٪ في الاستبيان القبلي أما بالنسبة لمدى احتياجهم للدورات التدريبية في الاستبيان البعدي بلغت النسبة 84,1٪ مما يوضح زيادة وعي الطالبات وحرصهم على الالتحاق بالدورات والبرامج التدريبية.
6. 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 48٪ أما بعد تقديم البرنامج التدريبي وتوضيح الفرق بين المصطلحين تمكنت عينة الدراسة من التفريق بين أمن المعلومات والأمن السيبراني حيث بلغت النسبة 90٪ مما يدل على فعالية البرنامج التدريبي في زياده الوعي لدى الطالبات وتوضيح الفوق بين المفهومين.
7. تبين لنا من نتائج البرنامج التدريبي أن عينة الدراسة لم تكن لديها المعرفة الكافية بمفهوم الجرائم المعلوماتية حيث بلغت النسبة في الاستبيان القبلي 39.6٪ أما بعد تقديم الدورة التدريبية بلغت النسبة في الاستبيان البعدي 91.5٪ مما يدل على زيادة الوعي لدى عينة الدراسة.
8. يستدل من النتائج أن عينة الدراسة لم يكن لديها الوعي الكافي بمفهوم التصيد الإلكتروني حيث بلغت النسبة 39.9٪ في الاستبيان القبلي وبعد تقديم الدورة زاد وعيهم وبلغت النسبة 93.1٪ في الاستبيان البعدي.

9. كشفت نتائج الدراسة فيما يخص مفهوم الهندسة الاجتماعية بأن عينة الدراسة لم يكن لديها الوعي الكافي بالمفهوم حيث بلغت النسبة 23.9٪ في الاستبيان القبلي وأما في الاستبيان البعدي بلغت النسبة 87.3٪ مما يدل على زيادة وعيهم بهذا المفهوم.
10. كشفت لنا نتائج البرنامج التدريبي فيما يخص المعرفة بخطورة تنزيل البرامج من الإنترنت أن عينة الدراسة لديهم وعي لا بأس به حيث بلغت النسبة في الاستبيان القبلي 76.6٪ ،ولكن في الاستبيان البعدي تزايد وعي العينة بشكل كبير وأصبح لديهم وعي كافي حيث أصبحت النسبة 95.7٪.
11. أوضحت نتائج الدراسة فيما يتعلق بسؤال عينة الدراسة حول المعرفة الكافية بمخاطر فتح روابط ومرفقات البريد الالكتروني أن عينة الدراسة لديهم وعي كافي حول هذه المخاطر الناتجة وما تؤدي إليه من أضرار حيث بلغت النسبة في الاستبيان القبلي 76,6٪، وبعد تقديم البرنامج التدريبي ارتفعت نسبة الوعي إلى 95.7٪.
12. استعرضنا في البرنامج التدريبي 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 متفاوت في مدى الوعي حيث بلغت النسبة في الاستبيان القبلي وقبل إجراء التجربة 47.4٪ وبعد تقديم البرنامج التدريبي ارتفعت نسبة الوعي الى 93.1٪.
13. كشفت النتائج فيما يتعلق بسؤال احذر كثيرا عند الاتصال بالشبكات العامة أن نسبة كبيرة من عينة الدراسة كان لديها وعي حيث بلغت ٦٨,٢٪ في الاستبيان القبلي وبعد تقديم البرنامج التدريبي زاد وعي البقية حيث بلغت النسبة 94.2٪ في الاستبيان البعدي.
14. يستدل من النتائج فيما يخص سؤال استخدم برنامج الحماية من الفيروسات بأن نصف عينة الدراسة لديها وعي حيث بلغت النسبة 53.2٪ في الاستبيان القبلي وبعد تقديم الدورة وتعريفهم على برامج الحماية زادت نسبة الوعي بنسبة 90.5٪.

التوصيات:

1. تقديم برامج تدريبية للطالبات لتوعيتهم بالأمن السيبراني.
2. إضافة مواد تعليمية متعلقة بالأمن السيبراني .

3. تقديم الدعم والتحفيز لزيادة إعداد البحوث والدراسات المتعلقة بالأمن السيبراني.
4. تحسين وعي الطالبات لتهيئتهم على مقاومة الجرائم في الفضاء السيبرانية بكافة أنواعها عن طريق عقد الدورات والبرامج التدريبية.
5. إقامة وورش عمل داخل الجامعة لتوعية الطالبات وأعضاء هيئة التدريس حول كيفية مواجهة مخاطر الأمن السيبراني .
6. نشر ثقافة الوعي بأهمية الأمن السيبراني وانه افضل الطرق لحماية الاجهزة والبيانات.
7. إنشاء مراكز إبلاغ واستجابة لحالات الطوارئ الخاصة بالأجهزة الإلكترونية.
8. تطوير أنظمة الجامعات التقنية، التي تمنع وصول العابثين والمخترقين لأنظمة الجامعات وحمايتها.
9. متابعة التطوير في البنى التحتية داخل الجامعات ومواكبة التكنولوجيا الجديدة.
10. ضرورة قيام إدارة الجامعات بعقد مناقشات وحوارات مع المختصين بالأمن السيبراني لمعرفة أحدث التطورات.
11. الاهتمام بالدمج بين الجانب النظري والجانب العملي في إعداد البرامج التدريبية.
12. استقطاب مؤهلين ومختصين في مجال الأمن السيبراني في الجامعات.
13. تفعيل دور الإدارات بالأمن السيبراني وتفعيل دورها في توعية طلبة الجامعة بالأمن السيبراني.
14. ضرورة إدراج مقرر الأمن السيبراني ضمن الخطط التدريسية لبرامج علم المعلومات.
15. تشجيع مجالات البحث العلمي والابتكار في مجال الأمن السيبراني.
16. تشجيع المؤسسات غير الحكومية العاملة في هذا المجال وتشجيع الاستثمار في تخصصات الأمن السيبراني.
17. تطوير المهارات وإعداد الكادر البشري لمجابهة أخطار الفضاء السيبراني وتوفير الأمن الكافي له لسد الفجوة بين القدرات الحالية والمستقبلية.
18. تطوير سبل تفعيل وتحسين أداء الوسائل الدفاعية الموجودة لحماية الفضاء السيبراني حالياً والتحقق من أدائها بشكل متقن .
19. الاعتماد على سياسات مرنة يمكن تغيرها وتطويرها لتحقيق الأمن وحماية الأجهزة والتقنيات والشبكات في الجامعات.

المراجع

المراجع العربية:

ال مسعود، علي يحيى (2020). الأمن السيبراني والياته في الحد من السلوكيات الانحرافية للاحداث في المملكة العربية السعودية:دراسة نظرية تحليلية.

أبو حسين، حنين جميل، و الحنيطي، مأمون أحمد راشد (2021). *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.(2019). 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 مواقع التصيد الإلكتروني . المجلة العربية الدولية للمعلوماتية، مج ٥، ع٩.

أحمد، عبدالخالق محمد. (2014). الهندسة الإجتماعية. *المال والاقتصاد: بنك فيصل الاسلامي السوداني*، ع*75*، 22 - 23. مسترجع من

http://search.mandumah.com.sdl.idm.oclc.org/Record/630305

البابلي. عمار ياسر محمد زهير (2021). التحديات الأمنية المعاصرة للهجمات السيبراني.

بيومي،عبدالفتاح (2007). مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت،مصر:دار الكتب القانونية.

جبور، منى الأشقر (2016). السيبرانية هاجس العصر. لبنان:جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية.

الجمل،حازم (2020).الحماية الجنائية للأمن السـيبراني في ضـوء رؤية 2030.مجلة البحوث الأمنية.

الجندي،علياء بنت عبدالله إبراهيم (2019). دور الممارسة التطبيقية للامن السيبراني في تنمية المهارات ودقة التطبيق العملي للامن المعلوماتي لدى طالبات الجامعة.

الخضري، جيهان سعد محمد، سلامي، هدى جبريل علي، و كليبي، نعمة ناصر مدبش. (٢٠٢٠). الأمن السـيبراني والذكاء الاصـطناعي في الجامعات السـعودية: دراسـة مقارنة. مجلة تطوير الأداء الجامعي: جامعة المنصـورة - مركز تطوير الأداء الجامعي، مج١٢، ع١، ٢١٧ - ٢٣٣. مسترجع من

http://search.mandumah.com.sdl.idm.oclc.org/Record/1154097

رباعية، عبداللطيف محمود (2016) . الجرائم الإلكترونية،التجريم والملاحقة والإثبات، مقدم إلى المؤتمر الأول للجرائم الالكترونية في فلسطين، جامعة النجاح الوطنية .

الزهراني، احمد (مايو 2014)، الهندسة الاجتماعية . الاكاديميون السعوديون . مسترجع من https://www.saudiacademics.com/article/computer-tech/item/1120

سـمحان، منى عبدالله صـالح (2020). متطلبات تحقيق الأمن السـيبراني لأنظمة المعلومات الإدارية بجامعة الملك سـعود. مجلة كلية التربية بالمنصـورة: جامعة المنصـورة - كلية التربية، ع١١١، ج١، ٢ - ٢٩. مسترجع

السواط. حمد بن حمود بن حميد (2020). العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية.

الشايع، خالد سعد (2018) الأمن السيبراني مفهومه وخصائصه وسياساتها الدار العالمية للنشر،الرياض.

الصانع، نورة عمر أحمد، عسران، عواطف سعد الدين، السواط، حمد بن حمود بن حميد، أبو عيشـة، زاهدة جميل نمر، و منصـور، إيناس محمد سـليمان علي. (٢٠٢٠). وعي المعلمين بالأمن السـيبراني وأسـاليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم

والهوية الوطنية لديهم. مجلة كلية التربية: جامعة أسـيوط - كلية التربية، مج٣٦، ع٦، ٤١ - ٩٠. مسترجع من

http://search.mandumah.com.sdl.idm.oclc.org/Record/1085483

صائغ، وفاء بنت حسن عبدالوهاب (2018). وعي أفراد الاسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الالكترونية.

الصحفي، روان عطية الله (٢٠٢٠). الجرائم السيبرانية.المجلة الإلكترونية متعددة التخصصات. ع٥٣،٢٤-١ مسترجع من

https://www.eimj.org/uplode/images/photo..الجرائم_السيبرانية/pdf

الصحفي، مصباح أحمد حامد، و عسكول، سناء بنت صالح. (٢٠١٩). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. مجلة البحث العلمي في التربية: جامعة عين شمس - كلية البنات للآداب والعلوم والتربية، ع٢٠، ج١٠، ٤٩٣ - ٥٣٤. مسترجع من

http://search.mandumah.com.sdl.idm.oclc.org/Record/1029923

الطيار، حسين بن سليمان بن راشد (2020). الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية. *مجلة جامعة الطائف للعلوم الإنسانية: جامعة الطائف، مج6، ع21*، 255 - 298. مسترجع من

http://search.mandumah.com.sdl.idm.oclc.org/Record/1061557

العتيبي، زياد بن محمد عادي (2021)، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث أشكالها، خصائصها، أركانها والدوافع من إرتكابها . المجلة الأكاديمية العالمية للدراسات القانونية، 3(1) . مسترجع من

http://iajour.com/index.php/lr/article/download/168/106

العريشي، جبريل حسن، و الدوسري، سلمى بنت عبدالرحمن بن محمد. (2018). دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع. مجلة مكتبة الملك فهد الوطنية: مكتبة الملك فهد الوطنية، مج24، ع2، 302 - 373. مسترجع من

http://search.mandumah.com/Record/947870

الفتلاوي، أحمد عبيس نعمة (2018). الهجمات السيبرانية،دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر،(ط1) . بيروت منشورات زين الحقوقية .

القحطاني، نورة بنت ناصر. (2019). مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية.

كمال، بن شايب، و عبدالرؤوف بن قيدة . (٢٠١٨) أخطار الهندسة الاجتماعية على المجتمع الإلكتروني . المركز الجامعي بوالصوف – ميلة الملتقى الوطني الثالث حول المستهلك والإقتصاد الرقمي: ضرورة الإنتقال وتحديات الحماية ٢٣و 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. (2020). 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، مج11، ع2، 71 - 84. مسترجع من

http://search.mandumah.com.sdl.idm.oclc.org/Record/1164982

محمد،هبه هاشم. (2020). برنامج مقترح قائم على جغرافية الحروب السيبرانية لتنمية الوعي بمخاطرها وتعزيز قيم المواطنة الرقمية.

مركز الأمن الإلكتروني[NCSC_SA] (2017،نوفمبر،20).رصد مركز الأمن الألكتروني هجوما إلكترونيا جديدا متقدما APT يستهدف المملكة العربية السعودية تعتمد انشطة الهجوم التي تم ملاحظتها على استخدام [نص] [تغريدة] تويتر.

مسلم، نبراس إبراهيم (2021). الجرائم السيبرانية وأثرها على الأمن السيبراني،مجلة القادسية، 12، (1). مسترجع من

https://www.iasj.net/iasj/download/a03a424a67ab7588

المطيري،مشاعل شبيب مطيران الظفيري. (2021). و اقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية.

المنتشرى، فاطمة يوسف، و حريري، رندة (2020). 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، ع١٤، ٩٥ – ١٤٠. مسترجع من

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

المنتشري،حليمة يوسف (٢٠١٩). الأمن السيبراني والمواطنة الرقمية.معهد الإدارة العامة. مسترجع من

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 (2013) . آليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري، مذكرة ماستر،كلية الحقوق، جامعة العقيد الحاج الخضر.

الهندي، رشا عبدالقادر محمد (2021). تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني.

هيئة الخبراء بمجلس الوزراء. مسترجع من

https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1

الهيئة الوطنية للأمن السيبراني [@NCA_KSA] (2018، 30 يوليو). الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة

وبرمجيات، وما تقدمه من [نص] [تغريدة].تويتر. استرجع في نوفمبر 5، 2022، مسترجع من

https//:twitter.com/nca_ksa/status/1023917241870557184?s=12

وريدة، خليلة (2021).إشـــكالية المواطنة في ظل قيم التكنولوجيا الحديثة بين حرية المواطن والأمن السيبراني. حوليات جامعة الجزائر،35(2).806-823.مسترجع من

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 والإلمام بأساسيات الأمن السيبراني وتوعية طالبات كلية الآداب والعلوم الإنسانية بخطورة الهجمات عند استخدام شبكة الانترنت ومواقع التواصل الاجتماعي ومعرفة العقوبات المترتبة عند حدوث الجرائم وأنواع المجرمين المرتكبين لها.

البيانات الشخصية للطالبة:

اسم الطالبة الثلاثي:				
العمر:	○ اقل من 20		من 21 -30	
التخصص:	○ الدراسات القرآنية	○ الاتصال والاعلام	○ اللغة العربية	○ اللغات والترجمة
	○ العلوم الاجتماعية	○ المعلومات ومصادر التعلم		○ الدراسات الاسلامية
المستوى الجامعي وفقا لخطتك الدراسية:	○ الثاني	○ الرابع	○ السادس	○ الثامن

الوعي بمفهوم الأمن السيبراني:

١-لدي معرفة سابقة بالأمن السيبراني؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٢- مفهوم الأمن السيبراني:				
	موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
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؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٤- أستطيع التفريق بين الأمن السيبراني وأمن المعلومات؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
لدي معرفة بمفهوم الهندسة الاجتماعية ؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
لدي معرفة بمفهوم التصيد الالكتروني ؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٥- لدى معرفة بكيفية التصرف في حال التعرض للاختراق؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٦- لدي معرفة بمخاطر فتح روابط ومرفقات البريد الالكتروني ؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة

٧- لدي معرفة بالإجراءات اللازمة لحماية حاسبي الشخصي من الإختراق ؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٨- لدي معرفة تامة بمخاطر تنزيل البرامج والملفات من الإنترنت ؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٩- لدي معرفة بالجرائم السيبرانية؟				
موافق	موافق بشدةً	محايد	غير موافق	غير موافق بشدة
١٠-اهتم بتغيير كلمات المرور الخاصة بدخول خدمات الإنترنت كل فترة؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
١١- تحد ثقافة الأمن السيبراني من التجسس والتخريب الإلكتروني على مستوى المجتمع؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
١٢- أحرص على الإبلاغ عن الرسائل المشكوك فيها للجهات المختصة؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
١٣- أحرص على تحميل التحديثات والبرامج الآمنه؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة

الوقاية من مخاطر الاختراق:

١-اتجنب وضع البيانات والصور الشخصية على مواقع التواصل الاجتماعي الا لضرورة؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٢- احتفظ بأرقامي السرية في المتصفح؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٣- استخدم نفس كلمة المرور لجميع مواقع التواصل الاجتماعي والبريد الإلكتروني؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٤- أقوم بقراءة شروط وتعليمات المستخدم لبرنامج مجاني قبل الضغط على أوافق؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٥- افتح رسالة الكترونية غير معروفة لدي؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٦- أقوم بعمل نسخة احتياطية للملفات المهمة؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٧- أعرف بمن اتصل في حال حدوث اختراق؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
٨- أقوم بتحديث نظام التشغيل بصورة دورية؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة

٩- اهتم بتغيير كلمة المرور بشكل منتظم؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
١٠-اختار كلمة مرور مكونة من حروف وأرقام ورموز؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
١١-اترك الحساب أو النظام مفتوح بدون تسجيل خروج عند المغادرة؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
١٢-اهتم بتطوير مهاراتي وزيادة معارفي بالآليات المناسبة لتحقيق الأمن السيبراني وطرق الوقاية من المشاكل السيبرانية؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
١٣-أقوم بالتخلص من رسائل البريد الإلكتروني مجهولة المصدر دون فتحها؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
١٤-احذر كثيرا عند الاتصال بالشبكات العامة؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
١٥-افحص جهازي الألي بصورة مستمرة؟				
موافق	موافق بشدة	محايد	عير موافق	غير موافق بشدة
١٦-ابتعد عن مشاركة معلوماتي الشخصية مع الغرباء على الإنترنت؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة
١٧-استخدم برنامج الحماية من الفيروسات بصورة مستمرة؟				
موافق	موافق بشدة	محايد	غير موافق	غير موافق بشدة

الملحق رقم(٢) الدورة التدريبية:

محاور الدورة
- الهدف من الدورة.
- تعريف الامن السيبراني.
-الفرق بين الأمن السيبراني وامن المعلومات.
- اهداف واهمية الامن السيبراني.
-عناصر الامن السيبراني.
- اثار ضعف الامن السيبراني.
- الهجمات الالكترونية وانواع البرمجيات الخبيثة.
-الجرائم السيبرانية ،وانواعها، واصناف المجرمين.
-التصيد الالكتروني واشكاله.
- 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 وتوعية طالبات كلية الأداب والعلوم الانسانية بخطورة 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
أمن المعلومات:هو كل شيء عن حماية المعلومات التي تركز بشكل عام على سرية وسلامة وتوافر المعلومات.
يهتمون بالمعلومات الرقمية
الأمن السيبراني: يتعلق بتأمين الأشياء المعرضة للخطر من خلال التكنولوجيا المعلومات والاتصالات.

اهداف الامن السيبراني :
❖ محاربة البرامج الخبيثة.
❖ اتخاذ الإجراءات والتدابير اللازمة 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.

أهمية الامن السيبراني :
❖ حفظ سلامة وسرية المعلومات والبيانات
❖ توفير بيئة امنة الكترونيا
❖ تقديم الحماية الكاملة للأجهزة والشبكات
❖ اكتشاف الثغرات والعمل على إصلاحها
❖ وضع قوانين وتشريعات لحماية الجميع
❖ حماية المجتمع من الهجمات السيبرانية

عناصر الامن السيبراني:

- السرية والأمان : التأكد من أن المعلومات لا يصل لها الا الاشخاص 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 النارية
- الأشخاص : يجب على مستخدمين النظام وضع كلمات مرور قوية وصعب تخمينها وتجانب فتح الروابط الخارجية
- الأنشطة والعمليات : توفير التقنيات والأشخاص المناسبين من أجل تطبيق

اثار ضعف الامن السيبراني :

- 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 مما يؤثر تأثيرا كبيرا على البنية التحتية لتلك المنشآت وعلى خدماتها واعمالها.
- الإرهاب والحرب السيبرانية: تعتمد الجرائم السيبرانية على تقنيات متقدمة وأجهزة تنصت وبرمجيات لفك الشفرات واختراق أنظمة أمن الشبكات وتسعى 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 والانتحال
- 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

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

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

تعريف التصيد الالكتروني:
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 .
اشكال التصيد :
❖ رسائل التصيد عبر البريد الالكتروني ورسائل تصيد البريد الالكتروني مع تحديد الهدف.
❖ التصيد الصوتي.
❖ تزوير المواقع الالكترونية .
❖ 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 النوافذ المنبثقة عند تصفح الويب.
❖ عدم نشر أي معلومات خاصة مع الأخرين على شبكة الإنترنت أو مواقع 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 غالبا مواقع 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 والاوراق المهمة بواسطة اجهزة مخصصة.

برمجيات تساعدك على مكافحة الفيروسات في حاسبك:
Kaspersky Free
Avast Free Antivirus
Bitdefender Antivirus Free Edition
PROTECTED

برمجيات تساعدك على مكافحة الفيروسات في حاسبك:
ZoneAlarm Free Antivirus
Microsoft Defender
Avira Free Antivirus

خدمة الابلاغ عن رسائل الاحتيال
سارع بالإبلاغ عنها بإعادة إرسال الرسالة النصية إلى الرقم
330330

رقم الجرائم الالكترونية في السعودية:

يُمكنكم 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 إلكترونيا من خلال الموقع الإلكتروني لوزارة الداخلية السعودية " خدمة أبشر"

قانون الجرائم الرقمية في المملكة العربية السعودية:

1-يعاقب بالسجن مدة لا تزيد عن سنه وغرامة مالية لا تزيد على خمسمائة الف ريال عند ارتكاب ما يلي:

- التنصت على ما هو مرسل عن طريق الشبكة العنكبوتية
- الدخول غير المشروع لغرض التهديد والابتزاز او التلف والتعديل
- التشهير بالأخرين والحاق الضرر بهم

2-يعاقب بالسجن مدة لا تزيد عن ثلاث سنوات وغرامة مالية لا تزيد عن مليوني ريال :

- الوصول دون مسوغ نظامي صحيح الى بيانات بنكية او ائتمانية

3-يعاقب بالسجن مدة لا تزيد عن اربع سنوات وغرامة مالية لا تزيد على ثلاث ملايين ريال:

- الدخول غير المشروع لإلغاء البيانات او حذفها
- إعاقة الوصول الى الخدمات التقنية

جهود المملكة في الامن السيبراني
الهيئة الوطنية للأمن السيبراني
الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY PROGRAMMING & DRONES
NCSC
تم انشاء الهيئة الوطنية للأمن السيبراني من منطلق أهمية البيانات والأنظمة التقنية بالإضافة الى البنى التحتية والتي لها صلة وثيقة بالشؤون الوطنية والتي لابد من توفير الحماية اللازمة لها من مخاطر وتهديدات الفضاء السيبراني
انشاء الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز في عام 2017 وذلك بهدف تنمية قدرات وامكانيات وطنية احترافية رائدة في مجال الامن .
إنشاء المركز الوطني الارشادي للأمن السيبراني وذلك بهدف تعزيز مستوى الوعي بالسيبراني والحد من المخاطر والتهديدات السيبراني وموجهة .

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 واليات العمل لمعالجة النقص في مهارات تكنولوجيا المعلومات والأمن السيبراني.
إعطاء ما يقارب 231 منحة دراسية للطلبة الذين يقرّرون دراسة تخصص الأمن السيبراني.
تدريب ما يقارب 751 موظفًا من 113 شركة، و288 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 كالاتي:
1. القيام بتوعية الطالبات بكيفية حماية البيانات الشخصية من المخاطر التي قد تعترضها
2. القيام بتوعية وتثقيف الطالبات بمختلف المخاطر المحتملة وذلك عند قيام الطالبات في عمليات البحث ومشاركة البيانات في شبكة الانترنت
3. استخدام التقنيات المختلفة والمتطورة التي تساهم في حماية البيانات والملفات وتأمينها من شتى المخاطر السيبرانية
4. القيام بزيارة التوعية فيما يتعلق بمخاطر الانترنت المختلفة من امثلتها التنمر الالكتروني ومواقع الانترنت التي تتضمن المحتوى السلبي
5. المساهمة في نشر وبث مختلف سياسيات وأنظمة الامن السيبراني والتنويه الى كل ماهو حديث وجديد وذلك بشكل دوري

2

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
nooodh741@gmail.com 3

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.