# مستوى وعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بالأمن السيبراني

# The level of awareness of students of the Faculty of Computing and Information Technology at Taif University of cybersecurity

**أ. نادية محمد جاهل العتيبي - إدارة التعليم بمحافظة العلا**

**E-mail: Nanana947@gmail.com**

**المستخلص:**

هدفت الدراسة إلى معرفة مستوى الوعي بمفاهيم الأمن السيبراني وأساليب وطرق تحقيقه، بالإضافة إلى الكشف عن الفروق بين استجابات طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف حول الوعي بأساليب وطرق تحقيق الأمن السيبراني تبعًا لمتغيرات (الدرجة العلمية، التخصص، السنة الدراسية)، وتكونت العينة من (٣٨٢) طالبة. وتم استخدم المنهج الوصفي المسحي، وبناء استبانة تكوّنت من (٢٨) فقرة موزعة على محورين.

وأظهرت النتائج بارتفاع مستوى الوعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بمفاهيم الأمن السيبراني، وأساليب وطرق تحقيقه، كذلك وجود فروق ذات دلالة إحصائية بين استجابات الطالبات حول الوعي بأساليب وطرق تحقيق الأمن السيبراني تبعًا لمتغير الدرجة العلمية لصالح طالبات البكالوريوس، ووجود فروق ذات دلالة إحصائية تبعًا لمتغير التخصص لصالح (علوم الحاسب، تقنية المعلومات، هندسة الحاسب)، بالإضافة إلى وجود فروق ذات دلالة إحصائية تبعًا لمتغير السنة الدراسية لصالح السنة (الأولى، الثالثة، الرابعة، الخامسة). وتم تقديم عدد من التوصيات في ضوء ما أسفرت عنه النتائج.

**الكلمات المفتاحية:** الأمن السيبراني، الهجمات السيبرانية، جامعة الطائف

**Abstract:**

The study aimed to know the level of awareness of the concepts of cybersecurity, and the degree of awareness of ways and methods of achieving cybersecurity for students at the College of Computers and Information Technology at Taif University, in addition to revealing the differences between the responses of students about awareness of ways and methods of achieving cybersecurity according to variables (degree, specialization, academic year), and the sample consisted of (382) students from the College of Computers and Information Technology. A descriptive survey design was utilised, and a questionnaire was designed which consisted of (28) items distributed on two domains.

The results of the study showed a high level of awareness of the concepts of cybersecurity, Methods, and ways to achieve it among students of the College of Computers and Information Technology at Taif University, There were statically significant differences between students' responses to awareness of methods and methods of achieving cybersecurity depending on the degree variable for female bachelor's students, as well as in the variable specialization in favor of specialization (CS, IT, CE), in addition to There are statistically significant depending on the variable of the academic year in favor the year (1st, 3rd, 4th, 5th). Some suggestion was made based on the results.

**Keywords:** Cybersecurity, Cyber-attack, Taif University (207 words)

**المقدمة:**

يتميز هذا العصر بالتغيرات السريعة النابعة عن التقدم العلمي والتقني، ومع ظهور الثورة الرقمية في تقنية المعلومات أصبح من الضروري مواكبة تلك التغيرات؛ للاستفادة منها ومواجهة المشكلات التي قد تنجم عنها.

حيث أدى التقدم التكنولوجي السريع بالعالم، -لا سيما من خلال استخدام الإنترنت- إلى ظهور الجرائم السيبرانية، والتي عرّضت المؤسسات والأفراد لمجموعة من المخاطر الحديثة الناتجة عن الهجمات السيبرانية، على سبيل المثال؛ هجمات حجب الخدمة (DOS) على الشبكات، واختراق البيانات للشركات والأجهزة الشخصية، والفيروسات التي يمكن أن تُعطل البُنى التحتية للكمبيوتر (Rege & Mbah, 2018).

إذ أنّ الهجمات السيبرانية تتخذ أشكالاً عديدة منها؛ البرامج الضارة وهي ملفات أو برامج تُستخدم لإلحاق الضرر بأجهزة الكمبيوتر، مثل الفيروسات المتنقلة، وفيروسات الكمبيوتر وأحصنة طروادة وبرامج التجسس. كذلك هجوم كلمات المرور التي تشكل خطرًا على المستخدم كما يعتمد هذا النوع من الهجوم على تخمين وكسر وتغيير كلمات المرور واستغلالها للدخول الغير مصرح به الى النظام (Graham et al., 2011). والهجوم بواسطة التصيد الاحتيالي (Phishing) وذلك بإرسال رسائل البريد الإلكتروني الاحتيالية التي تشبه رسائل البريد الإلكتروني الواردة من مصادر موثوقة؛ والقصد من تلك الرسائل هو سرقة البيانات الحساسة، مثل بطاقة الائتمان أو معلومات تسجيل الدخول (Rathee & Mann, 2022). علاوةً على ذلك، الهجوم بواسطة الهندسة الاجتماعية الذي يعتمد على التفاعل البشري لخداع المستخدمين لاختراق الإجراءات الأمنية من أجل الحصول على معلومات حساسة محمية عادة (صباغ، ٢٠٢١)؛ وهو ما أشارت إليه دراسة السلمي وآخرون (Alsulami et al., 2021) والتي هدفت إلى قياس الوعي بالهندسة الاجتماعية في القطاع التعليمي في المملكة العربية السعودية، وتمثلت عينتها في الطلاب والمعلمين وأعضاء هيئة التدريس والموظفين في المؤسسات التعليمية في المملكة العربية السعودية، وكان من أبرز نتائجها أن هناك اختلافات كبيرة في الممارسات والمهارات الأمنية بين المشاركين الذين لديهم معرفة بالهندسة الاجتماعية وأولئك الذين ليس لديهم معرفة بالهندسة الاجتماعية.

وعليه فقد ظهر الأمن السيبراني بهدف تقليل أو منع حدوث الانتهاكات الأمنية والعمل على استعداد المنظمات لمواجهة الهجمات السيبرانية سواءً للأفراد أو الشركات (Corallo et al., 2022)، والذي بدوره يقوم على كشف أي ثغرات أمنية أو تهديدات سيبرانية من خلال مراقبة أنظمة الكمبيوتر، وتحديد نقاط الضعف وإصلاحها (Raimundo & Rosário, 2022)، كما تقع مسؤولية الأمن السيبراني على جميع أفراد المجتمع وذلك بتطبيق الضوابط والإرشادات لحماية البرامج والشبكات، والأجهزة والأنظمة والبيانات من الهجمات الإلكترونية (Patel, 2021).

ومما لا شك فيه أنَّ هناك حاجة ملحة لتطبيق إجراءات وأساليب الحماية لكافة أفراد المجتمع في المؤسسات بمختلف أنواعها؛ للاستعداد بشكل أفضل للتهديدات والهجمات السيبرانية، ويتم ذلك من خلال تعزيز المعرفة بالأمن السيبراني، ورفع المهارات السيبرانية وبناء الكفاءات لتوفير فضاء سيبراني آمن للجميع.

وإدراكاً لأهمية تعزيز الأمن السيبراني لدى أفراد المجتمع والمؤسسات التعليمية؛ فقد تم انشاء الهيئة الوطنية للأمن السيبراني ممثلةً بالمركز الوطني الإرشادي للأمن السيبراني بتاريخ ٢٠١٧/١١/١، والتي تعمل على تعزيز جهود المملكة العربية السعودية في رفع مستوى الوعي بالأمن السيبراني، ونشر التحذيرات الدورية للثغرات الأمنية لحماية الأفراد والمنشآت والحفاظ على الأمن السيبراني الوطني، كذلك بناء شراكات محلية ودولية، والتعرّف على أفضل الممارسات في مجال التوعية بالأمن السيبراني لتفعيل البرامج التثقيفية التي تخاطب مختلف المستويات، ونشر أفضل الممارسات للتعامل مع الثغرات الأمنية (الهيئة الوطنية للأمن السيبراني، ٢٠١٨).

وسعيًا لتحقيق ذلك؛ تم إطلاق عدة مؤتمرات تعزز من المهارات السيبرانية لجميع فئات المجتمع من ضمنها مؤتمر ات هاك (Hack) الذي يُعد أضخم وأشهر حدث تقني في مجال الأمن السيبراني؛ بهدف تبادل الخبرات في مجال الأمن السيبراني، واستعراض آخر ما توصلت إليه التقنية في مجابهة التحديات المتعلقة بهذا المجال، متضمنًا مسابقات وتحديات سيبرانية، وأنشطة علمية (صحيفة سبق، ٢٠٢١).

ولذلك لابد من التأكيد على أن مسابقات الأمن السيبراني تعد من الطرق الفعالة والجذابة لتزويد الطلبة بخبرات عملية لتطبيق الأمان الرقمي في بيئات افتراضية منها مسابقة التقاط العلم Capture The Flag (CTF)، كما أنها تُقام بهدف منح الطلاب المشاركين خبرة في تأمين الأجهزة والاستجابة للهجمات السيبرانية، إضافةً إلى أنها ساهمت في إكساب الطلاب لمفاهيم الأمن السيبراني وتعزيز ثقتهم بأنفسهم، كذلك تطوير مهاراتهم السيبرانية في بيئة رقمية آمنة (Kucek & Leitner, 2020 ; Leune& Petrilli, 2017)، حيث أوضحت النتائج التي أوردها بوك وآخرون (Bock et al., 2018) بزيادة أعداد الطلاب المشاركين في مسابقة King of the Hill (KOTH) للتدريب على مهارات الأمن السيبراني الهجومية والدفاعية، والمنافسة مع الفرق الأخرى في اكتشاف الثغرات الأمنية للشبكات المستهدفة واختبار الاختراق، بالإضافة إلى أنها ساهمت في زيادة تعلم الطلاب للأمن السيبراني واكتشافهم للهجمات السيبرانية وتحديد أنواعها بدقة.

في ضوء هذه الجهود، ونظراً للأولوية العظمى التي توليها المملكة العربية السعودية للأمن السيبراني، وإدراكها بأنّه عنصر أساسي لحماية المصالح الحيوية لفضاء سيبراني آمن، فقد تم تضمين الأمن السيبراني في المؤسسات التعليمية، وفي مقدمتها الجامعات السعودية، والتي أهتمت بتدريس مواد ذات الصلة بالأمن السيبراني كالتشفير وأمن المعلومات وكيفية حماية البيانات، بالإضافة إلى تخصيص برامج في الدراسات العليا في ذلك المجال، مروراً بإنشاء الأندية الطلابية متضمنة نادي الأمن السيبراني ونادي التقنية والبرمجة، كذلك تفعيل برنامج أندية الطلبة المطورين المقدم من جوجل في الجامعات.

وأضاف على ذلك السمحان (٢٠٢٠) بأهم المتطلبات لتحقيق الأمن السيبراني والتي تتمثل في إدراج مواضيع الفضاء السيبراني ضمن المناهج الدراسية في المملكة العربية السعودية. وهذا يؤكد ما آلت عليه كريتزنجر (Kritzinger, 2017) بأنَّ هناك ضعف في مستويات الوعي بالأمن السيبراني لطلاب جنوب إفريقيا، وتُبيّن أن هذا الضعف بسبب قلة المحتوى بالمقررات الدراسية التي تتضمن مواضيع الأمن السيبراني وكيفية تحقيق طرق الحماية من التهديدات المختلفة، ويؤيد ذلك تيرومالا وآخرون (Tirumala et al, 2016) بانخفاض وعي الطلاب بما يتعلق بمفاهيم الأمن السيبراني الشائعة، وكيفية حماية أنفسهم ضد أي هجوم سيبراني.

كما بينت نتائج دراسة مي وتيك (Mai& Tick, 2021) بأن هناك تدني في مستوى وعي طلاب الجامعة بمختلف التخصصات والسنوات الدراسية بالأمن السيبراني؛ وبالتالي يؤدي ذلك إلى تدني في مستوى الوعي بالتهديدات السيبرانية.

بناءً على ما سبق؛ أكدت عدة دراسات بضرورة رفع الوعي بالأمن السيبراني لدى الطلبة، كما أوصت بتشجيعهم لتصميم وإنتاج ألعاب تعزز مفاهيم الأمن السيبراني واكتسابها (الشهراني وفلمبان، ٢٠٢٠)، وأنهم بحاجة إلى التثقيف لفهم مخاطر الحروب السيبرانية والتهديدات التي تشكلها على المجتمع، وفهم حقوقهم ومسؤولياتهم، والالتزام بالقواعد الصحيحة عند التعامل مع المحتوى الرقمي وتفعيل أساليب الأمان الشخصية عند استخدام الانترنت (محمد، ٢٠٢٠؛ Goran, 2017)

ومن هنا تتضح أهميَّة الوعي بالأمن السيبراني، وتكثيف الجهود في الدورات التدريبية للطالبات حتى تتمكن من الدفاع عن نفسها ضد أي هجوم سيبراني، والتي هي جزء أساسي من حركة التحول الرقمي، حيث ستساهم هذه الدراسة في الكشف عن مستوى الوعي بمفاهيم الأمن السيبراني، وأساليب وطرق تحقيقه لدى طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف.

وفيما يلي عرض لبعض الدراسات ذات العلاقة بموضوع الدراسة منها دراسة معلم ( Moallem, 2018) التي هدفت إلى التحقق من وعي الطلاب ومواقفهم تجاه الأمن السيبراني والمخاطر الناتجة في البيئة الرقمية، وتمثلت عينتها في طلاب وطالبات هندسة البرمجيات واستخدمت أداة الاستبيان لجمع البيانات وفق المنهج الوصفي المسحي وكان من أبرز نتائجها بأن الطلاب غير مدركين تمامًا لكيفية حماية بياناتهم، وإن مستوى استخدامهم للمصادقة الثنائية منخفض جدًا. وفي هذا السياق أُجريت دراسة غاربا وآخرون ( Garba, et.al, 2020) بهدف التحقق من وعي الطلاب بالمعرفة الأساسية للأمن السيبراني. وكانت عينتها طلبة علوم الحاسب بلغ عددهم (٢٠١)، والتي أظهرت نتائجها بوجود نقص في الوعي بشأن إدارة كلمات المرور، والتصيد الاحتيالي والمصادقة الثانية بالإضافة إلى عدم وجود برامج ذات فعالية لمعرفة مستوى الأمن السيبراني لدى الطلاب.

كذلك أجرى الجهني وآخرون (Aljohni et al, 2021) دراسة هدفت إلى قياس الوعي بالأمن السيبراني لدى طلاب الجامعات السعودية البالغ عددهم (١٣٦) طالب بمختلف التخصصات. وتم جمع البيانات من خلال استبانة وزعت عليهم. وخلصت نتائجها إلى أن هناك وعي واضح وعالي فيما يتعلق بمفاهيم الأمن السيبراني لدى طلاب أقسام الحاسب وتقنية المعلومات مقارنة بباقي التخصصات.

وفي مجال الاهتمام ذاته، قدّم أشافي وآخرون (Ashafee, et al ,2018) دراسة هدفت إلى قياس الوعي الأمني والاستعداد للهجمات الإلكترونية والسلوكيات الأمنية بين طلاب الدراسات العليا الذي يبلغ عددهم (٤٠٠) طالب بجميع الأقسام، وكان من أبرز نتائجها أنَّ طلاب تقنية المعلومات لديهم نسبة عالية بشكل ملحوظ بالوعي والسلوك الأمني مقارنة بالطلاب غير المتخصصين في تقنية المعلومات.

كما قام نديبويل وآخرون (Ndibwile et al, 2019) بدراسة هدفت إلى التحقق فيما إذا كان دور مستوى معرفة المستخدمين بالأمن السيبراني واهتمامهم وخلفيتهم السابقة لها تأثير على قدراتهم في التعرف على التصيد الاحتيالي. وفق المنهج الوصفي المسحي، وكانت أداة الدراسة استبانة لجمع البيانات لعينة من طلاب الجامعة، وتوصلت النتائج إلى أنَّ هناك تدني في مستوى الوعي بهجمات التصيد الاحتيالي لدى مستخدمي الأجهزة الذكية بالإضافة إلى وجود ضعف في المهارات السيبرانية لدى بعض المستخدمين.

أمّا دراسة طيبي وآخرون (Tibi, et al, 2019) فقد هدفت إلى قياس مستوى الوعي بالجرائم الالكترونية لدى الطلاب بمختلف التخصصات بلغ عددهم (٧٣) طالب، مستخدمة أداة الاستبانة، والتي أظهرت نتائجها بانخفاض مستوى وعي طلاب علوم الحاسب بالجرائم الالكترونية، وقدرتهم على حماية أنفسهم.

وهناك دراسة أجراها خالد وآخرون (Khalid,et al ,2018) هدفت إلى التحقق من وعي طلاب الجامعات بالأمن السيبراني حيث تمثلت عينتها في طلاب كلية التربية في أحد جامعات ماليزيا بعدد (١٤٢) طالب، واستخدمت أداة الاستبيان لجمع البيانات وفق المنهج الوصفي المسحي، وأشارت نتيجة هذه الدراسة بأنَّه على الرغم من أنَّ طلاب الجامعات من عينة الدراسة أظهروا مستوى عالٍ من الوعي بعناصر معينة في الأمن السيبراني مثل التنمر الإلكتروني والمعلومات الشخصية والخدمات المصرفية عبر الإنترنت، إلا أنه لا يزال هناك نقص في الوعي بشأن المواقع اللاأخلاقية وكيفية حماية الذات.

ويتضح من خلال عرض الدراسات السابقة أنها اتفقت جميعها على هدف واحد وهو التحقق من الوعي بالأمن السيبراني من أبعاد مختلفة، على الرغم من اختلاف عينة الدراسة؛ سواء كانت العينة من أعضاء هيئة التدريس، أو طلاب الدراسات العليا والجامعات، أو أفراد المجتمع من خارج المؤسسات التعليمية، إلا أن جميع الدراسات السابقة التي تم عرضها في هذه الدراسة لم تتطرق للكشف عن درجة الوعي بأساليب وطرق تحقيق الأمن السيبراني؛ وهو ما سوف تعمل الدراسة الحالية التطرق إليه والتعرف عليه، واختلفت الدراسة الحالية عن الدراسات السابقة في عينة الدراسة المتمثلة في طالبات التعليم العالي لكلية الحاسبات وتقنية المعلومات

بجامعة الطائف في المملكة العربية السعودية، وتم الاستفادة من الدراسات السابقة في تحديد منهجية الدراسة وتصميم وبناء الأداة، وتحديد محاورها، كذلك في تفسير ومناقشة النتائج.

**مشكلة الدراسة وأسئلتها:**

تستهدف رؤية المملكة العربية السعودية ٢٠٣٠ التنمية الشاملة للوطن والأمن والاقتصاد ورفاهية مواطنيها وتوفير الحياة الكريمة. وبطبيعة الحال، فإن أحد أهدافها هو التحول نحو العالم الرقمي وتطوير البنية التحتية الرقمية؛ بما يعبر عن مواكبة التقدم العالمي المتسارع في الخدمات الرقمية وفي الشبكات العالمية المتجددة، حيث أن هذا التحول يتطلب انسيابية المعلومات وأمانها وتكامل أنظمتها، ويستوجب المحافظة على الأمن السيبراني للمملكة العربية السعودية، وتعزيزه؛ لذلك أتى تأسيس الهيئة الوطنية للأمن السيبراني، من أجل رفع مستوى الوعي بالأمن السيبراني وتجنب مخاطر الهجمات السيبرانية National Cyber Security Authority, 2018).

ويُعدّ الوعي بالأمن السيبراني وأساليب وطرق تحقيقه قضية مهمة ومطلب ضروري؛ لامتلاك الخبرات والمهارات المعلوماتية التي تؤهل الفرد للدفاع بكفاءة وفاعلية ضد أي هجوم سيبراني، إذ مع بروز المخاطر الأمنية عبر شبكة الانترنت كان لابد من المؤسسات التعليمية أن ترفع من المستوى الثقافي لدى الطلبة بالأمن السيبراني.

وعلى صعيد البحوث العلمية فقد أكدت عدة دراسات على تدني مستوى الوعي بالأمن السيبراني لدى طلابها، وأن المؤسسات التعليمية ليس لديها برامج تدريبية فعالة لزيادة الوعي بين طلاب الجامعات ومعرفتهم بالأمن السيبراني، وكيفية حماية أنفسهم من الهجمات الإلكترونية المحتملة، كما أوصت بضرورة تعزيز وتثقيف الوعي بالأمن السيبراني، وطرق الوقاية من مخاطر الانترنت والهجمات السيبرانية إضافة إلى ضرورة عقد دورات تدريبية للطلاب بشكل مستمر (Alzubaidi,2021; Tirumala, et al.,2016; Moallem, 2018)؛ إذ يؤكّد أشافي وآخرون (Ashafee et al., 2018) بأنّه يجب على المؤسسات التعليمية زيادة وعي الطلاب سواءً المتخصصين أو غير المتخصصين في تقنية المعلومات؛ لحمايتهم من التهديدات الأمنية الحالية والمستقبلية، إضافة إلى ما ذكره شريف وأمين (Sharif& Ameen, 2020) في المؤتمر الدولي للعلوم والهندسة المتقدمة بضرورة وجود برامج متنوعة للتوعية الأمنية؛ لأنها من أفضل الطرق لزيادة الوعي الأمني.

ومن خلال ما تم عرضه في الدراسات السابقة يتضح أنَّ هناك تدني في مستوى الوعي بالأمن السيبراني لدى الطلبة، كما أنها لم تتناول مجال الكشف عن درجة الوعي بأساليب وطرق تحقيق الأمن السيبراني؛ لذلك جاءت هذه الدراسة لمعرفة مستوى وعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بمفاهيم الأمن السيبراني وأساليب وطرق تحقيقه، ومن هنا ظهرت الحاجة للإجابة عن الأسئلة الآتية:

١. ما مستوى وعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بمفاهيم الأمن السيبراني؟

٢. ما درجة وعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بأساليب وطرق تحقيق الأمن السيبراني؟

٣. هل توجد فروق ذات دلالة إحصائية عند ($\alpha \leq$ ٠,٠٥) بين متوسطات استجابة أفراد عينة الدراسة حول الوعي بأساليب وطرق تحقيق الأمن السيبراني تُعزى لمتغيرات (الدرجة العلمية، التخصص، السنة الدراسية)؟

**أهداف الدراسة:**

هدفت الدراسة إلى التعرف على مستوى وعي طالبات كلية الحاسبات وتقنية المعلومات بمفاهيم الأمن السيبراني، وتحديد درجة وعي طالبات كلية الحاسبات وتقنية المعلومات بأساليب وطرق تحقيق الأمن السيبراني، والكشف عمّا إذا كان هناك فروق بين استجابة أفراد عينة الدراسة حول الوعي بأساليب وطرق تحقيق الأمن السيبراني والتي تُعزى لمتغيرات (الدرجة العلمية، التخصص، السنة الدراسية).

**أهميةُ الدراسةِ:**

**يُمكنُ تناولُ أهميةِ الدراسةِ منْ جانبَينِ: الأهميةِ النظريةِ، وَالأهميةِ التطبيقيةِ، على النحوِ الآتي:**

**١. الأهميةُ النظريةُ:**

**يُتوقعُ أنْ تُسهمَ هذهِ الدراسةُ فيما يَلي:**

١. تَأتي هذهِ الدراسةُ استجابةً لِجهودِ حكومةِ المملكةِ العربيةِ السعوديةِ في مجالِ نشرِ الوعيِ بِالأمنِ السيبرانيِّ وفقاً لِرؤيةِ ٢٠٣٠.

٢. قدْ تَكونُ إضافةً لِلبُحوثِ العِلمية وَالدِراسات العَربية النادرة فِي هٰذا المَجال.

٣. قَد تَكُون الدِراسة الحالية نَواة لِأَبحاث وَدِراسات مُستقبلية.

**٢. الأَهمية التَطبيقية:**

**يُمكنُ إيجازُ الأهميةِ التطبيقيةِ لِلدِراسة فِي النِقاط التالية:**

١. تَوجيه القائمين عَلى تَطوير المَناهج الدِراسية بِأَهمية إدراج مَفاهيم الأَمن السيبراني وَأَساليب وَطُرق تَحقيقهِ ضِمن المُقررات الدِراسية.

٢. ضَرورة تَبني إنشاء مِنصات تَعليمية قائمة عَلى المُسابقات وَالتَحديات، وَتَتَوفر بِها أَحدث أَدوات الحِماية لِتَعزيز تَعليم الأَمن السيبراني.

٣. لَفت اِنتباه المَسؤولين فِي الجامعة بِإقامة العَديد مِن الدَورات التَدريبية بِاستمرار لِلطالباتِ.

٤. جذْب اهْتمام المسْؤولينَ في الجامعة نحْو تطْوير برامج الأنْدية السيبرانية للطالِبات.

**حدود الدراسة:**

تقتصر حدود الدراسة الموضوعية على تحديد مستوى الوعي بمفاهيم الأمن السيبراني، وقياس درجة الوعي بأساليب وطرق تحقيق الأمن السيبراني، والحدود البشرية التي تشتمل على طالبات كلية الحاسبات وتقنية المعلومات، والحدود المكانية حيث أُجريت الدراسة في جامعة الطائف، والحدود الزمانية التي تم تطبيق الدراسة بها في الفصل الدراسي الثاني من العام الدراسي ١٤٤٣هـ.

**التعريفات الاصطلاحية والإجرائية:**

**الأمن السيبراني (Cybersecurity):**

هو مجموعة من التقنيات والعمليات والممارسات المصممة؛ لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به.(Rai et al.,2019)

ويمكن تعريفه إجرائيًا: هو الاستخدام الأمثل لحماية أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات وتعزيز الكفاءات البشرية للدفاع ضد الهجمات السيبرانية.

**الهجمات السيبرانية (Cyber-attack):**

هي محاولة من قبل المتسللين لإتلاف أو تدمير شبكة أو نظام كمبيوتر (Abu et al., 2018).

ويُعرف إجرائيًا: بأنها هجمات غير قانونية عبر الانترنت تستهدف أجهزة الكمبيوتر وأنظمة المعلومات والبرامج وبيانات المستخدمين؛ بهدف تعطيل أو إتلاف البيانات أو الاستحواذ عليها.

**الطريقة والإجراءات:**

**منهجية الدراسة:**

اتَّبعت الدراسة المنهج الوصفي بأسلوب الدراسات المسحية نظراً لملاءمته لطبيعة الدراسة.

**مجتمع الدراسة وعينتها:**

تكوّن مجتمع الدراسة من جميع طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف للفصل الدراسي الثاني عام ١٤٤٣هـ، وتم اختيار (٣٨٢) طالبة من كلية الحاسبات وتقنية المعلومات بجامعة الطائف بالطريقة العشوائية البسيطة. وتوضح الجداول التالية توزيع العينة تبعًا لمتغيرات الدراسة.

**جدول (١) توزيع عينة الدراسة وفقًا لمتغير الدرجة العلمية**

| الدرجة العلمية | دبلوم | بكالوريوس | المجموع |
|---|---|---|---|
| التكرارات | ٩٢ | ٢٩٠ | ٣٨٢ |
| النسبة المئوية % | ٢٤,١٪ | ٧٥,٩٪ | ١٠٠٪ |

يتضح من الجدول (١) أن أفراد عينة الدراسة الحاصلين على درجة الدبلوم بلغ عددهم (٩٢) بنسبة (٢٤,١٪)، بينما الذين حصلوا على درجة البكالوريوس بلغ عددهم (٢٩٠) بنسبة (٧٥,٩٪)، وهم عينة ممثلة لمجتمع الدراسة.

**جدول (٢) توزيع عينة الدراسة وفقًا لمتغير التخصص**

| التخصص | صيانة الحاسب | تقنية البرمجة | تقنية وأمن الشبكات | علوم الحاسب | تقنية المعلومات | هندسة الحاسب | المجموع |
|---|---|---|---|---|---|---|---|
| التكرارات | ٣١ | ٢٧ | ٣٤ | ٩٥ | ٩١ | ١٠٤ | ٣٨٢ |
| النسبة المئوية | ٨,١٪ | ٧,١٪ | ٨,٩٪ | ٢٤,٩٪ | ٢٣,٨٪ | ٢٧,٢٪ | ١٠٠٪ |

يتضح من الجدول (٢) أن أفراد عينة الدراسة تكونت من (٣١) طالبة في تخصص صيانة الحاسب الآلي بنسبة (٨,١٪)، و(٢٧) طالبة في تخصص تقنية البرمجة بنسبة (٧,١٪)، و(٣٤) طالبة في تخصص تقنية وأمن الشبكات بنسبة (٨,٩٪)، و(٩٥) طالبة في تخصص علوم الحاسب بنسبة (٢٤,٩٪)، و(٩١) طالبة في تخصص تقنية المعلومات بنسبة (٢٣,٨٪) بالإضافة إلى (١٠٤) طالبة في تخصص هندسة الحاسب بنسبة (٢٧,٢٪)، وهي عينة ممثلة لتخصصات طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف.

**جدول (٣) توزيع عينة الدراسة وفقًا لمتغير السنوات الدراسية**

| السنة الدراسية | الأولى | الثانية | الثالثة | الرابعة | الخامسة | المجموع |
|---|---|---|---|---|---|---|
| التكرارات | ١١٣ | ٨٢ | ١١١ | ٤١ | ٣٥ | ٣٨٢ |
| النسبة المئوية % | ٢٩,٦٪ | ٢١,٥٪ | ٢٩,١٪ | ١٠,٧٪ | ٩,٢٪ | ١٠٠٪ |

يتضح من الجدول (٣) أن أفراد عينة الدراسة تكونت من (١١٣) طالبة في السنة الأولى بنسبة (٢٩,٦٪)، و(٨٢) طالبة في السنة الثانية بنسبة (٢١,٥٪)، و(١١١) طالبة في السنة الثالثة بنسبة (٢٩,١٪)، و(٤١) طالبة في السنة الرابعة بنسبة (١٠,٧٪)، و(٣٥) طالبة في السنة الخامسة بنسبة (٩,٢٪)، وتعتبر العينة ممثلة للسنوات الدراسية لطالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف.

**أداة الدراسة:**

في سبيل الحصول على البيانات اللازمة من عينة الدراسة للإجابة عن تساؤلات الدراسة فقد تم استخدام الاستبانة للدراسة الحالية؛ نظراً لمناسبتها لأهداف الدراسة ومنهجها ومجتمعها وذلك بعد مراجعة الدراسات ذات الصلة مثل: (السواط وآخرون، ٢٠٢٠؛ الصانع وآخرون، ٢٠٢٠؛ الصحفي وعسكول، ٢٠١٩).

ولتطوير أداة الدراسة؛ تم تحديد المحاور التي ينبغي تضمينها بالدراسة، تحديد المجالات الرئيسة، وتوزيع العبارات على محاور الدراسة ووضع الاستبانة في صورتها الأولية في عباراتها ومجالاتها.

كما تضمنت الاستبانة (٣٨) عبارة؛ للتعرف على مستوى وعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بمفاهيم الأمن السيبراني، وأساليب وطرق تحقيق الأمن السيبراني، وقُسمت إلى محورين رئيسية، محور الوعي بمفاهيم الأمن السيبراني وتكوّن من ١١ عبارة، ومحور الوعي بأساليب وطرق تحقيق الأمن السيبراني وتكوّن من ٢٧ عبارة.

**صدق الأداة:**

تم التأكد من صدق أداة الدراسة من خلال:

**١. الصدق الظاهري:**

تم عرض الاستبانة بصورتها الأولية على مجموعة من المحكمين، متخصصين في تقنيات التعليم؛ لإبداء الملاحظات حول وضوح العبارات، ومناسبتها وانتمائها للمحاور، وطلب منهم تعديل أو حذف أو إضافة ما يرونه مناسبًا. وبعد الأخذ بآرائهم؛ تم حذف وتعديل وصياغة بعض العبارات، وأصبحت الاستبانة في صورتها النهائية مكونة من (٢٨) عبارة بعد أن كانت (٣٨) عبارة.

**٢. صدق البناء (construct validity):**

للتحقق من صدق عبارات الاستبانة، تم تطبيقها على عينة استطلاعية خارج عينة الدراسة تكوّنت من (٣٠) طالبة من كلية الحاسبات وتقنية المعلومات بجامعة الطائف، ثم حساب معامل ارتباط بيرسون بين درجة كل عبارة ودرجة المحور الذي تنتمي إليه، ويعرض الجدول (٤) تلك النتائج.

**جدول (٤) معاملات ارتباط بيرسون لعبارات الأداة مع الدرجة الكلية للمحور**

| المحور الأول: الوعي بمفاهيم الأمن السيبراني | | المحور الثاني: الوعي بأساليب وطرق تحقيق الأمن السيبراني | | | |
|---|---|---|---|---|---|
| رقم العبارة | الارتباط | رقم العبارة | الارتباط | رقم العبارة | الارتباط |
| ١ | **٠,٧٥٠ | ١ | **٠,٦٥٠ | ١١ | **٠,٥٢١ |
| ٢ | **٠,٥٥٩ | ٢ | **٠,٦٥٧ | ١٢ | **٠,٦٤٩ |
| ٣ | **٠,٥٠٦ | ٣ | **٠,٥٩٤ | ١٣ | **٠,٦٨١ |
| ٤ | **٠,٥٣٩ | ٤ | **٠,٧٧٥ | ١٤ | **٠,٧١٥ |
| ٥ | **٠,٧٥٨ | ٥ | **٠,٧٦٩ | ١٥ | **٠,٧٢٥ |
| ٦ | **٠,٧٩٩ | ٦ | **٠,٧١٠ | ١٦ | **٠,٦٥٤ |
| ٧ | **٠,٤٨٦ | ٧ | **٠,٦٧٥ | ١٧ | **٠,٦٣٢ |
| ٨ | **٠,٦٦١ | ٨ | **٠,٧٠٩ | ١٨ | **٠,٧٢٦ |
| | | ٩ | **٠,٥٧٨ | ١٩ | **٠,٥٠٥ |
| | | ١٠ | **٠,٥٤٧ | ٢٠ | *٠,٤٥١ |

*دال عند مستوى الدلالة (٠,٠٥) **دال عند مستوى الدلالة (٠,٠١)

يتضح من الجدول (٤) أن قيم معامل الارتباط بين درجة كل عبارة والمحور الذي تنتمي إليه تراوحت بين (٠,٤٥١) و (٠,٧٩٩)، وهي قيم مقبولة، وتؤكد صدق الأداة في جمع بيانات الدراسة.

كما تم حساب معامل ارتباط بيرسون بين درجة كل محور من المحاور والدرجة الكلية للاستبانة، ويوضح جدول (٥) تلك النتائج.

**جدول (٥) معاملات ارتباط بيرسون للمحاور مع الدرجة الكلية للاستبانة**

| المحاور | عدد العبارات | معامل الارتباط |
|---|---|---|
| الوعي بمفاهيم الامن السيبراني | ٨ | **٠,٧٧١ |
| الوعي بأساليب وطرق تحقيق الأمن السيبراني | ٢٠ | **٠,٩٦٤ |

**دال عند مستوى الدلالة (٠,٠١)

يتضح من الجدول (٥) أن قيم معامل الارتباط بين درجة كل محور والأداة ككل بلغت (٠,٧٧١)، (٠,٩٦٤) على التوالي؛ وهي قيم عالية تؤكد صدق الأداة في جمع بيانات الدراسة.

**ثبات أداة الدراسة:**

تم التأكد من ثبات الاستبانة من خلال استخدام معامل الثبات ألفا كرونباخ، ويوضح جدول (٦) قيم معاملات الثبات لكل محور من محاور الاستبانة مع الثبات الكلي.

**جدول (٦) معامل ألفا كرونباخ لقياس ثبات الاستبانة**

| الاستبانة | المحور | عدد العبارات | ثبات المحور |
|---|---|---|---|
| الأمن السيبراني | الوعي بمفاهيم الامن السيبراني | ٨ | ٠,٧٤٧ |
| | الوعي بأساليب وطرق تحقيق الأمن السيبراني | ٢٠ | ٠,٩١٥ |
| الثبات الكلي | | ٢٨ | ٠,٩٠٤ |

يتضح من الجدول (٦) أن قيم معامل ألفا كرونباخ لحساب ثبات الاستبانة بلغت (٠,٧٤٧) و(٠,٩١٥) على التوالي، بينما بلغ الثبات الكلي للاستبانة (٠,٩٠٤)؛ مما يدل على تمتع أداة الدراسة بثبات عالٍ يؤكد صلاحيتها لجمع بيانات الدراسة.

**تصحيح أداة الدراسة:**

تم استخدام مقياس ليكرت الخماسي للحصول على استجابات عينة الدراسة، وفق التدرج التالي: (موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة). ومن ثم التعبير عن هذا المقياس كميًا، بإعطاء كل عبارة من العبارات السابقة درجة، وفقًا للتالي: موافق بشدة (٥) درجات، موافق (٤) درجات، محايد (٣) درجات، غير موافق (٢) درجتان، غير موافق بشدة (١) درجة واحدة.

وتم تحديد معيار الاستجابة لمقياس ليكرت الخماسي، وذلك بتحديد طول خلايا مقياس ليكرت الخماسي بحساب المدى (٥-١=٤) وتقسيمه على أكبر قيمة في المقياس للحصول على طول الخلية (٥÷٤= ٠,٨٠)، ثم إضافة هذه القيمة إلى أقل قيمة في المقياس (الواحد الصحيح)، وأصبحت أطوال الخلايا كما هو موضح في جدول (٧).

**جدول (٧) تقسيم مقياس ليكرت الخماسي (Likert Scale)**

| الفئة | غير موافق بشدة | غير موافق | محايد | موافق | موافق بشدة |
|---|---|---|---|---|---|
| الدرجة | ١ | ٢ | ٣ | ٤ | ٥ |
| متوسط الدرجة | من ١ إلى أقل من ١,٨٠ | من ١,٨٠ إلى أقل من ٢,٦٠ | من ٢,٦٠ إلى أقل من ٣,٤٠ | من ٣,٤٠ إلى أقل من ٤,٢٠ | من ٤,٢٠ إلى ٥ |
| معيار الاستجابة | ضعيفة جدًا | ضعيفة | متوسطة | عالية | عالية جدًا |

**سادسًا: الأساليب الإحصائية المستخدمة في الدراسة:**

للإجابة عن السؤالين الأول والثاني من أسئلة الدراسة، تم استخدام المتوسطات الحسابية والانحرافات المعيارية، وللإجابة عن السؤال الثالث، تم استخدام اختبار (ت) لعينتين مستقلتين، لتحديد الفروق بين استجابات أفراد العينة تبعًا لمتغير الدرجة العلمية، واختبار تحليل التباين الأحادي (ANOVA)، للتحقق من دلالة الفروق لعينة الدراسة لمتغيري التخصص والسنة الدراسية واختبار شيفيه (*Scheffe*) البعدي، لتحديد اتجاه الفروق.

**النتائج:**

**نتائج السؤال الأول: ما مستوى وعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بمفاهيم الأمن السيبراني؟**

للإجابة عن هذا السؤال تم حساب المتوسطات الحسابية، والانحرافات المعيارية لاستجابات العينة، وتم ترتيب العبارات حسب المتوسطات الحسابية تنازليًا، كما هو موضح في جدول (٨).

**جدول (٨): المتوسطات الحسابية والانحرافات المعيارية لاستجابات العينة حول "الوعي بمفاهيم الأمن السيبراني"**

| الترتيب | العبارة | العبارة | المتوسط الحسابي | الانحراف المعياري | درجة الموافقة |
|---|---|---|---|---|---|
| ١ | ٥ | أعي خطورة التجسس على جهاز الحاسب | ٤,٤٦ | ٠,٨٦ | عالية جدًا |
| ٢ | ٨ | أعي بأن الأمن السيبراني نظام رقمي وتدابير أمنية | ٤,٤٠ | ٠,٩١ | عالية جدًا |
| ٣ | ٧ | أعي بأن ما يجب حمايته يتمثل في أجهزة الكمبيوتر والأجهزة الذكية والراوترات والشبكات والسحابة الالكترونية والبرامج | ٤,٢٩ | ٠,٩٥ | عالية جدًا |
| ٤ | ٦ | لدي وعي بمخاطر الهجوم السيبراني | ٤,٢٠ | ١,٠٢ | عالية جدًا |
| ٥ | ٤ | الردع السيبراني يقصد به التصدي للهجمات السيبرانية | ٤,١٨ | ٠,٩٥ | عالية |
| ٦ | ١ | لدي إلمام بمفهوم الأمن السيبراني | ٣,٨٦ | ٠,٩٩ | عالية |
| ٧ | ٣ | الهندسة الاجتماعية تعني مجموعة من الحيل والتقنيات المستخدمة لخداع الآخرين من أجل الحصول على معلوماتهم الشخصية | ٣,٥٩ | ١,٢٦ | عالية |
| ٨ | ٢ | لدي معرفة بمفهوم التصيد الاحتيالي (Phishing) | ٣,٥٧ | ١,١٦ | عالية |
| | | المتوسط العام | ٤,٠٧ | ٠,٦٦ | عالية |

يتضح من الجدول (٨) أن المتوسط العام لمستوى وعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بمفاهيم الأمن السيبراني بلغ (٤,٠٧) بانحراف معياري بلغ (٠,٦٦)، بدرجة (عالية). كما تراوحت المتوسطات الحسابية لعبارات المحور بين (٣,٥٧) و (٤,٤٦).

يتبين من الجدول (٨) أن كل من العبارة رقم (٨، ٥) حصلت على أعلى متوسط حسابي بلغ (٤,٤٠) و (٤,٤٦) على التوالي بدرجة عالية جدًا، كما حصلت كل من العبارة رقم (٢، ٣) على أقل متوسط حسابي بلغ (٣,٥٧) و (٣,٥٩) على التوالي بدرجة عالية.

**نتائج السؤال الثاني: ما درجة وعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بأساليب وطرق تحقيق الأمن السيبراني؟**

للإجابة عن هذا السؤال تم حساب المتوسطات الحسابية، والانحرافات المعيارية لاستجابات العينة، وتم ترتيب العبارات حسب المتوسطات الحسابية تنازليًا، كما هو موضح في جدول (٩).

**جدول (٩) المتوسطات الحسابية والانحرافات المعيارية لاستجابات العينة حول " الوعي بأساليب وطرق تحقيق الأمن السيبراني"**

| الترتيب | العبارة | العبارة | المتوسط الحسابي | الانحراف المعياري | درجة الموافقة |
|---|---|---|---|---|---|
| ١ | ٧ | لدي معرفة بخطورة مشاركة كلمة المرور مع الاخرين | ٤,٦٢ | ٠,٧٤ | عالية جدًا |
| ٢ | ١٧ | أحرص على استخدام متصفحات آمنه | ٤,٤٩ | ٠,٨٤ | عالية جدًا |
| ٣ | ١ | أحرص على اختيار كلمات سر قوية لجميع التطبيقات والمواقع التي استخدمها | ٤,٤٨ | ٠,٨٧ | عالية جدًا |
| ٤ | ٩ | أحرص على عدم فتح أي رابط يصلني قبل التأكد من هويته | ٤,٤٤ | ٠,٩٥ | عالية جدًا |
| ٥ | ١٣ | أحرص على عدم الرد على الرسائل النصية المشابهة لرسائل مشغلي الشبكة | ٤,٣٨ | ١,٠١ | عالية جدًا |

| | | | | | |
|---|---|---|---|---|---|
| ٦ | ١١ | أحرص على عدم الدخول على المواقع الغير موثوق بها | ٤,٣٥ | ٠,٩١ | عالية جدًا |
| ٧ | ١٥ | أستخدم المصادقة –التحقق بخطوتين- في برامج التواصل الاجتماعي | ٤,٣٥ | ١,٠٤ | عالية جدًا |
| ٨ | ٢ | أحرص على عدم إرسال أي معلومات أو بيانات مهمة من خلال التطبيقات التقنية المختلفة أو البريد الالكتروني | ٤,٢٦ | ١,٠٢ | عالية جدًا |
| ٩ | ٥ | أحرص على تحديث التطبيقات والأجهزة الإلكترونية باستمرار | ٤,٢١ | ١,٠٩ | عالية جدًا |
| ١٠ | ٣ | أحرص على إبلاغ الجهات المسؤولة عن أي اختراقات تقنية تحدث معي | ٤,١٧ | ١,١١ | عالية |
| ١١ | ٨ | أحرص على عدم أستخدم شبكات الواي فاي في الأماكن العامة | ٤,١١ | ١,١٥ | عالية |
| ١٢ | ١٨ | أهتم بتنصيب برامج الحماية | ٤,١٠ | ١,١١ | عالية |
| ١٣ | ١٢ | أحرص على اختيار كلمات مرور مختلفة للمواقع والتطبيقات والحسابات الخاصة بي | ٤,٠٧ | ١,١٢ | عالية |
| ١٤ | ٤ | أحرص على توفير نسخ احتياطية من البيانات والملفات للحفاظ عليها | ٤,٠٦ | ١,١٢ | عالية |
| ١٥ | ٢٠ | أحرص على عدم السماح للتطبيقات بمشاركة موقعي الجغرافي | ٣,٩٥ | ١,٢٣ | عالية |
| ١٦ | ١٠ | أقرأ الاتفاقيات والعقود التي تطلبها المواقع والتطبيقات الالكترونية بشكل دقيق قبل التسجيل والمشاركة فيها | ٣,٦٧ | ١,٢٦ | عالية |
| ١٧ | ١٦ | أحرص على تغيير كلمات المرور الخاصة بالتطبيقات والمواقع الالكترونية بشكل دوري | ٣,٥٤ | ١,٣٢ | عالية |
| ١٨ | ٦ | أقوم بتشفير الملفات المهمة عند ارسالها للآخرين | ٣,٣٨ | ١,٣٧ | متوسطة |
| ١٩ | ١٤ | لا أقوم بفتح رسائل الكترونية من مصدر مجهول | ١,٧٦ | ١,٠٣ | ضعيفة جدًا |
| ٢٠ | ١٩ | لا أستجيب لأي شخص يطلب مني كود تم إرساله إلى جوالي | ١,٤٧ | ٠,٩٠ | ضعيفة جدًا |
| المتوسط العام | | | ٣,٨٩ | ٠,٤٧ | عالية |

يتضح من الجدول (٩) أن المتوسط العام لدرجة وعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بأساليب وطرق تحقيق الأمن السيبراني بلغ (٣,٨٩) بانحراف معياري بلغ (٠,٤٧)، بدرجة (عالية). كما تراوحت المتوسطات الحسابية لعبارات المحور بين (١,٤٧) و (٤,٦٢).

يتبين من الجدول (٩) أن كل من العبارة (١٧، ٧) حصلت على أعلى متوسط حسابي بلغ (٤,٤٩) و (٤,٦٢) على التوالي بدرجة عالية جدًا، بينما حصلت كل من العبارة (١٦، ١٠) على أقل متوسط حسابي بلغ (٣,٥٤) و(٣,٦٧) على التوالي بدرجة عالية.

كما حصلت العبارة رقم (٦) على متوسط حسابي بلغ (٣,٣٨) بدرجة متوسطة، بينما عبارة رقم (١٤) حصلت على متوسط حسابي بلغ (١,٧٦) بدرجة ضعيفة جدًا، وعبارة رقم (١٩) بلغ متوسطها الحسابي (١,٤٧) بدرجة ضعيفة جدًا.

**نتائج السؤال الثالث: هل توجد فروق ذات دلالة إحصائية عند ($\alpha \leq ٠,٠٥$) بين متوسطات استجابة أفراد عينة الدراسة حول الوعي بأساليب تحقيق الأمن السيبراني تُعزى لمتغيرات (الدرجة العلمية، التخصص، السنة الدراسية)؟**

للإجابة عن هذا السؤال ومعرفة درجة وعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بأساليب وطرق تحقيق الأمن السيبراني تبعًا لمتغير الدرجة العلمية؛ تم استخدام اختبار (ت) لعينتين مستقلتين؛ للكشف عن دلالة الفروق الإحصائية لمتوسطات استجابات أفراد العينة، كما هو موضح في جدول (١٠):

**جدول (١٠): نتيجة اختبار (ت) لعينتين مستقلتين لتحديد الفروق بين استجابات أفراد العينة تبعًا لمتغير الدرجة العلمية.**

| الدرجة العلمية | اختبار ليفين | | العدد | المتوسط الحسابي | الانحراف المعياري | درجة الحرية | قيمة (ت) | الدلالة |
|---|---|---|---|---|---|---|---|---|
| | ف | الدلالة | | | | | | |
| دبلوم | ٢,١١ | ٠,١٥ | ٩٢ | ٣,٥٤ | ٠,٤٨ | ٣٨٠ | ٨,٨٧- | ٠,٠٠٠ |
| بكالوريوس | | | ٢٩٠ | ٤,٠١ | ٠,٤١ | | | |

يتضح من الجدول (١٠) أن قيمة (ت) بلغت (٨,٨٧-) وهي قيمة دالة عند مستوى ($\alpha \leq$ ٠,٠٥) حيث أن مستوى الدلالة بلغت (٠,٠٠٠) وهي قيمة أصغر من مستوى الدلالة ($\alpha \leq$ ٠,٠٥)؛ مما يعني وجود فروق ذات دلالة إحصائية بين متوسطات استجابة طالبات كلية الحاسبات وتقنية المعلومات حول الوعي بأساليب وطرق تحقيق الأمن السيبراني لصالح البكالوريوس.

**متغيري التخصص والسنة الدراسية:**

لمعرفة درجة وعي طالبات كلية الحاسبات وتقنية المعلومات بجامعة الطائف بأساليب وطرق تحقيق الأمن السيبراني تبعًا لمتغيري التخصص والسنة الدراسية، تم استخدام اختبار تحليل التباين الأحادي؛ للكشف عن مستوى دلالة الفروق الإحصائية لمتوسطات استجابات أفراد العينة، كما هو موضح في جدول (١١).

**جدول (١١): نتيجة اختبار تحليل التباين الأحادي (ANOVA) لتحديد دلالة الفروق بين استجابات أفراد العينة تبعًا لمتغيري التخصص والسنة الدراسية**

| المتغير | مصدر التباين | مجموع المربعات | درجة الحرية | متوسط المربعات | قيمة (ف) | الدلالة الإحصائية |
|---|---|---|---|---|---|---|
| التخصص | بين المجموعات | ١٦,٢٨٥ | ٥ | ٣,٢٥٧ | ١٧,٣٢٢ | ٠,٠٠٠ |
| | داخل المجموعات | ٧٠,٧٠١ | ٣٧٦ | ٠,١٨٨ | | |
| | المجموع | ٨٦,٩٨٦ | ٣٨١ | | | |
| السنة الدراسية | بين المجموعات | ٥,٩٢١ | ٤ | ١,٤٨٠ | ٦,٨٨٣ | ٠,٠٠٠ |
| | داخل المجموعات | ٨١,٠٦٦ | ٣٧٧ | ٠,٢١٥ | | |
| | المجموع | ٨٦,٩٨٦ | ٣٨١ | | | |

يتضح من الجدول (١١) أن قيمة اختبار (ف) بلغت (١٧,٣٢٢) و (٦,٨٨٣) على التوالي، وبلغت قيم مستوى الدلالة (٠,٠٠٠) وهي قيم دالة إحصائيًا عند ($\alpha \leq$ ٠,٠٥)؛ مما يعني وجود فروق ذات دلالة إحصائية بين أي متوسطين من متوسطات مجموعات الدراسة، ولتحديد اتجاه الفروق، تم استخدام اختبار(شيفيه) البعدي كما هو موضح في جدول (١٢):

**جدول (١٢): نتيجة اختبار شيفيه البعدي لتحديد اتجاه الفروق تبعًا لمتغيري التخصص والسنة الدراسية**

| المحور | التخصص(I) | التخصص(J) | الفرق بين المتوسطات | مستوى الدلالة |
|---|---|---|---|---|
| تحقيق الأمن السيبراني | علوم الحاسب | صيانة الحاسب الآلي | ٠,٣٦٨ | *٠,٠٠٥ |
| | علوم الحاسب | تقنية البرمجة | ٠,٦٥٩ | *٠,٠٠٠ |
| | علوم الحاسب | تقنية وأمن الشبكات | ٠,٤٥٧ | *٠,٠٠٠ |
| | تقنية المعلومات | صيانة الحاسب الآلي | ٠,٣٢٨ | *٠,٠٢٢ |
| | تقنية المعلومات | تقنية البرمجة | ٠,٦١٩ | *٠,٠٠٠ |
| | تقنية المعلومات | تقنية وأمن الشبكات | ٠,٤١٨ | *٠,٠٠٠ |
| | هندسة الحاسب | صيانة الحاسب الآلي | ٠,٣٣٥ | *٠,٠١٥ |
| | هندسة الحاسب | تقنية البرمجة | ٠,٦٢٦ | *٠,٠٠٠ |
| | هندسة الحاسب | تقنية وأمن الشبكات | ٠,٤٢٤ | *٠,٠٠٠ |
| وعي بأساليب وطرق | السنة الدراسية (I) | السنة الدراسية (J) | الفرق بين المتوسطات | مستوى الدلالة |
| | السنة الأولى | السنة الثانية | ٠,٢٤٦ | *٠,٠١٠ |

| | | | | |
|---|---|---|---|---|
| | السنة الثالثة | السنة الثانية | ٠,٢٨٤ | *٠,٠٠٢ |
| | السنة الرابعة | السنة الثانية | ٠,٢٩٦ | *٠,٠٢٦ |
| | السنة الخامسة | السنة الثانية | ٠,٤٠٣ | *٠,٠٠١ |

* دالة عند مستوى (٠,٠٥) فأقل

يتضح من الجدول (١٢) وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة حول الوعي بأساليب وطرق تحقيق الأمن السيبراني تبعًا لمتغير التخصص الدراسي بين علوم الحاسب و (صيانة الحاسب الآلي، تقنية البرمجة، وتقنية وأمن الشبكات) لصالح متخصصي (علوم الحاسب) حيث بلغت قيم مستوى الدلالة على التوالي (٠,٠٠٥) و (٠,٠٠٠) و (٠,٠٠٠) وهي قيم أقل من مستوى الدلالة (α≤٠,٠٥)؛ ودالة إحصائيًا.

ويتضح من الجدول (١٢) وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة حول الوعي بأساليب وطرق تحقيق الأمن السيبراني تبعًا لمتغير التخصص الدراسي بين تقنية المعلومات و(صيانة الحاسب الآلي، تقنية البرمجة وتقنية وأمن الشبكات) لصالح متخصصي (تقنية المعلومات) حيث بلغت قيم مستوى الدلالة على التوالي (٠,٠٢٢) و(٠,٠٠٠) و(٠,٠٠٠) وهي قيم أقل من مستوى الدلالة (α≤٠,٠٥)؛ ودالة إحصائيًا.

كما يتضح من الجدول (١٢) وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة حول الوعي بأساليب وطرق تحقيق الأمن السيبراني تبعًا لمتغير التخصص الدراسي بين هندسة الحاسب و(صيانة الحاسب الآلي، تقنية البرمجة وتقنية وأمن الشبكات) لصالح متخصصي (هندسة الحاسب) حيث بلغت قيم مستوى الدلالة على التوالي (٠,٠١٥) و(٠,٠٠٠) و(٠,٠٠٠) وهي قيم أقل من مستوى الدلالة (α≤٠,٠٥)؛ ودالة إحصائيًا.

بالنظر لجدول (١٢) يتبين وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة حول الوعي بأساليب وطرق تحقيق الأمن السيبراني تبعًا لمتغير السنة الدراسية بين طالبات (السنة الأولى، والسنة الثالثة والسنة الرابعة والسنة الخامسة) وطالبات (السنة الثانية) لصالح الطالبات اللاتي يدرسن في السنة (الأولى، الثالثة، الرابعة والخامسة)

حيث بلغت قيم مستوى الدلالة على التوالي (٠,٠١٠) و(٠,٠٠٢) و (٠,٠٢٦) و(٠,٠٠١) وهي قيم أقل من مستوى الدلالة (α≤٠,٠٥)؛ ودالة إحصائيًا.

**مناقشة النتائج:**

بيَّنت النتائج أنَّ هناك مستوىً مرتفعًا بوعي طالبات كلية الحاسبات وتقنية المعلومات بمفاهيم الأمن السيبراني، وقد يعود ذلك لاهتمام كلية الحاسبات وتقنية المعلومات بجامعة الطائف بإقامة المعسكرات الصيفية والأندية السيبرانية للطالبات، وفق ما ذكر ماونترويدو وآخرون (Mountrouidou et al., 2018) بأنَّ الدورات التعليمية وسيلة فعالة لإبراز أهمية الأمن السيبراني وإكساب الطلاب المفاهيم الأساسية المتعلقة بالأمن السيبراني، وإطلاق العديد من المبادرات التثقيفية بالأمن السيبراني؛ والتي أوصت بها دراسة الخضري وآخرون (٢٠٢٠) بضرورة رفع الوعي بالأمن السيبراني من خلال توفير برامج توعوية للتعريف بالأمن السيبراني، وآليات تعزيزه في المؤسسات التعليمية، وهذا يتفق مع ما جاء في دراسة الجهني وآخرون (Aljohni et al, 2021) التي توصلت إلى أن الطلاب لديهم وعي عالي بالأمن السيبراني، بينما اختلفت مع نتيجة دراسة تيرومالا وآخرون (Tirumala et al, 2016) التي كشفت نتائجها عن انخفاض مستوى وعي الطلاب بمفاهيم الأمن السيبراني الشائعة، ودراسة نديبويل وآخرون (Ndibwile et al,2019) التي أظهرت نتائجها أن المستخدمين ليس لديهم الوعي الكافي بهجمات التصيد الاحتيالي، ويُعزى سبب الاختلاف إلى الفارق الزمني بين الدراستين.

كما أشارت النتائج إلى ارتفاع درجة وعي الطالبات بأساليب وطرق تحقيق الأمن السيبراني، ويُرجح ذلك إلى اهتمام جامعة الطائف ممثلة بكلية الحاسبات وتقنية المعلومات بتفعيل برنامج أندية الطلبة المطورين المقدم من جوجل متضمنة مواضيع تتعلق بالأمن السيبراني، بالإضافة إلى مشاركة إدارة الأمن السيبراني بجامعة الطائف للتوعية بالأمن السيبراني لدى الطالبات عن طريق البريد الإلكتروني، إذ أكدَّ الشوابكة (٢٠١٩)

بأنَّ الإجراءات الأمنية في الحد من مخاطر أمن المعلومات ومنع اختراق الشبكات في جامعة الطائف جاءت بدرجة عالية، إضافة إلى ما أشار إليه كارلين ومانسون (Carlin& Manson, 2016) بأن أنشطة التطوير الإضافية، مثل النوادي الطلابية والتدريبات العملية والمعسكرات والمسابقات، والمؤتمرات تعمل على تطوير مهاراتهم في الأمن السيبراني، وتمكنهم من حماية أنفسهم ضد أي هجوم سيبراني محتمل.

واختلفت هذه النتيجة مع نتائج دراسة معلم (Moallem, 2018) التي أظهرت نتائجها أن الطلاب غير مدركين تمامًا لكيفية حماية بياناتهم، ولعل ذلك يُعزى لاختلاف الجوانب التي تناولتها هاتين الدراستين.

وفي الجانب الآخر بيَّنت نتائج الدراسة، أنَّ هناك تدني في بعض جوانب درجة الوعي بأساليب وطرق تحقيق الأمن السيبراني؛ ولعل ذلك يرجع لانخفاض اهتمام الطالبات بتطبيق بعض تقنيات الأمن السيبراني، بعدم تشفير الملفات قبل ارسالها للآخرين، وهذا يؤكد ما آلت إليه دراسة الجندي ومحمد (٢٠١٩) بأهميَّة دور الممارسة التطبيقية لتقنيات الأمن السيبراني حيث تُسهم في تنمية المهارات ودقة التطبيق العملي لأمن المعلومات لدى طالبات الجامعة، إضافةً إلى ما ذكره الصائغ (٢٠١٨) بضرورة تشفير المعاملات الإلكترونية بحيث لا يستطيع المتسللون أو المهاجمون من الوصول بسهولة إلى هذه البيانات والتطبيقات، كذلك عدم فتح رسائل الكترونية من مصادر مجهولة، والابتعاد عن الاستجابة لأي شخص يطلب كود تم ارساله إلى الهاتف المحمول، والذي أوصت به دراسة السواط وآخرون (٢٠٢٠) بأهمية عقد برامج تثقيفية تخاطب مختلف المستويات بكيفية التعامل مع الأشخاص مجهولي الهوية في مواقع التواصل الاجتماعي؛ لحماية أنفسهم من الهجمات الالكترونية، إضافةً إلى ذلك الجامعة بحاجة إلى بذل المزيد من الجهد لرفع مستوى القدرات الرقمية اللازمة لتحقيق الأمن السيبراني (فرج، ٢٠٢٢). واتفقت هذه النتيجة مع دراسة خالد وآخرون (Khalid et al, 2018) التي خلصت إلى أن طلاب الجامعات بالرغم من أنهم أظهروا مستوى عالٍ من الوعي بعناصر معينة في الأمن السيبراني إلا أنه لا يزال هناك نقص في الوعي بشأن المواقع اللاأخلاقية وكيفية حماية الذات.

وأظهرت نتائج الدراسة بوجود فروق ذات دلالة إحصائية بين متوسطات استجابة طالبات كلية الحاسبات وتقنية المعلومات حول الوعي بأساليب وطرق تحقيق الأمن السيبراني تُعزى لمتغير الدرجة العلمية، ولصالح طالبات البكالوريوس ويعود ذلك إلى ارتفاع المستوى المعرفي وامتلاك الخبرات والمهارات السيبرانية نتيجة اكتسابهم للمعارف التي تسهم في تحقيق الأمن السيبراني، حيث أشار سالم وآخرون (Salem et al., 2021) بأن الطلاب الذين لديهم مستوى عالٍ من المعرفة في مجال الوعي الأمني تصرفوا بطريقة أكثر احترافًا تجاه التهديدات الإلكترونية، واختلفت هذه النتيجة مع دراسة طيبي وآخرون (Tibi et al.,2019) التي أكدت على أن طلاب علوم الحاسب ليس لديهم الوعي الكافي بالجرائم الالكترونية، وقدرتهم على حماية أنفسهم. ولعل السبب وراء هذا الاختلاف يعود إلى عدم وجود برامج توعوية ذات فعالية لزيادة المعرفة بالأمن السيبراني.

كما كشفت نتائج الدراسة عن وجود فروق ذات دلالة إحصائية بين متوسطات استجابة الطالبات كلية الحاسبات وتقنية المعلومات حول الوعي بأساليب وطرق تحقيق الأمن السيبراني تُعزى لمتغير التخصص، ولصالح تخصصات البكالوريوس (علوم الحاسب، تقنية المعلومات، هندسة الحاسب)؛ ويمكن تفسير هذه النتيجة في ضوء طبيعة مقررات تخصصات البكالوريوس التي تختص بأمن المعلومات والشبكات وأمن نظم الحاسبات، وأيضًا تمتعهم بمستوى عالٍ من الخبرة في كيفية تطبيق أساليب وإجراءات الأمن السيبراني، فيؤكد ريدمان وآخرون (Redman et al,2020) بوجود قدرات ومهارات سيبرانية مختلفة لدى الطلاب تم اكتسابها من خلال دراسة المقررات التي تتعلق بالأمن السيبراني، حيث يعتمد ارتفاع الوعي بالأمن السيبراني على تعلم مفاهيم تقنية المعلومات الأساسية ومهارات محو الأمية الرقمية بين طلاب تقنية المعلومات ( Frydenberg &Lorenz, 2020)، بالإضافة إلى أن تثقيف الطلبة بالممارسات التي تحقق الأمن السيبراني تتم من خلال تضمينها في المقررات والمناهج الدراسية (فرج، ٢٠٢٢) .

وتتفق هذه النتيجة مع نتيجة دراسة أشافي وآخرون (Ashafee et al, 2018) في أن الطلاب المتخصصين في تقنية المعلومات لديهم وعي عالي بجميع ما يتعلق بالأمن السيبراني، في حين اختلفت هذه النتيجة مع نتيجة دراسة غاربا وآخرون (Garba et al.,2020) التي خلصت إلى أن الطلاب المتخصصين في علوم الحاسب لديهم نقص في الوعي بشأن أساليب وطرق الحماية وأنهم أكثر عرضة للهجمات الالكترونية، وقد يعود سبب الاختلاف إلى اختلاف بيئة الدراسة.

إضافةً إلى ذلك، وجود فروق ذات دلالة إحصائية بين متوسطات استجابة طالبات كلية الحاسبات وتقنية المعلومات حول الوعي بأساليب وطرق تحقيق الأمن السيبراني تُعزى لمتغير السنة الدراسية، ولصالح طالبات السنة (الأولى، الثالثة، الرابعة، الخامسة)، ويمكن تفسير هذه النتيجة بأن طالبات السنة الأولى يمتلكن دافع وشغف فيما يتعلق بأمن المعلومات، ويرغبن في إظهار مهاراتهن وكفاءتهن في كيفية حماية أنفسهن ضد أي هجوم سيبراني، إذ أكَّد كام وكاتراتاناكول (Kam& Katerattanakul, 2014) بأن دافعية طلاب السنة الأولى في اكتساب المعرفة لأمن المعلومات مرتفعة مما يؤدي ذلك إلى ارتفاع وعيهم الأمني. كما أن ارتفاع الوعي بأساليب وطرق تحقيق الأمن السيبراني لدى طالبات السنة الثالثة والسنة الرابعة والسنة الخامسة قد يعود السبب في ذلك إلى أن الطالبات عبر سنوات دراستهن الجامعية أصبحت لديهن خبرات معلوماتية ومهارات تطبيقية لتقنيات الأمن السيبراني في سبيل تحقيق أساليب وطرق الحماية لديهن؛ وفقًا لما أشار إليه كيسومبينج (Quisumbing, 2019) عند انتقال الطلاب لسنة دراسية أعلى يزداد وعيهم وفهمهم بأمن المعلومات بشكل ملحوظ.

واختلفت هذه النتيجة مع ما توصلت إليه دراسة مي وتيك (Mai& Tick, 2021) التي أكدت على انخفاض وعي طلاب الجامعة بمختلف التخصصات والسنوات الدراسية بالأمن السيبراني؛ مما يؤدي ذلك إلى تدني في مستوى الوعي بالتهديدات السيبرانية، ويمكن أن يُعزى السبب في ذلك اختلاف التخصص الدراسي.

**توصيات الدراسة:**

توصي الدراسة بتنظيم دورات تدريبية شاملة للوعي بالأمن السيبراني متضمنة خطورة مشاركة المعلومات مع الآخرين، وتطوير برامج الأندية الطلابية (نادي الأمن السيبراني، نادي التقنية والبرمجة) التي تختص بمواضيع التدريبات العملية بكلية الحاسبات وتقنية المعلومات، كذلك زيادة الاهتمام بتوعية الطالبات بمخاطر الهجمات السيبرانية من قبل الخبراء في الأمن السيبراني.

**المراجع والمصادر:**


الجندي، علياء بنت عبد الله إبراهيم ومحمد، نهير طه حسن (٢٠١٩). دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة. مجلة عالم التربية، ٣ (٦٧)، ١٤-٨٤.

الخضري، جيهان وسلامي، هدى وكليبي، نعمة (٢٠٢٠). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية. مجلة تطوير الأداء الجامعي، ١٢(١)، ٢١٧-٢٣٣.

السمحان، منى عبد الله (٢٠٢٠). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية بجامعة المنصورة، ١(١١١)، ٢-٢٩.

السواط، حمد والصانع، نورة وأبو عيشة، زاهدة وسليمان، ايناس وعسران، عواطف (٢٠٢٠). العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف. مجلة البحث العلمي في التربية، ٢١(٤)، ٢٧٨-٣٠٦.

الشهراني، بيان محمد وفلمبان، فدوى ياسين (٢٠٢٠). أثر برنامج تدريبي قائم على تصميم ألعاب تعليمية إلكترونية باستخدام برنامج (Game Maker) لإكساب مفاهيم الأمن السيبراني لدى طالبات المرحلة المتوسطة. مجلة البحث العلمي في التربية، ٢١(٩)، ٦١٤-٦٥١.

الشوابكة، عدنان عواد (٢٠١٩). دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف. مجلة دراسات وأبحاث، ١١ (٤)، ١٦٤-١٨٧.

الصانع، نورة والسواط، حمد وأبوعيشة، زاهدة وسليمان، ايناس وعسران، عواطف (٢٠٢٠). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. المجلة العلمية لكلية التربية بجامعة أسيوط، ٣٦(٦)، ٤١-٩٠.

الصائغ، وفاء حسن (٢٠١٨) وعي أفراد الأسرة بمفهوم الأمن السيبرانى وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية، المملكة العربية السعودية. المجلة العربية للعلوم الاجتماعية، ١٤(٣)،١٨-٧٠.

صباغ، محمد هاني (٢٠٢١). دليل الأمان الرقمي. أكاديمية حسوب.

الصحفي، مصباح وعسكول، سناء (٢٠١٩) مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. مجلة البحث العلمي في التربية، ١٠(٢٠)، ٤٩٣-٥٣٤.

صحيفة سبق (٢٠٢١)، انطلاق مؤتمر "@Hack" في الرياض بمشاركة عباقرة الأمن السيبراني في العالم، نُشرت في ٢٠٢١/١١/٢٨.

فرج، علياء عمر كامل (٢٠٢٢). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي جامعة الأمير سطام بن عبد العزيز نموذجًا. المجلة التربوية لكلية التربية سوهاج، ١ (٩٤)، ٥٠٩-٥٣٧.

محمد، هبة هاشم محمد (٢٠٢٠). برنامج مقترح قائم على جغرافية الحروب السيبرانية لتنمية الوعي بمخاطرها وتعزيز قيم المواطنة الرقمية للطلاب المعلمين بكلية التربية. مجلة كلية التربية في العلوم التربوية، ٤٤(٣)، ٨١-١٥٠.

الهيئة الوطنية للأمن السيبراني. (٢٠١٨). الضوابط الأساسية للأمن السيبراني، https://ega.ee/wp-content/uploads/٢٠١٩/٠٣/Essential-Cybersecurity-Controls.pdf

Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371-379.

Aljohni, W., Elfadil, N., Jarajreh, M., &Gasmelsied, M. (2021). Cybersecurity awareness Level: The case of saudi arabia university students. *International Journal of Advanced Computer Science and Applications,12* (3), 276-281.

Alsulami, M. H., Alharbi, F. D., Almutairi, H. M., Almutairi, B. S., Alotaibi, M. M., Alanzi, M. E., Alotaibi, K. G. &Alharthi, S. S. (2021). Measuring awareness of social engineering in the educational sector in the kingdom of saudi arabia. *Journal of Information, 12*(5), 208.

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Journal of Heliyon*, *7*(1), 1-8.

Ashafee, T. L., Moh, S., Zakaria, N. H., Mohamad Tahir, H., Katuk, N., & Omar, M. N. (2018). Security behaviors on social network sites used for academic purposes: a comparison of security preparedness and awareness among IT and non-IT postgraduate students. *The Journal of Social Sciences Research*, *1*(4), 839-846.

Bock, K., Hughey, G., & Levin, D. (2018). King of the hill: A novel cybersecurity competition for teaching penetration testing. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*.

Carlin, A., & Manson, D. (2016). Polytechnic education for the cybersecurity workforce: Leaders in polytechnic education prepare the next generation with hands-on cyber risk training. *Strategic Finance*, *98*(1), 62-64.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*, 103-123.

Frydenberg, M., & Lorenz, B. (2020). Lizards in the street! introducing cybersecurity awareness in a digital literacy context. *Information Systems Education Journal*, *18*(4), 33-45.

Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A Study on cybersecurity awareness among students in Yobe State university, nigeria: A Quantitative approach. *International Journal on Emerging Technologies*, *11*(5), 41-49.

Goran, I. (2017). *Cyber security risks in public high schools*. [master's thesis, university of New York]. CUNY Academic Works.

Graham, J., Howard, R., Olson, R. (2011). *Cyber Security essentlals*. CRC Press.

Kam, H. J., & Katerattanakul, P. (2014). *Out-of-class learning: A Pedagogical Approach of promoting information security education* [paper presentation]. Twentieth Americas Conference on Information Systems, Savannah.

Khalid, F., Daud, M. Y., Rahman, M. J. A., & Nasir, M. K. M. (2018). An investigation of university students' awareness on cyber security. *International Journal of Engineering & Technology*, *7*(4.21),11-14.

Kritzinger, E., Bada, M., & Nurse, J. R. (2017, May*). A study into the cybersecurity awareness initiatives for school learners in South Africa and the U K* [paper presentation]. In IFIP World Conference on Information Security Education (pp. 110-120). Springer, Cham.

Kucek, S., & Leitner, M. (2020). An empirical survey of functions and configurations of open-source capture the flag (CTF) environments. *Journal of Network and Computer Applications*, *151*,102470.

Leune, K., & Petrilli Jr, S. J. (2017, September). *Using capture-the-flag to enhance the effectiveness of cybersecurity education* [paper presentation]. In Proceedings of the 18th Annual Conference on Information Technology Education, Rochester, NY, USA.

Mai, P. T., & Tick, A. (2021). Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytech. Hung*, *18*, 67-89.

Moallem, A. (2018, July). *Cyber security awareness among college students* [paper presentation]. In International Conference on Applied Human Factors and Ergonomics(pp.79-87). Springer, Cham.

Mountrouidou, X., Li, X., & Burke, Q. (2018, July). *Cybersecurity in liberal arts general education curriculum* [paper presentation]. In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education, ACM, New York.

Ndibwile, J. D., Luhanga, E. T., Fall, D., Miyamoto, D., Blanc, G., & Kadobayashi, Y. (2019). An empirical approach to phishing countermeasures through smart glasses and validation agents. *IEEE Access*, *7*, 130758-130771.

Patel, R. (2021). A Research of the awareness level among Technical and Non-technical students of cyber security in Parul University. *International Research Journal of Management Sociology & Humanity*,*12* (2), 116-119.

Rai, S. k., yadav, Sh. K., mishra, p.&pandey, M. Ch. (2019). *cyber security*. Book Bazooka publication.

Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the Internet of Things in Industrial Management. *Applied Sciences*, *12*(3), 1598.

Redman, S. M., Yaxley, K. J., & Joiner, K. F. (2020). Improving general undergraduate cyber security education: A Responsibility for ll universities? *Creative Education*, *11*(12), 2541- 2558.

Rege, M., & Mbah, R. B. K. (2018, November). *Machine learning for cyber defense and attack* [paper presentation]. The Seventh International Conference on Data Analytics, Athens, Greece.

Salem, Y., Moreb, M., & Rabayah, K. S. (2021, July). *Evaluation of information security awareness among palestinian learners* [paper presentation]. In 2021 International Conference on Information Technology (ICIT), Amman, Jordan.

Sharif, K. H., & Ameen, S. Y. (2020, December). *A review of security awareness approaches with special emphasis on gamification* [paper presentation]. In 2020 International Conference on Advanced Science and Engineering (ICOASE), Duhok, Iraq.

Tibi, M. H., Hadeje, K., & Watted, B. (2019). Cybercrime awareness among students at a teacher training college. *International Journal of Computer Trends and Technology (IJCTT)*, *67* (6), 11-17.

Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016, December). A survey on Internet usage and cybersecurity awareness in students [paper presentation]. In 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand.

Rathee, D., & Mann, S. (2022). Detection of E-mail phishing attacks–using machine learning and deep learning. *International Journal of Computer Applications*, *183*(1), 7.