حوليات آداب عين شمس المجلد 50 (عدد إبريل – يونيو 2022)
http://www.aafu.journals.ekb.eg
(دورية علمية محكمة)
جامعة عين شمس
كلية الآداب

الفروق في الوعي بالأمن السبيراني لدى الشباب الكويتي في ضوء بعض المتغيرات الديموغرافية والعوامل الخمسة الكبرى للشخصية.

تركي بندر العنزي*

عقيد دكتور – وزارة الداخلية
Turki19111974@gmail.com

المستخلص:

هدفت الدراسة إلى الكشف عن مستوى الوعي بالأمن السيبراني الشباب الكويتي وأيضا الكشف عن الفروق في مستوى الوعى بالامن السبيرانى في ضوء بعض المتغيرات الديموجرافية والعوامل الخمسة الكبرى للشخصية وتكونت عينة الدراسة من مستخدمي الانترنت قوامها من(145) كويتى من الجنسين و متوسط أعمارهم (33) عاما بانحراف معياري (2.3) عاما ، وتم اختيار العينة بالطريقة العشوائية البسيطة. منهجية الدراسة وأدواتها: استخدم الباحث المنهج الوصفي لمناسبته هذه الدراسة. وتم تطبيق مقياس الوعى بالأمن السبيرانى: مقياس فرعي مشتق من مقياس الوعى بالأمن السبيرانى من إعداد نورة الصانع وأخرون(2020) وقائمة العوامل الخمسة الكبرى للشخصية :من اعداد كوستا وماكري أعد القائمة باللغة العربية بدر الانصاري(2002): • أظهرت النتائج ارتفاع مستوى الوعى بالأمن السبيرانى لدى الشباب الكويتى ، وجود فروقا دالة إحصائيا بين الذكور والإناث في مستوى الوعى بالأمن السبيرانى والفروق في صالح الذكور مقارنة بالإناث،: عدم وجود فروق في الوعى بالأمن السبيرانى تعزي الي المستوي التعليمي، كما كشفت الدراسةأن منخفضي الانبساطية ومرتفعي يقظة الضمير والعصابية أكثر وعيا بالأمن السبيرانى

الكلمات المفتاحية: الوعى بالأمن السبيرانى/ العوامل الخمسة الكبرى

مقدمة

ثمة اعتقاد لدى معظم الناس أنّ الأمن لن يخرج عن نطق مفهومه التقليدي المعروف لدى الكثيرين، إلا أن الدائرة اتسعت مؤخرًا وظهر نوع من أنواع الأمن، يأتي في مقدمتها الأمن السيبراني الذي يعني في أبسط تعريف له أنه حماية المعلومات الموجودة على أجهزة وشبكات الحاسب الآلي، في مواجهة أي تدخل غير مصرح به قد يستهدف إحداث تغيير في المعلومات أو إتلافها أو الحرمان من الوصول إليها (Hadlington & Parsons, 2017) .

والأمن السيبراني مشهد دائم التطور، ومن الأهمية بمكان زيادة الوعي بالتقنيات الإلكترونية التخريبية التي تُنتج التهديداتِ الجديدةَ التي ظهرت في الآونة الأخيرة (Wiederhold,2014).

وخلال عشر السنوات الماضية أحدثت تكنولوجيا المعلومات تغييرًا في استخدام التطبيقات الرقمية والأجهزة المحمولة التي نستخدمها في حياتنا اليومية، وجعلت الحياة في أماكن مختلفة أيسر كثيرًا عن طريق إتاحة التكنولوجيا للاستخدام وزيادة استخدام الإنترنت في العملية التعليمية والسياحة والبيع بالتجزئة، ومن تلك الاستخدامات: تصفُّح الويب، وتقديم الدعم لأنظمة التوصية في هيئة أدوات تدعيم القرار، قراءة الصحف الرقمية، والاستعانة بمحركات البحث من أجل الحصول على المحتوى المطلوب، وتَصفُّح وسائل التواصل الاجتماعي (Sabillon et al., 2021).

وقد أحدث الإنترنت ثورة في إدارة مهام الحياة، وتمكينها التواصل مع أشخاص جدد من خلال الشبكات الاجتماعية، و فتح آفاق اقتصادية جديدة للمعاملات عبر الهاتف المحمول لكل من الأفراد والمؤسسات (Aloul ,2012,Saadatdoost et al.,2015,Lee et al.,2017

وقد أدى استخدام هذه الأجهزة إلى ظهور تحديات جديدة وتهديدات أمنية خطيرة، حيث يُمكن للمهاجمين استغلال هذه الأجهزة للوصول إلى المعلومات الشخصية والسرية والاستفادة منها، ونشر هجمات أكثر خطورة؛ والتي منها البرامج الضارة، وهي نوع ضار من البرامج المكتوبة بقصد إتلاف الأجهزة، وسرقة البيانات (Alzubaidi, 2021).

وتعد الدراسة النفسية للأمن السيبراني مجالًا ناشئًا ومهمًا للبحث في مجال علم النفس السيبراني؛ نظرًا لأن عامل الفشل البشري هو السبب الأكثر شيوعًا لأى هجوم إلكتروني ناجح، وقد أشار باحثون إلى أن العامل البشري يعد عاملا جوهريا في الأمن السيبراني؛ ولذلك انتبه علماء النفس لدراسة خصائص الأشخاص المعرضين للفشل في المحافظة على أمن المعلومات السيبرانية، وأنواع سيناريوهات الفشل في المحافظة على أمن هذه المعلومات، وكذلك دراسة العوامل التي تؤثر في الفشل في المحافظة على أمن المعلومات السيبرانية، ومنها الثقة المفرطة. وانتبه علماء النفس لدراسة السلوك البشري أثناء الهجوم الإلكتروني وكيفية توعية الأفراد بالأمن السيبراني(Linkov et al.,2019

وقد يساعد علماء النفس في تحسين الأمن السيبراني بطرق مختلفة، وذلك حيث إن الأشخاص يتباينون في قدرتهم على تقييم مخاطر الأمن السيبراني بشكل موضوعي، حيث وجد هادلينجون (Hadlington, 2021) أن حوالي (23 ٪) فقط من الأفراد يمكِنهم التعامل مع سيناريوهات الأمن السيبراني بصورة صحيحة، وحوالي (4 ٪) من الأفراد يستطيعون التعامل مع ما يزيد عن (90 ٪) من سيناريوهات الأمن السيبراني.

ومن هنا يمكن القول: إن تحقيق الأمن السيبراني لا يقتصر فقط على مجرد التحكم التكنولوجي، بل الأمر يتعلق بوعي كل من الأفراد الذين تستهدفهم والأفراد الذين يستهدفونك من خلال اتباع منهج نفسي، يحقق المحافظة على الأفراد والأنظمة، وتكون البيانات الخاصة في مأمن من "الهاكرز" الذين قد يؤذون الناس (البيشي، 2021).

لذلك أصبح تعزيز الوعي بالأمن السيبراني هدفًا رئيسًا للعديد من المنظمات، حيث يؤدي زيادة الوعي بحالة البيئات إلى تحسين عملية اتخاذ القرار، فالوعي هو عملية تَعلُّم تمهد الطريق للتدريب من خلال تغيير المواقف الفردية والتنظيمية؛ لإدراك أهمية الأمن والعواقب السلبية لفشلها. والوعي مهم للغاية في مجال أمن تكنولوجيا المعلومات والاتصالات؛ لأن تصرفات الفرد يمكن أن تؤثر على المؤسسة بأكملها، ويمكن أن يتسبب عدم وعي الفرد المسؤول في أضرار جسيمة وخسارة للمؤسسة، فالوعي الأمني السيبراني هو كل شيء عن نقل المعلومات (Yunos et al., 2016).

لذلك جاءت هذه الدراسة للبحث عن الأساس النفسي للوعي بالأمن السيبراني، ومعرفة أسس التمييز بين أولئك الذين يلتزمون بتكنولوجيا المعلومات والمبادئ التوجيهية الأمنية على الأرجح، وأولئك الذين ليسوا كذلك، وذلك من خلال نموذج العوامل الشخصية الخمسة (عوامل الشخصية).

مشكلة الدراسة

دخلت الكويت عالم الأمن السيبراني متأخرةً مقارنة بدول مجلس التعاون لدول الخليج العربي، إذ أعلنت الحكومة الكويتية عمّا يسمى "باستراتيجية الكويت للأمن السيبراني 2017 ــ 2020 " وهي استراتيجية فنية قائمة على ثلاثة أمور: الرؤية والمهمة والأهداف، وأهداف هذه الاستراتيجية هي تعزيز ثقافة الأمن السيبراني التي تدعم الاستخدام الآمن والصحيح للفضاء الإلكتروني، بالإضافة إلى الهدف الثاني وهو حماية الأصول والبنى التحتية الحيوية والمعلومات الوطنية والشبكة المعلوماتية بالكويت ومراقبتها، والهدف الثالث هو إتاحة سبل التعاون والتنسيق وتبادل المعلومات فيما بين مختلف الجهات المحلية والدولية في مجال الأمن السيبراني. فلا يزال مجال الأمن السيبراني مجالاً غير مرغوب فيه من الناحية الدراسية أو الوظيفية، إذ لم يتقدم أي شخص ليشغل مقعد ضابط اختصاص في مجال الأمن السيبراني وذلك في التخصصات التي طرحتها وزارة الداخلية.
(https://www.mentharkw.com/ar/view/Kuwaiti-Cybersecurity).

لذا يجب إعطاء الأولوية للأمن السيبراني عبر المؤسسة، وليس فقط في قسم تكنولوجيا المعلومات. فالسبب الرئيسي للزيادة العالمية في حوادث الأمن السيبراني يعود إلى أنّ معظم الناس لا يتبعون بدقة القواعد والتعليمات الأمنية الدقيقة المتوفرة في مكان العمل. مما يشكل تهديدًا أمنيًا كبيرًا يجعل الأصول التنظيمية عُرضة للتأثيرات الخارجية والداخلية(Whitman,2011 &Mattord).

ولا يزال كثير من الأشخاص يواجهون مخاطر أمن المعلومات من مجموعة واسعة من التهديدات، تتراوح هذه التهديدات من بسيطة إلى كارثية الهجمات. قد تكون الأولى عبارة عن رسائل بدائية غير مرغوب فيها تأتي عبر البريد الإلكتروني، في حين أنّ الثانية تشمل مجموعات الجريمة الإلكترونية المنظمة التي تستخدم برامج ضارة لسرقة البيانات وإتلافها على نطاق واسع، فالعامل الرئيسي في حفظ المعلومات من المخاطر الأمنية هي مستوى الوعي الفردي بالأمن السيبراني، وهذه المخاطر يمكن وصفها بشكل مفيد بأنها منخفضة أو متوسطة أو عالية.

وتشمل التوعية بعض السلوكيات التي تنتج عن عدم الانتباه أو إهمال التنبيهات الأمنية، والتي يتم تقديمها تلقائيًا في معظم الحالات بواسطة التطبيقات، مثل: عند الوصول إلى شبكات مفتوحة مجانية مثل (Wi-Fi) مع الأجهزة المحمولة وأجهزة الكمبيوتر المحمولة. قد يتسم مستوى الوعي المتوسط بالإهمال المعبر عنه بـــ عملية تقنية غير لائقة. وأخيرًا هناك الوعي المرتفع الذي ينطوي على معرفة بالتهديدات السيبرانية والإجراءات القادرة على الوقاية منها(Moti et al.,2020).

وتجدر الإشارة إلى أن العديد من مستخدمي الإنترنت لا يزالون يفتقرون إلى الوعي الكافي بتهديدات الإنترنت المختلفة والتي تُعرف أيضًا باسم "المخاطر الإلكترونية"، وغالبًا ما يفشلون في امتلاك الحد الأدنى المطلوب لحماية أجهزتهم الحاسوبية في أسوأ السيناريوهات، حيث يعاني الأفراد من نقص تام في الوعي بمخاطر الإنترنت، ومن ثم فإن استعدادهم لاستخدام تدابير الحماية الأمنية السيبرانية غير موجودة (Emm, 2021).

إن معظم الدراسات السابقة المتعلقة بدراسة الأمن السيبراني قد ركزت على عامل واحد فقط، هو تحسين التكنولوجيا بدلاً من النظر إلى العوامل البشرية، بالرغم من أن التكنولوجيا وحدها تفتقر إلى الحد من التهديدات السيبرانية والتي منها الجرائم الإلكترونية؛ لذلك أوصت دراسات عدة منها (Stanton et al.,2004, Moti et al.,2020,.Mattord&Whitman,2011 بالاهتمام بالعلوم البشرية لأنها تعد عوامل ذات تأثير جوهري على الأمن السيبراني. وقد كان ستانتون وآخرون(Stanton et al. (2004) من أوائل من اعترفوا بأهمية العامل البشري الذي يكمن وراء الأمن السيبراني، وفي السنوات الخمس الماضية. وقد ركزت مجموعة متنامية من الأبحاث على العوامل النفسية و الوعي الأمني السيبراني، على سبيل المثال: أشار ماكورماك وزملاؤه (McCormac et al.,2017 .)إلى وجود علاقة طردية بين العمر والوعي بأمن المعلومات، الذي يتحسن مع تقدم العمر. و أظهرت دراسة أخري أجراها ماكورماك وآخرون (McCormac et al.,2018) إلى وجود علاقة بين المرونة وضغوط العمل و الوعي بأمن المعلومات. وتم العثور على بحث تم بواسطة (Hadlington ,2018) التي رأت أن توظيف الأشخاص في

المؤسسات الكبيرة يميل إلى تنمية الوعي بالمخاطر السيبرانية، والتي يمكن تفسيرها من خلال تحسين موارد الميزانية وسياسات الإنفاذ التنظيمية. كما هو الحال أيضًا على تحسين الوعي الأمني السيبراني بين المديرين أو الموظفين الإداريين، مع التأكيد على الالتزام باللوائح والمبادئ التوجيهية السيبرانية، وكذلك وضع السياسات الأمنية، ومع ذلك لا يزال الافتقار إلى الوعي السيبراني عالميًا مشكلة خطيرة، لذا يجب على المنظمات والمؤسسات التعليمية تطوير برامج التدريب المناسبة.

وحديثا ظهر اهتمام من قبل الباحثين بدراسة الشخصية ودورها المؤثر في الأمن السيبراني، وخاصة عند دراسة الوعي بالأمن السيبراني، وقد أظهرت الدراسات أن عوامل الشخصية عوامل لها تأثير كعوامل نفسية تمييز بين أولئك الذين يلتزمون بالمبادئ التوجيهية الأمنية لتكنولوجيا المعلومات، وأولئك غير الملتزمين بالمبادئ التوجيهية الأمنية لتكنولوجيا المعلومات، وقد أظهرت هذه الدراسات أن ثمة علاقات بين سمات الشخصية وفئات مختلفة من الوعي بالأمن السيبرانى، فعلى سبيل المثال ، وجدت دراسة ,(Claar 2011) أن عامل المقبولية له تأثير فعال على اهتمام الفرد بخصوصية المعلومات، كما أن عامل العصابية له تأثير كبير على قلق الكمبيوتر. وفي دراسة (Cooper et al.,2010) عن سمات الشخصية والخصوصية في سياق الخدمات القائمة على المواقع الالكترونية، وجدت الدراسة أن عامل المقبولية ويقظة الضمير كان لهما أهمية كبيرة في ثلاثة عوامل تصورت الخصوصية: الخطأ، والاستخدام غير المصرح به، والوصول غير السليم.

وعلى الرغم من تلك الأهمية لدراسة موضوع الوعي بالأمن السيبراني عبر العوامل النفسية – وبخاصة عوامل الشخصية – فإنه لم يأخذ حظه في البحث كباقي الدراسات النفسية لمجال الإنترنت في حدود ما اطلع عليه الباحث، إذ تبين قلة البحوث في هذا الموضوع على المستوى العربي، فضلا عن ندرة الدراسات الأجنبية التي تناولت الوعي بالأمن السيبراني عبر العوامل الخمسة الكبرى للشخصية، كما لا يوجد دراسة عربية أو محلية تناولت هذا الموضوع كما تناوله البحث الحال.

وكل ما سبق دفع الباحث إلى معرفة العلاقة بين الوعي بالأمن السيبراني وعوامل الخمسة الكبرى للشخصية، والمفارقة بين الأفراد في الوعي بالأمن السيبراني وفقا لبعض المتغيرات الديموجرافية، كما أن دراسة هذا الموضوع نبعت من قناعة مفادها أهمية التركيز علي الشخصية، لما لها من خصائص مستقرة من دور في توجيه السلوك.

وفي ضوء ما تقدم يمكن تحديد مشكلة الدراسة في التساؤل الرئيس الذي ينص على:" ما مستوى الوعي بالأمن السيبرانى لدى الشباب الكويتي في ضوء العوامل الخمسة الكبرى للشخصية؟ ويتفرع عن هذا التساؤل الرئيس عدة أسئلة فرعية، هي:

1- ما مستوى الوعي بالأمن السيبراني لدى الشباب الكويتي؟

2- ما الفروق في مستوى الوعي بالأمن السيبراني وفقا للنوع والمستوى التعليمي والتفاعل بينهما؟

3- ما الفروق في الوعي بالأمن السيبراني بين مرتفعي العوامل الخمسة الكبرى للشخصية ومنخفضيها؟

أهداف الدراسة:

- الكشف عن الفروق في مستوى الوعي بالأمن السيبراني.

2- تعرف الفروق في مستوى الوعي بالأمن السيبرانى وفقا للنوع والمستوى التعليمي والتفاعل بينهما.

3- الكشف عن الفروق في الوعي بالأمن السيبراني بين مرتفعي العوامل الخمسة الكبرى للشخصية ومنخفضيها.

أهمية الدراسة

يمكن إيجاز الأهمية النظرية والتطبيقية للدراسة في النقاط التالية:

أولا: الأهمية النظرية:

1- تعد الدراسة الحالية من الدراسات النفسية العربية القليلة التي تتناول الوعي بالأمن السيبراني في ضوء العوامل الخمسة الكبرى للشخصية، والتي يمكن أن تثرى الإنتاج العلمي في هذا المجال.

2- تنبع أهمية الدراسة الحالية من موضوعها من أهمية العينة التي تجري عليها وهم الشباب في المجتمع الكويتي، إذ إنهم الفئة العمرية الأكثر استخدما للإنترنت ولوسائل التواصل الاجتماعي وما ترتب عليها من آثار اجتماعية نتج عنها الكثير من المشكلات النفسية والاجتماعية نتيجة لعدم الوعي بالأمن السيبراني.

ثانيا: الأهمية التطبيقية:

1- توجيه اهتمام الجهات المعنية سواء أكان ذلك في مجال الأمن أو في مجال التعليم إلى أهمية إدراج مفاهيم الأمن السيبراني ضمن برامج التدريب والتعليم للمجتمع.

2- رفع درجة الوعي لدى أفراد المجتمع الكويتي بخصوص الأمن السيبراني وأهمية الالتزام بمفاهيم الأمن السيبراني عند التعامل مع مصادر المعلومات المختلفة.

3- يمكن الاستفادة من نتائج الدراسة الحالية في إعداد برنامج إرشادي لتنمية الوعي بالأمن السيبراني لدى الفئات المعنية والمستهدفة للتهديدات السيبرانية.

مفاهيم الدراسة:

الوعي بالأمن السيبراني: يُعَرف شو وآخرونl(Shaw et al.,2009.p:93) الوعي بالأمن السيبراني على أنه "درجة الفهم من المستخدمين حول أهمية أمن المعلومات ومسؤولياتهم عن ممارسة مستويات كافية من مراقبة أمن المعلومات؛ لحماية البيانات المنظمة، والشبكات على نطاق واسع، ويتم تحديد مستوى الوعي بالأمن السيبراني من خلال مقياس الوعي بالأمن السيبراني المستخدم في الدراسة الحالية.

العوامل الخمسة للشخصية تشير إلى خمس سمات للشخصية هي: يقظة الضمير، والعصابية، والانفتاح على الخبرة، والانبساطية، والمقبولية (John et al 2008.,). ويتم تحديد درجة المشارك على كل سمة من هذه السمات من خلال مقياس العوامل الخمسة الكبرى المستخدم في الدراسة الحالية.

الإطار النظري للدراسة والدراسات السابقة

أولا: الوعي بالأمن السيبراني:

زادت تكنولوجيا المعلومات بشكل كبير في العقد الماضي، مع معدلات عالمية هائلة لاستخدام الإنترنت من قبل الأفراد والمؤسسات، بدءًا من الأوساط الأكاديمية والحكومية إلى القطاعات الصناعية(Jalali et al.2019).

ومع تزايد الاستخدام للإنترنت لا يزال الكثير من مستخدمي الإنترنت يفتقرون إلى الوعي الكافي بتهديدات الإنترنت المختلفة والتي تُعرف أيضًا باسم "المخاطر الإلكترونية(Lee et al.,2017)

في الواقع غالبًا ما يفشل مستخدمو الإنترنت في امتلاك الحد الأدنى المطلوب من الوعي لحماية أجهزتهم الحاسوبية، ففي أسوأ السيناريوهات يعاني الأفراد من نقص تام في الوعي بمخاطر الإنترنت؛ ومن ثم فإن استعدادهم لاستخدام تدابير الحماية الأمنية السيبرانية غير موجود(Zwiling et al.,2020)

ويمكن تعريف الأمن السيبراني وفقا للتقرير الصادر عن الاتحاد الدولي للاتصالات (2011) الأمن السيبراني: بأنه مجموعة من المهمات مثل (تجمع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات.

كذلك يُعَرف الأمن السيبراني Cybersecurity بأنه" :النشاط الذي يؤمن حماية الموارد البشرية، والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة(الظويفري،2021).

ويعرف الدواد وسكينر(Aldawood, & Skinner,2018 .P:63) الوعي بأمن الإنترنت أو الوعي بالأمن السيبراني بمدى معرفة مستخدمي الإنترنت بتهديدات السيبرانية التي تواجهها شبكاتهم، والمخاطر التي يتعرضون لها والتخفيف من أفضل الممارسات الأمنية لتوجيه سلوكهم.

تهديدات الأمن السيبراني:

وقد حصرت دراسات (السرحان والمشاقبة، 2020 وبونيف، 2019 والصحفي،2019 والمنتشري،2020 أهم التهديدات السيبرانية في الآتي:

* **الاحتيال الإلكتروني:** يتخذ الاحتيال الإلكتروني أشكالًا متعددة، منها: إيهام الضحية (المجني عليه) بوجود مشروع كاذب، وقد يتخذ اسمًا أو صفة، فهو يتخذ أشكالا كاذبة؛ تمكّنه من الاستيلاء على الضحية؛ فيتم التواصل مع الضحية من خلال اتصال الجاني بالضحية عن طريق الشبكة؛ أو قد يتعامل الجاني مباشرة مع بيانات الحاسب، فيستعمل البيانات الكاذبة التي تساعده في الخداع والاحتيال عليه .

* **التنمر الإلكتروني:** يُقصد به استخدام تكنولوجيا الاتصالات لأغراض التحرش والمضايقة والإزعاج، والتهديد، والابتزاز، وقد انتشر التنمر الإلكتروني كأحد أشكال المخاطر السيبرانية بصورة كبيرة مع انتشار الأجهزة اللوحية والهواتف الذكية.

* **هجمات مستهدفة:** وهي القيام باختراق شبكة أو جهاز إلكتروني بهدف سرقة المعلومات المخزّنة فيه، والتي عادة ما تكون على درجة كبيرة من الأهمية؛ سواءً أكانت معلومات عسكرية؛ أم اقتصادية؛ أم صناعية؛ أم تجارية، أم غيرها، وهو ما يترتب عليه آثار استراتيجية فادحة في الطرف المستهدف.

* **تسريب البيانات:** إن أشهر الجرائم انتشارًا هي جرائم الدخول غير المشروع إلى البريد الإلكتروني للآخرين، وإنشاء مواقع للتشهير.

* **الهندسة الاجتماعية:** تشير إلى عملية تلاعب بالبشر وخداعهم بهدف الحصول على بيانات أو معلومات؛ كانت ستظل خاصة وآمنة، ولا يمكن الوصول إليها بهدف اختراق النظامر.

* **الابتزاز الإلكتروني:** استخدام وسائل التقنية الحديثة للحصول على مكاسب مادية ومعنوية عن طريق الإكراه من شخص إلى آخر أو أشخاص أو مؤسسات، ويكون ذلك بالتهديد بفضح سر من أسرار المُبتَز بعد أن ينشب الجاني أنيابه في الضحية.

* **التغرير والاستدراج:** غالب ضحايا هذا النوع من صغار السن من مستخدمي شبكة الإنترنت، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة على الإنترنت، وقد تتطور إلى التقاء مادي بين الطرفين (متولي، 2015).

* **التجسس الإلكتروني:** يتم التجسس الإلكتروني بواسطة برامج معينة، تحصل سرا على معلومات عن المستخدم عن طريق ربط بالإنترنت، وخاصة بدعاوى دعائية وإعلانية، وعادة ما يتم تضمين برامج التجسس في شكل مكونات مجانية خفية، أو برامج مشاركة يمكن تنزيلها من شبكة المعلومات، وبمجرد تركيب برنامج التجسس يبدأ بمراقبة حركة المستخدم على الإنترنت، وينقل المعلومات إلى الجهة المهاجمة (القحطانى، 2015).

* **الإرجاف الإلكتروني:** يُقصد به بث الأخبار المحبطة والمسيئة ونشر الشائعات بغرض إحداث الخوف والاضطرابات وزعزعة الأمن النفسي، وبث هذه الأخبار وغيرها يندرج تحت الشائعات، فهي وسيلة خطيرة لإرباك الرأي العام، ويستخدم الإرجاف الإلكتروني بشكل عام بصفته وسيلة لتحطيم مصادر الأخبار الحقيقة، وطُعما للحصول على الحقيقة، حيث تشاع أخبار كاذبة عن موضوع معين بقصد الوصول إلى الأنباء الصحيحة (Buckholz,2017).

دور عوامل الشخصية في الوعي بالأمن السيبراني:

تشير النتائج إلى أن الشخصية تلعب دورًا مهمًا في فهم سلوكيات الأمن السيبراني، وهو ما يتوافق مع مجموعة متزايدة من الأدبيات التي تسلط الضوء على الوعي باعتباره مؤشرًا قويًا على سلوكيات الأمن السيبراني، إذ تشير نتائج الدراسات إلى أن بنية الشخصية مرتبطة بسلوكيات الأمن السيبراني، وأن الضمير والانفتاح قد يكونان بارزين بشكل خاص في هذه العلاقة (Shappie,et al.,2020).

كذلك تتنبأ متغيرات الشخصية بشكل أفضل بسلوك الأمن السيبراني، وغالبًا ما يتصرف الناس بطرق لا تتوافق مع ما يقصدونه، بافتراض أن معظم الناس لديهم نية الامتثال للممارسات الآمنة، فليس من المستغرب أن ينتهك الأشخاص السياسات، ويعرضون البيانات الحساسة للخطر بانتظام(McCormac,et al.,2017) .

ويشير هوفمان إلى أن كل من الانبساط والمقبولية ويقظة الضمير والاتزان الوجداني والتفتح على الخبرة ويقظة الضمير، والاندفاعية – بوصفها خصائص للشخصية – هي المسؤولة عن أن يكون الفرد أقل محافظة على المعلومات السيبرانية، وأكثر استهدافا ليكون ضحية لمختلف التهديدات السيبرانية.(Aldawood, & Skinner, 2018).

ثانيا–العوامل الخمسة الكبرى للشخصية The big five factor of personally

إن معنى الشخصية من أشد معاني علم النفس تعقيدًا أو تركيبًا؛ وذلك لأنها تشمل الصفات الجسمية والوجدانية والعقلية والخلقية في حالة تفاعلها مع بعضها لشخص معين يعيش في بيئة اجتماعية معينة (الميلادي، 2006:).

وتعرف الشخصية بأنها المجموع الكلي لأنماط السلوك الفعلية أو الكامنة لدى الكائن الحي. (الأغا، 2009: 8).

لذا يمكن القول: إن تكامل الشخصية يعتبر مظهرًا من مظاهر الصحة النفسية لدى الفرد، وعلامة التوافق الذاتي والتكيف الاجتماعي مما يجعله إيجابيا يُؤثر ويتأثر بمحيطه.

وعرف ألبورت الشخصية بأنها: "التنظيم الدينامي داخل الفرد للأجهزة النفسية الفيزيقية التي تحدد للفرد طابعه المميز في السلوك والتفكير"(عبد الخالق، 1992، ص. 39).

وتعرف جمعية علم النفس الأمريكية (APA)عام 2014 الشخصية: بأنها الأنماط الفريدة من التفكير والشعور والسلوك، ويعد نموذج العوامل الخمسة الكبرى للشخصية أحد النماذج الأوسع تمثيلا لتصنيف منتظم لسمات الشخصية، ويفضل الباحثون نموذج العوامل الخمسة الكبرى للشخصية على حد قول كوستا ومكري McCrae, & Costa عام 2008حينما يرغبون في تمثيل مجال عوامل الشخصية بشكل منتظم وواسع و متكامل لوصف الشخصية(Dugan &Gadbois,,2015).

وبصورة عامة يكاد يتفق علماء النفس على أن الشخصية هي نمط سلوكي مركب ثابت إلى حد كبير يميز الفرد عن غيره من الأفراد، ويتكون من تنظيم فريد لمجموعة من الوظائف والسمات والأجهزة المتفاعلة معا، والتي تضم القدرات العقلية والانفعالية والتركيب الجسمي الوراثي والوظائف الفسيولوجية والأحداث التاريخية الحياتية التي تحدد طريقة الفرد الخاصة في الاستجابة وأسلوبه المميز في التكيف مع البيئة. (الصاحب، 2011: 42)

والعوامل هي: "مفهوم رياضي يُفسر سيكلوجيًا، يُستَمد من استخدام منهج التحليل العاملي لمعاملات الارتباط بين مجموعة من المقاييس السلوكية." (عبد الخالق، 1992، ص. 158)

استخلصت نماذج العوامل الخمسة المفسرة للشخصية من خلال منحيين هما: المنحى القاموسي، ومنحى قوائم العبارات، وفي المنحى القاموسي يقدم للمفحوص صفات مستمدة من القواميس اللغوية، وترتبط بالسمات المراد قياسها، ويقوم منحى العبارات على صياغة عبارة تعبر عن سلوك معتاد يتصف بها الفرد يقدم للمفحوص، ويطلب منه أن يحدد مدى انطباقها عليه أو على شخص آخر (يونس وخليل،2007)

ويعرف كابلن وزملاؤه(Kaplan,et,al,2012) العوامل الخمسة الكبرى بأنها:" تصنيف موسع لسمات الشخصية تبعا لخمسة أبعاد، وهي: العصابية، ويقظة الضمير، والانفتاح على الخبرة، والانبساطية، والمقبولية الاجتماعية، ويشير الباحثون إلى أن هذا التصنيف له أساس بيولوجي. ويمكن عرض العوامل الخمسة الكبري للشخصية على النحو الآتى:

1–**العصابية:** Neuroticism: هي سمة تظهر الخبرات السلبية مثل الخوف والتشاؤم والحزن والقلق والغضب والاكتئاب وعدم الاستقرار النفسي (Stefan,et,al,2012). والعصابية بطبيعتها سلبية، وأن الأفراد العصابيين غالبا ما يخبرون الأحداث السلبية الكربة، كما يقحمون أنفسهم في المواقف التي تعزز من هذه التأثيرات السلبية مقارنة بالآخرين. ومن أبرز التعريفات هو التعريف الذي قدمه كوستا ومكري McCrae, 1992 & Costa(في عبد المجيد،2010).

2–**الانبساطية:** Extraversion وهى سمة تشير إلى نشاط الفرد الاجتماعي ورغبته في تأكيد الذات والثقة بالنفس ومختلف المشاعر الإيجابية (Stefan,et,al,2012).

ويوصف الانبساطي بأنه شخص يقبل على حقائق الحياة من غير ضجر وتبرم، وأن عقله منفتح، وأنه يرمى إلى الابتكار، وهو ذو سلوك مبني على أساس أحاسيسه الداخلية، ويعتمد في توجيه سلوكه على الأحاسيس النفسية أكثر من اعتماده على الفكر والمنطق (مصطفى وبتو،2012).

3- **الانفتاح على الخبرة:** Openness on experience وهي سمة تتضمن الجوانب المعرفية كحب الاستطلاع والحساسية للجمال والمرونة المعرفية والجدة والإبداع(Kaplan,et,al,2012).

ويري جرجس (2007) أن عامل الانفتاح على الخبرة مرتبط بالحاجة للفهم، خاصة عند (موراي)، والانفتاح على الخبرة مرتبط بمفهوم الحاجة إلى المعرفة، والمتأمل في العديد من الدراسات التي اهتمت بدراسة عوامل الشخصية الكبري يجد أن الانفتاح على الخبرة يتضح في الخيال والحساسية الجمالية وعمق المشاعر والمرونة السلوكية والاتجاهات الحديثة غير التقليدية والأفكار الجديدة والحدس، والتحدي والأصالة والاتقان والبراعة والبصيرة والإبداع والتوقد الذهني وسرعة البديهة.

4- **المقبولية الاجتماعية:** Agreeableness وهي سمة تصف الفرد بميله لمشاركة الآخرين والتعاطف معهم والمعاضدة وحب الإيثار (Kaplan,et,al,2012).

ويضم عامل المقبولية الاجتماعية سمات أهمها الثقة الذاتية والاعتدال والإيثار والإذعان والتواضع وعدم التطرف في الرأي (Casta,et,al,2008).

5- **يقظة الضمير** Conscientiousness: وتعنى ضبط الذات والمثابرة والتروي والمسؤولية والميل للتنظيم والتخطيط (Kaplan,et,al,2012).

ويشير كوستا ومكري McCrae, 1992 & Costa إلى يقظة الضمير بأنها: "عامل يتضمن عددًا من السمات من أهمها: الكفاءة أي: (البراعة، والتصرف الحكيم) والتنظيم، (كالترتيب، والدقة، والأناقة)، والإخلاص (كالإخلاص الذي يمليه الضمير، والتقيد بالقيم الأخلاقية) والسعي نحو الإنجاز (كالكفاح، والطموح، والمثابرة، وتحديد الأهداف) وضبط الذات مثل: (الاستمرار في إنجاز عمل دون ملل، وإنجاز الأعمال دون حاجة إلى تشجيع من الآخرين) والتأني أو الروية مثل: (التفكير في الأعمال قبل القيام بها، والحرص، والحذر، والتروي) (في عبد المجيد،2010).

- **المحور الأول: دراسات تناولت الوعي بالأمن السيبراني:**

* تناولت دراسة "بانفيلد" (Banfield, 2016) فاعلية برنامج الوعي بالأمن السيبراني على السلوك الأمني لدى المستخدم النهائي في المؤسسات المتوسطة الحجم، وقد تكون مجتمع الدراسة من العاملين في مؤسسة متوسطة الحجم في الولايات المتحدة، واشتملت العينة على (400) من العاملين في المؤسسات المتوسطة الحجم، واعتمد الباحث على المنهج المسحي والكمي، كما استعانت الدراسة بالأداة المسحية الإلكترونية التي تم توزيعها على المشاركين في الدراسة، وقد توصلت الدراسة إلى العديد من النتائج أهمها: 1/ عدم وجود تأثير ذي دلالة لتطبيق برنامج الوعي بالأمن السيبراني على تغيير السلوكيات الأمنية لدى العاملين. 2/ وجود علاقة ارتباطية بين برنامج الوعي بالأمن السيبراني والسلوك الأمني لدى المستخدم النهائي. 3/ تعد برامج الوعي المعلوماتي من العناصر المهمة في الأمن المعلوماتي الشامل، حيث إن التكنولوجيا بدون برنامج الوعي بالأمن السيبراني تعد خطة أمنية غير كاملة.

* وأجري "بادا وآخرون" (Bada et al., 2019) دراسة هدفت الدراسة إلى بحث حملات الوعي بالأمن السيبراني، وتعرف العوامل الأساسية التي تؤدي إلى إخفاق هذه الحملات في تغيير سلوكيات الأمن لدى الأشخاص، واعتمدت على المنهج الوثائقي القائم على مراجعة الأدبيات الحالية بناء على النظريات النفسية المتعلقة بالوعي والسلوك في مجال الأمن السيبراني، وقد توصلت الدراسة إلى العديد من النتائج أهمها: 1/ تعد المعرفة والوعي شرطين أساسيين في تغيير السلوك؛ لذا يساعد دمج السلوكيات

الإيجابية للأمن السيبراني في تعزيز الممارسات المتعلقة بالتفكير والثقافة المرتبطتين بالأمن السيبراني. 2/ يتم قياس التغير السلوكي في بيئة الأمن السيبراني من خلال خفض المخاطر وليس من خلال ما يعرفه ومالا يعرفه الأشخاص أو من خلال ما يتجاهله الشخص. 3/ يقوم تغيير السلوك من خلال حملات الوعي بالأمن السيبراني على قدرة الأشخاص على استيعاب وتطبيق النصائح وتحفيزهم وتعزيز رغبتهم في تنفيذ النصائح وإحداث التغيرات في الاتجاهات والسلوكيات.

* وسعت دراسة نورة القحطانى (2019) إلى تعرف مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي من وجهة نظرهم؛ من خلال تعرف آرائهم حول المفهوم الأقرب له، وأهم الجرائم التي يتعامل معها، وطرق الوقاية المجتمعية من جرائم الفضاء السيبراني، والمعوقات المجتمعية لتحقيق الوقاية من هذه الجرائم، وقد استخدمت الدراسة منهج المسح الاجتماعي بأسلوب العينة، واعتمدت على استخدام الدراسة الوصفية بالتطبيق على عينة عشوائية من طلاب وطالبات الجامعات السعودية في المستويات الدراسية المختلفة، وبلغت عينة الدراسة (486) طالبًا وطالبة، واعتمدت الدراسة على الاستمارة الإلكترونية لتجميع البيانات، ودلت النتائج على أن أقرب مفهوم للأمن السيبراني من وجهة نظر عينة الدراسة هو: "استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعاملات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها"، في حين جاءت جريمة "الاحتيال الإلكتروني/النصب الإلكتروني" كأكثر جريمة يتعامل معها الأمن السيبراني؛ في حين تعد التوعية الإعلامية للمجتمع حول طرقه هي أهم طرق الوقاية المجتمعية لمشكلات الفضاء السيبراني، كما دلت النتائج على وجود معوقات اجتماعية له في تحقيق الوقاية للمجتمع السعودي، وأن أهم هذه المعوقات هو التطور الهائل في نظم المعلومات، ووسائل التكنولوجيا التي يتعامل معها أفراد الأسرة دون المعرفة الكاملة لمشكلات هذه الوسائل وكيفية تجنبها، كما كشفت الدراسة عن عدم وجود فروق ذات دلالة بين الذكور والإناث في مستوى الوعي بالأمن السيبراني.

* كما هدفت دراسة "بوتجيتر" (Potgieter, 2019) إلى الكشف عن السلوك المتعلق بالوعي لدى الطلاب حول الوعي بالأمن السيبراني باستخدام منصات التواصل الاجتماعي في الجامعة المركزية للتكنولوجيا، وتكون مجتمع الدراسة من الطلاب في الجامعة المركزية للتكنولوجيا في جنوب إفريقيا، واشتملت العينة على (43 طالبا: 33 من الذكور، و 10 من الإناث)، واعتمدت على المنهج المسحي والكمي، كما استعانت الدراسة بالاستبانة المسحية الإلكترونية، وقد توصلت الدراسة إلى العديد من النتائج أهمها: 1/ وجود قصور لدى الطلاب فيما يتعلق بالمشاركة في المبادرات المتعلقة بالوعي بالأمن السيبراني المتوفرة عبر منصات التواصل الاجتماعي. 2/ يستخدم الطلاب البريد الإلكتروني والمواقع الإلكترونية للحصول على المواد المتعلقة بالوعي بالأمن السيبراني. 3/ يستخدم الطلاب فيسبوك بوك ويوتيوب باعتبارهما من منصات التواصل الاجتماعي الأكثر شيوعًا مرة واحدة على الأقل أسبوعيًا.

* وهدفت دراسة "تشانج وكوبيل" (Chang & Coppel, 2020) إلى تسليط الضوء على برنامج ممول من أستراليا مقدم من قبل جامعة موناش للتغلب على الإرهاب السيبراني لتعزيز الوعي بالأمن السيبراني في ميانمار، واعتمدت على المنهج التحليلي القائم على تحليل الممارسات المتعلقة ببناء الوعي بالأمن السيبراني، من خلال برامج المساعدة في التطوير بتقديم برنامج أسترالي لدعم الوعي والقدرات المتعلقة بالأمن السيبراني في ميانمار، وتوصلت الدراسة إلى عدة نتائج أهمها: 1/ تقوم البرامج التي تعزز الوعي والكفاءة المتعلقة بالأمن السيبراني في برامج دعم التطوير على حماية المواطنين من التنمر الإلكتروني وخطابات الكراهية والاحتيال، وتدعم المؤسسات التي تكافح الجرائم الإلكترونية والأنشطة الحاسوبية المشبوهة، وتدعم البرامج التي تعزز الوعي بالأمن السيبراني القوة في الخدمات الإلكترونية، بما في ذلك التعامل المصرفي النقال والحكومة الإلكترونية ونظام المدفوعات الإلكترونية. ويساعد برنامج Cyber Baykin في تعزيز بناء الوعي والكفاءة فيما يتعلق بالأمن السيبراني في ميانمار.

* وتناول ناصر القحطانى(2020) دراسة مستوى الوعي بالأمن السيبراني في مدارس بوابة المستقبل الثانوية في المملكة العربية السعودية، الأهداف الفرعية: ومستوى مهارات معلمي طلاب مدرسة بوابة المستقبل الثانوية في الأمن السيبراني. • موقف مشرفي مدرسة بوابة المستقبل الثانوية للأمن السيبراني. وتكونت عينة الدراسة: تم اختيار 100 مشارك من كل قسم محدد، مما

جعل إجمالي حجم العينة 300 مشارك. طبقت الدراسة استبانة لقياس الوعي بالأمن السيبراني، وكشفت الدراسة فعالية نموذج نظرية الألعاب لزيادة الوعي بالأمن السيبراني بين طلاب مدارس بوابة المستقبل الثانوية في المملكة العربية السعودية.

المحور الثانى: دراسات تناولت الوعي بالأمن السيبراني في ضوء العوامل الخمسة الكبرى للشخصية وبعض المتغيرات الديموغرافية.

* هدفت دراسة هاليفى وآخرين (Halevi et al.,2016) إلى الكشف عن العلاقة بين الوعي بالأمن السيبراني وكل من المتغيرات الثقافية والشخصية والديموغرافية .وقد أجريت هذه الدراسة في أربعة بلدان مختلفة وتقدم وجهة نظر متعددة الثقافات للأمن السيبراني، فإنه ينظر إلى كيفية تأثر الأمن السيبراني بكل من السلوك والكفاءة الذاتية وموقف الخصوصية بالثقافة، مقارنة بالمتغيرات النفسية والديموغرافية الأخرى، مثل: النوع والخبرة بالكمبيوتر. كما يفحص نوع البيانات التي يميل الأشخاص إلى مشاركتها عبر الإنترنت، وكيف تؤثر الثقافة على هذه الاختيارات، ويدعم هذا العمل فكرة تطوير واجهة المستخدم القائمة على الشخصية؛ لزيادة الأمن السيبراني للمستخدمين. وقد أظهرت النتائج أن سمات الشخصية تؤثر على سلوك المستخدم المتعلق بالأمن السيبراني عبر الثقافات المختلفة.

* كان الغرض من دراسة مكورماك وآخرين (McCormac et al.,2017) فحص العلاقة بين الوعي بالأمن السيبراني لدى الأفراد وبعض المتغيرات النفسية والديموغرافية منها: العمر والجنس وسمات الشخصية والميل إلى المخاطرة، وتم قياس ذلك باستخدام الجوانب البشرية لاستكشاف أمن المعلومات (HAIS-Q) ، وتم قياس المتغيرات النفسية والديموغرافية من مقاييس خاصة بذلك، وتكونت عينة الدراسة من (505) من العاملين الأستراليين. وقد وجد أن كلًا من يقظة الضمير، والمقبولية، والاستقرار العاطفي، والميل إلى المخاطرة، يفسر التباين الجوهري بين الأفراد في الوعي بالأمن السيبراني، في حين أن العمر والجنس ليس لهما تأثير في تباين الأفراد في الوعي بالأمن السيبراني.

* وهدفت دراسة هادلينجتون وآخرين (Hadlington et al.,2020) إلى استكشاف علاقة العوامل الخمسة الكبرى للشخصية والخوف من ضياع المعلومات والوعي بالأمن السيبراني لدى الموظفين. وتكونت عينة الدراسة من (718) مشاركًا، متوسط أعمارهم (38) عامًا، طبق عليهم عبر الإنترنت استبانة تضمنت مقياس الوعي بالأمن السيبراني ومقياس العوامل الخمسة الكبرى للشخصية. وقد أظهرت النتائج وجود مستويات مرتفعة من الخوف من ضياع المعلومات، ومستوى أقل في الوعي بالأمن السيبراني، حيث يمتلكون معرفة أقل، وموقف أكثر سلبية، والانخراط في سلوكيات أكثر خطورة فيما يتعلق بالأمن السيبراني، كما أظهرت الدراسة أن كلًا من العصابية ويقظة الضمير والمقبولية والعمر والنوع ذات تأثير فعال في تشكيل مستوى الوعي بالأمن السيبراني.

*وهدفت دراسة كل(Shappie,et al.,2020) إلى الكشف عن علاقة العوامل الخمسة الكبرى بالوعي بالأمن السيبراني، وتم جمع البيانات من (676) طالبًا جامعيًا خضعوا لإدارة استبانة المعتقدات في سلوك الأمن عبر الإنترنت للموظفين، وتم تطبيق مقياس العوامل الخمسة الكبرى للشخصية، وقد كشفت الدراسة وجود ارتباطات موجبة دالة إحصائيا بين سلوكيات الأمن السيبراني وكل من يقظة الضمير والمقبولية والانفتاح على الخبرة، وفسرت عوامل الشخصية التباين في سلوكيات الأمن السيبراني.

تعقيب:

ويظهر لي من خلال الدراسات السابقة استخلاص عدد من المؤشرات نجملها في التالي:

1- يوجد تباين ثقافي في أغلب الدراسات المعنية بمشكلة الدراسة الحالية، تنتمي إلى مجتمعات ذات أطر ثقافية مختلفة، والذي يمكن أن تسهم على نحو ما في اختلاف النتائج المتعلقة بفهم المشكلة ونتائجها؛ وبناء على ما سبق استعراضه من دراسات سابقة ظهر لي أن مشكلة الوعي بالأمن السيبراني لم يتم دراستها بالتصميم على المستوى المحلى؛ لذلك مازالت هناك حاجة للبحث في البيئة المحلية لمعرفة دور المتغيرات النفسية المؤثرة في الوعي بالأمن السيبراني.

2-أجمعت الدراسات السابقة التي عنيت بالوعي بالأمن السيبراني في العوامل الخمسة الكبري على وجود تأثير للعوامل الخمسة الكبرى في مستوى الوعي بالأمن السيبراني.

3- ثمة تناقض بين نتائج الدراسات السابقة بشأن الفروق بين الجنسيين في الوعي بالأمن السيبراني، فمثلا دراسة نورة القحطانى (2019) كشفت عن وجود فروق ذات دلالة بين الذكور والإناث في مستوى الوعي بالأمن السيبراني، والفروق في اتجاه الذكور، بينما انتهت دراسةMcCormac et al.,2017 إلى أن العمر والجنس ليس لهما تأثيران في تباين الأفراد في الوعي بالأمن السيبراني.

منهج الدراسة وإجراءاتها:

أ-التصميم البحثي: تعتمد هذه الدراسة على المنهج الوصفي؛ لكونه أكثر موائمة لتحقيق أهداف الدراسة والإجابة عن تساؤلاتها، والتحقق من فروضها من خلال الفنيات السيكو مترية التي تم تفصيلها بما يتناسب مع العينة في ضوء المتغيرات الدراسة الحالية.

ب-عينة الدراسة:

أ-العينة الاستطلاعية: تكونت من (40) من الشباب الكويتي من الجنسين ممن تراوحت أعمارهم بين (22إلى33) عامًا، وقد بلغ متوسط عمر أفراد العينة (32) بانحراف معياري قدره (1,3).

ب-العينة الأساسية:

اعتمدت على عينة عشوائية من مستخدمي الإنترنت، قوام العينة (145) كويتيًا، من الجنسين ومتوسط أعمارهم (33) عامًا بانحراف معياري (2.3) عاما، وتم تطبيق أدوات الدراسة عليهم. والجدول (2) يوضح خصائص عينة الدراسة.

جدول (1) يوضح خصائص العينة من حيث المستوى التعليمي والنوع والمهنة

المهنة	ك	%	مستوى تعليم	ك	%
طلاب جامعيون	31	%21.7	جامعي	104	%71.7
رجل أمن	16	%11	دراسات عليا	14	%9.7
موظف إداري	42	%28.9	متوسط	27	%18.6
معلم	20	%13.7	النوع	ك	%
مهندس	6	%4,13	ذكر	100	%69
لا يعمل	17	%4.8	أنثى	45	%31
طيب	6	%4,13			
ممرضات	7				
الإجمالى	145	%100			

أدوات الدراسة:

1-مقياس الوعي بالأمن السيبراني: مقياس فرعي مشتق من مقياس الوعي بالأمن السيبراني من إعداد: نورة الصانع وآخرين (2020)، ويتكون المقياس من (20) بندًا لقياس الوعي بالأمن السيبراني، ويتمتع هذا الجزء من المقياس في صورته الأصلية بخصائص سيكو مترية جيدة من ثبات وصدق، من ناحية الصدق تم التحقق من صدق المقياس من قبل معده بطريقتين: الصدق

الظاهري، وصدق الاتساق الداخلي. وأما ثبات المقياس فقد تم التحقق من الجزء من المقياس عن طريق ثبات ألفا، والذي بلغ 0.91 ويتم تصحيح المقياس من خلال بدائل خمسة: (تنطبق تماما – تنطبق– محايد– لا تنطبق– لا تنطبق تماما) والدرجات من (1 – 5).

2–قائمة العوامل الخمسة الكبرى للشخصية: من إعداد كوستا وماكري، وأعد القائمة باللغة العربية: بدر الأنصاري(2002) بهدف قياس العوامل الأساسية للشخصية بواسطة مجموعة من البنود(60) بندًا. ويتضمن هذا المقياس خمسة مقاييس فرعية تقيس كلًا من: (العصابية– والانبساطية– والمقبولية الاجتماعية– ويقظة الضمير– والانفتاح على الخبرة). وتوزعت عبارات المقياس بمعدل (12) عبارة لكل مقياس فرعي، وليس هناك وقت محدد لتطبيق المقياس باختيار بديل واحد من خمسة بدائل للإجابة (موافق بشدة– موافق – محايد– معارض – معارض بشدة). وتقدر الدرجات على البدائل على نحو مايلي: (1–2–3–4–5) على التوالي، وتعكس في حالة البنود السلبية، ويبلغ الحد الأعلى للدرجة على مقياس فرعي(60) درجة(حيث أقصى درجة على مقياس الشدة 1X=60 درجة). وقائمة مرفقة بمفتاح خاص بها، عِلمًا بأن القائمة لا تعطى درجة كلية واحدة كونها تقيس أبعاد الشخصية.

وتتمتع القائمة بخصائص سيكو مترية جيدة من حيث الصدق والثبات سواء في المستوي الأجنبي أو العربي، فعلى المستوي الأجنبي حسب صدق هذه القائمة بعدة طرق، منها: الصدق العاملي، فقد توصل جون وزملاؤه ,John,et,alعام1998 باستخدام التحليل العاملي إلى خمسة عوامل، هي: العصابية والانبساط والانفتاح على الخبرة والقبول والاتقان، وذلك على عينة مكونة من (170) فردًا، واستخلص كوستا وزملاؤهCosta,et,al,2002 عام2002 العوامل نفسها، وذلك على عينة ضمت (337) فردا تراوحت أعمارهم بين (18 – 67) سنة، وكانت التشبعات على جميع العوامل مرتفعة(من خلال شويخ،2012)

كذلك قام ماكري وآخرون ,MacCrae,et,al في عام2002 بحساب الصدق العاملي لقائمة العوامل الخمسة الكبرى المعدلة من خلال مقارنتها بالصورة الأصلية، وأظهرت النتائج تطابقا كبيرا في الصدق العاملي في النسختين (من خلال أحمد،2012)

وعلى المستوي العربي تحقق بدر الأنصاري (1997) من صدق القائمة بحساب الصدق الاتفاقي والاختلافي مع مقاييس أخرى، وأظهرت النتائج تفاوت معاملات ثبات المقاييس الفرعية لقائمة– بين مرتفع ومنخفض بطريقة ألفا وطريقة القسمة النصفية، حيث كانت معاملات الثبات مقبولة لمقياس العصابية ويقظة الضمير فقط.

التحقق من خصائص السيكو مترية للمقاييس بالدراسة الحالية:

طبقت أدوات الدراسة على عينة استطلاعية قوامها (40) من طلاب وموظفين إداريين بجامعة الكويت، متوسط أعمارهم (31) سنة وانحراف معياري (4.9) حيث تم التحقق من صدق وثبات الأدوات بالطرق الآتية:

–حساب صدق المقاييس:

تم التحقق من صدق الأدوات بالطرق التالية:

صدق المحكمين: عرضت أدوات الدراسة على مجموعة مكونة من (6) أعضاء هيئة من المتخصصين في علم النفس بكليتي الآداب بجامعة الكويت؛ لإبداء آرائهم وملاحظاتهم حول مناسبة فقرات المقاييس ومدى وضوح صياغاتها اللغوية، وكانت نسبة الاتفاق بينهم على عبارات كل المقاييس من 80–90 %.

الصدق التمييزي لفروق المقارنة الطرفية:

قام الباحث بترتيب الدرجات الكلية على مقاييس الدراسة الحالية لأفراد العينة الاستطلاعية ترتيبا تنازليا، وتم تقسيم الدرجات إلى طرفين: علوي وسفلى، وتم أخذ أعلى (25%) من الدرجات وأقل (25%) من درجات الأفراد على المقاييس، وتم حساب المتوسطات والانحرافات المعيارية للدرجات وحساب قيمة (ت)، واختبار مستوى الدلالة كما يوضح الجدول (2)

جدول(2) يوضح دلالة الفروق بين المجموعتين الطرفيتين من العينة الاستطلاعية فى درجات الكلية للمقاييس الدراسة

المقاييس	المراهقون						الراشدون					
	الأرباعي الأعلى25%		الأرباعي الأدنى25%		ت	الدلالة	الأرباعي الأعلى25%		الأرباعي الأدنى25%		ت	الدلالة
	م	ع	م	ع			م	ع	م	ع		
الوعي بالأمن السيبراني	28	1.1	17.1	2.9	11	0.01	32	1	21	1.8	15.4	0.01
أبعاد قائمة العوامل الخمسة												
العصابية	45	2.6	30	3.7	10,1	0,01	46.1	2	29.9	6.2	7.7	0,01
الانبساطية	47,7	1,2	35,9	3	11,15	0,01	47.4	2.1	34.5	4.1	8.1	0,01
الانفتاح على الخبرة	39,8	1	28,7	1,7	17.1	0,01	39.6	1.6	28.6	1.4	14.1	0,01
المقبولية الاجتماعية	46,8	2	33,9	2,1	13.4	0,01	46.8	3.3	33.1	2.3	10	0,01
يقظة الضمير	53,7	2,7	41,6	2,9	9,4	0,01	56.5	0.97	35	5.7	9.7	0,01

يشير الجدول (2) إلى أن المتوسطات الحسابية والانحرافات المعيارية للأرباعي الأعلى في الدرجات الكلية لمقاييس الدراسة كانت أعلى من المتوسطات الحسابية والانحرافات المعيارية للأرباعي الأدنى لنفس المقاييس، كما أن قيمة (ت) كانت دالة جميعها عند مستوى (0,01)، مما يدل على أن مقاييس الدراسة تتمتع بالقدرة على التمييز بين المستويين: القوى والضعيف، مما يعنى تمتع المقاييس بدرجة مقبولة من الصدق.

- **حساب ثبات المقاييس:** تم التحقق من ثبات المقاييس على أفراد العينة الاستطلاعية باستخدام عدة طرق، منها: حساب معامل ثبات ألفا والتجزئة النصفية.

جدول(3) معاملات ثبات الفا التجزئة النصفية للمقاييس الدراسة(ن=40)

المقاييس			
	معامل ثبات إعادة التطبيق	معامل ثبات ألفا	معامل ثبات التجزئة النصفية
الوعي بالأمن السيبراني		.78	0.88
أبعاد قائمة العوامل الخمسة			
العصابية	0.78	0.87	0.70
الانبساطية	0.73	0.84	0.63
الانفتاح على الخبرة	0.34	0.51	0.50
المقبولية الاجتماعية	0.60	0.75	0.63
يقظة الضمير	0.90	0.95	0.74

يتضح من الجدول السابق أن جميع معاملات الثبات بين المقبولة والمرتفعة.

الأساليب الإحصائية المستخدمة بالدراسة:

1- النسبة المئوية والمتوسطات والانحرافات المعيارية.

2- تحليل التباين الثنائي.

3- اختبار (ت)

- جمع البيانات:

1- قام الباحث بالتطبيق مع الاستعانة بالأخصائيين النفسيين والاجتماعيين بالأماكن التي سحبت منها العينة، وتم التطبيق في جلسات جمعية، تراوحت أعدادها من (10 إلى 20) فردا لعينة الطلاب، ومن (3 إلى 5) من عينة المعلمين والموظفين، وكان التطبيق يجري في القاعات الدراسية أو في حجرات الاجتماعات في مختلف الإدارات الحكومية التي سحبت العينة منها.

1- استغرق التطبيق شهرين على عينة الدراسة، أما مدة جلسة التطبيق فقد كانت من 20 دقيقة إلى 30 دقيقة، وكان التطبيق الميداني من شهر 2 / 2/ 2022 إلي5/4/ 2022.

سادسا- نتائج الدراسة ومناقشتها: سنعرض النتائج التي توصلت إليها الدراسة ومناقشتها وفقاً لترتيب التساؤلات على النحو التالي:

نتائج الإجابة عن السؤال الأول ومناقشتها: للإجابة عن السؤال الأول الذي نص على: "ما مستوى الوعي بالأمن السيبراني لدى الشباب الكويتي؟ تم حساب المتوسطات والانحرافات المعيارية وترتيبها تنازليا كما في الجدول (4)

جدول(4) يوضح المتوسطات والانحرافات المعيارية لدرجة وعي بالأمن السيبراني لدى عينة من الشباب الكويتي(ن=145)

الترتيب	رقم العبارة	العبارة	المتوسط	الانحراف المعياري	الترتيب
7	1	أختار كلمة مرور قوية تحتوي على مجموعة من الحروف والأرقام	3.8493	1.20540	عالية
1	2	تجنب فتح أي رابط من شخص غير معروف	4.3904	.99913	عالية جدا
2	3	أحرص على عدم فتح أي رسائل الكترونية مجهولة المصدر	4.3082	1.08637	عالية جدا
3	4	أتجنب إرسال معلوماتي الشخصية عبر الرسائل الإلكترونية	4.1712	1.12256	عالية جدا
5	5	أحرص على استخدام متصفح آمن للإنترنت	4.1096	1.15145	عالية جدا
13	6	أحذر كثيرا من الاتصال بالشبكات العامة	3.4795	1.24966	عالية
12	7	أفحص الروابط التي تبدو أنها ضارة	3.6301	1.30787	عالية
15	8	أدعم البيانات المخزنة على جهازي بإعداد نسخة احتياطة من الخدمة السحابية	3.3630	1.31768	عالية
6	9	أحرص على الإبلاغ عن المواقع المشكوك فيها	3.8836	1.27852	عالية
18	10	أتجنب الكشف عن أي بيانات شخصية أو عائلية أثناء تصفحي على الإنترنت	3.0068	1.33647	عالية
4	11	أهتم بتحميل برامج آمنه لمكافحة الفيروسات	4.2877	1.25922	عالية جدا

14	12	أدرك أهمية الأمن السيبراني	3.4247	1.39870	عالية
9	13	لدى إلمام بمفهوم الأمن السيبراني	3.6507	1.53844	عالية
17	14	لدى معرفة بمخاطر فيروسات الهواتف الذكية	3.1986	1.48380	عالية
8	15	أقوم بتحديث برنامج للحماية من الفيروسات بصورة مستمرة	3.8151	1.52226	عالية
12	16	أقوم بتغيير كلمة المرور الخاصة بانتظام	3.5068	1.63685	عالية
19	17	أقوم بقراءة اتفاقيات المستخدم لبرنامج مجاني قبل الضغط على أوافق	2.9384	1.60698	متوسطة
20	18	أستخدم جدار الحماية على جهاز الحاسوب الخاص بي	2.9178	1.66301	متوسطة
11	19	لا أتسوق أو أشتري سلعة معلنا عنها في أي من مواقع التواصل الاجتماعي	3.6370	1.80757	عالية
16	20	أتجنب الكشف عن أي بيانات شخصية	3.2192	1.81371	عالية
المتوسط مجموع العبارات			71.8414	12.94361	عالية

بالنظر في الجدول(4) تبين أن المتوسطات والانحرافات المعيارية الخاصة بالوعي بالأمن السيبراني لدى عينة من الشباب الكويتي تتراوح ما بين(2.9178إلى 4.3904) وهى متوسطات عالية إلى عالية جدا، وقد حصلت الفقرات(أتجنب فتح أي رابط من شخص غير معروف) و(أحرص على عدم فتح أي رسائل إلكترونية مجهولة المصدر) و(أتجنب إرسال معلوماتي الشخصية عبر الرسائل الإلكترونية) و(أهتم بتحميل برامج آمنه لمكافحة الفيروسات) و(أحرص على استخدام متصفح آمن للأنترنت)على أعلى متوسطات في حين الفقرات(أستخدم جدار الحماية علي جهاز الحاسوب الخاص بي) و(أقوم بقراءة اتفاقيات المستخدم لبرنامج مجانى قبل الضغط على أوافق) و(أتجنب الكشف عن أي بيانات شخصية أو عائلية أثناء تصفحي علي الإنترنت) حصلت على أقل المتوسطات وبلغ المتوسط العام(71.8) وهو متوسط عالٍ، وهذا يدل على ارتفاع مستوى الوعي بالأمن السيبراني، فقد أظهرت النتائج ارتفاع مستوى الوعي بالأمن السيبراني لدى الشباب الكويتي، وربما يرجع ذلك إلى اتساع حجم استخدام وسائل الاتصال عبر الإنترنت، وخبرة ودراية الشباب الكويتي بمختلف التهديدات ووسائل الحماية المتاحة من تلك التهديدات والذى تمثل في اتباع مجالات ووسائل الحماية من مخاطر التهديدات السيبرانية، وتتفق هذه النتيجة مع نتائج دراسة نورة القحطاني (2019) التي كشفت عن مستوى مرتفع من الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية، كما تتفق هذه النتيجة مع دراسة منى الصانعي وآخرين(2020) التي كشفت عن درجة من الوعي الكبير جدا في مجال التعامل الآمن مع خدمات الإنترنت، وتتفق النتيجة الحالية مع نتيجة دراسة مكورماك وآخرين (McCormac et al.,2017) التي توصلت الي ارتفاع مستوى الوعي بالأمن السيبراني.

نتائج الإجابة عن السؤال الثاني ومناقشتها: للإجابة عن السؤال الثاني الذي نص على: " ما الفروق في مستوى الوعي بالأمن السيبراني وفقا للنوع والمستوى التعليمي والتفاعل بينهما؟

استخدم الباحث اختبار تحليل التباين الثنائي وجاءت النتائج كما في الجدول (5).

جدول (5) يوضح نتائج تحليل التباين الثنائي للمقارنة في مستوى الوعي بالأمن السيبراني حسب النوع والمستوى التعليمي

مصادر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	ف	الدلالة
النوع	848.779	1	848.779	5.080	.026
المستوى الدراسي	320.351	2	160.175	.959	.386
النوع* المستوى الدراسي	518.748	2	259.374	1.552	.215
تباين الخطأ	23224.661	139	167.084		
الكلى	772497.000	145			

بالنظر إلي الجدول (5) السابق يتضح: عدم وجود فروق في الوعي بالأمن السيبراني تُعزا إلي المستوي التعليمي، حيث تراوحت قيمة ف(.959)، وهي قيمة غير دالة عند أي من مستويات الدلالة الإحصائية، في المقابل وجود فروق دالة إحصائيا في الوعي بالأمن السيبراني تُعزا للنوع، حيث بلغت قيمة ف (5.080) وهي قيمة دالة عند مستوي (0.02). وهذه النتيجة استوجبت حساب مقارنات ثنائية باستخدام معادلة LSD للوقوف على اتجاه ودلالة الفروق بين الذكور والإناث في مستوى الوعي بالأمن السيبراني.

وتشير النتائج الواردة في جدول (6) إلى النتائج الخاصة بأثر النوع الاجتماعي.

جدول(6) يوضح الفروق واتجاهاتها بين الذكور والإناث في التأثير على مستوى الوعي باللأمن السيبراني

المتغير	مجموعات المقارنة	عدد الأفراد(ن)	المتوسطات	متوسط الفروق (1/ 3)
الوعي بالأمن السيبراني	**(1) ذكور**	**100**	73.272	***2,1**
	(2) إناث	**45**	**65.518**	

بالنظر في جدول (6) يتضح أن ثمة فروقا دالة إحصائيا بين الذكور والإناث في مستوى الوعي بالأمن السيبراني، حيث جاء الذكور أكثر وعيا بالأمن السيبراني مقارنة بالإناث.

ويرجع الباحث عدم وجود فروق ذات دلالة في مستوى الوعي بالأمن السيبراني وفقا للمستوى التعليمي (جامعي – دراسات عليا– متوسط) بين الشباب الكويتي إلى متابعتهم لمستجدات الأمن السيبراني نتيجة انتشار استخدام ووسائل التواصل عبر الإنترنت بين الشباب الكويتي، بغض النظر عن المستوى التعليمي وما يرتبط به من اطلاعهم على تطورات ونشرات وأبعاد مستحدثة لكل ما يخص الحاسب وبرامج الحماية من التهديدات السبيرانية.

وتتفق هذه النتيجة مع دراستي (الصحفي، 2019، " Bada et al., 2019) اللتين كشفتا عن عدم وجود فروق ذات دلالة إحصائية في مستوى الوعي بالأمن السبيراني وفقا للمستوى التعليمي.

أما عن تفسير وجود فروق دالة إحصائيا بين الذكور والإناث في مستوى الوعي بالأمن السيبراني حيث جاءت الفروق في صالح الذكور مقارنة بالإناث فالراجح لدى الباحث أن السبب في هذا يعود إلى أن الذكور مقارنة بالإناث هم أكثر استخداما للإنترنت، ومن الطبعي أن يكونوا أكثر التزاما ومعرفة ببرامج الحماية، وبالتالي أكثر وعيا بمختلف التهديدات السيبرانية.

وتدعم هذه النتيجة ما أشار إليه (Jin et al.,2018) من أن الإناث– مقارنة بالذكور – قليلات في ممارسة سلوكيات التوعية السيبرانية، وهذا ينعكس في عدم الانتباه أو إهمال التنبيهات الأمنية التي يتم تقديمها تلقائيًا في معظم الحالات بواسطة التطبيقات، مثل: عند الوصول إلى شبكات مفتوحة مجانيا مع الأجهزة المحمولة وأجهزة الكمبيوتر المحمولة. كما يتسم مستوى وعي الإناث مقارنة بالذكور بالإهمال بـــ عملية التقنية، وانخفاض مستوى الوعي بالتهديدات السيبرانية وإجراءات الحماية التكنولوجية.

ويدعم هذه النتيجة أيضا ما أشار إليه (Linkoy et al.,2019) من أن الإناث أكثر عرضة للإصابة بالهجمات والتهديدات المتعلقة بالأمن السيبراني. كما أن الإناث أكثر عرضه للروابط في رسائل البريد الإلكتروني للتصيد الاحتيالي.

وتتفق هذه النتيجة مع دراسات (Jin et al.,2018,Daengsi et al.,2021,Zwilling et al.,2022) التي كشف عن وجود فروق في مستوى الوعي بالأمن السيبراني بين الذكور والإناث والفروق في اتجاه الذكور.

نتائج الإجابة عن السؤال الثالث ومناقشتها: وللإجابة عن السؤال الذي نصه: " ما الفروق في الوعي بالأمن السيبراني بين مرتفعي العوامل الخمسة الكبرى للشخصية ومنخفضيها؟ استخدم الباحث اختبار(ت) بين مرتفعي العوامل الخمسة الكبرى للشخصية ومنخفضيها من خلال ترتيب درجات الأفراد على العوامل الخمسة وحساب الإرباعي الأدنى والأعلى لكل بُعد للمقارنة في مستوى الوعي بالأمن السيبراني.

جدول (7) دلالة الفروق في المتوسطات والانحرافات المعيارية والقيم (ت) في مستوى الوعي بالأمن السيبراني بين مرتفعي ومنخفضي العوامل الخمسة الكبرى للشخصية

متغيرات المقارنة	المجموعات	متوسطات	الانحراف المعياري	درجة ت	مستوى الدلالة
الانبساطية	مرتفعي	60.8955	6.94379	20.422	000
	منخفضي	88.6154	6.36857		
المقبولية	مرتفعي	71.0800	9.26427	.713	.478
	منخفضي	73.0625	12.62132		
يقظة الضمير	مرتفعي	88.3750	6.46762	23.793	.000
	منخفضي	54.0357	4.84181		
العصابية	مرتفعي	81.7778	12.85135	9.812	.000
	منخفضي	61.0577	8.32293		
التفتح على الخبرة	مرتفعي	72.1121	12.88529	.502	.616
	منخفضي	70.7586	13.34877		

تشير الجدول (7) النتائج التالية

– توجد فروق ذات دلالة إحصائية بين مرتفعي الانبساطية في مستوى الوعي بالأمن السيبراني ومنخفضيها، والفروق في اتجاه منخفضي الانبساطية.

– توجد فروق ذات دلالة إحصائية بين مرتفعي يقظة الضمير في مستوى الوعي بالأمن السيبراني ومنخفضيها، والفروق في اتجاه مرتفعي يقظة الضمير.

–توجد فروق ذات دلالة إحصائية بين مرتفعي العصابية في مستوى الوعي بالأمن السيبراني ومنخفضيها، والفروق في اتجاه مرتفعي العصابية.

– لا توجد فروق ذات دلالة إحصائية بين مرتفعي التفتح على الخبرة في مستوى الوعي بالأمن السيبراني ومنخفضيها.

– لا توجد فروق ذات دلالة إحصائية بين مرتفعي المقبولية الاجتماعية في مستوى الوعي بالأمن السيبراني ومنخفضيها.

وعن مناقشة نتائج التساؤل الثالث فقد أظهرت مجمل نتائج السؤال الثالث أن سمات الشخصية تؤثر على سلوك المستخدم المتعلق بالأمن السيبراني، منها ما كشفت عنه نتائج السؤال الثالث من أن منخفضي الانبساطية ومرتفعي يقظة الضمير والعصابية أكثر

وعيا بالأمن السيبراني من خلال قيامهم بمختلف الإجراءات الاحترازية للحماية من التهديدات السيبرانية، وهذا يعني أن هذه العوامل الثلاثة للشخصية لها أهمية كبرى في الخصوصية، والحذر من الخطأ والاستخدام غير المصرح به والوصول غير السليم للمواقع غير المعروفة.

ويفسر الباحث أن النتيجة التي أشارت إلى أن منخفضي الانبساطية كانوا أكثر وعيا بالأمن السيبراني قد جاءت منطقية؛ لأن الأفراد الأقل اجتماعيًا، والأكثر عزلة، وذوي المستوى المنخفض من الانبساطية، هم أكثر وعيا بالأمن السيبراني من خلال منع أنفسهم من مشاركة المعلومات الحساسة، مثل: كلمة المرور الخاصة بهم، على العكس من ذلك، فإن الفرد الذي يتمتع بمستوى عالٍ من سمات الانبساط يريد أن يكون مقبولًا من قبل الآخرين، مما يجعله يتنازل عن معلومات مهمة.

وبناءً على النتائج في تحليل الارتباط، كان للانبساط التأثير الأعلى على سلوك المستخدم الذي لم يكن عرضة للتصيد الاحتيالي. فقد لوحظ أن النتائج قد جاءت متفقة مع نتائج تلك الدراسات السابقة التي فحصت تأثير الانبساط باعتباره صفة تجعل المستخدم أكثر عرضة لخطر الوقوع فريسة لهجوم تصيد احتيالي، منها دراسات (Darwish et al.,2012,Ueblacker &Quiel,2014.

ويرى الباحث أن النتيجة التي أظهرت أن مرتفعي يقظة الضمير كانوا أكثر وعيا بالأمن السيبراني مقارنة بمنخفضي يقظة الضمير يمكن تفسيرها من خلال الخصائص التي يتمتع بها أصحاب الضمائر الحية كالكفاءة والتنظيم بدلًا من اللامبالاة والفوضوية مما يجعلهم أكثر محافظة وحماية ووعيا بأساليب حماية المعلومات.

ويدعم هذه النتيجة ما أشار إليه كل من(Alqahtani, H., & Kavakli-Thorne,2020) بأن الأشخاص ذوي الضمائر العالية أكثر تنظيماً وحذرًا وانضباطا ذاتيا وموجهًا نحو المحافظة على أمن المعلومات، وتبنيًا للاستراتيجيات التي تركز على حماية سرية المعلومات وقواعد البيانات الخاصة، والمحافظة عليها.

وهذه النتيجة تتفق مع نتائج دراسات (McCormac et al.,2017, Halevi et al.,2016, Zwilling et al.,2022 التي أظهرت وجود فروق بين مرتفعي يقظة الضمير ومنخفضيها في الوعي بالأمن السيبراني.

ومن جهة ثانية تتسق هذه النتيجة مع نتيجة دراسة كل(Shappie,et al.,2020) التي كشفت عن وجود علاقة ارتباطية موجبة ودالة إحصائية بين يقظة الضمير والوعي بالأمن السيبراني. كما تتفق هذه النتيجة مع نتيجة دراسة (Hadlington et al.,2020)اس التي أظهرت أن يقظة الضمير ذات تأثير فعال في تشكيل مستوى الوعي بالأمن السيبراني.

أما عن تفسير النتيجة التي أظهرت أن مرتفعي العصابية أكثر وعيا بالأمن السيبراني فيمكن إرجاعها إلى أن الخصائص النفسية التي يتصف به العصابيون كالقلق والتوتر تدفعهم إلى التزام تنبيهات الأمن السيبراني محاولة منهم للحد من قلقهم وتوترهم.

وتتفق هذه النتيجة مع نتائج دراسات (Hadlington et al.,2020, Alqahtani, H., & Kavakli-Thorne,2020) Shappie,et al.,2020) التي كشفت وجود ارتباط بين العصابية والوعي بالأمن السيبراني.

واللافت لانتباه الباحث أن النتيجة التي أظهرت عدم وجود تأثير لكل من الانفتاح على الخبرة والمقبولية على مستوى الوعي بالأمن السيبراني– كانت تلك النتيجة مغايرة لمختلف النتائج السابقة التي أظهرت أن كلًا من المقبولية، والتفتح على الخبرة لهما تأثير كبير بالوعي بالأمن السيبراني، وممارسات الأمن السيبراني أكثر ارتباطا بكل من المقبولية والتفتح على الخبرة مثل دراسات((Halevi et al., 2016; McCormac et al., 2017; Shropshire et al., 2015

وربما ترجع النتيجة الحالية إلى طبيعة المقبولية والتفتح على الخبرة في البيئة العربية بشكل عام، والكويتية بشكل خاص، فالمقبولية سمة من سمات الشخصية التي تعنى التهيؤ للتكيف الاجتماعي، والإعجاب، والامتثال، والحب والرحمة، والتعاطف، ومجاراة الآخرين، كما أن التفتح على الخبرة تعنى الرغبة في الاستكشاف، وتحمل الغموض، والبحث عما هو جديد. وهذه الخصائص يمكن أن تكون لا تأثير لها في مستوى الوعي بالأمن السيبراني.

مناقشة النتائج

حللت الدراسة الحالية مستوى الوعي بالأمن السيبراني بين الشباب الكويتى، وقد جاءت النتائج الحالية دليلاً على ارتفاع مستوى الوعي بالأمن السيبراني بين الشباب الكويتي، وبخاصة الذكور مقارنة بالإناث، كما أبانت الدراسة الحالية العلاقة بين الشخصية ممثلة في العوامل الخمسة الكبرى وسلوكيات الأمن السيبراني، حيث أظهرت عوامل الشخصية، مثل: (الانبساط ويقظة الضمير والعصابية) ارتباطا كبيرا بالوعي بالأمن السيبراني وسلوكياته المختلفة. وهذا يتماشى مع نتائج العديد من الدراسات السابقة.

ومجمل النتائج الحالية لها آثار مهمة؛ لأنها أظهرت أن سمات شخصية معينة قد تسبب ضعفًا أكبر في التصيد الاحتيالي على وجه التحديد، كما أبانت الدراسة الحالية أيضا أن النساء قد يَكنَّ أكثر عرضة للإصابة بالهجمات السيبرانية.

التوصيات:

بناء على ما سبق تطرح الدراسة الحالية عدة توصيات ومقترحات بحثية، أهمها:

- الاهتمام بتنمية الوعي بالأمن السيبراني وأساليبه لدى الإناث على وجه الخصوص.
- دمج الأمن السيبراني في برامج الدراسات الأمنية الموجودة حاليا.
- الاستعانة بالخبرات في مجال علم النفس الشخصية في برامج ودورات الأمن السيبراني.
- تدريب أخصائيين نفسيين في برامج تنمية الوعي بالأمن السيبراني.

المقترحات البحثية المستقبلية

- اجراء دراسة مماثلة على عينات من المراهقين من الجنسين.
- اجراء دراسة إرشادية لتنمية الوعي بالأمن السيبراني.
- اجراء دراسة لخصائص أخري ومتغيرات أخرى في الشخصية كمنبئات بمستوى الوعي بالأمن السيبراني.

Abstract

Differences in cybersecurity awareness among Kuwaiti youth in light of some demographic variables and the five major personality factors.

By Turki Bandar Al-Anzi

The study aimed to study the level of the study in awareness level of cyber security of Kuwaiti youth, as well as to reveal the differences in the level of awareness of cyber security in some demographic variables and the big five factors of personality . In order to verify the hypotheses of this study, a battery of questionnaires included the Big Five Personality Factors, and questionnaires of awareness of cyber security. After fulfilling the psychometric requirements of the battery, the data was collected from a sample (n = 145) Kuwaiti youth . The Results showed that there were Significant Statistical Differences in between males, females differ from Males. • The Results showed that there were Significant Statistical Differences due to the big five factors of personality , There were no statistically significant differences between the average responses of the study sample members at the level of significance (00,05) in the degree of awareness level of cyber security in cyber security due to (education level). Finally, the results showed a high level of awareness of cyber security among Kuwaiti youth.

Keyword: awareness of cyber security . Big Five Personality Factors

المراجع

الأنصاري، بدر محمد (1997) مدى كفاءة قائمة العوامل الخمسة الكبرى للشخصية في المجتمع الكويتى. دراسات نفسية. 2. 277-314

السرحان، حسنين عبد المهدى. والمشاقبة، محمد ناصر.(2020). أثر تطبيق سياسية الأمن السبيرانى على جودة المعلومات. رسالة ماجستير رسالة غير منشورة. جامعة اليرموك. الأردن

الصفحى، مصباح محمد.(2019). مدى الوعى بالأمن السبيرانى لدى معلمات الحاسب الألى للمرحلة الثانوية بمدينة جدة. مجلة البحث العلمى في التربية. ج10 . 493- 534

القحطانى، نورة بنت ناصر.(2019). مدى توافر الوعي بالأمن السيبرانى لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. مجلة شؤون اجتماعية. 85-120

المنتشري، فاطمة يوسف.(2020). درجة وعى المعلمات المرحلة المتوسطة بالأمن السبيرانى في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية. مج 4. 95-140

يونس، فيصل، وخليل ألهام (2007) نموذج العوامل الخمسة لشخصية: التحقق من الصدق واعادة الإنتاج عبر الحضاري. دارسات نفسية. 17 . 3 . 553-583

Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. In 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE) (pp. 62-68). IEEE.

Aloul, F. A. (2012). The need for effective information security awareness. Journal of advances in information technology, 3(3), 176-183.

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cyber security awareness (cybar). Information, 11(2), 121.

Alqahtani, H., & Kavakli-Thorne, M. (2020,). Factors affecting acceptance of a mobile augmented reality application for cyber security awareness. In Proceedings of the 2020 4th International Conference on Virtual and Augmented Reality Simulations (pp. 18-26).

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), e06016

Bada, M., & Nurse, J. R. (2019). Developing cyber security education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security .

Banfield, J. M. (2016). A study of information security awareness program effectiveness in predicting end-user security behavior. Eastern Michigan University .

Buchholz, A., Delano, R., Gold, M., Lu, F., Matthews, K., & Takala, S. (2017). Biting Off More than You Can Chew: An Assessment of Student's Understanding of Dalhousie's Food System .

Buckholz, A. Martin, M. J., Sturge-Apple, M. L., Davies, P. T.,& Romero, C. V (2017). A process model of the implications of spillover from co-parenting conflicts into the parent–child attachment relationship in adolescence. Development and psychopathology, 29(2), 417-431.

Casta, P., Charles, R., & Pahl, H. Nemecek, T., von Richthofen, J. S., Dubois, G., (2008). Environmental impacts of introducing grain legumes into European crop rotations. European journal of agronomy, 28(3), 380-393 .

Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. Computers & Security, 97, 101959.

Claar, C. L. (2011). The adoption of computer security: An analysis of home personal computer user behavior using the health belief model. Utah State University.

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. Journal of Computer Information Systems, 52(4), 20-29 .

Cooper, A. R., Page, Wheeler, B. W., A. S., & Jago, R. (2010). Green space and children's physical activity: a GPS/GIS analysis of the PEACH project. Preventive medicine, 51(2), 148-152 .

Cooper, A. J., L. D. Smillie, and P. J. Corr. 2010. "A Confirmatory Factor Analysis of the Mini-IPIP Five-Factor Model Personality Scale." Personality and Individual Differences 48 (5): 688–691.

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cyber security Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. Education and Information Technologies, 1-24.

Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P., & Utakrit, N. (2021,). A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization. In 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 102-106). IEEE.

Darwish, A.; El Zarka, A.; and Aloul, F. (2012). Towards understanding phishing victims' profile. Proceedings of International Conference on Computer Systems and Industrial Informatics (ICCSII). Sharjah, United Arab Emirates, 1-5.

Emm, D. (2021). Gasification–can it be applied to security awareness training?. Network Security, 2021(4), 16-18.

Gadbois, E. A., & Dugan, E. (2015). The big five personality factors as predictors of driving status in older adults. Journal of aging and health, 27(1), 54-74.

Hadlington LJ.(2018) Employees attitudes towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom. Int J Cyber Criminol.;12:269–81.

Hadlington, L., & Parsons, K. (2017). Can cyber loafing and Internet addiction affect organizational information security?. Cyber psychology, Behavior, and Social Networking, 20(9), 567-571.

Hadlington, L., Binder, J., & Stanulewicz, N. (2020). Fear of missing out predicts employee information security awareness above personality traits, age, and gender. Cyber psychology, Behavior, and Social Networking, 23(7), 459-464.

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., ... & Chen, J. (2016, November). Cultural and psychological factors in cyber-security. In Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services (pp. 318-324).

Jalali MS, Siegel M, Madnick S.(2019) Decision-making and biases in cyber security capability development: evidence from a simulation game experiment. Journal of Strategic Information Systems;28(1):66–82.

Jin, Z. Gao, Y., Li, B., Wang, W., Xu, W., ., & Zhou, C (2018). Watching and safeguarding your 3D printer: Online process monitoring against cyber-physical attacks. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2(3), 1-27.

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cyber security education for high school students. Journal of Education and Learning (EduLearn), 12(1), 150-158.

John, O. P.& Soto, C. J (2009). Using the California Psychological Inventory to assess the Big Five personality domains: A hierarchical approach. Journal of Research in Personality, 43(1), 25-38 .

Kaplan, S. N., Klebanov, M. M., & Sorensen, M. (2012). Which CEO characteristics and abilities matter?. The journal of finance, 67(3), 973-1007 .

Lee, K. G., Chong, C. W., & Ramayah, T. (2017). Website characteristics and web users' satisfaction in a higher learning institution. International Journal of Management in Education, 11(3), 266-283.

Linkov, I, Wood, M. D., Wells, E. M. &., Rice, G., (2019). Quantifying and mapping resilience within large organizations. Omega, 87, 117-126 .

Linkov, V., Zámečník, P., Havlíčková, D., & Pai, C. W. (2019). Human factors in the cyber security of autonomous vehicles: Trends in current research. Frontiers in psychology, 10, 995.

McCormac A, Calic D, Parsons K, Butavicius M, Pattinson M, Lillie M. The effect of resilience and job stress on information security awareness. Inf Comput Secur. 2018 Jul 9;26(3):277–89 .

Moti, Z., Hashemi, S., & Jahromi, A. N. (2020,). A Deep Learning-based Malware Hunting Technique to Handle Imbalanced Data. In 2020 17th International ISC Conference on Information Security and Cryptology (ISCISC) (pp. 48-53). IEEE.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. Computers in Human Behavior, 69, 151-156.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. Computers in Human Behavior, 69, 151-156.

Mišeikis, J., Caroni, P., Duchamp, P., Gasser, A., Marko, R., Mišeikienė, N., ... & Früh, H. (2020). Lio-a personal robot assistant for human-robot interaction and care applications. IEEE Robotics and Automation Letters, 5(4), 5339-5346 .

Moti Zwilling, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin & Hamdullah

Nejat Basim (2020): Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, DOI: 10.1080/08874417.2020.1712269

Potgieter, P. (2019). The Awareness Behaviour of Students On Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. Kalpa Publications in Computing, 12, 272-280 .

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. AMCIS 2006 Proceedings, 415.

Saadatdoost, R., Sim, A. T. H., Jafarkarimi, H., & Mei Hee, J. (2015). Exploring MOOC from education and Information Systems perspectives: a short literature review. Educational Review, 67(4), 505-518.

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2021). An effective cyber security training model to support an organizational awareness program: The Cyber security Awareness

TRAining Model (CATRAM). A Case Study in Canada. In Research Anthology on Artificial Intelligence Applications in Security (pp. 174-188). IGI Global.

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cyber security behavior. Psychology of Popular Media, 9(4), 475–480.

Shaw RS, Chen CC, Harris AL, Huang HJ(2009.) The impact of information richness on information security awareness training effectiveness. Computer Educ.;52(1):92–100 .

Shaw, L. M., Vanderstichele, H., Knapik-Czajka, M., Clark, C. M., Aisen, P. S., Petersen, R. C., ... & Alzheimer's Disease Neuroimaging Initiative. (2009). Cerebrospinal fluid biomarker signature in Alzheimer's disease neuroimaging initiative subjects. Annals of neurology, 65(4), 403-413.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. computers & security, 49, 177-191 .

Simsim, M.T(2011.) Internet usage and user preferences in Saudi Arabia. J. King Saud Univ. Eng. Sci., 23, 101–107

Stefan, G Scott, D., & Hall, C. M.,. (2012). Tourism and climate change: Impacts, adaptation and mitigation. Routledge.

Uebelacker, S.; and Quiel, S. (2014). The social engineering personality framework. Proceedings of Workshop on Socio-Technical Aspects in Security and Trust (STAST) .

Vienna, Austria, 24-30.Wee, C., & Bashir, M. (2016). Understanding the personality characteristics of cyber security competition participants to improve the effectiveness of competitions as recruitment tools. In Advances in Human Factors in Cyber security (pp. 111-121). Springer, Cham.

Whitman, M. E., & Mattord, H. J. (2011). Threats To Information Security Revisited. Journal of Information System Security, 8.(1)

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. Cyber psychology, Behavior, and Social Networking, 17(3), 131-132.

Yunos, Z., Ab Hamid, R. S., & Ahmad, M. (2016). Development of a cyber security awareness strategy using focus group discussion. In 2016 SAI Computing Conference (SAI) (pp. 1063-1067). IEEE.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 1-16.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97