درجة ممارسة سلوك الأمن السيبراني بين افراد المجتمع السعودي، وعلاقته ببعض المتغيرات

د. عبد الرحمن بن فهد المطرف
جامعة الملك سعود

تاريخ الاستلام: 2022/11/17 تاريخ القبول:2023/01/11

ملخص: هدفت هذه الدراسة الكشف عن درجة ممارسة أفراد المجتمع السعودي لسلوك الأمن السيبراني، وفيما أذا كانت درجة ممارستهم تختلف باختلاف النوع الاجتماعي والمستوى التعليمي والتخصص. استخدمت الدراسة المنهج الوصفي التحليلي، ولتحقيق أهداف الدراسة تبنى الباحث مقياس سلوك الأمن السيبراني الذي طوره (Muniandy, Muniandy & Samsudin, 2017)، وقد تكون من (50) فقرة موزعة على خمس محاور (البرامج الخبيثة، استخدام كلمات المرور، الهندسة الاجتماعية، التصيد الالكتروني، الاحتيال عبر الانترنت)، تكونت عينة الدراسة من (700) فرداً من أفراد المجتمع السعودي. أظهرت نتائج الدراسة أن درجة ممارسة أفراد المجتمع السعودي سلوك الأمن السيبراني كانت بدرجة متوسطة (أحياناً)، كما أظهرت نتائج تحليل التباين عدم وجود فروق دالة إحصائياً في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تعزى لمتغير النوع الاجتماعي، فيما عدا محور الهندسة الاجتماعية وكانت الفروق لصالح الإناث، كما أظهرت النتائج عدم وجود فروق ذات دلالة إحصائية في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تبعاً لمتغير المستوى التعليمي، كما أظهرت النتائج وجود فروق في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي من المتخصصين من الكليات الصحية والكليات العلمية لصالح المتخصصين من الكليات العلمية في محور استخدام كلمات المرور، ووجود فروق في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي من المتخصصين في الكليات العلمية والكليات الصحية لصالح الكليات الصحية في محور التصيد الإلكتروني، والكليات الإنسانية والكليات الصحية لصالح الكليات الإنسانية في ذات المحور، ووجود فروق في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي لصالح المتخصصين من الكليات العلمية والكليات الصحية لصالح الكليات العلمية في محور الهندسة الاجتماعية، حيث كان المتوسط الحسابي لاستجاباتهم أعلى.

الكلمات المفتاحية: سلوك، الأمن السيبراني، سلوك الأمن السيبراني، أفراد المجتمع السعودي.

Practicing Cybersecurity Behavior among Members of the Saudi Society and Its Relation with Some Variables

Dr. Abdulrahman Al-Motrif

Abstract

The purpose of this study is to explore the degree to cyber-security behavior practice of Saudi society members, and does the degree of practice differ according to gender, educational level and specialization? The study used the descriptive analytical method. To achieve the objectives of the study, the researcher used the cyber-security behavior scale which developed by (Muniandy et al., 2017), the scale consisted of (50) items distributed over five areas (malware, the use of passwords, social engineering, phishing, online fraud), the study sample consisted of (700) members of the Saudi community. The results of the study showed that the degree to which members of Saudi society practice cyber-security behavior was moderately (sometimes), The results also showed that there were no statistically significant differences in the degree of cyber-security behavior among members of the Saudi society due to the gender variable, with the exception of the social engineering axis, and the differences were in favor of females. The results also showed that no statistically significant differences in the degree of cyber-security behavior among members of Saudi society according to the educational level variable. There are differences in the degree of cyber-security behavior practice among Saudi society specialists from health colleges and science colleges in favor of specialists from science colleges in the field of using passwords. There are differences in the degree of cyber-security behavior practice among Saudi society specialists in scientific and health colleges in favor of health colleges in phishing field, humanities and health colleges for the benefit of humanities colleges in the same field. There are differences in the degree of cyber-security behavior practice among Saudi society members in favor of specialists from scientific and health colleges in favor of scientific colleges in the social engineering axis.

Keywords: behavior, cyber security, cyber security behavior, Saudi society members.

مقدمة الدراسة

يعد الانترنت وأحداً من أكثر التقنيات تطوراً على الإطلاق، والانترنت والتقنيات المرتبطة به تتطور باستمرار، ويزداد عدد مستخدمي الانترنت، والاعتماد على الشبكة في أداء الكثير من الأعمال بشكل متزايد كل يوم في العالم (Daka Advisory, 2014)، لقد تزايد عدد مستخدمي الإنترنت في المملكة العربية السعودية، فقد جاء في النشرة الإحصائية للعام 2019م أن (92.77%) من الأسر السعودية لديها إمكانية النفاذ إلى الإنترنت، وقد بلغت نسبة الأفراد (15 سنة فأكثر) الذين يستخدمون الإنترنت بشكل يومي (88.6%)، كما أن الغالبية العظمى من السعوديين (93.81%) يستخدمون الإنترنت مرة واحدة على الأقل في اليوم، وغالباً ما يتم الوصول إلى الإنترنت واستخدامه على نطاق واسع للأفراد الذين ترتبط أنشطتهم في التصفح بشكل أساسي من خلال شبكات التواصل الاجتماعي، وممارسة تحميل الألعاب والأفلام والصور والموسيقى ومقاطع الفيديو، أو الاتصال الهاتفي عبر الإنترنت (الهيئة العامة للإحصاء، 2019، 20).

لقد كان للتطور التكنولوجي تأثيراً كبيراً على أنماط حياة الأفراد خلال العصر الحالي، لكن لهذا الاستخدام جانب مظلم ففي عام 2017م، قدر معهد بونيمون التأثير الاقتصادي للانتهاكات الأمنية بنحو نصف تريليون دولار على مستوى العالم، مع زيادة تكلفة اختراق البيانات كل عام (Ponemon Inst, 2017)، تنتشر الانتهاكات الأمنية باستمرار، وتزداد تعقيدًا وخطورة، فقد تغيرت صورة المستخدم النهائي للتكنولوجيا وتطبيقاتها، فالمستخدم العادي ليس بالضرورة متعلماً تقنياً، بل هو على الأرجح لم يدرس الأمن السيبراني في تعليمه أو خلال دراسته السابقة. ويُعرَّف الأمن السيبراني بأنه نظام قائم على الكمبيوتر، والذي يتضمن التكنولوجيا والأشخاص والمعلومات والعمليات (JTF, 2017). وعلى الرغم من وعي المستخدمين إلى حد ما بالمخاطر الأمنية في استخدام تكنولوجيا المعلومات والانترنت إلا أن معظمهم ليسوا متأكدين من الكيفية التي يجب أن يتصرفوا بها لتحقيق الأمن السيبراني فعلى سبيل المثال حتى لو سمعوا عن التصيد الاحتيالي، فإن بعض المستخدمين غير متأكدين من كيفية التعرف على المشكلة أو التصرف بشكل مناسب لذاك كانوا هم الضحية (Wiederhold, 2014).

لقد أكد كل من سوبراتمان ووحي الدين (Supratman & Wahyudin, 2017) أن التكنولوجيا لا تشتمل على مكون برمجي فحسب، بل تتطلب أيضًا تكلفة عالية للأمان الشخصي عندما يتعلق الأمر بالاتصال عبر الإنترنت، كما ذكر كريجن وآخرون (Craigen, et al., 2014) أن الأمن السيبراني مجال واسع يشمل العناصر التكنولوجية والبشرية، وتحدث معظم الخروقات الأمنية بسبب سوء التقدير، أو أخطاء المستخدم، أو مزيج من الاثنين.

لقد أصبح من الواضح أنه يمكن لمستخدمي الكمبيوتر ذوي السلوك السيئ تعريض المؤسسات والأفراد للخطر، فقد أثرت العديد من انتهاكات الخصوصية على ملايين الأفراد في جميع أنحاء العالم، وتتضمن عمليات التجسس على الشبكة افتقار المستخدم للوعي إضافة لجهل البعض أو الإهمال أو اللامبالاة، كما تؤكد انتهاكات البيانات التي تم الإبلاغ عنها على أهمية التدريب الكافي على الوعي الأمني لزيادة فهم مستخدمي الكمبيوتر وإحداث تغييرات سلوكية إيجابية لديهم (Safa, Sookhak, Von Solms, Furnell, Ghani, & Herawan, 2015).

إن النظام الآمن هو النظام الذي يتصرف بطريقة يمكن التنبؤ بها بشكل منطقي؛ ومع ذلك كما يتضح من البحوث النفسية إن سلوك الإنسان وعمليات صنع القرار متعددة الأوجه وغالباً لا يمكن التنبؤ بها، ومن أجل تحسين ممارسات الأمن السيبراني، هناك حاجة للمناقشة التي تؤكد أن الأمن السيبراني هو بطبيعته نظام اجتماعي تقني معقد، إن هذا المفهوم ليس جديداً في البحث النفسي، ففي الواقع في عام 1951 اقترح تريست وبامفورث (Trist & Bamforth,

1951)، فكرة أن التغييرات في النظام التكنولوجي يجب أن ترافقها تغييرات في النظم الاجتماعية، لأنه قد يؤدي القيام بأحدهما دون الآخر إلى فشل الأنظمة، فإذا كان المرء مهتماً بالأمن السيبراني، فيجب التحقيق في العنصر البشري بعمق، لأن العنصر البشري إذا لم يؤخذ بعين الاعتبار عندما يتعلق الأمر بالسلوك البشري فإن النظام محكوم عليه بالفشل قبل أن يبدأ (Benson, McAlaney & Frumkin, 2018).

في هذه الدراسة يتم تحليل سلوك الأمن السيبراني لدى الأفراد في المملكة العربية السعودية، ومستوى وعي الأفراد بالانتهاكات التي يمكن أن تقع خلال تعاملهم مع شبكة الانترنت، ونوعية تلك الانتهاكات أو المخاطر التي قد يتعرضون لها، وبناءً عليه تم تنظيم الورقة بالطريقة التالية؛ يستعرض أولاً الخلفية النظرية للدراسة حيث تعرض الدراسات والأبحاث ذات الصلة بسلوك الأمن السيبراني وسؤال البحث المطروح، ثم يتم مناقشة المنهجية المعتمدة، وبعد ذلك يتم عرض النتائج وتقدم مناقشة للنتائج وتفسيرها من أجل تحقيق قدر أكبر من الوضوح والتفسير لمشكلة الدراسة.

مشكلة الدراسة:

تعد قضية سلوك الأمن السيبراني من القضايا بالغة الأهمية، والتي يهتم بها الباحثين لدى مستخدمي الانترنت جميعاً ليس في المملكة العربية السعودية بل في جميع أنحاء العالم. حيث يتفق محترفو الأمن السيبراني على أن الأمن يعتمد على الأشخاص أكثر من اعتماده على الضوابط الفنية والإجراءات المضادة، وتُظهر المراجعات الحديثة لمشهد تهديدات الأمن السيبراني أنه لا يوجد قطاع محصن ضد الهجمات الإلكترونية، هذا ويتصدر القطاع العام قائمة الحوادث الأمنية المستهدفة (Benson, 2017). هذا وقد وجدت الأبحاث أنه إذا تعرض شخص ما لتهديد إلكتروني، أو أدرك مثل هذا التهديد، فمن المتوقع أن يكون يقظاً (Chen & Zahedi, 2016)، حيث أنه من المتوقع أن يستمر مجرمو الإنترنت في سرقة المعلومات الشخصية على وسائل التواصل الاجتماعي، أو مواقع الانترنت، لهذا يجب على الشخص اتخاذ جميع التدابير الأمنية اللازمة أثناء تفاعله مع الشبكات الاجتماعية، أو قيامه بالمعاملات المصرفية، أو الاتصال عبر الإنترنت (Kalhoro, Rehman, Ponnusamy & Shaikh, 2021)، وغالباً ما يفشل المستخدمون العاديون في تبني تدابير الأمان الأساسية، أو فهم مشكلات الأمان الشائعة مثل البريد الإلكتروني العشوائي أو رسائل البريد الإلكتروني الاحتيالية (Alshammari, Mylonas, Sedky, Champion & Bauer, 2015)، فالفضاء الإلكتروني والإنترنت ينطويان على مخاطر جسيمة لانتهاكات أمن المعلومات، حيث يمتلك المتسللون تقنيات متنوعة لتغيير السرية والنزاهة وتوافر المعلومات لمصلحتهم، في هذه المرحلة يصبح المستخدمون ضحايا الإنترنت بسبب إهمالهم وجهلهم أو ممارسة سلوكيات غير مقصودة مثل مشاركة كلمات المرور الخاصة بهم مع الآخرين أو تنزيل أي برنامج من الإنترنت أو استخدام أرقام الضمان الاجتماعي الخاصة بهم ككلمات مرور (Safa, Sookhak, Von Solms, Furnell, Ghani, & Herawan, 2015).

لقد تقدم علم السلوك السيبراني بشكل كبير في السنوات الأخيرة، حيث تم إجراء العديد من الدراسات حول سلوك الأمن السيبراني، خصوصاً سلوك الإنسان ومهاراته الإدراكية والعاطفية، وذلك لأن العنصر البشري سيكون دائماً هو الحلقة الأضعف وعرضة للفشل والخطأ في منظومة استخدام التقنية وشبكة الانترنت، فقد أثبتت العديد من الأبحاث وجود صلة بين الخصائص البشرية والممارسات الأمنية غير الفعالة (Egelman, Harbach, & Peer, 2016; Gratian, Bandi, Cukier, Dykstra & Ginther, 2018)، ومن هنا جاءت أهمية دراسة درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع، ومعرفة مدى وعيهم بنوعية الانتهاكات والمخاطر التي قد يتعرضون، حيث يواجه مستخدمو تقنية المعلومات العاديون لتهديدات أمنية عديدة (مثل الهجمات على البرامج، وكلمات المرور الضعيفة، والتصيد الاحتيالي) ويحتاجون إلى حماية أنفسهم من خلال اتخاذ تدابير أمنية مثل النسخ الاحتياطي وإنشاء كلمات مرور آمنة وتثبيت برامج الأمان.

أسئلة الدراسة:

1. ما درجة ممارسة سلوك الأمن السيبراني في مجالات (البرامج الخبيثة، استخدام كلمات المرور، الهندسة الاجتماعية، التصيد الالكتروني، الاحتيال عبر الانترنت) بين أفراد المجتمع السعودي؟
2. هل توجد فروق ذات دلالة في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تعزى لمتغير النوع الاجتماعي؟
3. هل توجد فروق ذات دلالة في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تعزى لمتغير المستوى التعليمي (أقل من الثانوية، بكالوريوس، ماجستير، دكتوراه)؟
4. هل توجد فروق ذات دلالة في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تعزى لمتغير للتخصص (علمي، انساني، صحي)؟

أهداف الدراسة:

تهدف هذه الدراسة إلى:

– التعرف إلى درجة ممارسة سلوك الأمن السيبراني في مجالات (البرامج الخبيثة، استخدام كلمات المرور، الهندسة الاجتماعية، التصيد الالكتروني، الاحتيال عبر الانترنت) بين أفراد المجتمع السعودي.

– التعرف إلى الفروق في متوسطات استجابات عينة الدراسة في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تبعاً لمتغير النوع الاجتماعي.

– التعرف إلى الفروق في متوسطات استجابات عينة الدراسة في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تعزى لمتغير المستوى التعليمي (أقل من الثانوية، بكالوريوس، ماجستير، دكتوراه).

– التعرف إلى الفروق في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تعزى لمتغير للتخصص (علمي، انساني، صحي).

أهمية الدراسة:

- إن أهمية هذه الدراسة تنبع من أهمية وحداثة الموضوع الذي تناولته وهو ممارسة سلوك الأمن السيبراني بين الأفراد مستخدمي شبكة الانترنت أو تطبيقات الهواتف الذكية.
- يعتقد الباحث أن هذه الدراسة من أوائل الدراسات إن لم تكن الأولى التي تناولت موضوع ممارسة سلوك الأمن السيبراني لدى الأفراد في المملكة العربية السعودية.
- تقدم الدراسة إطاراً نظرياً حول ممارسة سلوك الأمن السيبراني.
- تفتح هذه الدراسة المجال أمام الباحثين للعناية بهذا المجال والقيام بإجراء دراسات متنوعة تتناول عينات وفئات مجتمعية مختلفة في المملكة وفي الوطن العربي.
- تقدم هذه الدراسة نوعاً من التغذية الراجعة للمهتمين بالأمن السيبراني وطبيعة السلوك البشري في التعامل مع القضايا المختلفة المتعلقة به، للعمل على زيادة وعي الأفراد والمنظمات بسبل وآليات مواجهة أي تهديدات قد يتعرضون لها عبر الفضاء السيبراني.

حدود الدراسة:

تتحدد نتائج الدراسة بالمحددات التالية:

1- الحدود البشرية: تقتصر هذه الدراسة على أفراد المجتمع السعودي.

2- الحدود المكانية: تم تطبيق هذه الدراسة في المملكة العربية السعودية.

3- الحدود الزمانية: تم تطبيق هذه الدراسة في شهر حزيران 2021م\ جمادي الآخرة 1442هـ.

التعريفات الاصطلاحية والإجرائية:

السلوك:

يعرف السلوك بأنه: " "الاستجابات المنظمة داخلياً (رد الفعل أو عدم رد الفعل) للكائنات الحية الكاملة (أفراد أو مجموعات) للمثيرات الداخلية أو الخارجية، باستثناء الاستجابات التي يسهل فهمها على أنها تغيرات نمائية" (Levitis, Lidicker, & Freund, 2009, 108)

الأمن السيبراني:

حماية الأنظمة المتصلة بالإنترنت، بما في ذلك الأجهزة والبرامج والبيانات، من الهجمات الإلكترونية، ويشمل الأمن الأمن السيبراني والأمن المادي كلاهما تستخدمهما الأفراد والمؤسسات للحماية من الوصول غير المصرح به إلى مركز البيانات والأنظمة المحوسبة الأخرى (Seemma, Nandhini, & Sowmiya, 2018). وهو مجال يتعلق بأي تقنية جديدة ويشكل جزءاً منها مثل الذكاء الاصطناعي وإنترنت الأشياء والبيانات الضخمة والحوسبة المتنقلة المتقدمة والحوسبة السحابية والتجارة الإلكترونية (Elango, Matilda & Jeyasankari, 2020).

أما سلوك الأمن السيبراني فيعرف بأنه: "أفعال الفرد وردود أفعاله وسلوكياته وسلوكه العام في المجال السيبراني" (Blazy & Yeun, 2018, 147)، ويعرف إجرائياً بالدرجة التي يحصل عليها المستجيب على مقياس سلوك الأمن السيبراني.

الإطار النظري والدراسات السابقة:

لقد أصبح استخدام شبكة الانترنت أمر لا مفر منه من قبل الأفراد والمنظمات، الصغار والكبار، الأمر الذي جعل إمكانية التعرض لتهديد الأمن السيبراني أمر ممكن الحدوث للجميع، ويشير الأمن السيبراني إلى عمليات حماية البيانات والأنظمة من الهجمات الإلكترونية، فقد أصبح تأمين البيانات واحداً من أكبر المهام في يومنا الحاضر، ومن هذا المنطلق جاءت أهمية نشر وتعميم سلوكيات الأمن السيبراني على مستوى الأفراد والجماعات والمنظمات لحمايتهم من أي تهديد محتمل قد يتعرضون له.

مفهوم سلوك الأمن السيبراني:

تعد سيبراني "Cyber" بادئة تشير إلى الفضاء الإلكتروني وتشير إلى شبكات الاتصال الإلكترونية والواقع الافتراضي (Oxford, 2014). أما الأمن السيبراني فيعرف بأنه: "يتضمن الأمن السيبراني الحد من مخاطر الهجوم الضار على البرامج وأجهزة الكمبيوتر والشبكات، حيث يشتمل الأدوات المستخدمة لاكتشاف عمليات الاختراق، وإيقاف استخدامات الفيروسات، وحظر الوصول الضار، وفرض المصادقة، وتمكين الاتصالات المشفرة" (Amoroso, 2006). كما يعرف بأنه: "مجموعة التقنيات والعمليات والممارسات وتدابير الاستجابة والتخفيف المصممة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به لضمان السرية والنزاهة وامكانية الوصول" (Pub-lic Safety Canada, 2014). كما ويعرف بأنه: " النشاط أو العملية أو القدرة أو الإمكانية أو الحالة التي يتم بموجبها حماية أنظمة المعلومات والاتصالات والمعلومات الواردة أو الدفاع ضد الضرر أو الاستخدام غير المصرح به أو التعديل أو الاستغلال" (DHS, 2014). وعرف بأنه: "علم مصمم لحماية أجهزة الكمبيوتر الخاص بالفرد وكل ما يرتبط بها في

البيئة المادية ومحطات العمل والطابعات والكابلات والأقراص ووحدات الذاكرة ووسائط التخزين الأخرى (Patterson & Winston - Proctor, 2019, 32). ويتكون إطار الأمن السيبراني من شبكة مترابطة من البنى التحتية لنظم المعلومات والتي تشمل أنظمة الإنترنت والاتصالات والكمبيوتر، وتعمل معاً لحماية المعلومات في الفضاء السيبراني (Elango, Matilda & Jeyasankari, 2020).

أما سلوك الأمن السيبراني فيعرف بأنه: "استخدام العوامل النفسية والاجتماعية والمعرفية والعاطفية كبيانات لتحسين الفهم والحماية والدفاع عن نظم المعلومات والاتصالات من أي أعمال غير مصرح بها"، وعلى الرغم من وجود تداخل جوهري بين أمن المعلومات والأمن السيبراني، لكن لا يمكن القول أن المفهومين متشابهين تماماً، لذلك لا ينبغي النظر للأمن السيبراني فقط كحماية للفضاء السيبراني نفسه، ولكنه حماية الأفراد الذين يعملون في الفضاء السيبراني أيضاً، بالإضافة إلى حماية أصولهم التي يمكن الوصول إليها عبر الفضاء الإلكتروني، في ضوء ذلك يمكن أن يعرف الأمن السيبراني بأنه: "حماية الفضاء الإلكتروني نفسه والمعلومات الإلكترونية ومعلومات والتكنولوجيا والاتصالات التي تقدم الدعم للفضاء السيبراني ومستخدمي الفضاء السيبراني سواء بصفتهم الوطنية أو المجتمعية أو الشخصية، مع مراعاة مصالحهم (سواء كانت ملموسة أو غير ملموسة)، والتي يمكن أن تكون عرضة لهجمات الفضاء السيبراني" (Fatokun, Hamid, Norman, & Johnson, 2020, 19).

وتتبع أهمية الأمن السيبراني كونه المجال الذي يتعامل مع التطورات التكنولوجية المستمرة لإنشاء أنظمة آمنة وتطوير آليات دفاع ضد الهجمات الخبيثة، فقد تهدد الهجمات في الفضاء الإلكتروني سلامة وسرية وتوافر أنظمة الكمبيوتر والشبكات والبرامج والبيانات، ويتضمن الأمن السيبراني التقنيات والسياسات الأمنية وآليات الدفاع واستراتيجيات الحماية من أجل:

- تحديد وإدارة مخاطر الأمن السيبراني للبيانات والأنظمة والأصول والقدرات.
- منع الهجمات الإلكترونية وحماية الأنظمة والشبكات والبرامج والبيانات، وفي النهاية الأفراد.
- كشف الهجمات الإلكترونية.
- الاستجابة لحوادث الأمن السيبراني والتصدي للهجمات الإلكترونية.
- التعافي من الهجمات الإلكترونية (Craigen et al., 2014).

الهندسة الاجتماعية: (Social Engineering (SE): هي هجمات إلكترونية تهدف إلى استغلال نقاط ضعف العامل البشري، وهذا المفهوم ليس جديداً بل له جذوره في فن الاحتيال والخداع، ومع ذلك فإن الطبيعة "الساذجة" للبشر والاستخدام المكثف لوسائل التواصل الاجتماعي هو الذي أعاد هذه التقنية إلى الظهور من جديد، ومن خلال تقنيات الهندسة الاجتماعية يهدف الفاعل الخبيث (بشري أو برنامج) إلى إقناع الضحايا المحتملين بالمضي قدماً في إجراءات معينة (كالكشف عن المعلومات السرية، وتوفير الوصول إلى المواقع المحظورة – المادية أو الرقمية) من خلال استغلال نقاط ضعفهم (Tenove, & Moscrop, 2018)، لقد أظهرت الأبحاث أنه في عام 2020م كانت 70٪ من خروقات البيانات ناتجة عن سرقة بيانات الاعتماد وأن 22٪ منها كانت بسبب هجمات الهندسة الاجتماعية (Francois, Mercia & Venter, 2014).

التصيّد (Phishing): يعد التصيد الاحتيالي نوعاً من هجمات الهندسة الاجتماعية، حيث يتم استخدامه لسرقة معلومات المستخدم، بالإضافة إلى بيانات اعتماد تسجيل الدخول وأرقام بطاقات الصراف الآلي، ويحدث ذلك عندما ينتحل أحد

المهاجمين صفة شخص موثوق به أو أي منظمة، أو عندما يفتح الضحية رابطًا ضاراً أو بريداً إلكترونياً، والذي يمكنه تثبيت البرامج الضارة في نظام الضحية وسرقة بياناته (Thakur, Qiu, Gai & Ali, 2015).

البرامج الخبيثة (Malware): هي برامج ضارة جدًا للأنظمة لأنها تلحق الضرر بنظام الكمبيوتر أو تعمل على تعطيله، كما أنها تسمح بالتحكم في نظام الكمبيوتر للشخص منشئ تلك البرمجيات الخبيثة، وهي برامج تقوم بتثبيت نفسها في الجهاز الذي يتم انتهاكه بشكل غادر من أمثلتها (Trojan horse, Virus, Backdoor, Rootkit, Ransomware) (Tomar & Singh, 2021).

كلمات المرور (Password usage): كلمات المرور هي أكثر أشكال التعريف الشخصي المستخدمة شيوعاً لردع الوصول غير المصرح به إلى أنظمة وشبكات الكمبيوتر، تم تطوير معيار استخدام كلمة المرور لضمان التخزين الآمن لكلمات المرور ومعالجتها، هذا المعيار هو واحد في سلسلة من معايير وإرشادات أمان الكمبيوتر الصادرة عن المكتب الوطني للمعايير (NBS)، وكلمة المرور عبارة عن سلسلة من الأحرف يتم إنشاؤها أو تحديدها من مجموعة من الحروف والرموز المقبولة، حيث يحتوي نظام كلمات المرور الجيد على مجموعة كبيرة جداً من الحروف والرموز المتاحة، وكلما كانت المجموعة أكبر زادت صعوبة تخمين كلمة المرور الصالحة لأي شخص غير مصرح له (Branstad & Gallegos, 1988).

الاحتيال عبر الإنترنت (Online scam): تهدف عمليات الاحتيال عبر الإنترنت إلى الاحتيال على الضحايا، حيث يستخدم المحتالون طرقاً مختلفة لسرقة المعلومات الخاصة بالضحايا وتضليلهم لدفع مبالغ مالية (Vahdati & Yasini, 2015)، أحد أشهر أنواع عمليات الاحتيال عبر الإنترنت هو الاحتيال عبر عمليات الشراء، حيث يقوم المحتالون بجمع معلومات بطاقة الائتمان الخاصة بمستخدمي الإنترنت وأرقام PIN، والتي يستخدمونها بعد ذلك لسحب الأموال من الحساب المالي للضحية (Yazdanifard, WanYusoff, Behora, & Sade, 2011).

الدراسات السابقة:

يستعرض هذا الجزء الدراسات السابقة التي تناولت موضوع الدراسة الحالية، وتم استعراضها بتسلسل من الأحدث للأقدم:

أجرى سليمان وفوزي وحسين وبدر (Sulaiman, Fauzi, Hussain, & Wider, 2022)، دراسة هدفت إلى التعرف إلى سلوك الأمن السيبراني بين موظفي الحكومة في ماليزيا ودور نظرية دافع الحماية والمسؤولية تحسين هذا السلوك. استخدمت الدراسة منهج البحث الكمي، وتم جمع بيانات الدراسة بواسطة استبيان ذاتي الكتروني، تكونت عينة الدراسة من (446) مشاركاً، أظهرت نتائج الدراسة أن الموظفين الذين لديهم دافعية بدرجة عالية واحساس بالخطورة وفعالية الاستجابة والكفاءة الذاتية لديهم مرتفعة يمارسون سلوك الأمن السيبراني، كما أظهرت النتائج إن دمج تصورات المستخدمين للضعف والقوة يسهل التغيير السلوكي ويزيد من فهم دور سلوك الأمن السيبراني في معالجة تهديدات الأمن السيبراني لا سيما تأثير الاستجابة للتهديد في التنبؤ بسلوك الأمن السيبراني لموظفي الحكومة.

أجرى خان وفاروق وخان واكرام (Khan, Yaqoob, Khan, & Ikram, 2022)، دراسة هدفت إلى القاء نظرة شاملة على البحوث السلوكية المتعلقة بالأمن السيبراني المتوفرة في الأدب المنشور، استخدمت الدراسة المنهج النوعي، تم جمع بيانات الدراسة من خلال مراجعة الدراسات والأبحاث السابقة، تكونت عينة الدراسة من (107) دراسة في سلوك الأمن السيبراني، أظهرت نتائج الدراسة أن مجال سلوك الأمن السيبراني مجال ناشئ للبحوث السلوكية ولا يزال في مرحلة تطوير النظرية بسبب حداثة المساعي البحثية لتحديد اللبنات النظرية لهذا كانت النتائج غير متسقة في البحوث

التجريبية، تعتبر المعتقدات المعرفية والأنطولوجية السائدة ذات طبيعة إيجابية مع ندرة الأبحاث التي تستخدم نماذج أخرى لدراسة الجانب الإنساني من الأمن السيبراني.

اجرى كل من هونج وفورنيل (Hong & Furnell, 2021)، دراسة هدفت إلى فحص تشكيل العادات السلوكية للأمن السيبراني لدى الطلبة، استخدمت الدراسة مسح سلوك الأمن السيبراني تم تطبيقه على (393) طالباً جامعياً، استخدمت الدراسة المنهج الوصفي، أظهرت النتائج أن الفعالية والشمولية السلوكية تتنبأ بالعادات السلوكية للأمن السيبراني، إن الفعالية لها تأثير إيجابي على الشمولية السلوكية؛ إن الدعم الظرفي له تأثير إيجابي على الفعالية، كما تشير النتائج إلى أن العادات السلوكية للأمن السيبراني يمكن تشكيلها من خلال تعزيز تنوع تدابير الأمن السيبراني المتبعة (الشمولية السلوكية) والفعالية.

أجرى علي وآخرون (Ali, Dominic, Ali, Rehman & Sohail, 2021)، دراسة هدفت إلى تحديد الخطوات العملية في تحول الموظفين من سلوك عدم الامتثال إلى سلوك الامتثال لسياسة أمن المعلومات. استخدمت الدراسة المنهج النوعي، ومن خلال مراجعة الأدب السابقة والدراسات المتعلقة بالموضوع تم جمع بيانات الدراسة، تم تحليل وترميز نتائج (80) دراسة، أظهرت نتائج مراجعة الأدبيات أن الثقافة الوطنية لها تأثيرات مختلف على سلوك امتثال الموظفين لأمن المعلومات، حيث أظهرت دراسات متعددة أن الثقافة الوطنية يمكن أن تؤثر على سلوك أمن المعلومات في المنظمات، كما أظهرت النتائج أن الدوافع الداخلية والخارجية لدى الموظف لديها تأثير على سلوك الامتثال، كما ظهر أن ثقافة أمن المعلومات والوعي لدى الموظفين يعزز سلوك الامتثال، ووجدت الدراسة أن الإجهاد / التحييد المرتبط بالأمن، وتضارب القيم، والردع هي الفئات الرئيسية الثلاث للعوامل التي تؤدي إلى عدم الامتثال. وقدمت الدراسة نموذجاً لخطوات التحول من عدم الامتثال إل الامتثال لسلوك أمن المعلومات الذي يمكن أن تتبعه المنظمات.

أجرى بابستروشا وآخرون (Papatsaroucha, Nikoloudakis, Kefaloukos, Pallis & Markakis, 2021)، دراسة مفاهيمية تحليلية هدفت إلى تقييم نقاط الضعف البشرية والتي تعد جانباً أساسياً من جوانب الأمن السيبراني، ومحاولة تقديم حلول تحفز العامل البشري على الالتزام بالسلوك السيبراني الآمن من خلال التدريب والتكتيكات الأمنية وزيادة الوعي. قامت الدراسة على مراجعة الأدب والدراسات السابقة، أظهرت النتائج أن هناك العديد من الخصائص المختلفة التي تؤثر أو تشكل نقاط ضعف بشرية في الآمن السيبراني، تلك النقاط التي يحاول العديد من الأشخاص استغلال لصالحهم بطريقة خبيثة من خلال استخدام العديد من استراتيجيات الإقناع والخداع للأفراد مستخدمي شبكة الإنترنت، وأهم هذه الخصائص:

- السمات الشخصية.
- العمليات المعرفية، مثل (معالجة المعلومات، واتخاذ القرار، ونوايا السلوك المتعلقة بالأمن، دافعية الحماية والمخاطرة).
- التركيبة السكانية مثل الجنس والعمر والخلفية الثقافية.
- المهنة والخبرة الحاسوبية.
- الأوضاع الاجتماعية الحالية، مثل تفشي مرض كوفيد –19.
- عبء العمل والاجهاد والضغط في بيئة العمل.

كما أظهرت نتائج هذه الورقة أن الحفاظ على الأمن يتطلب زيادة كبيرة في وعي المستخدم النهائي تجاه حوادث الأمن السيبراني، لهذا يحتاج المستخدمون إلى تثقيفهم حول أفضل ممارسات وتكتيكات الأمن السيبراني التي يمكن أن

يستخدموها لحماية أنفسهم من الانتهاكات.

أجرى فاتوكان وآخرون (Fatokun et al., 2020)، دراسة هدفت إلى فحص سلوك الأمن السيبراني لدى طلبة مؤسسات التعليم العالي وعلاقته ببعض المكونات مثل الضعف المتصور، فعالية الاستجابة، سلوك الأقران، مهارات الحاسوب، الخبرة السابقة في الأمان السيبراني، واستكشاف العلاقة بين سلوك الأمن السيبراني وهذه المكونات لدى الطلبة. استخدمت الدراسة المنهج الوصفي التحليلي، تكونت عينة الدراسة (435) طالباً وطالبة في مؤسسات التعليم العالي من منطقة وادي كالانج\ماليزيا، تم توزيع استبيان عن طريق الانترنت لجمع بيانات الدراسة، أظهرت النتائج أن هناك علاقة بين جميع المكونات في الدراسة وسلوك الأمن السيبراني لدى عينة الدراسة، كما أظهرت أن أهم العوامل ذات الصلة بسلوك الأمن السيبراني لدى طلبة مؤسسات التعليم العالي في ماليزيا، هي: الكفاءة الذاتية للأمان، والتجارب السابقة مع سلوكيات أمان الكمبيوتر.

أجرت ماكيل وتومسون (McGill & Thompson, 2018)، دراسة هدفت إلى استكشاف الفروق بين الجنسين في تصورات وسلوك الأمن السيبراني لديهم، وتحديد آثار هذه التصورات في تأمين المعلومات الشخصية والبرامج، استخدمت الدراسة المنهج الوصفي التحليلي، وتكونت عينة الدراسة من (624) فرداً من مستخدمي الانترنت تم اختيارهم بطريقة عشوائية، تم جمع بيانات الدراسة بواسطة استبيان تم توزيعة عن طريق الانترنت، أظهرت نتائج الدراسة أن الذكور بشكل عام لديهم سلوك أمن سيبراني أعلى من الإناث، لكن لم تظهر فروق بين الجنسين في تمكين التحديث التلقائي للبرامج، وتأمين الأجهزة بكلمات مرور واستخدام برامج الأمان، كما أظهرت النتائج أيضاً أن الإناث يظهرن مستويات أقل في مهارات تكنولوجيا المعلومات والتدريب على أمن المعلومات.

أجرى ماشيان وكريتزنجر (Mashiane & Kritzinger, 2018)، دراسة مفاهيمية هدفت إلى توفير تصور واضح حول سلوك الأمن السيبراني في مكان العمل من خلال مراجعة الدراسات السابقة، كانت الدراسات السابقة موحدة وممثلة بيانياً على رسم بياني واحد، حيث مثلت الأبحاث السابقة نوايا مستخدمي سلوك الأمن السيبراني على خط متصل يتراوح من النوايا الخبيثة إلى النوايا الصالحة، وقامت الدراسة بتقسيم النوايا إلى وحدات قياس أصغر، أظهرت نتائج الدراسة أن هناك أربع فئات لوصف نوايا سلوك الأمن السيبراني للمستخدم، أما في الجزء الثاني من الدراسة والذي ركز على سلوك الأمن السيبراني لدى المستخدم المنزلي، وجد أن هناك ثماني فئات لوصف النوايا في سلوك الأمن السيبراني لدى مستخدم المنزلي. تساعد هذا الدراسة في تعديل السؤال من "كيف نغير سلوك الأمن السيبراني؟" إلى "كيفية تغيير سلوك الأمن السيبراني لدى المستخدمين المنزليين الذين يظهرون سلوك الكسل المعرفي؟

أجرى هدلينجتون (Hadlington, 2018)، دراسة هدفت إلى استكشاف وجود علاقة بين تكرار الانخراط في سلوكيات الأمن السيبراني المحفوفة بالمخاطر وعمر الفرد، وموقفه تجاه الأمن السيبراني وحجم المنظمة التي يعمل بها الفرد، تم توزيع استبيان عبر الإنترنت، استجاب له (538) مشاركاً من المملكة المتحدة، استخدمت الدراسة مقياسين الأول مقياس سلوك الأمن السيبراني المحفوفة بالمخاطر (Risky cyber security behaviours scale (RScB)، والاتجاه نحو الامن السيبراني في مكان العمل (Attitudes towards cyber security in business (ATC-IB). أظهرت نتائج الدراسة أن موقف المشاركين تجاه الأمن السيبراني في مكان العمل ليس هو الشاغل الرئيسي لهم، ويتزايد احساسهم بعدم المسؤولية المفوضة لهم بشكل أكبر كلما كان الفرد يعتقد أنه محمي من خلال التدخلات التقنية التي توفرها منظمته المضيفة مما يدفعه إلى الإنخراط في سلوكيات أمنية إلكترونية أكثر خطورة، كما أظهرت النتائج وجود فروق ذات دلالة

في سلوك الأمن السيبراني لدى المشاركين تعزى للعمر، وموقفه تجاه الأمن السيبراني، وحجم المنظمة، حيث يُظهر الأفراد في الفئة العمرية الأعلى موقفاً أكثر إيجابية تجاه الأمن السيبراني، حيث ويرون أن الانخراط في ممارسات الأمن السيبراني الجيدة هو جزء أساسي من حياتهم العملية، وأن المشاركين الذين يعملون مع شركات لديها (250) موظفاً أو أكثر كانوا يتمتعون بأعلى مستوى من المشاركة في سلوكيات الأمن السيبراني المحفوفة بالمخاطر، وتنخفض هذه المشاركة في الشركات التي يزيد عدد موظفيها عن (250) موظفاً.

أجرى جيسكي وشيك (Jeske & Schaik, 2017)، هدفت إلى استكشاف مدى إلمام ودراية الطلبة بالتهديدات المختلفة عبر الانترنت، والمقارنة بين ثقافات مختلفة (الولايات المتحدة، بريطانيا) في درجة إلمام الطلاب ودرايتهم بالتهديدات عبر الانترنت وسلوكهم تجاهها، كما تفحص الدراسة إلى أي مدى تعد الدراية والألفة مع الانترنت (الخبرة السابقة) متغير وسيط في الاجراءات الأمنية والسلوك الأمني السيبراني الذي يمارسه الطلاب. تكونت عينة الدراسة من (169) طالباً من الولايات المتحدة، و(154) من بريطانيا)، تم جمع بيانات الدراسة بواسطة الاستبيان، أظهرت نتائج الدراسة أن عينة الولايات المتحدة وبريطانيا كان لديهم تشابه في إلمامهم ودرايتهم ب (16) تهديداً قد يتعرضون لها أثناء استخدام شبكة الانترنت، كما أظهرت النتائج أن هنا فروق بين مدى دراية وإلمام المجموعات بحيث قسمت إلى ثلاث مجموعات، مجموعة على دراية كبيرة بالتهديدات وصفت بالخبراء، ومجموعة على إلمام ودراية أقل بالتهديدات، وكان لدى المجموعة الأخيرة إلمام أعلى بقليل من المتوسط بمعظم التهديدات الستة عشر، كما أظهرت النتائج أن الألفة والدراية بالتهديدات هي وسيط مهم بين استخدام الإنترنت والسلوكيات الأمنية – مما يجعلها متغيراً وسيطاً مهماً يجب مراعاته من حيث التدريب على التدخلات المستقبلية الموجهة نحو التهديد والتي تهدف إلى تطوير وتحسين س الأمنية السيبرانية.

أجرى موناندي وآخرون (Muniandy et al., 2017)، دراسة هدفت إلى استكشاف واقع سلوك الأمن السيبراني لدى طلبة الدراسات العليا في ماليزيا، استخدمت الدراسة المنهج الوصفي التحليلي، واستخدم الاستبيان لجمع بيانات الدراسة، تكونت عينة الدراسة من (128) طالباً وطالبة من طلبة الدراسات العليا، أظهرت نتائج الدراسة أظهرت الدراسة أن سلوك الأمن السيبراني بين المستجيبين كان غير مرض بشكل عام في جميع قضايا الأمن السيبراني الخمس التي تمت دراستها (البرامج الخبيثة، استخدام كلمة المرور، الغش الالكتروني، الهندسة الاجتماعية (فن اختراق العقول)، احتيال عبر الإنترنت).

التعليق على الدراسات السابقة:

يتبين مما تم عرضه من الدراسات السابقة أنها جميعها ركزت على سلوك الأمن السيبراني باختلاف طريقة تناول الموضوع، ومعظم الدراسات استخدمت المنهج الوصفي وهي تتفق مع الدراسة الحالية، ما عدا بعضها مثل دراسة ماشيان وكريتزنجر (Mashiane & Kritzinger, 2018)، ودراسة بابستروشا وآخرون (Papatsaroucha et al., 2021)، حيث كانت دراسات مفاهيمية تعتمد مراجعة الأدبيات السابقة وتحليلها، ودراسة علي وآخرون (Ali et al., 2021)، التي اعتمدت المنهج النوعي. استفادت الدراسة الحالية من الدراسات السابقة في بناء الإطار النظري، وأداة الدراسة، كما استفادت في مناقشة نتائج الدراسة والمقارنة بينها وبين نتائج الدراسات السابقة، من حيث مدى الاتفاق والاختلاف فيما بينها.

الطريقة والإجراءات:

منهجية الدراسة: اعتمدت الدراسة على استخدام المنهج الوصفي التحليلي كونه المنهج المناسب للدراسة الحالية.

مجتمع وعينة الدراسة: تكون مجتمع الدراسة من الأفراد في المملكة العربية السعودية من مستخدمي شبكة الإنترنت، وتطبيقات الهواتف الذكية المختلفة، وعبر استبيان عبر الإنترنت من خلال (Qualtrics Online Sampling)، في الفترة من 15 إلى 20 حزيران 2021م، أكمل (712) مشاركاً الاستطلاع تم استهدافهم بطريقة عشوائية من خلال موقع تويتر ومجموعات التليجرام والواتس آب والفيسبوك، وكان مقرهم جميعاً في المملكة العربية السعودية، تم حذف بيانات (12) مشاركاً واستبعادهم من التحليل بسبب البيانات غير المكتملة أو المفقودة، وبهذا تكون عينة الدراسة النهائية (700) مشاركاً، توزعوا حسب متغيرات الدراسة الديموغرافية كما يظهر الجدول رقم (1):

الجدول رقم (1) توزيع مجتمع الدراسة حسب الخصائص الديموغرافية (n=700)

المتغير		العدد	النسبة المئوية
النوع	ذكر	215	30.7%
	أنثى	485	69.3%
	المجموع	700	100%
المستوى التعليمي	ما دون الثانوية	260	37.1%
	بكالوريوس	395	56.4%
	دراسات عليا	45	6.4%
	المجموع	700	100%
التخصص	كليات صحية	413	59%
	كليات إنسانية	72	10.3%
	كليات علمية	215	30.7%
	المجموع	700	100%

وبالنظر إلى الجدول السابق نلاحظ أن (31%) من عينة الدراسة كانوا من الذكور مقابل (69%) من الإناث، وأن (56%) من عينة الدراسة هم من حملة شهادة البكالوريوس، مقابل (6%) فقط من حملة الشهادات العليا، و(37%) من حملة الشهادة الثانوية، كما تبين أن (59%) هم من منتسبي الكليات الصحية، فيما كان (31%) من منتسبي الكليات العلمية، وكانت النسبة الأقل هي منتسبي الكليات الإنسانية حيث كانت نسبتهم من عينة الدراسة (10%) من مجموع أفراد عينة الدراسة.

أداة الدراسة: اعتمدت الدراسة على المقياس الذي أعده (Muniandy, Muniandy & Samsudin, 2017)، بعد أن قام الباحث بترجمته إلى اللغة العربية، وتم اختيار ما يتناسب مع الدراسة الحالية، وقد اشتمل المقياس على قسمين، هما: القسم الأول من المقياس يحتوي على معلومات حول (النوع، والمستوى التعليمي، والتخصص). والقسم الثاني يغطي أهم سلوكيات الأمن السيبراني بين الأفراد مستخدمي الإنترنت. ويكون الميزان التقديري وفقاً لمقياس ليكرت الثلاثي كما يلي:

جدول رقم (2) ميزان تقديري وفق مقياس ليكرت الثلاثي

المتوسط المرجح	المستوى
من 1 إلى 1,66	قليل جداً
من 1,67 إلى 2,33	أحياناً
من 2,34 إلى 3	غالباً

دلالات صدق وثبات أداة الدراسة:

عرض الباحث المقياس بعد ترجمته على (10) محكماً من أعضاء هيئة التدريس في جامعة الملك سعود وجامعة أم القرى، وذلك للتأكد من صحة الترجمة، وذلك بإرفاق النص باللغة الانجليزية والترجمة العربية معاً لمعرفة مدى ملاءمتها

للبيئة السعودية، وللكشف عن مدى مناسبة الفقرات لقياس ما وضعت لقياسه، ومدى ووضوحها وسلامتها اللغوية.

وللتأكد من ثبات أداة الدراسة (المقياس)، فقد تم التحقق بطريقة الاختبار وإعادة الاختبار (test-retest) بتطبيق المقياس، وإعادة تطبيقها بعد أسبوعين على مجموعة مكوّنة من (20) فرداً، ومن ثم تم حساب معامل ارتباط بيرسون بين درجاتهم في المرتين اذ بلغ (0.92). وتم أيضاً حساب معامل الثبات بطريقة الاتساق الداخلي حسب معادلة كرونباخ ألفا، اذ بلغ (0.86) واعتبرت هذه القيم ملائمة لغايات هذه الدراسة.

المعالجة الإحصائية: من اجل الإجابة عن أسئلة الدراسة تم معالجة البيانات باستخدام الرزمة الإحصائية للعلوم الاجتماعية (SPSS) على نحو استخدام المتوسطات الحسابية والانحرافات المعيارية واختبار (ت) (t-test)، وتحليل التباين، واختبار اقل فرق معنوي LSD.

تحليل نتائج الدراسة:

السؤال الأول: ما درجة ممارسة سلوك الأمن السيبراني في مجالات (البرامج الخبيثة، استخدام كلمات المرور، الهندسة الاجتماعية، التصيد الالكتروني، الاحتيال عبر الانترنت) بين أفراد المجتمع السعودي؟

للإجابة عن سؤال الدراسة الأول تم استخراج المتوسطات الحسابية، والانحرافات المعيارية والرتبة لفقرات درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي، والجداول من (3)–(8) توضح تلك النتائج.

جدول رقم (3) المتوسطات الحسابية والإنحرافات المعيارية والرتبة لمحاور مقياس سلوك الأمن السيبراني

م	الرتبة	المحور	المتوسط الحسابي	الانحراف المعياري	الاتجاه العام
1	الأول	الهندسة الاجتماعية	2.1820	.40952	أحياناً
2	الثاني	استخدام كلمات المرور	2.1590	.42401	أحياناً
3	الثالث	البرامج الخبيثة	2.1310	.52067	أحياناً
4	الرابع	التصيد الإلكتروني	2.0850	.48051	أحياناً
5	الخامس	الاحتيال عبر الإنترنت	1.9740	.48141	أحياناً

يتضح من خلال النتائج الموضحة في الجدول رقم (3) أن المتوسط المرجح لكافة المحاور تراوح بين (1.97–2.18)، وهذا يشير إلى أن الاتجاه العام لجميع محاور ممارسة سلوك الأمن السيبراني إلى أحياناً، بينما جاء محور الاحتيال عبر الإنترنت هو المحور الأخير والذي يدل على أن الأفراد حذرين أن يقعوا ضحية للاحتيال عبر الانترنت لهذا فإنهم يسلكون سلوكاً أمناً أثناء التعرض لانتهاكات الاحتيال. وفيما يلي عرض لبيانات كل محور من المحاور الخمسة.

جدول رقم (4) المتوسطات الحسابية والانحرافات المعيارية والرتب والاتجاه العام لفقرات محور البرامج الخبيثة (n=700)

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الرتبة	الاتجاه العام
1	أنت على استعداد لفتح مرفق بريد إلكتروني من أشخاص غرباء.	2.64	.652	الثانية	غالباً
2	يؤدي بك العنوان المثير للإهتمام الى فتح المرفق داخل رسائل البريد الإلكتروني.	2.25	.903	السابعة	أحياناً
3	أنت متأكد جدًا من حالة برامج مكافحة الفيروسات في حاسوبك الشخصي.	2.54	.722	السادسة	غالباً
4	أنت مهتم بفتح مرفق ذا إمتدادات متعددة.	2.57	.731	الثالثة	غالباً
5	تشعر بأنه حصل خطأ ما اذا بدأ حاسوبك بالتباطؤ.	1.44	.751	العاشرة	قليل جداً
6	تُحمل برمجيات/برامج مجانية من على الإنترنت.	2.70	.580	الأولى	غالباً
7	تفحص الأقراص القابلة للإزالة قبل إستخدامها على حاسوبك الشخصي.	2.64	.652	الثانية	غالباً
8	تُحمل برامج مكافحة الفيروسات وجدران الحماية ومكافحة التجسس.	2.25	.903	السابعة	أحياناً
9	أنت على استعداد لتحميل مواد من مواقع غير موثوقة.	2.54	.722	السادسة	غالباً

10	تطبق التصحيحات الأمنية في أسرع وقت ممكن.	2.57	.731	الثالثة	غالباً
11	الاتجاه العام للمحور	2.1310	.52067	أحياناً	

يتضح من خلال النتائج الموضحة في الجدول رقم (4) أن المتوسط المرجح تراوح بين (2.70–1.44)، وأن الاتجاه العام لمحور البرامج الخبيثة هو (أحياناً)، وقد كانت الفقرات ذات المرتبة الأولى هي (تحمل برمجيات/برامج مجانية من على الإنترنت) هي الفقرة التي حصلت على أعلى متوسط ترجيحي يقدر ب (2.70)، وهو سلوك غالباً ما يقوم به أفراد الدراسة، مما يدل على أن هذه ثغرة واضحة في في سلوك الأمن السيبراني لديهم. جاءت بعدها في الترتيب الفقرة التي حصلت على متوسط حسابي يقدر ب (2.64)، وهي (أنت على استعداد لفتح مرفق بريد إلكتروني من أشخاص غرباء)، وهي السلوك الثاني في ترتيب الخطورة الذي يعرض أفراد الدراسة للانتهاكات عبر شبكة الانترنت، وعدم اخذ الحيطة والحذر بالالتزام بسلوك آمن أثناء استخدام الفضاء السيبراني. فيما جاءت الفقرة الأخيرة في الترتيب، والتي حصلت على متوسط ترجيحي يقدر ب (1.44)، وهي (تشعر بأنه حصل خطأ ما اذا بدأ حاسوبك بالتباطؤ)، مما يدل على عدم ملاحظة أفراد العينة وجود خطأ ما في الحاسوب، وربط هذا التباطؤ بوجود برامج خبيثة في الجهاز.

جدول رقم (5) المتوسطات الحسابية والانحرافات المعيارية والرتب والاتجاه العام لفقرات محور استخدام كلمات المرور (n=700)

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الرتبة	الاتجاه العام
1	تستخدم كلمة سر لا تتبع نمط لوحة المفاتيح.	2.50	.778	الثالثة	غالباً
2	تشارك كلمة السر مع الآخرين.	1.29	.652	عاشرة	قليل جداً
3	تستخدم كلمات سر مختلفة لتطبيقات مختلفة.	2.31	.894	الخامسة	أحياناً
4	تستخدم كلمة سر تحتوي على أحرف كبيرة، أحرف صغيرة، أرقام، أشكال مختلفة.	2.71	.647	الأولى	غالباً
5	تستخدم كلمات سر أطول من 8 مقاطع/أحرف.	2.56	.770	الثانية	غالباً
6	تستخدم كلمات سر تعتمد على معلوماتك شخصية.	1.89	.940	الثامنة	أحياناً
7	لم تغير كلمة السر مطلقاً.	1.80	.908	تاسعة	أحياناً
8	تستخدم خيار "تذكر كلمة السر"	2.22	.923	السادسة	أحياناً
9	أنت معتاد على كتابة كلمات السر في مكان ما لحفظها.	2.32	.892	الرابعة	أحياناً
10	لم تستخدم أبداً خيار "تلميح" لاستعادة كلمة السر.	1.99	.897	السابعة	أحياناً
11	الاتجاه العام للمحور	2.1590	.42401	أحياناً	

يتضح من خلال النتائج الموضحة في الجدول رقم (5) أن المتوسط المرجح تراوح بين (2.71–1.29)، وأن الاتجاه العام لمحور استخدام كلمات المرور هو (أحياناً)، وقد كانت الفقرات ذات المرتبة الأولى هي: (تستخدم كلمة سر تحتوي على أحرف كبيرة، أحرف صغيرة، أرقام، أشكال مختلفة)، هي الفقرة التي حصلت على أعلى متوسط ترجيحي يقدر ب (2.71)، وهو سلوك غالباً ما يقوم به أفراد الدراسة، تلتها الفقرة (تستخدم كلمات سر أطول من 8 مقاطع/أحرف)، بمتوسط بلغ (2.56)، وجاءت في المرتبة الثالثة الفقرة (تستخدم كلمة سر لا تتبع نمط لوحة المفاتيح)، بمتوسط ترجيحي (2.50)، وكانت الفقرة (تشارك كلمة السر مع الآخرين)، هي الفقرة التي احتلت المرتبة الأخيرة في هذا المحور بمتوسط ترجيحي بلغ (1.29).

جدول رقم (6) المتوسطات الحسابية والانحرافات المعيارية والرتب والاتجاه العام لفقرات محور الهندسة الاجتماعية (n=700)

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الرتبة	الاتجاه العام
1	لست مهتماً بقراءة القضايا الهندسية الاجتماعية.	2.23	.833	السادسة	أحياناً
2	أنت على استعداد لكشف اسم المستخدم وكلمة المرور لأي شخص يدعي أنه مسؤول نظام.	1.54	.786	العاشرة	قليل جداً
3	لست هدف لهجمات الهندسة الاجتماعية بسبب وضعك كطالب.	2.04	.795	السابعة	أحياناً
4	لست على استعداد للرد على المكالمات، الرسائل القصيرة، أو رسائل البريد الإلكتروني الودية / للغرباء الغير مهددين.	2.35	.822	الرابعة	غالباً
5	لديك الرغبة لإتباع تعليمات معطاة من خلال أشخاص يتكلموا بسلطة.	1.77	.804	الثامنة	أحياناً
6	لديك الرغبة بتوفير كلمة السر الى مكتب المساعدة.	1.69	.818	التاسعة	أحياناً
7	أتأكد من رخصة أو هوية الشخص قبل التكلم عن أي مشكلة.	2.63	.687	الثانية	غالباً
8	لا أشعر بالخوف من الأسئلة الموجهة من شخص ما.	2.31	.842	الخامسة	أحياناً
9	لن أتواصل مع الغرباء حتى إذا كان مظهره/ا يستدعي التعاطف.	2.54	.741	الثالثة	غالباً
10	لن أكشف عن أي معلومات سرية تحت أي ظروف.	2.72	.602	الأولى	غالباً
11	الاتجاه العام للمحور	2.1820	.40952	أحياناً	

يتضح من خلال النتائج الموضحة في الجدول رقم (6) أن المتوسط المرجح تراوح بين (2.72–1.54)، وأن الاتجاه العام لمحور الهندسة الاجتماعية هو (أحياناً)، وقد كانت الفقرة ذات المرتبة الأولى هي: (لن أكشف عن أي معلومات سرية تحت أي ظروف)، هي الفقرة التي حصلت على أعلى متوسط ترجيحي يقدر ب (2.72)، وهو سلوك غالباً ما يقوم به أفراد الدراسة، تلتها الفقرة (أتأكد من رخصة أو هوية الشخص قبل التكلم عن أي مشكلة)، بمتوسط بلغ (2.63)، وجاءت في المرتبة الثالثة الفقرة (لن أتواصل مع الغرباء حتى اذا كان مظهره/ا يستدعي التعاطف)، بمتوسط ترجيحي (2.54)، وجاءت في المرتبة الرابعة وباتجاه (غالباً) الفقرة (لست على استعداد للرد على المكالمات، الرسائل القصيرة، أو رسائل البريد الإلكتروني الودية / للغرباء الغير مهددين)، بمتوسط ترجيحي (2.35)، وكانت الفقرة (أنت على استعداد لكشف اسم المستخدم وكلمة المرور لأي شخص يدعي أنه مسؤول نظام)، هي الفقرة التي احتلت المرتبة الأخيرة في هذا المحور بمتوسط ترجيحي بلغ (1.54).

جدول رقم (7) المتوسطات الحسابية والانحرافات المعيارية والرتب والاتجاه العام لفقرات محور التصيد الإلكتروني (n=700)

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الرتبة	الاتجاه العام
1	توسع معرفتك بالتصيد من خلال قراءة مواد التصيد.	2.83	.752	الأولى	غالباً
2	أنت لست هدف لهجمة تصيد بسبب وضعك كطالب.	2.05	.804	السابعة	أحياناً
3	أنت على استعداد لتقديم معلومات سرية لأي نوع بريد إلكتروني يصلك.	1.40	.686	العاشرة	قليل جداً
4	أنت على استعداد للضغط على الروابط التشعبية في أي بريد إلكتروني يصلك.	1.44	.718	الثامنة	قليل جداً
5	تثق في أي بريد إلكتروني يقدم مسابقات/جوائز.	1.44	.704	الثامنة	قليل جداً
6	لابد أن يبدأ الرابط الذي تستخدمه ب "https" إذا كنت أنقل معلومات شخصية.	2.29	.746	الخامسة	أحياناً
7	لابد أن يتواجد شعار القفل لأنقل أي معلومات حساسة.	2.50	.730	الثالثة	غالباً
8	أفضل كتابة الرابط في متصفح جديد عوضاً عن ضغط الروابط التشعبية.	2.41	.742	الرابعة	غالباً
9	استلام بريد إلكتروني مشبوه سوف يدفعني للتواصل مع الجهة المعنية للتأكد من صحة المعلومات/البريد.	2.28	.851	السادسة	أحياناً

10	سأتأكد من إملاء الرابط قبل إجراء أي عمليات/صفقات.	2.66	.619	الثانية	غالباً
11	الاتجاه العام للمحور	2.0850	.48051	أحياناً	

يتضح من خلال النتائج الموضحة في الجدول رقم (7) أن المتوسط المرجح تراوح بين (2.83–1.40)، وأن الاتجاه العام لمحور التصيد الالكتروني هو (أحياناً)، وقد كانت الفقرة ذات المرتبة الأولى هي: (توسع معرفتك بالتصيد من خلال قراءة مواد التصيد)، هي الفقرة التي حصلت على أعلى متوسط ترجيحي يقدر ب (2.83)، وهو سلوك غالباً ما يقوم به أفراد الدراسة، تلتها الفقرة (سأتأكد من إملاء الرابط قبل إجراء أي عمليات/صفقات)، بمتوسط بلغ (2.66)، وجاءت في المرتبة الثالثة الفقرة (لابد أن يتواجد شعار القفل لأنقل أي معلومات حساسة)، بمتوسط ترجيحي (2.50)، وجاءت في المرتبة الرابعة وباتجاه (غالباً) الفقرة (أفضل كتابة الرابط في متصفح جديد عوضاً عن ضغط الروابط التشعبية)، بمتوسط ترجيحي (2.41)، وكانت الفقرة (أنت على استعداد لتقديم معلومات سرية لأي نوع بريد إلكتروني يصلك)، هي الفقرة التي احتلت المرتبة الأخيرة في هذا المحور بمتوسط ترجيحي بلغ (1.40).

جدول رقم (8) المتوسطات الحسابية والانحرافات المعيارية والرتب والاتجاه العام لفقرات محور الاحتيال عبر الانترنت (n=700)

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الرتبة	الاتجاه العام
1	حققت علاقات موثوقة مع الغرباء على الإنترنت.	1.68	.856	السادسة	أحياناً
2	أتجاهل رسائل البريد الإلكتروني التي تصل على شكل إعلان من الشركات والمؤسسات المعروفة	2.44	.797	الثانية	غالباً
3	أرد على إعلانات المسابقات التي تحتوي كمية هائلة من المال في الرسائل القصيرة.	1.48	.763	التاسعة	قليل جداً
4	لا أثق بمعلومات الغرباء الشخصية المعطاة على الإنترنت.	2.56	.763	الأولى	غالباً
5	لم أفكر أبدًا في تقديم أي مبلغ من المال مقابل الخدمات التي يقدمها موقع على الإنترنت.	2.39	.836	الرابعة	غالباً
6	أنت على استعداد لتحويل مال طلب منك من صديق على الإنترنت.	1.49	.767	الثامنة	قليل جداً
7	أنت واعٍ ولديك القدرة على تحديد آخر عمليات الاحتيال على الإنترنت.	2.44	.732	الثانية	غالباً
8	تثق بصور الغرباء المنشورة على الإنترنت.	1.36	.685	العاشرة	قليل جداً
9	لم تتلق أي طرود أو هدايا من أصدقاء الإنترنت.	2.26	.913	الخامسة	أحياناً
10	لن تتردد في عمل مكالمة فيديو مع أصدقاء الإنترنت.	1.64	.857	السابعة	قليل جداً
11	الاتجاه العام للمحور	1.9740	.48141	أحياناً	

يتضح من خلال النتائج الموضحة في الجدول رقم (8) أن المتوسط المرجح تراوح بين (2.56–1.36)، وأن الاتجاه العام لمحور الاحتيال عبر الإنترنت هو (أحياناً)، وقد كانت الفقرة ذات المرتبة الأولى هي: (لا أثق بمعلومات الغرباء الشخصية المعطاة على الإنترنت)، هي الفقرة التي حصلت على أعلى متوسط ترجيحي يقدر ب (2.56)، وهو سلوك غالباً ما يقوم به أفراد الدراسة، تلتها الفقرتين (أنت واعٍ ولديك القدرة على تحديد آخر عمليات الاحتيال على الإنترنت)، و (أتجاهل رسائل البريد الإلكتروني التي تصل على شكل إعلان من الشركات والمؤسسات المعروفة)، بمتوسط ترجيحي (بمتوسط بلغ (2.44)، وجاءت في المرتبة الرابعة الفقرة (لم أفكر أبدًا في تقديم أي مبلغ من المال مقابل الخدمات التي يقدمها موقع على الإنترنت)، بمتوسط ترجيحي (2.39)، وجاءت باتجاه (غالباً)، وكانت الفقرة (تثق بصور الغرباء المنشورة على الإنترنت)، هي الفقرة التي احتلت المرتبة الأخيرة في هذا المحور بمتوسط ترجيحي بلغ (1.36).

السؤال الثاني: هل توجد فروق ذات دلالة في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تعزى لمتغير النوع الاجتماعي؟

للإجابة على هذا السؤال تم حساب المتوسطات الحسابية والانحرافات المعيارية لكل من الذكور والإناث من أفراد المملكة العربية السعودية كما هو موضح في الجدول التالي:

جدول رقم (9) المتوسطات الحسابية والانحرافات المعيارية لاستجابات عينة الدراسة على مقياس سلوك الأمن السيبراني حسب متغير النوع الاجتماعي

المحور	النوع	العدد	المتوسط الحسابي	الانحراف المعياري
البرامج الخبيثة	ذكر	215	.121	.642
	أنثي	485	.542	.700
استخدام كلمات المرور	ذكر	215	.062	.742
	أنثي	485	.442	.841
الهندسة الاجتماعية	ذكر	215	.121	.762
	أنثي	485	.642	.862
التصيد الإلكتروني	ذكر	215	.282	.738
	أنثي	485	.911	.724
الاحتيال عبر الإنترنت	ذكر	215	.142	.637
	أنثي	485	.632	.688
المقياس ككل	ذكر	215	19.2	.642
	أنثى	485	34.1	656.

وللتأكد من تجانس التباين تم استخدام اختبار ليفين (Levene's Test)، كما يتضح في الجدول التالي:

جدول رقم (10) اختبار تجانس التباين بالنسبة لمتغير النوع الاجتماعي

المحور		قيمة F	مستوى الدلالة	قيمة t	Df	مستو ى الدلالة	الفروق بين المتوسطات	الخطأ	Confidence %95 Interval of the Difference	
									الأدنى	الأعلى
محور البرامج الخبيثة	يوجد تجانس للتباين	2.751	.098	-.123	698	.902	-.02915	.23669	-.49387	.43556
	لا يوجد تجانس للتباين			-.129	462.107	.897	-.02915	.22535	-.47200	.41369
محور استخدام كلمات المرور	يوجد تجانس للتباين	5.853	.016	-.789	698	.431	-.20403	.25873	-.71201	.30396
	لا يوجد تجانس للتباين			-.759	375.441	.449	-.20403	.26896	-.73289	.32483
محور التصيد الإلكتروني	يوجد تجانس للتباين	6.279	.012	-1.183	698	.237	-.30971	.26191	-.82393	.20451

	لا يوجد تجانس للتباين			-1.261	480.248	.208	-.30971	.24556	-.79221	.17279
محور الهندسة الاجتماعية	يوجد تجانس للتباين	1.235	.267	-3.513	698	.000	-.91964	.26179	-1.43363	-.40564
	لا يوجد تجانس للتباين			-3.537	416.778	.000	-.91964	.26002	-1.43075	-.40852
محور الاحتيال عبر الانترنت	يوجد تجانس للتباين	2.129	.145	-.222	698	.824	-.06368	.28694	-.62705	.49970
	لا يوجد تجانس للتباين			-.215	380.989	.830	-.06368	.29632	-.64630	.51895
المقياس ككل	يوجد تجانس للتباين	.806	.370	-1.786	698	.075	-1.52620	.85452	-3.20395	.15154
	لا يوجد تجانس للتباين			-1.800	417.774	.073	-1.52620	.84790	-3.19288	.14047

يتضح من الجدول رقم (10) تجانس تباينات المجموعتين من خلال عدم دلالة اختبار ليفين على المقياس ككل، وأن قيمة الفرق بين الذكور والإناث في درجة ممارسة سلوك الأمن السيبراني تبلغ (1.52620-) وهو فرق غير دال احصائياً لدلالة الطرفين. وتبين من النتائج أن هناك تجانس للتباين بين المجموعتين بوجود دلالة لاختبار ليفين على محور الهندسة الاجتماعية، وأن قيمة الفرق بين الذكور والإناث في درجة ممارسة سلوك الأمن السيبراني تبلغ (91964.-)، وهو فرق دال إحصائياً لصالح الإناث.

السؤال الثالث: هل توجد فروق ذات دلالة في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تعزى لمتغير المستوى التعليمي (أقل من الثانوية، بكالوريوس، ماجستير، دكتوراه)؟

للإجابة عن هذا السؤال تم استخراج المتوسطات الحسابية لدرجة ممارسة سلوك الأمن السيبراني من أفراد المجتمع السعودي، تبعاً لمتغير المستوى التعليمي (أقل من الثانوي، بكالوريوس، دراسات عليا)، ولتحديد فيما اذا كانت الفروق بين المتوسطات الحسابية ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$)، تم تطبيق تحليل التباين الأحادي، وجاءت النتائج كما تظهر في الجدول (11):

جدول رقم (11) نتائج تحليل التباين الاحادي لإيجاد الفروق بين المتوسطات الحسابية لدرجة ممارسة بسلوك الأمن السيبراني بين أفراد المجتمع السعودي تبعاً لمتغير المستوى التعليمي

مصدر التباين		مجموع المربعات	درجة الحرية	متوسط المربعات	F	مستوى الدلالة
محور البرامج الخبيثة	بين المجموعات	9.005	2	4.503	.540	.583
	داخل المجموعات	5816.343	697	8.345		
	الكلي	5825.349	699			
محور استخدام كلمات المرور	بين المجموعات	20.933	2	10.467	1.050	.350
	داخل المجموعات	6945.745	697	9.965		
	الكلي	6966.679	699			

محور التصيد الإلكتروني	بين المجموعات	51.300	2	25.650	2.520	.081
	داخل المجموعات	7095.344	697	10.180		
	الكلي	7146.644	699			
محور الهندسة الإجتماعية	بين المجموعات	13.903	2	6.952	.669	.512
	داخل المجموعات	7238.056	697	10.385		
	الكلي	7251.959	699			
محور الاحتيال عبر الانترنت	بين المجموعات	23.393	2	11.696	.955	.385
	داخل المجموعات	8538.242	697	12.250		
	الكلي	8561.634	699			
الدرجة الكلية	بين المجموعات	228.031	2	114.015	1.045	.352
	داخل المجموعات	76044.099	697	109.102		
	الكلي	76272.130	699			

تشير نتائج الجدول (11) إلى عدم وجود فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) في الدرجة الكلية أو درجة كل محور على حدة في ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تبعاً لمتغير المستوى التعليمي، حيث بلغت القيمة الفائية (1.045)، وبمستوى دلالة (.352)، ولم تكن الفروق ذات دلالة إحصائية في المحاور الخمسة للدراسة.

السؤال الرابع: هل توجد فروق ذات دلالة في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تعزى لمتغير للتخصص (كلية علمية، كلية انسانية، كلية صحية)؟

للإجابة عن هذا السؤال تم استخراج المتوسطات الحسابية لدرجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تبعاً لمتغير التخصص (كلية علمية، كلية انسانية، كلية صحية) ولتحديد فيما اذا كانت الفروق بين المتوسطات الحسابية ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$)، تم تطبيق تحليل التباين الأحادي، وجاءت النتائج كما تظهر في الجدول (12):

جدول رقم (12) نتائج تحليل التباين الاحادي لإيجاد الفروق بين المتوسطات الحسابية لدرجة ممارسة بسلوك الأمن السيبراني لدى الأفراد في المملكة العربية السعودية تبعاً لمتغير التخصص

مصدر التباين		مجموع المربعات	درجة الحرية	متوسط المربعات	F	مستوى الدلالة
محور البرامج الخبيثة	بين المجموعات	21.709	2	10.854	1.304	.272
	داخل المجموعات	5803.640	697	8.327		
	الكلي	5825.349	699			
محور استخدام كلمات المرور	بين المجموعات	81.526	2	40.763	4.127	.017
	داخل المجموعات	6885.153	697	9.878		
	الكلي	6966.679	699			
محور التصيد الإلكتروني	بين المجموعات	150.608	2	75.304	7.502	.001
	داخل المجموعات	6996.037	697	10.037		
	الكلي	7146.644	699			
محور الهندسة الإجتماعية	بين المجموعات	75.539	2	37.770	3.668	.026
	داخل المجموعات	7176.419	697	10.296		
	الكلي	7251.959	699			
محور الاحتيال	بين المجموعات	29.739	2	14.870	1.215	.297

عبر الانترنت	داخل المجموعات	8531.895	697	12.241		
	الكلي	8561.634	699			
الدرجة الكلية	بين المجموعات	182.416	2	91.208	.835	.434
	داخل المجموعات	76089.714	697	109.167		
	الكلي	76272.130	699			

أظهرت نتائج الجدول (12) عدم وجود فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) في الدرجة الكلية لممارسة سلوك الأمن السيبراني لدى أفراد المجتمع السعودي تبعاً لمتغير التخصص، حيث بلغت القيمة الفائية (.835)، وبمستوى دلالة (.434)، ووجدت فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) في محور (استخدام كلمات المرور)، حيث بلغت القيمة الفائية (4.127)، ومستوى دلالة (.017) وهي أقل من ($\alpha \leq 0.05$)، كما وجدت فروق ذات دلالة إحصائية في محور (التصيد الإلكتروني)، حيث بلغت القيمة الفائية (7.502)، ومستوى دلالة (.001)، وهي أقل من ($\alpha \leq 0.05$)، كما وجدت فروق ذات دلالة إحصائية في محور (الهندسة الاجتماعية)، حيث بلغت القيمة الفائية (3.668)، ومستوى دلالة (.026)، وهي أقل من ($\alpha \leq 0.05$). ولمعرفة عائدية الفروق على هذه المحاور الثلاث تم استخدام اختبار LSD لمعرفة أقل فرق معنوي، والجدول (13) يوضح نتائج المقارنة البعدية.

جدول رقم (13) نتائج اختبار أقل فرق دال LSD للمقارنة بين متوسطات فئات المستوى التعليمي، في محاور الدراسة الخمسة

	الكلية I	الكلية J	I-J	الخطا	مستوى الدلالة	الحد الأدنى	الحد الأعلى
محور البرامج الخبيثة	كليات علمية	كليات صحية	.36841	.36852	.318	-.3551	1.0920
		كليات إنسانية	-.24509	.24267	.313	-.7215	.2314
	كليات صحية	كليات علمية	-.36841	.36852	.318	-1.0920	.3551
		كليات إنسانية	-.61350	.39291	.119	-1.3849	.1579
	كليات إنسانية	كليات علمية	.24509	.24267	.313	-.2314	.7215
		كليات صحية	.61350	.39291	.119	-.1579	1.3849
محور استخدام كلمات المرور	كليات علمية	كليات صحية	-1.09820*	.40139	.006	-1.8863	-.3101
		كليات إنسانية	-.38864	.26432	.142	-.9076	.1303
	كليات صحية	كليات علمية	1.09820*	.40139	.006	.3101	1.8863
		كليات إنسانية	.70956	.42795	.098	-.1307	1.5498
	كليات إنسانية	كليات علمية	.38864	.26432	.142	-.1303	.9076
		كليات صحية	-.70956	.42795	.098	-1.5498	.1307
محور التصيد الإلكتروني	كليات علمية	كليات صحية	1.55162*	.40461	.000	.7572	2.3460
		كليات إنسانية	.37223	.26644	.163	-.1509	.8953
	كليات صحية	كليات علمية	-1.55162*	.40461	.000	-2.3460	-.7572
		كليات إنسانية	-1.17939*	.43139	.006	-2.0264	-.3324
	كليات إنسانية	كليات علمية	-.37223	.26644	.163	-.8953	.1509
		كليات صحية	1.17939*	.43139	.006	.3324	2.0264
محور الهندسة الإجتماعية	كليات علمية	كليات صحية	.93617*	.40980	.023	.1316	1.7408
		كليات إنسانية	.52157	.26985	.054	-.0082	1.0514
	كليات صحية	كليات علمية	-.93617*	.40980	.023	-1.7408	-.1316
		كليات إنسانية	-.41460	.43691	.343	-1.2724	.4432
	كليات إنسانية	كليات علمية	-.52157	.26985	.054	-1.0514	.0082

		كليات صحية	.41460	.43691	.343	-.4432	1.2724
محور الاحتيال عبر الانترنت	كليات علمية	كليات صحية	-.17131	.44682	.702	-1.0486	.7060
		كليات إنسانية	-.45852	.29423	.120	-1.0362	.1192
	كليات صحية	كليات علمية	.17131	.44682	.702	-.7060	1.0486
		كليات إنسانية	-.28721	.47639	.547	-1.2225	.6481
	كليات إنسانية	كليات علمية	.45852	.29423	.120	-.1192	1.0362
		كليات صحية	.28721	.47639	.547	-.6481	1.2225
الكلي	كليات علمية	كليات صحية	1.58670	1.33437	.235	-1.0332	4.2066
		كليات إنسانية	-.19845	.87868	.821	-1.9236	1.5267
	كليات صحية	كليات علمية	-1.58670	1.33437	.235	-4.2066	1.0332
		كليات إنسانية	-1.78514	1.42266	.210	-4.5784	1.0081
	كليات إنسانية	كليات علمية	.19845	.87868	.821	-1.5267	1.9236
		كليات صحية	1.78514	1.42266	.210	-1.0081	4.5784

تشير نتائج الجدول (13)، إلى وجود فروق في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي من المتخصصين من الكليات الصحية والكليات العلمية لصالح المتخصصين من الكليات العلمية في محور استخدام كلمات المرور، ووجود فروق في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي من المتخصصين في الكليات العلمية والكليات الصحية لصالح الكليات الصحية في محور التصيد الإلكتروني، والكليات الإنسانية والكليات الصحية لصالح الكليات الإنسانية في ذات المحور، ووجود فروق في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي بين المتخصصين من الكليات العلمية والكليات الصحية لصالح الكليات العلمية في محور الهندسة الاجتماعية، حيث كان المتوسط الحسابي لاستجاباتهم أعلى.

مناقشة النتائج

- تظهر نتائج الدراسة أن درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي جاءت متوسطة، حيث أشارت نتائج تحليل بيانات الدراسة أن (أحياناً)، هي الاستجابة الأكثر تكراراً لدى أفراد العينة في كافة محاور مقياس سلوك الأمن السيبراني، مما يفسر أن أفراد المجتمع السعودي يتعرضون للعديد من الانتهاكات أثناء استخدامهم لشبكة الإنترنت وتطبيقات الهاتف الجوال، وتتفق هذه النتيجة مع نتيجة دراسة علي وآخرون (Ali et al., 2021)، ودراسة فاتوكان وآخرون (Fatokun et al., 2020)، ودراسة موناندي وآخرون (Muniandy et al., 2017)، التي أظهرت أن سلوك الأمن السيبراني بين المستجيبين كان غير مرض بشكل عام في جميع قضايا الأمن السيبراني الخمس.
- وقد كان محور الاحتيال عبر الإنترنت هو المحور الذي حصل على أقل متوسط مرجح من استجابات عينة الدراسة، مما يعني أن سلوك الأمن السيبراني لدى أفراد المجتمع السعودي في مجال الاحتيال عبر الإنترنت تحتاج لإعادة بناء وتطوير ودعم، والاحتيال عبر الإنترنت هو النصب عن طريق الدفع مقدماً، وذلك عندما يتم اقناع شخص ما بإرسال مبلغ من المال مقابل أرباح سيتم ارسالها له فيما بعد، أو ارسال رسائل مضللة تتعلق بالاستثمار في مجال معين، أو فرصة الفوز في اليانصيب، ويرى الباحث أن ممارسة سلوك الأمن السيبراني في مجال الاحتيال عبر الإنترنت بين أفراد المجتمع السعودي متدنية بسبب طبيعة الفرد التي تميل به إلى الثقة بالآخرين، واعتقاده بأنه يمكن له أن يحقق ربحاً مضموناً من خلال تلقي الوعود بذلك الربح من أفراد أو عصابات متخصصة في سبل الاحتيال

المختلفة، وتمرسهم في ممارسة إقناع الآخرين للاحتيال عليهم وابتزازهم، ويمكن أن يعزى ذلك أيضاً إلى أن الرغبة في الربح السريع وبطرق سهلة لا تحتاج إلى بذل جهد وضياع وقت يجعل الأفراد يقعون ضحية لمثل هذه الانتهاكات.

- وجاء محور التصيد الإلكتروني في الترتيب التالي من حيث إنخفاض المتوسط المرجح لاستجابات أفراد عينة الدراسة، حيث أظهرت النتائج أن أفراد المجتمع السعودي يمارسون سلوك الأمن السيبراني في محور التصيد الإلكتروني (أحياناً)، مما يشير إلى أن أفراد المجتمع قد يقعون ضحية هذه الانتهاكات من خلال استقبال معلومات عن طريق البريد الإلكتروني أو رسائل الهواتف المحمولة تطلب منهم معلومات شخصية، أو التصيد عن طريق الرسائل الصوتية والرسائل النصية القصيرة، وذلك بالضغط على الروابط في الرسائل النصية القصيرة غير موثوقة المصدر. ويعزو الباحث ذلك إلى أن عدم الحذر والثقة المفرطة أحياناً التي يبديها أفراد المجتمع تجاه جهات يتفاعلون معها عبر الفضاء السيبراني تصل بهم درجة أن يشاركوهم معلومات شخصية كأرقام الهواتف، وتواريخ الميلاد، والأوراق الثبوتية، خصوصاً أساليب الاحتيال الجديدة التي تظهر للأفراد على أنها شركات توفر فرص عمل بعائد مرتفع جداً، أو ارسال روابط توصي به جهات معينة يحتوي على معلومات مثيرة تثير شغف الفضول لدى الأفراد العاديين الذين يمتلكون أدنى حد من المعلومات والوعي حول أساليب وطرق التصيد الإلكتروني، وتتفق هذه النتيجة مع دراسة موناندي وآخرون (Muniandy et al., 2017)،
- وجاء محور الهندسة الاجتماعية كأفضل ممارسات سلوكية في الأمن السيبراني بين أفراد المجتمع السعودي، حيث كان المتوسط المرجح لهذا المحور هو الأعلى بين محاور الدراسة الخمسة، وأظهرت النتائج أن أفراد المجتمع السعودي كانوا على درجة وعي مميزة وبدرجة (غالباً) للممارسة السلوكية، حيث أكدت عينة الدراسة أنهم حريصين جداً في عدم الكشف عن أية معلومات سرية للآخرين على الفضاء السيبراني تحت أي ظروف، كما أكدت عينة الدراسة على ضرورة التأكد من هوية الشخص قبل التحدث معه عن أي مشكلة كانت، وأن استدعاء العطف لن يكون مبرراً للتواصل مع الغرباء، ويعزو الباحث ذلك إلى الخبرة التراكمية الطويلة لدى مستخدمي الفضاء السيبراني من خلال شبكات الانترنت أو تطبيقات الجوالات جعلت أفراد المجتمع السعودي قادرين على تحديد مواطن الخطر التي قد تأتي منها الانتهاكات، والتي قد تعرضهم وتعرض خصوصياتهم للخطر، فاصبحوا قادرين على التصدي لها خصوصاً تلك القادمة من خلال تفاعلهم من الآخرين سواء من خلال شبكات التواصل الاجتماعي أو من خلال تبادل الايميلات أو بأي طريقة سيبرانية أخرى.
- أظهرت النتائج عدم وجود دلالة لاختبار ليفين على مقياس سلوك الأمن السيبراني ككل لدى عينة الدراسة، وأن قيمة الفرق بين الذكور والإناث في درجة ممارسة سلوك الأمن السيبراني غير دالة احصائياً لدلالة الطرفين. لكنها أظهرت أن قيمة الفرق بين الذكور والإناث في درجة ممارسة سلوك الأمن السيبراني دال إحصائياً لصالح الإناث في محور الهندسة الاجتماعية، ويعزو الباحث ذلك إلى طبيعة الإناث حيث أن المرأة عادة ما تكون أكثر حذراً في التعامل مع الآخرين، ولا تثق بسهولة بالطرف الآخر خصوصاً إن لم تكن هناك معرفة شخصية، كما أن المرأة بطبيعتها تخشى المجهول والتعامل معها، وتخشى أن تكون هدفاً بأي شكل من الأشكال للإساءة أو الابتزاز لهذا نجدها لا تقدم أي معلومات شخصية تدل عليها، ونلاحظ أن الكثير جداً من السيدات وخصوصاً السيدات في المجتمع السعودي تشارك في شبكات التواصل الاجتماعي من خلف اسم مستعار لا يتضمن أو معلومات خاصة، الأمر الذي جعل

إمكانية تعرضها للانتهاكات السيبرانية أقل من الرجال الذين عادة ما يكونون أكثر قابلية للمخاطرة بسبب الثقة بالنفس وعدم الخوف من التعرض لأنواع الانتهاكات المختلفة، أو لثقتهم المرتفعة بأنهم يملكون المعرفة والوعي الكافي الذي يحميهم من التعرض لمثل تلك الانتهاكات، وتختلف هذه النتيجة عما جاء في نتائج دراسة اكيل وتومسون (McGill & Thompson, 2018)، ولا تتفق هذه النتيجة مع ما توصلت له العديد من الدراسات فقد أظهر دراسة (Öztezcan and Cetinkaya, 2017) التي تم إجراؤها مع أعضاء هيئة التدريس والموظفين الإداريين في إحدى الجامعات أن مستوى وعي النساء بحماية البيانات الشخصية أقل من الرجال، ووجت دراسة (Halevi, Lewis & Memon, 2013) أنه بالنسبة للنساء هناك علاقة بين عدم الاستقرار العاطفي وكونهن أكثر عرضة للتصيد الاحتيالي من الرجال، لكن شنغ وآخرون (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010) وجدوا أن النساء اللواتي تتراوح أعمارهن بين (18 و 25) عاماً والطلاب الذين يدرسون العلوم الاجتماعية أكثر وعياً بهجمات التصيد الالكتروني.

- وأظهرت النتائج عدم وجود فروق ذات دلالة إحصائية في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي تبعاً لمتغير المستوى التعليمي، ويعزو الباحث ذلك إلى توزيع عينة الدراسة حيث أن نسبة المشاركين في الدراسة من حملة الشهادات العليا كانت لا تتجاوز 7%، فيما كانت النسبة الأكبر لحملة شهادة البكالوريوس، تلاهم حملة الثانوية العامة الأمر الذي جعل الفروق بين متوسطات الاستجابات متقاربة ولم تظهر أي فروق بين تلك المتوسطات، وتختلف هذه النتيجة مع ما جاء في نتائج دراسة هدلينجتون (Hadlington, 2018).
- وأظهرت النتائج وجود فروق في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي من المتخصصين من الكليات الصحية والكليات العلمية لصالح المتخصصين من الكليات العلمية في محور استخدام كلمات المرور، ويرى الباحث أن هذا الأمر منطقي حيث أن المتخصصين في الكليات العلمية غالباً ما يمتلكون الوعي والمعرفة الأكبر في مجال الحاسب والفضاء السيبراني، ومن المنطقي أن يكونوا على معرفة بمكامن الخطورة ومصادر الانتهاكات خصوصاً فيما يتعلق باستخدام كلمات المرور، ولهذا فإنهم غالباً ما يحتاطون من تسرب من خلال عدم مشاركتها مع الآخرين، أو تغييرها بين فترة وفترة، أو استخدام أكثر من طريقة لحماية الحسابات الشخصية بالاضافة لكلمات المرور. كما أظهرت النتائج وجود فروق في درجة ممارسة سلوك الأمن السيبراني بين أفراد المجتمع السعودي من المتخصصين في الكليات العلمية والكليات الصحية لصالح الكليات الصحية في محور التصيد الإلكتروني، والكليات الإنسانية والكليات الصحية لصالح الكليات الإنسانية في ذات المحور، ويعزو الباحث ذلك إلى أن معظم المشاركين في الدراسة كانوا من الإناث من متخصصي الكليات الصحية والإنسانية وربما لذلك كانت الأفضلية لهن في الفروق وذلك كما ذكرنا سابقاً أن الإناث غالباً يتحاشين التعرض للانتهاكات عبر الفضاء السيبراني بأشكاله المختلفة بسبب طبيعتهم وطبيعة المجتمع المحافظ الذي يعشن فيه، وخشيتهن من تعرض خصوصيتهن للخطر. كما أظهرت النتائج وجود فروق بين متوسطات الكليات العلمية والكليات الصحية لصالح الكليات العلمية في محور الهندسة الاجتماعية، ويعزو الباحث ذلك إلى أن المتخصصين من الكليات العلمية غالباً ما يمتلكون معرفة ووعي كبيرين في مجال الفضاء السيبراني يؤهلهم لمعرفة مصادر الانتهاكات والتصدي لها، وتتفق هذه النتيجة في جزء منها مع نتائج دراسة جيسكي وشيك (Jeske & Schaik, 2017)، كما تتفق في جزء منها مع نتائج دراسة فاتوكان وآخرون (Fatokun et al., 2020).

التوصيات:

- تعزيز ثقافة الأمن السيبراني، بينما أصبحت الإنترنت جانباً لا غنى عنه في الحياة الشخصية والمهنية، إلا أنه في الوقت نفسه جعل العديد من الأفراد عرضة لتهديدات الأمن السيبراني، لهذا فإن الترويج لسلوكيات الأمن السيبراني يمكن أن يحمي الأفراد بشكل فعال من هذه التهديدات. ولأن ممارسة سلوكيات الأمن السيبراني لا تأتي بالضرورة بشكل طبيعي، يحتاج الأفراد المجتمع إلى الدعم والتشجيع لتطويرها واعتمادها لديهم لتصبح جزء من ممارساتهم اليومية أثناء استخدام الفضاء السيبراني.
- دعوة المدارس والجامعات إلى تفريد مساق تدريسي يتعلق بالفضاء السيبراني، والأمن السيبراني، وسلوك الأمن السيبراني لتنمية وتطوير هذه المعارف والسلوكيات لدى الأفراد الأكثر استخداماً لشبكة الإنترنت.
- العمل على استخدام بنية تحتية لتكنولوجيا المعلومات تكون محمية بواسطة مجموعة متنوعة من الإجراءات التقنية المضادة المصممة لمنع الانتهاكات المحتملة في الأجهزة الشخصية.
- تصميم دورات تدريبية وورش عمل مجانية للتدريب على ممارسات سلوك الأمن السيبراني التي يجب أن يمتلكها الأفراد سواء في أماكن العمل أو من قبل الجهات الحكومية والمنظمات الخاصة.

المراجع

الهيئة العامة للإحصاء (2019). نشرة مسح نفاذ واستخدام تقنية المعلومات والاتصالات للأسر والأفراد. موقع الهيئة العامة للإحصاء، المملكة العربية السعودية، الرياض، https://www.stats.gov.sa/sites/default/files/nshr_msh_nfdh_wstkhdm_tqny_lmlwmt_wltslt_llsr_wlfrd_2019m_0.pdf

Ali, R., Dominic, P., Ali, S., Rehman, M. & Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Appl. Sci, 11*, 3383.

Alshammari, N., Mylonas, A., Sedky, M., Champion, J., & Bauer, C. (2015). Exploring the Adoption of Physical Security Controls in Smartphones, in: *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust. Switzerland: Springer International Publishing,* pp. 287-298. Anderson, C.L., and Agarwal, R. 2010. "Pract.

Amoroso, E. (2006). *Cyber Security*. New Jersey: Silicon Press.

Benson, V. (2017). *The State of Global Cyber Security: Highlights and Key Findings.* London: LT Inc.

Benson, V; McAlaney, J & Frumkin, L. (2018). *Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape*. In: McAlaney, John; Frumkin, Lara A. and Benson, Vladlena eds. Psychological and Behavioral Examinations in Cyber Security. IGI Global, pp. 266–271.

Blazy, B. & Yeun, Y. (2018). Information Security Theory and Practice: *12th IFIP WG 11.2 International Conference, WISTP 2018*, Brussels, Belgium, December 10–11, 2018.

Branstad, D. & Gallegos, F. (1988). Auditing Password Usage. Retrieved August 1, 2021: https://www.gao.gov/assets/137402.pdf.

Chen, Y. & Zahedi, F. (2016). Individual's Internet Security Perceptions and Behaviors: Polycontextual Contrasts between the United States and China. *MIS Quarterly, 40*(1), 205222.

Craigen, D., Diakun-Thibault, N., Purse, R. (2014). Defining cybersecurity. *Technol. Innov. Manag. Rev*, 4, 13–21.

Daka Advisory. (2014). Digital development in Malaysia – An analysis of cyber threats and Responses. Retrieved August 1, 2021 http://dakaadv

DHS. (2014). A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. Retrieved August 1, 2021 http://niccs.us-cert.gov/glossary#letter_c.

Egelman, S., Harbach, M., & Peer, E. (2016). Behaviour ever follows intention? A validation of the Security Behaviour Intentions Scale (SeBIS). *In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems,* San Jose, CA, USA, 7–12 May 2016; pp. 5257–5261.

Elango, B, Matilda, S. & Jeyasankari, J. (2020). Redefining Search Terms for Cybersecurity: A Bibliometric Perspective. *Proceedings of the International Conference on Recent Advances in Computational Techniques (IC-RACT)* 2020.

Elango, B, Matilda, S. & Jeyasankari, J. (2020). Redefining search terms for Cybersecurity: a bibliometric perspective. https://www.researchgate.net/profile/Elango-B/publication/346169339.

Fatokun, F., Hamid, S., Norman, A., & Johnson, F. (2020). Relating Factors of Tertiary Institution Students' Cybersecurity Behavior. Conference: *International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*, 18-21 March 2020, Lagos, Nigeria.

Fatokun, F., Hamid, S., Norman, A., Fatokun, J. & Eke, Ch. (2020). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian universities. *Journal of Physics: Conference Series 1339* (1), 012098.

Francois, L., Mercia M., & Venter, H. (2014). Towards an ontological model defining the social engineering domain. *In IFIP International Conference on Human Choice and Computers,* Springer, 266–279.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behaviour intentions. *Comput. Secur*, *73*, 345–358.

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior andpersonality traits. *In Proceedings of the 22nd international conference on world wide web* (pp. 737-744).

Hong, Y. & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications, 57*, 2214-2126.

Jeske, D. & Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. https://research.tees.ac.uk/ws/files/4184386/620760.pdf

Kalhoro, Sh., Rehman, N, Ponnusamy, V. & Shaikh, F. (2021). Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review. *IEEE Aerospace and Electronic Systems Magazine, 19*, 99339-99363.

Khan, F., Yaqoob, A. Khan, M., & Ikram, N. (2022). The cybersecurity behavioral research: A tertiary study. *Computers & Security, 120*, September 2022, 102826.

Levitis, D. Lidicker, W. & Freund, G. (2009). Behavioural biologists do not agree on what constitutes behaviour. *Animal Behaviour, 78*, 103-110.

Mashiane, Th. & Kritzinger, E. (2018). Cybersecurity Behaviour: A Conceptual Taxonomy. *IFIP International Conference on Information Security Theory and Practice WISTP 2018*: Information Security Theory and Practice pp 147-156.

McGill, T. & Thompson, N. (2018). Gender Differences in Information Security Perceptions and Behaviour. *ACIS 2018 - 29th Australas. Conf. Inf. Syst*. (2018), 1–11. DOI:https://doi.org/10.5130/acis2018.co

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber Security Behaviour among Higher Education Students in Malaysia. *Journal of Information Assurance & Cyber security*, 13.

Oxford University Press. (2014). Oxford Online Dictionary. Oxford: Oxford University Press. http://www.oxforddictionaries.com/definition/english/Cybersecurity.

Papatsaroucha, D., Nikoloudakis, Y., Kefaloukos, I., Pallis. E. & Markakis, E. (2021). A Survey on Human and Personality Vulnerability Assessment in Cyber-security: Challenges, Approaches, and Open Issues. *ArXiv, 1*, 1-39.

Patterson, W. & Winston - Proctor, C. (2019). *Behavioral Cybersecurity: Applications of Personality Psychology and Computer Science*. Boca Raton, FL: Taylor & Francis.

Ponemon Inst. LLC. (2017). Cost of data breach study: Global overview. Tech. Rep., 2017, North Traverse City, MI, USA. Retrieved August 1, 2021 https://www.ibm.com/downloads/cas/ZYKLN2E3

Public Safety Canada. (2014). Terminology Bulletin 281: Emergency Management Vocabulary. Ottawa: Translation Bureau, Government of Canada. http://www.bt-tb.tpsgc.

Safa, N., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N., & Herawan, T. (2015). Information securityconscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78.

Safa, N., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations*. Comput. Secur., 53*, 65–78.

Seemma, P., Nandhini, S. & Sowmiya, M. (2018). Overview of Cyber Security. *IJARCCE, 7*(11), 125-128.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? Ademographic analysis of phishing susceptibility and effectiveness of interventions. *In Proceedings of theSIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382).

Sulaiman, N, Fauzi, M., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating. *Information*,13, 413. https://doi.org/10.3390/

Supratman, P. & Wahyudin, A. (2017). Digital Media Literacy to Higher Students in Indonesia. Int. J. English Lit. *Soc. Sci. 2*(5). 51–58.

Tenove, Ch. & Moscrop, D. (2018). *DigitalThreats Report-FINAL*. https://www.academia.edu/40016906/DigitalThreats_Report_FINAL

Thakur, K., Qiu, M., Gai, K. and Ali, M. (2015). An Investigation on Cyber Security Threats and Security Models*. IEEE 2nd International Conference on Cyber Security and Cloud Computing,* New York, NY, 2015, pp. 307-311.

Tomar, S. & Singh, P. (2021). Cyber Security Methodologies and Attacks. *Journal of Management and Service Science, 1*(1), 2, 1-8.

Trist, E.; Bamforth, K. (February 1951). Some Social and Psychological Consequences of the Longwall Method of Coal-Getting: An Examination of the Psychological Situation and Defences of a Work Group in Relation to the Social Structure and Technological Content of the Work System. *Human Relations, 4* (1), 3–38.

Vahdati, S., & Yasini, N. (2015). Factors affecting internet frauds in private sector: A case study in cyberspace surveillance and scam monitoring agency of Iran. *Computers in Human Behavior, 51,* 180e187.

Wiederhold, B. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychol., Behav., Social Netw., 17* (3),131–132.

Yazdanifard, R., WanYusoff, W., Behora, A., & Sade, A. (2011). Electronic banking fraud: The need to enhance security and customer trust in online banking. *Advances in Information Sciences & Service Sciences, 3*(10), 505e509.