مجلة جامعة أم القرى
للهندسة والعمارة
الموقع الإلكتروني: https://uqu.edu.sa/jea

دور التوعية بالأمن السيبراني في الحد من أثر تعقيد وسائل التحقق الرقمي من الهوية على سلوك المستخدم الطرفي

ياسر محمد هوساوي [أ،*]

[أ] قسم تقنية المعلومات، معهد الإدارة العامة، فرع منطقة مكة المكرمة.

The role of Cybersecurity Awareness in Reducing the Complexity Impact of Authentication Methods on End-user's Behavior

Yasser M. Hauwsawi [a,*]

[a] *Department of Information Technology Institute of Public Administration*

معلومات عن البحث

تاريخ الاستلام: ١٢/١١/٢٠١٩

تاريخ القبول: ٤/٣/٢٠٢٠

الكلمات المفتاحية

الأمن السيبراني، أمن المعلومات، السلوك المتعلق بالأمن السيبراني، آليات تحقيق الأمن السيبراني، التحقق الرقمي من الهوية، التوعية بالأمن السيبراني.

ملخص البحث

أضحى الامن السيبراني وتحقيقه من الأمور ذات الأهمية المتزايدة على المستوى القومي، إذ بات عنصراً مهماً في تحسين فاعلية البيئة الرقمية وفق رؤية المملكة العربية السعودية ٢٠٣٠. ونظراً لكون المستخدم الطرفي (العادي) يعتبر من ضمن الركائز الأساسية لنجاح تحقيق الامن السيبراني من خلال تفاعله مع آليات ووسائل تحقيقه بطرق مناسبة، فإنه من الأهمية بمكان التعرف على أهمية دور التوعية بالأمن السيبراني في الحد من التصرفات السلبية التي تصدر من قبل ذلك المستخدم العادي أثناء تعامله مع تلك الآليات. ويعتبر التحقق الرقمي من الهوية من أهم مراحل تحقيق الأمن السيبراني وهو يمثل المرحلة الاساسية التي تكون بمثابة مفتاح الحماية. ويعد نجاح آليات تحقيق الأمن السيبراني الاخرى معتمداً بشكل كبير على قوة ونجاعة أنظمة التحقق الرقمي من الهوية ودقة نتائج عمليات التحقق، بحيث تكون معدلات القبول الخاطئ والرفض الخاطئ بأقل قدر ممكن . ولكن نظراً لكون عمليات التحقق الرقمي من الهوية هي في الأساس تعتبر من آليات تحقيق الأمن السيبراني ذات العلاقة المباشرة بالعنصر البشري من حيث التفاعل والتعامل، فإن دور ذلك العنصر البشري يعتبر محورياً وممكناً اساسياً لنجاح عمليات التحقق. وإذا ما سلمنا بمحورية واهمية دور العنصر البشري، فإن الوعي بالطرق والسلوكيات السليمة للتعامل والتفاعل مع وسائل التحقق الرقمي من الهوية يعتبر من الممارسات التي يتم اتباعها من اجل الوصول إلى أفضل النتائج وأدقها في عمليات التحقق .لذا تأتي هذه الدراسة البحثية لتلقي الضوء على مدى فاعلية برامج التوعية بالأمن السيبراني ودورها في تحسين نتائج عمليات التحقق الرقمي من الهوية. وقد تم إتباع المنهج الوصفي التحليلي في إجراء الدراسة الحالية وفقاً لما تقتضيه طبيعة البيانات التي تم الحصول عليها من عينة الدراسة التي بلغ حجمها ٣٨٩ مفردة اعتماداً على إستبانة إلكترونية متحققة الصدق والثبات. هذا وقد أظهرت نتائج التحاليل الإحصائية المتمثلة في تحليل التباين الاحادي باستخدام برنامج الحزم الإحصائية الاجتماعية (SPSS) وجود دور مهم وفاعل لبرامج التوعية بالأمن السيبراني في الحد من الأثر الانعكاسي لوسائل التحقق الرقمي من الهوية على سلوك المستخدمين.

Abstract

Cybersecurity has become an increasingly important issue at the national level as it has become an important factor in improving the effectiveness of the digital environment in accordance with Saudi Arabia's vision 2030. Since the end-user is one of the main pillars for the success of achieving cybersecurity goals through its proper interaction with the right mechanisms, therefore, it is crucial to recognize the importance of the role of cybersecurity awareness in reducing the negative behaviors that might be acted by that end-user while dealing with such mechanisms. Authentication is one of the most important stages of achieving cybersecurity and represents the basement that serves as the key to success protection. The success of other cybersecurity mechanisms depends heavily on the strength and efficiency of authentication systems and the accuracy of the results of verification processes, so that the false accept and false reject rates are minimized. However, since authentication is essentially a mechanism for achieving cybersecurity that is directly related to the human in terms of interaction and usage, the role of that human is essential to the success of verification processes. Acknowledging the importance of the role of the human, awareness of proper behaviors to deal and interact with authentication methods is one of the best practices to achieve best and most accurate results of verification processes. This study is designed to shed light on the effectiveness of cybersecurity awareness programs and their role in improving the results of authentication processes. The analytical descriptive method was adopted in the current study according to the nature of the data obtained from the participants which reached 389 individuals based on reliable and credible questionnaire. The results of the statistical analysis (One-way ANOVA) using SPSS show an important and effective role of cybersecurity awareness programs in reducing the reflexive effect of authentication methods on user behavior.

Keywords

Cybersecurity, Information Security, Security behaviors, Security Mechanisms, Authentication, Security Awareness

[*] **بيانات التواصل:**

قسم تقنية المعلومات، مدير إدارة شئون المتدربين، معهد الإدارة العامة، فرع منطقة مكة المكرمة.

البريد الإلكتروني: (hawsawiy@ipa.edu.sa) *ياسر محمد هوساوي*

مقدمة

تعد الثورة التقنية في العالم الرقمي من أبرز مسرعات التطور في الأعمال، إذ باتت حاسمةً في إحداث نقلة نوعية في التحولات الاقتصادية والاجتماعية على جميع الأصعدة. وحيث أن الامن السيبراني من الأهمية بمكان للحفاظ على طبيعة المعلومات والخصوصية المرتبطة بالمنظمات، فقد بات من الضروري وضع التدابير اللازمة لتوفير الحماية على سرية وسلامة وإتاحة المعلومات في إطار البيئة التي تحتويها.

ولما كان تحقيق الأمن السيبراني له انعكاساته المباشرة على سلوك المتعاملين معه، فإن الدراسة الراهنة تهتم بفهم ورصد دور الوعي بالأمن السيبراني في الحد من الأثر الإنعكاسي لوسائل التحقق الرقمي من الهوية على سلوك المستخدم العادي.

وحيث أن طبيعة التفاعل تقتضي وجود ثلاثة أطراف هي: العنصر البشري، والبيئة التقنية الرقمية، وأمن المعلومات؛ فإنه يمكن تلخيص ذلك التفاعل الثلاثي على أن أي نظام أو آلية أو وسيلة تستخدم بهدف تحقيق الأمن السيبراني تكون قابلة للتطبيق والاستخدام في البيئة التقنية الرقمية إذا كان العنصر البشري قادر على التعامل بل والتفاعل معها بسهوله وسلاسة وفاعلية في ظل مستوى عال من الاعتمادية، ولكن في الوقت ذاته تكون معقدة وصعبة الاختراق بالنسبة لغير المخولين (Hausawi, 2015). وهنا يلعب الوعي الأمني المعلوماتي دوراً محورياً في إنجاح ذلك التفاعل المذكور آنفاً.

أولاً: إشكالية الدراسة

تشهد ثورة التطور التقني الذي نواكبها منذ منتصف التسعينات من القرن الماضي إلى وقتنا الحاضر تسارعاً غير تقليدياً مقارنة بالثورات السابقة، إذ بات العالم يعتمد في الآونة الأخيرة على المعلومات المتدفقة بقوة من خلال تسخير تقنية المعلومات التي أدت إلى ظهور الكثير من المجالات والتخصصات المتعلقة بالمعلومات والتقنيات المرتبطة بها، وهو ما تجلى في استحداث مجالات جديدة ومستحدثة مثل مجال الأمن السيبراني الذي يرتبط ارتباطاً وثيقاً بأطر تبادل وحفظ ومعالجة المعلومات في العالم الرقمي (الهيئة الوطنية للأمن السيبراني، ٢٠١٨).

وعليه، فقد اضحى الأمن السيبراني مجالاً يلامس اهتمام كل من له علاقة بالعالم الرقمي سواءً كان من الأفراد او المنظمات او الحكومات، لذلك بات من الأهمية بمكان تحقيق الامن السيبراني من خلال استخدام الآليات والوسائل الممكنة التي تساعد على تحقيقه. ومن أجل ذلك، تم إنشاء الهيئات والمنظمات والاتحادات والشركات والكليات وغيرها من الكيانات التي تهتم بإيجاد وابتكار وتطوير وتشريع وضبط آليات ووسائل تحقيق الأمن السيبراني.

وبالرغم من كل الجهود المبذولة لإنجاح تلك الوسائل والآليات المبتكرة، والعمل الجاري على التشريعات والأنظمة واللوائح التي تؤطر وتضع الضوابط لاستخدام تلك الآليات والوسائل، إلا أنه لا يزال تحقيق الأمن السيبراني في نتاجه المأمول امراً يتسم بالصعوبة والتعقيد، وهو ما يعود في نظر مختصو الأمن السيبراني إلى وجود العنصر البشري في حلقة الأمن وكونه النقطة الأضعف في تلك الحلقة (Pfleeger, Sasse, and Furnham, 2014). وبالرغم من دعم الكثير من الأدبيات السابقة حول كون العنصر البشري أضعف نقطة في حلقة الأمن السيبراني (Heartfield and Loukas, 2018; Safa, Solms, and Futcher, 2016)، إلا أن الأغلبية منها تتناول العلاقة بين آليات ووسائل التحقيق من جهة، والعنصر البشري من جهة أخرى باتجاه واحد هو دراسة وتحليل طريقة تعامل العنصر البشري مع تلك الآليات والوسائل والتعمق في ذلك الاتجاه. وحيث أن جل الاهتمام يتمركز في سياق ذلك الإتجاه المذكور آنفاً، فإنه من الأهمية بمكان دراسة مدى تأثير الممكنات والأساليب المتبعة للتغلب على المشاكل والعقبات التي من المفترض أن تلعب دوراً محورياً في تحسين تلك العلاقة في ظل تعقيداتها وصعوبة التعامل معها (Hausawi, Allen, and Bahr, 2014).

لذا تأتي هذه الدراسة لتسلط الضوء على الدور الذي تلعبه برامج التوعية بالأمن السيبراني بمختلف مستوياتها وانواعها، وتحديد مدى نجاحها في تحسين العلاقة التعاملية بين المستخدم العادي ممثلاً في سلوكه المتبع ووسائل التحقق الرقمي من الهوية بإعتبارها من جملة الآليات الأساسية لتحقيق الأمن السيبراني.

ومن أجل تحقيق أهداف البحث والإجابة على تساؤلاته، فإن الدراسة ركزت على المستخدم العادي نظراً لتزايد الإعتماد على المعلومات وتقنياتها، الامر الذي يجعل العلاقة والتعامل بين الطرفين أمراً حتمياً، هذا وتسعى جميع القطاعات للوصول إلى مستويات متقدمة في إستخدام التقنية والإعتماد عليها وتسخيرها في التعامل مع العملاء بكافة شرائحهم ومستوياتهم. فالمملكة العربية السعودية تسعى نحو تحقيق التحول الرقمي كأحد الأهداف التي تلتزم بها رؤية المملكة العربية السعودية ٢٠٣٠ [*] وصولاً إلى مصاف المراكز الخمسة الأولى في مؤشر الحكومات الإلكترونية التابع للأمم المتحدة. وحيث أن هناك الكثير من الآليات المستخدمة في إطار فضاء الأمن السيبراني لتحقيق أهدافه مثل الجدران النارية ومصائد العسل والمناطق منزوعة السلاح في الشبكات، والشبكات الافتراضية، وأنظمة كشف التسلل وغيرها، إلا أنها لا تتفاعل بشكل مباشر مع المستخدم النهائي (Kaur, Malhotra, and Singh, 2014). لذا، تم التركيز على دراسة دور برامج التوعية بالأمن السيبراني في الحد من الأثر الإنعكاسي لوسائل التحقق الرقمي من الهوية على سلوك المستخدمين بصورة مباشرة (Bano and Zowghi, 2015; Mayron, Hausawi, and Bahr, 2013). وتعد هذه الدراسة امتداداً منطقياً لدراسة سابقة تم إجراؤها حديثاً من قبل الباحث (هوساوي، ٢٠١٩)، في ظل ذات الإطار النظري والخلفيات المرجعية، ولكن وفق منطلق مختلف ومجتمع وعينة دراسة وتساؤلات وفرضيات ومتغيرات مختلفة، إضافة إلى تحليل إحصائي مختلف يتناسب مع منطلق وظروف هذه الدراسة الحالية المكملة للدراسة السابقة.

ثانياً: أهداف الدراسة

في ضوء ما تقدم فإن هذه الدراسة تهدف إلى فهم ورصد دور برامج التوعية بالأمن السيبراني في الحد من انعكاسات وسائل التحقق الرقمي من الهوية على المستخدمين؛ ويمكن تلخيص أهداف الدراسة الحالية بالتالي:

[*] راجع ذلك في المحور الثالث المرتبط "وطن طموح" في: رؤية المملكة العربية السعودية ٢٠٣٠ (رؤية المملكة العربية السعودية ٢٠٣٠، ٢٠١٦)

- التعرف على طبيعة العلاقة بين برامج التوعية بالأمن السيبراني والتعامل مع وسائل التحقق الرقمي من الهوية من قبل المستخدمين.
- تحديد طبيعة السلوك الصادر من قبل المستخدمين الناتج عن تعاملهم مع وسائل التحقق الرقمي من الهوية.

ثالثاً: أسئلة الدراسة

من خلال شرح الهدف العام للدراسة وتحديد الأهداف الفرعية، فإنه يمكن صياغة السؤال الرئيس للدراسة بما يلي: **ما طبيعة العلاقة بين برامج التوعية بالأمن السيبراني وتعامل المستخدمين مع وسائل التحقق الرقمي من الهوية؟**

وانطلاقاً من السؤال الرئيس للدراسة، فهناك مجموعة من الأسئلة الفرعية التي تفرض نفسها للوفاء بأهداف الدراسة وما تثيره من إشكاليات، ولعل أهمها:

١. ما مستوى الوعي بالأمن السيبراني لدى المستخدمين بشكل عام؟
٢. ما طبيعة السلوك الصادر من المستخدمين تجاه وسائل التحقق الرقمي من الهوية؟

رابعاً: فرضيات الدراسة

وفقاً لأهداف وأسئلة الدراسة، فإنه يمكن صياغة فرضيات الدراسة وفق الأدبيات ذات العلاقة. وعليه، فإن فرضية العدم تنص على أنه "لا يوجد دور لبرامج التوعية بالأمن السيبراني في تحسين تعامل المستخدمين مع وسائل التحقق الرقمي من الهوية".

ومن خلال نص فرضية العدم فإن الفرضية البديلة تنص على أنه " يوجد دور لبرامج التوعية بالأمن السيبراني في تحسين تعامل المستخدمين مع وسائل التحقق الرقمي من الهوية".

خامساً: أهمية الدراسة (العلمية والعملية)

تكمن أهمية هذه الورقة في كشف وتحديد مدى نجاعة وأهمية الدور الذي من المفترض أن تلعبه برامج التوعية بالأمن السيبراني في العلاقة التعاملية بين المستخدمين ووسائل التحقق الرقمي من الهوية، والوقوف على الوضع الراهن لتلك العلاقة وتقديمها للمختصين، الأمر الذي قد يسهم بدوره في تطوير برامج التوعية بالأمن السيبراني بما يكفل لنا المساهمة في تحسين نتائج عمليات التحقق الرقمي من الهوية ووضع نموذج إرشادي لكي تتوافق مع واقع وطبيعة تلك العلاقة على المستوى المنظور. وإذا كان ما سبق يمثل الأهمية العملية، فإن الأهمية العلمية تتجسد في الخروج بنتائج وتوصيات تسهم في تحسين آليات ووسائل التحقق الرقمي من الهوية (من حيث الدرجة) وارتباطها بتعاطي وتفاعل المستخدمين معها.

سادساً: الإطار النظري

لما كانت البحوث العلمية تسترشد في عملها بالنماذج النظرية التي تستند على مجموعة من المقولات النظرية والمفاهيم العلمية، فإن البحث الراهن يستند على مجموعة من المفاهيم والموجهات التي سيتم التطرق لها وهي:

١. مفهوم الأمن السيبراني:

تتابع تطور مجال تقنية المعلومات وتوسعت مجالاته وتفرعاته، ونتيجة لذلك التطور توسعت تفرعات أمن المعلومات بشكل مضطرد وظهر المصطلح الحديث لمجال حماية المعلومات والفضاء الذي يحتوي كل ماله علاقة بتلك المعلومات وانتشر على نطاق واسع وهو "الأمن السيبراني" وأصبح مصطلحاً شاملاً يضم كل المصطلحات والتعريفات المتعلقة بالمعلومات وحمايتها في جميع الصور (رقمياً وغير رقمي). فبحسب تعريف الهيئة الوطنية للأمن السيبراني، ينص تعريف الأمن السيبراني على "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك" (الهيئة الوطنية للأمن السيبراني، ٢٠١٨).

وتاريخياً قبل ظهور مصطلح الأمن السيبراني، تعاقبت الآليات والوسائل المستخدمة لحفظ وحماية المعلومات وفقاً للفترات الزمنية والمراحل التي مرت بها المعلومات المراد الحفاظ عليها وحمايتها. وكانت تلك الآليات والوسائل تتماشى مع النهضة العلمية الموجودة في كل حقبة إلى أن ظهرت الرقمنة وتقنية المعلومات وبدأت ثورتها التي لا نزال نعيش في أوجها منذ ستينات القرن الماضي (De Leeuw, Michael, and Bergstra, 2007). وقد كانت تلك الآليات والوسائل التي تعنى بحماية المعلومات والبيئة المحيطة بها إلى وقت قريب تصنف تحت مصطلح أمن المعلومات الذي يمكن تعريفه على أنه " تطبيق لأفضل الأساليب والاستراتيجيات والسياسات والمبادئ والإجراءات التي تتكامل مع بعضها البعض لإخفاء نقاط ضعف مكونات البيئة الرقمية بهدف تأمين المعلومة من خلال ضمان سريتها وسلامتها و توفرها للمخولين، بالإضافة إلى المساءلة التي تتمثل في ضمان عمليات التدقيق و عدم الانكار (Hausawi, 2015).

٢. برامج التوعية بالأمن السيبراني

في شرح سابق لبرامج التوعية بالأمن السيبراني (هوساوي، ٢٠١٩)، تعتبر برامج التوعية الأمنية من جملة الآليات والوسائل غير التقنية التي تسهم في تحقيق أهداف الأمن السيبراني (SANS Awareness, 2017). ويمكن تعريف برامج التوعية الأمنية بحسب المعهد الوطني للمعايير والتقنية بالولايات المتحدة الأمريكية على أنها عبارة عن حملات تستخدم جميع الوسائل الممكنة لجذب اهتمام المستهدفين وتوجيه تركيزهم نحو الأمن السيبراني وأهميته بهدف جعلهم مدركين للمخاوف والأخطار والتهديدات الأمنية والوقاية منها، والتعامل معها بالطرق السليمة (Bada, Sasse, & Nurse 2019). وفي هذا الإطار هناك عدة أساليب وسياسات يمكن اتباعها في تنفيذ برامج التوعية بالأمن السيبراني، ويعتمد تنفيذها على عدة عوامل منها الحالة الأمنية التي تمر بها المنظمة أو البيئة المحيطة بها. ويمكن تلخيص تلك الأساليب والسياسات في التوعية بأسلوب التعليم والتدريب، والتوعية بأسلوب الترغيب والتشجيع، والتوعية بأسلوب الفرض والإجبار، واخيراً التوعية بأسلوب العقاب (Hausawi, 2015). وإذا كانت الأساليب والسياسات السابقة هي التي يمكن تطبيقها لتحقيق التوعية بالامن السيبراني، إلا أن أروقة البحث العلمي تتفق على أن أفضل برامج التوعية بالأمن السيبراني هي التي تستخدم جميع الأساليب المذكورة بشكل متدرج تباعاً.

٣. التحقق الرقمي من الهوية

تعد عملية التحقق من الهوية من أبجديات ضمان الأمن والسلامة سواءً في العالم الرقمي أو غير الرقمي، حيث تمثل الخطوة الأولى لإجراء الوصول إلى الأشياء، ومن ثم تعتمد باقي خطوات إجراءات الوصول على مدى نجاح عملية التحقق (Hausawi, Allen, and Bahr, 2014). ويعرف التحقق من الهوية في

عمومه على أنه إجراء يتم القيام به للتأكد من الهوية اعتماداً على إحدى الوسائل التي يتم الحصول عليها من الشخص المراد التحقق من هويته (Rodionova, Titova, and Pomerantsev, 2016). وفي هذا السياق فإنه يمكن للتحقق من أن يكون تقليدياً أو الكترونياً في البيئة الرقمية، وذلك ما يجعل التحقق الرقمي من الهوية إجراءً مهماً يتم القيام به الكترونياً للتأكد من الهوية اعتماداً على إحدى الوسائل التي يتم الحصول عليها من الشخص المراد التحقق من هويته بعد تحويلها إلى شكل رقمي (Jain, Ross, and Nandakumar, 2011). وبشكل عام، هناك ثلاثة أنواع للتحقق الرقمي من الهوية، منها نوعين رئيسيين هما: المطابقة والتعرف؛ إضافة إلى نوع ثالث هجين يتمثل في المصادقة المزدوجة أو التحقق الثنائي (Raja et al., 2015).

آليات تحقيق الأمن السيبراني

قامت شركة أي بي أم الأمريكية بتعريف آليات تحقيق الأمن السيبراني على أنها الأدوات التقنية والتقنيات المستخدمة لتطبيق الخدمات التي يعتمد عليها في تحقيق الأمن السيبراني (IBM, 2018). ووفقاً لتعريف مصطلح الأمن السيبراني السابق ذكره آنفاً الصادر من الهيئة الوطنية للأمن السيبراني والذي كان جل تركيزه على حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، فإنه لابد من وجود آليات وطرق ووسائل وتقنيات يتم بنائها وتصميمها خصيصاً من أجل توفير تلك الحماية المنشودة. وعليه، فإن جميع تلك الوسائل والطرق التي يتم تصميمها لكي تستخدم من أجل الوقاية، والاكتشاف، والمعالجة من المشاكل السيبرانية يمكن أن تدخل ضمن إطار مصطلح آليات تحقيق الأمن السيبراني (Stallings, 2017).

ولعل من أبرز تلك الآليات والوسائل التي يتم استخدامها بشكل دائم من قبل كافة المستخدمين هي وسائل التحقق من الهوية الرقمية بمختلف أنواعها، حيث أنه يمكن اعتبارها من اهم الآليات المستخدمة لتحقيق الأمن السيبراني ذات العلاقة بالعنصر البشري (Joseph, Kathrine, and Vijayan, 2014).

٤. التفاعل بين البشر والكمبيوتر والأمن السيبراني

بدأ التفاعل بين البشر والكمبيوتر منذ ظهور أول جهاز حاسب آلي في ستينات القرن الماضي (Kitchin, 2014)، ولكن الاهتمام بذلك التفاعل لم يتم التطرق إليه بشكل واضح في دوائر البحث العلمي إلا في نهاية السبعينات وبداية الثمانينيات من القرن الماضين وتحديداً بين عامي ١٩٧٦ م و١٩٨٢ م، وذلك بسبب التزايد المضطرد لعدد المستخدمين الطرفيين الذين يتعاملون مع أجهزة الكمبيوتر جراء إنتشار الأجهزة الشخصية والتوسع في استخدامها (Lazar, Feng, and Hochheiser, 2017). أما في عام ٢٠٠٣، فقد توسعت دائرة الاهتمام تلك لتشمل الأمن السيبراني كأحد اهم أوجه التفاعل بين البشر والكمبيوتر، وكان ذلك تحت مسمى "التفاعل بين البشر والكمبيوتر وأمن المعلومات" Human-Computer Interaction and Security، والجدير بالذكر أن أمن المعلومات يعتبر حالياً أحد أعمدة الأمن السيبراني وفق تعريف الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية (الهيئة الوطنية للأمن السيبراني، ٢٠١٨).

سابعاً: الدراسات السابقة

بالرغم من الاهتمام البحثي الدائر حول العلاقة بين سلوك العنصر البشري (المستخدم الطرفي) ونجاح آليات ووسائل التحقق الرقمي من الهوية، إلا أنه هناك مجال واسع لتناول هذه العلاقة من منظور الدور الذي تلعبه برامج التوعية بالأمن السيبراني على سلوك العنصر البشري عند تعامله مع وسائل التحقق الرقمي. وحيث أن البحث العلمي يعتمد على التراكمية المعرفية، إما بالإضافة إلى ما هو موجود من ادبيات وقوانين علمية، وابتكارات تطبيقية؛ أو بالتحقق مما وصل إليه الآخرون والإستفادة منه، فإن الباحث وفق طبيعة هذه الدراسة قد تمكن من رصد مجموعة من الدراسات السابقة التي تتناول تلك العلاقة بهدف الإستفادة منها في معالجة إشكالية البحث والإجابة على التساؤلات الرئيسية فضلاً عن زيادة العمق التحليلي.

بادا وباحثين آخرين عملا على تحديد الأسباب الرئيسية التي يمكن اعتبارها كعوامل نجاح أو فشل حملات التوعية بالأمن السيبراني. حيث قام الباحثون على دراسة مسحية شاملة على الأدبيات البحثية الموجودة في دوائر البحث العلمي ذات التركيز على الحملات التوعوية للأمن السيبراني المؤثرة على سلوك الموظفين والعملاء والمواطنين (المستخدمين الطرفيين بشكل عام). وقد خلصت الدراسة إلى أن الاعتماد على نقل المعرفة حول أفضل الأساليب والممارسات في الأمن السيبراني غير كافٍ لتحقيق الأهداف التوعوية والحد من المخاطر السيبرانية المعلقة بالمستخدم الطرفي، فضلاً عن كون السبب الرئيسي لعدم جدوى حملات التوعية بالأمن السيبراني هو أن السياسات الأمنية والأنظمة التي تحاكي تطبيقها تعتبر سيئة التصميم. وفي نهاية المقال البحثي تم ذكر ٥ عوامل رئيسية قد تقود إلى نجاح الحملات التوعوية وهي: ضرورة أن تكون الحملات التوعوية معدة ومنظمة باحتراف، عدم الاعتماد على اساليب التخويف في الحملات التوعوية، التعليم والتدريب للأمن السيبراني يجب أن يتعدى الجانب المعلوماتي إلى الجانب التطبيقي، ضرورة الاعتماد على التدريب المعتمد على التغذية الرجعية لضمان استدامة فاعلية الحملات خلال فترات تغيير السلوك، وأخيراً الأخذ في الاعتبار البعد الثقافي وجوانب الاختلاف بين المجتمعات (Bada, Sasse, & Nurse 2019).

وفي بحث آخر أجراه وايلي وباحثين آخرين حول العلاقة السلوكية بين الثقافة (التنظيمية والأمنية) من جهة، وحملات التوعية بالأمن السيبراني من جهة أخرى؛ تم إجراء البحث على عينة تتكون من ٥٠٨ مفردة عن طريق الاستبانات الإلكترونية. وكانت نتائج البحث تشير إلى أن الثقافة الأمنية تلعب دوراً وسيطاً ذو أهمية بالغة في الربط بين الثقافة التنظيمية ونجاح حملات التوعية بالأمن السيبراني. ووصى فريق العمل البحثي على التركيز على الثقافة الأمنية بدلاً من التركيز على ثقافة التنظيمية من أجل انجاح حملات التوعية بالأمن السيبراني في المنظمات (Wiley, 2020).

قام باركر ومعاونوه بإجراء دراسة مسحية على ٥١٠ عينة مفردة من مجتمع مستخدمي الهواتف الذكية لإختبار مستوى الوعي الأمني لديهم وتبني الضوابط الأمنية من قبلهم. وقد كان التركيز على قياس درجة الفاعلية في التعامل مع وسائل التحقق من الهوية الرقمية وضوابط مكافحة السرقة. وكانت النتيجة تشير إلى أن المبحوثين لديهم مستوى مقبول من الوعي الأمني وذلك بخلاف نتائج الدراسات السابقة، إلا أنه هناك مشكلة في اتباع الضوابط الأمنية. وعليه، فقد اقترح الفريق البحثي أن يتم تبني تعليم المستخدمين وفق تصميم بسيط غير تقني يسهم في رفع مستوى الوعي الأمني وتشجيع اتباع الضوابط الأمنية والامتثال لها(Parker, 2015) .

وفي سياق متصل أجرى فريق بحثي بقيادة سميث-كرياسي دراسة بحثية قياسية حول أثر الوعي بطرق أداء الأنشطة الحركية (كالمشي على سبيل المثال) وكذلك القدرة المعرفية للتعامل مع الإضاءة بالشكل السليم في خفض معدل الخطأ عند التعامل مع وسيلة التحقق الرقمي بالسمة الحيوية (الوجه). وقد

نتجت الدراسة عن وجود أثر فعلي للوعي بالأنشطة الحركية في خفض معدل الخطأ بنسبة ٤.٠٥٪، إضافة إلى أثر القدرة على التعامل مع الإضاءة على خفض معدل الخطر بنسبة ٤.٣٩٪(Smith-Creasey, 2018) .

وفي ضوء ما تقدم فهناك بحث أُجريَ من قبل ستانتون وآخرون (٢٠٠٤) حول سلوكيات التعامل مع أنظمة امن المعلومات نظراً لكون نجاح تطبيق تلك الأنظمة مرتبط بسلوكيات المستخدمين. فقد تم اجراء دراستين اعتمدتا على الأسلوب الكيفي، من خلال استخدام أسلوب المقابلات التي تم تطبيقها في دراسة أولية على (١١٠) مفردة من المستخدمين العاديين، والمدراء، وأخصائيي تقنية المعلومات. أما في الدراسة الثانية فقد تم الإعتماد على الإستبانات، وتم تطبيقها على عينة قوامها (٢٩٨) مفردة من المستخدمين والمدراء الذين يعتمدون على تقنية المعلومات في تأدية مهام اعمالهم. ومن خلال تلك الدراستين تم الحصول على قائمة تتألف من (٩٤) سلوكاً مرتبطاً بأمن المعلومات، صنفت إلى ستة أصناف في مخطط تصنيف موزع على بعدين هما: القصد أو النية من السلوك والخبرة في التقنية واستخداماتها. فضلاً عن تحديد تسعة سلوكيات تعتبر من الأكثر تأثير (منها ٣ سلوكيات سلبية، ٦ سلوكيات إيجابية) على أنظمة أمن المعلومات ودور التوعية بأمن المعلومات في الحد من تبني السلوكيات السلبية (Stanton et al., 2004) .

في بحث آخر أُجريَ من قبل "إن جي ورفاقه" (٢٠٠٩) حول فهم العوامل التي تسهم في التأثير على سلوك الموظفين سلباً أو إيجاباً عند تعاملهم مع أنظمة أمن المعلومات (تأمين البريد الإلكتروني على وجه التحديد)، ومدى أهمية ذلك في تطوير أنظمة أمن المعلومات وقدرتها على توجيه سلوكياتهم للتعامل بشكل سليم مع تلك الأنظمة. قام الباحثون بتبني نموذج يسمى نموذج المعتقدات الصحية الذي من خلاله يتم توجيه المرضى لإتباع السلوكيات الصحية السليمة وتبنيها لتفادى التهديدات والمخاطر الصحية، وهو ما تم تكييفه وفق بيئة تقنية وأمن المعلومات بهدف فهم الأسباب التي تؤثر على سلوك الموظفين تجاه أنظمة أمن المعلومات، إذ من خلال تطبيق أداة الإستبانة على عينة قوامها (١٣٤) موظفاً، أفادت منها النتائج بأن الرغبة والقابلية، والفوائد المدركة، والكفاءة الذاتية، ومستوى الوعي تعتبر هي المحددات الرئيسة لسلوك الموظفين نحو حماية البريد الإلكتروني (Ng, Kankanhalli, and Xu, 2009).

وفي دراسة أخرى قام هادلينقتون (٢٠١٧) بدراسة للوقوف على العلاقة بين السلوكيات السلبية تجاه الأمن السيبراني، وإدمان استخدام الإنترنت، والإندفاع نحو استخدام التقنية في بيئة العمل؛ إضافة إلى التعرف على الآراء حول الجرائم السيبرانية. ومن خلال استبانات إلكترونية وزعت على (٥٣٨) موظفاً في بريطانيا، فقد تم التوصل إلى وجود علاقة قوية بين كل من مستوى الوعي، وإدمان استخدام الإنترنت، والاندفاع نحو استخدام التقنية من جهة، وتبني السلوكيات السيئة تجاه الأمن السيبراني من جهة أخرى (Hadlington, 2017).

وفي توجه آخر قام كيلي (٢٠١٨) بإجراء دراسة حول مدى تأثير وعي المستخدمين بالأمن السيبراني على سلوكياتهم المتمثلة في العادات الوقائية السليمة (Cyber Hygiene)، وطبيعة الاستجابة للتهديدات الأمنية (Threat Response) تجاه الآليات المستخدمة لتحقيق الامن السيبراني. وقد تم إختبار (١٩٤) من المستخدمين بواسطة بطاقات فرز مكتوب على كل بطاقة منها أحد السلوك (سلبي أو إيجابي) تجاه الامن السيبراني على الإنترنت، إذ تم الطلب منهم توزيع تلك البطاقات وفق السلوك المكتوب عليها على (قائمة التهديدات أو قائمة الحماية). هذا وقد نتج عن الدراسة وجود علاقة دلالية بين سلوكيات العادات الوقائية السليمة وسلوكيات الاستجابة للتهديدات الأمنية (Kelley, 2018) .

وللوقوف على ما قام به هيرث وآخرون (٢٠١٤) من محاولة لتطوير نموذج نظري تكاملي إنطلاقاً من نموذج تقبل التقنية ونظرية تجنب التهديدات التقنية وذلك بهدف دراسة وتحليل الخصائص المؤثرة على توجه المستخدمين نحو تبني سلوك يتكيف طواعية مع خدمة التحقق من هوية البريد الإلكتروني ويتعامل معها باعتبارها إحدى آليات تحقيق الامن السيبراني. ومن خلال إختبار النموذج الذي تم تطويره بواسطة استبانتين تم تقديمها إلى عينه تتألف من (٣٨٩) مستخدماً، تم التوكيد على أهمية وجود خاصيتي سهولة الإستخدام والفائدة اللتان يلعب الوعي دوراً أساسياً في تحققهما، إلا أن خاصية تبيان المخاطر والتهديدات تعتبر ذات تأثير كبير على تبرير فوائد آليات تحقيق الأمن السيبراني بشكل عام، ناهيك عن تأثيرها على سلوك المستخدمين بشكل خاص (Herath et al., 2014).

وبالاطلاع على ما قام به سيتوفا ومن معه من الباحثين (٢٠١٦) لتحديد المستوى والنوعية المناسبة لوسيلة التحقق الرقمي من الهوية في الأجهزة الذكية لكل مستخدم اثناء الاستخدام، من خلال تقديم ثلاثة خصائص للسمات الحيوية هي: حركة اليد عند العمل على شاشة الجهاز الذكي، وطريقة حمله، وطريقة الإمساك به، باعتبارها سلوكيات يمكن الإستفادة منها كخصائص إضافية. وقد تبين بأن هذه السلوكيات أو الخصائص تلعب دوراً محورياً في تحديد النوعية المناسبة لوسيلة التحقق الرقمي من الهوية في الأجهزة الذكية، تلك التي تؤثر بالضرورة على تخفيض نسبة أخطاء التحقق إلى (١٥,٧ %) بدلاً من النسب التي تم التوصل إليها عند الاعتماد على حساب معدل الوقت المستغرقة في الضغط على محتويات شاشة الجهاز الذكي (٢٥,٧ %)، وطريقة الضغط على تلك المحتويات (٣٤,٢ %) (Sitová, et al., 2016).

وحول بحث تم إجراؤه من قبل بار وآلن (٢٠١٣) حول التفاعل المهذب بين العنصر البشري وأنظمة الأمن السيبراني (رسائل التحذير الأمني على وجه الخصوص)، فإن الباحثان يشيران إلى أن من أكثر الأسباب التي تؤدي إلى فشل أنظمة الامن السيبراني التي تتعامل مع العنصر البشري هي أن اخصائيي الأمن السيبراني يقومون بتطوير تلك الأنظمة بناءً على اعتقاد خاطئ هو أن الأمن السيبراني يعتبر ذو أولوية قصوى، دون الإهتمام إلى مستوى الوعي لدى المستخدمين المستهدفين ومدى أهمية وأولوية تلك الأنظمة بالنسبة لهم. في حين أن واقع الأمر يفضي إلى أن الأمن السيبراني لا يعتبر ذو أولوية قصوى لدى المستخدمين العاديين. وبناءً على هذا الإستنتاج، قام الباحثان بوضع مبادئ للتصميم الذي يضمن التفاعل المهذب بين العنصر البشري وأنظمة الأمن السيبراني، حيث أن تلك المبادئ التي تتبنى دور التوعية بالأمن السيبراني تهدف إلى جعل العنصر البشري يبدي اهتماماً بتلك الأنظمة الأمنية (Bahr and Allen, 2013)

وفي إطار الإهتمام بوسائل التحقق من الهوية أجرى مايرون ومعاونوه (٢٠١٣) بحثاً حول مدى إمكانية اعتماد السمات الحيوية كوسائل للتحقق الرقمي من الهوية لتتناسب مع مختلف شرائح العنصر البشري وتجعل التفاعل بينهم أكثر قابلية وسهولة في الإستخدام والتطبيق. وقد اقترح فريق البحث مجموعة من المبادئ والأسس التي قد تسهم في تحسين طريقة تطوير أنظمة التحقق الرقمي المعتمدة على السمات الحيوية وجعلها ذات تأثير على سلوك العنصر البشري بشكل إيجابي في ظل وجود مستوى مقبول من الوعي بأهمية

تلك الأنظمة والطرق الصحيحة للتعامل معها (Mayron, Hausawi, and Bahr, 2013).

وفي نهاية إستعراضنا للدراسات السابقة، يمكن التعليق عليها وتبيان مدى الإختلاف بين توجهاتها ونتائجها وبين الدراسة الراهنة. فمن خلال ما تم استعراضه، بدا جلياً بأن إطار تناول طبيعة العلاقة التفاعلية بين العنصر البشري ووسائل التحقق الرقمي من الهوية يتركز حول التوكيد على أهمية ومحورية دور التوعية بالامن السيبراني عموماً دون التركيز على وسائل التحقق الرقمي من الهوية بإعتبارها نقطة الأساس في تعامل المستخدم العادي مع الفضاء السيبراني، وهو ما تركز عليه هذه الدراسة على وجه الخصوص، ناهيك عن الإختلاف الإطاري في بيئة البحث ومنهجيته. إضافة إلى ذلك، فإن أغلب الدراسات السابقة قد تم القيام بها في مجتمعات قد تختلف من حيث الثقافة والقيم والمبادئ، فضلاً عن عدم تطرق اغلبها لبيئة القطاع الحكومي وموظفيه باستثناء العمل البحثي الذي قام به هادلينقتون (Hadlington, 2017).

ثامناً: منهجية الدراسة

لما كانت الدراسة الراهنة تتعلق ببحث دور التوعية بالأمن السيبراني في الحد من إنعكاسات وسائل التحقق الرقمي من الهوية على سلوك المستخدمين العاديين، وأن تصميمها المنهجي يقتضي ضرورة الوقوف على البيانات الأساسية للمبحوثين كالجنس، والعمر، والمستوى التعليمي، ومستوى الوعي بالأمن السيبراني، فإن المنهج الوصفي التحليلي يفرض ذاته لإتمام عمليات التحليل من اجل الحصول على نتائج صحيحة تقود إلى الخروج بتوصيات منطقية وفق أهداف الدراسة[*]، وهو ما فرض أيضاً تعيين إطار المعاينة (مجتمع البحث وعينته) والأدوات المستخدمة.

تاسعاً: مجتمع الدراسة

تم تطبيق الدراسة على مجتمع يتمثل في إحدى مؤسسات القطاع الحكومي بعد أن تم الحصول على إذن رسمي من قبل صاحب الصلاحية في تلك المؤسسة لإجراء الدراسة البحثية. وحيث أن أهدف الدراسة الحالية لا تقتضي تقييم درجة الوعي بالأمن السيبراني في تلك المؤسسة، ولا بتقييم وسائل التحقق الرقمي من الهوية الموجودة فيها بأي حال من الأحوال، إضافة إلى أن الدراسة البحثية الحالية ركزت على منسوبي تلك المؤسسة كمفردات مستقلة دون الربط بينها وبين المؤسسة التي يعملون بها؛ عليه فقد ارتأى الباحث عدم ذكر إسم تلك المؤسسة مراعاةً لخصوصيتها وضمان عدم المساس بشخصيتها الإعتبارية بصرف النظر عن النتائج التي سيتم عرضها لاحقا، وكذلكً لإنعدام العلاقة بينها و بين أهداف الدراسة بشكل قطعي. وإذا كان عدم ذكر إسم المؤسسة التي تمثل مجتمع الدراسة مبرراً بما لا يتنافى مع أسس ومنطلقات البحث العلمي، إلا أنه من الأهمية بمكان استعراض المعلومات الأساسية التي تقتضي مبادئ واصول البحث العلمي عرضها وبيانها في أتون الدراسة.

وبناءً على ما سبق تبريره اعلاه، فيبلغ عدد منسوبي تلك المؤسسة (١٥٥٢) موظف بحسب وقائع تقرير وزارة الخدمة المدنية للعام المالي ١٤٣٧هـ/١٤٣٨ هـ (وزارة الخدمة المدنية بالمملكة العربية السعودية، ٢٠١٧). ويمكن وصف موظفي تلك المؤسسة على أنهم موظفون (رجالاً ونساءً) مثبتون على عدد من سلالم الموظفين التابعة لكلٍ من نظام الخدمة المدنية والمؤسسة العامة للتأمينات الاجتماعية.

عاشراً: عينة الدراسة

تمثل عينة الدراسة مجموعة من المبحوثين ضمن مجتمع الدراسة المتمثل في منسوبي المؤسسة الحكومية، وقد تم اختيارهم بشكل عشوائي بعد تحديد حجمهم وفق معادلة كوكرن الأساسية (Cochran, 1977; Israel, 1992) التي تنص على الآتي:

$$n_0 = \frac{Z^2\, pq}{e^2}$$

حيث Z تمثل مستوى الثقة عند (٩٥ %) وتساوي (١,٩٦) ، و p تمثل القيمة القصوى المقدرة للنسبة الحقيقية من مجتمع الدراسة وتساوي (٠,٥) ، و q تمثل حاصل طرح p من واحد (١) وتساوي (٠,٥)، وأخيراً e تمثل حد الخطأ المسموح به وتساوي (٠,٠٥). وبذلك يكون حجم عينة الدراسة المفترض n_0 هو (٣٨٥) مفردة.

هذا وقد تم التجاوب مع أداة الدراسة من قبل (٣٩٦) مفردة من اجمالي إطار المعاينة، كان منها صحيحاً وتاماً (٣٨٩) مفردة تلك التي تم خضوعها للتفريغ والتحليل والتعليق على جداولها وهي أكبر من الحجم المفترض لعينة الدراسة المحدد وفق معادلة كوكرن.

إحدى عشر: أداة الدراسة

الأداة المستخدمة في الدراسة هي استبانة إلكترونية تم إرسالها إلى عينة الدراسة. وتألفت الاستبانة الإلكترونية من ثلاثة محاور: المحور الأول يعنى بالحصول على المعلومات العامة (الجنس، الفئة العمرية، المستوى التعليمي، المستوى الوظيفي، ومستوى الوعي بالأمن السيبراني)، والمحور الثاني معني بجمع معلومات تتعلق بتعامل العنصر البشري مع وسائل التحقق من الهوية الرقمية، والمحور الثالث يتم من خلاله الحصول على معلومات ذات علاقة بمستوى الوعي بالأمن السيبراني. وقد تم اعتماد مقياس ليكرت الخماسي للإجابة على فقرات الإستبانة وفق اطوال الخلايا التي تم تحديدها بواسطة حساب مدى المقياس وذلك بطرح أصغر قيم المقياس من اكبرها (٥-١=٤)، وبعد ذلك تم تقسيم الناتج على عدد الخيارات (٥/٤=٠,٨) وهي ٥ خيارات كالتالي: دائماً، أحياناً، محايد، نادراً، لا إطلاقاً. مع الإشارة إلى أن بعض فقرات الإستبانة قد صيغت بنمط سلبي، حيث أن الخيار لا إطلاقاً يساوي (٥)، نادراً يساوي (٤)، محايد يساوي (٣)، أحياناً يساوي (٢)، دائماً يساوي (١). وبناءً على ذلك، فإن طول الخيارات التي تمثل الخلايا يكون كما هو مبين في الجدول ١:

جدول ١: حساب طول الخيارات مقياس ليكرت الخماسي للدراسة

م	الخيار	طول الفترة	مستوى القيمة
١	دائماً	من ١ إلى ١,٧٩	منخفض جداً
٢	أحياناً	من ١,٨٠ إلى ٢,٥٩	منخفض
٣	محايد	من ٢,٦٠ إلى ٣,٣٩	متوسط
٤	نادراً	من ٣,٤٠ إلى ٤,١٩	مرتفع
٥	لا إطلاقاً	من ٤,٢٠ إلى ٥,٠٠	مرتفع جدا

[*] تم التركيز على بعض التصرفات السلوكية ذات العلاقة بوسائل التحقق الرقمي من الهوية التي تم تحديدها ودراستها من قبل باحثو وخبراء الأمن السيبراني وفقاً للمصادر التالية (Department of Homeland Security, 2013; Kelley 2018; and Hausawi, 2016)

وقد تم إجراء الإختبارات القياسية لقياس صدق أداة الدراسة وثباتها كما يلي:

١. إختبارات صدق وثبات أداة الدراسة

إن إختبار صدق أداة الدراسة وثباتها يعتبران من الخطوات الضرورية ذات الفائدة الملحوظة تقود إلى قوة وكفاءة الأداة (Gliem and Gliem, 2003)، وتعد مؤشراً لإستيفائها للمعايير القياسية التي يتطلب تحققها في أداة الدراسة حتى يمكن تحقيق الغرض من استخدامها المتمثل الحصول على بيانات ذات جودة ونوعية قابلة للتحليل والدراسة من أجل الخروج بنتائج جيدة تساعد في وضع توصيات منطقية مفيدة وقابلة للتطبيق. وعليه، فقد تمت الاستعانة بمجموعة من الأكاديميين ذوي الخبرة في تحكيم الإستبانة وعددهم (٣) أبدو بعض الملاحظات التي يتراوح مستواها بين الجوهري والسطحي، وقد تم الأخذ بجميعها وتحسين أداة الدراسة وفقاً لأولويتها واهميتها.

أما فيما يتعلق بثبات أداة الدراسة والصدق الذاتي لأجزائها، فقد تم الإعتماد على إختبارَي معامل الثبات كرونباخ الفا (Cronbach's Alpha) ومعامل الصدق الذاتي باعتباره الجذر التربيعي لمعامل الثبات مع الأخذ في الإعتبار ضرورة أن تكون قيم المعاملات تساوي أو أكبر من (٠,٦٠) وفقاً للحد الأدنى الموصى به إحصائياً (Sekaran and Bougie, 2006). وجميع نتائج اختبار الثبات التي أجريت على عينة أولية تتكون من (٢٥) مفردة بينت مدى قوة وترابط أجزاء الإستبانة، حيث تراوحت قيم معامل كرونباخ الفا بين (٠,٦٤٩) و (٠,٧٠٤)، وكذلك قيم معامل الصدق الذاتي تراوحت بين (٠,٨٠٦) و (٠,٨٣٩) كما يظهر في الجدول ٢:

جدول ٢: قيم معاملات الثبات

المحور	كود العبارة	العبارات	معامل الفا كرونباخ	معامل الصدق الذاتي
وسائل التحقق الرقمي من الهوية	١	لا اعطي معلومات الدخول الخاصة بي ككلمات المرور لشخص آخر بهدف تسهيل العمل	٠,٦٥٧	٠,٨١١
	٢	لا اترك الحساب أو النظام مفتوحاً بدون تسجيل خروج عند المغادرة حتى في حال الرغبة للعودة إليه مرة أخرى	٠,٦٦٤	٠,٨١٥
	٣	لا أعتمد على استخدام خاصية التذكر التلقائي الموجودة في المتصفحات لتجاوز مرحلة التحقق من معلومات الدخول	٠,٦٥٥	٠,٨٠٩
	٤	لا اقوم باستخدام لوحة المفاتيح لإدخال معلومات الدخول الخاصة بي أمام الآخرين	٠,٦٤٩	٠,٨٠٦
	٥	لا اكرر استخدام المعرفات الخاصة بي (كلمات المرور على سبيل المثال) في أكثر من موقع وحساب إلكتروني	٠,٦٥٥	٠,٨٠٩
	٦	أقوم بتغيير معلومات التحقق من الهوية الخاصة بي من فترة إلى اخرى	٠,٦٦٤	٠,٨١٥
	٧	في اعتقادي أنه لا يوجد شخص جدير بالثقة في معرفة معلومات الدخول الخاصة بي	٠,٦٥٠	٠,٨٠٦
	٨	لا أقوم بكتابة أو تدوين معلومات الدخول الخاصة بي في مكان ما حتى لو كان ذلك يسهل استخدامها وتذكرها	٠,٦٧٣	٠,٨٢٠
الإهتمام بالأمن السيبراني	٩	اهتم بتطوير مهاراتي وزيادة معارفي بالآليات المناسبة لتحقيق الأمن السيبراني وطرق الوقاية من المشاكل السيبرانية	٠,٦٧٣	٠,٨٢٠
	١٠	أقوم بإعطاء أقل قدر ممكن من الصلاحيات للآخرين (بما يساعد على إنجاز المهام فقط)	٠,٧٠٤	٠,٨٣٩
	١١	أقوم بمراجعة الصلاحيات الافتراضية التي تكون معدة مسبقاً في الأجهزة وأقنعها بما يتناسب مع الحاجة الفعلية للتعامل معها	٠,٦٧٥	٠,٨٢٢
	١٢	لا اعتمد على الصلاحيات الافتراضية التي تكون معدة مسبقاً في البرمجيات والتطبيقات فهي قد لا تتناسب مع الحاجة الفعلية للتعامل معها	٠,٦٨٨	٠,٨٢٩
	١٣	أقوم بإخفاء محتويات شاشة الجهاز الذي اعمل عليه عند مغادرتي للمكان وذلك بإقفالها	٠,٦٧٨	٠,٨٢٣
	١٤	لا أقوم بإرسال بعض الوثائق والملفات إلى عناوين بريد إلكتروني غير البريد الذي اريد الإرسال له عن طريق الخطأ	٠,٦٧١	٠,٨١٩
	١٥	لا أقوم بطباعة بعض الوثائق على طابعات غير التي اريد الطباعة عليها عن طريق الخطأ	٠,٦٦٢	٠,٨١٤
	١٦	لا أقوم باختيار أسئلة تذكر سهلة بهدف تبسيط استرجاع معرفات الدخول (كلمة المرور مثلاً) عند نسيانها	٠,٦٦٧	٠,٨١٧
	١٧	لا أقوم بالدخول على حساباتي وحسابات العمل عن طريق الشبكات العامة بحجة إنجاز الأعمال في وقتها وضمان عدم التأخر في إنجازها	٠,٦٥٦	٠,٨١٠
	١٨	لا استخدم أدوات التخزين المتنقلة (كالفلاش) لحفظ الوثائق المهمة بها بحجة أنها سهلة الحمل والإستخدام	٠,٦٧٢	٠,٨٢٠
	١٩	امتثل للسياسات الأمنية وآخذها على محمل الجد وأسعى لتطبيق بنودها	٠,٦٧٣	٠,٨٢٠
	٢٠	أقوم بالتواصل مع مسئولي أمن المعلومات فوراً في حال وجود حدث يستدعي ذلك	٠,٦٧٣	٠,٨٢٠
	٢١	أقوم بالتخلص من رسائل البريد الإلكتروني مجهولة المصدر دون فتحها	٠,٦٧١	٠,٨١٩
	٢٢	لا أقوم بتجريب بعض الأنظمة والتطبيقات الرقمية للوقوف على ايجابياتها وسلبياتها من باب حب الاستطلاع	٠,٧٠٣	٠,٨٣٨

وبعد أن تم اختبار صدق وثبات أداة الدراسة من قبل المحكمين وقيم معاملات كرونباخ الفا والصدق الذاتي تم نشرها على العينة المستهدفة وفقاً للأسس العلمية المتبعة في نشر الاستبانات.

٢. المعالجة الإحصائية لبيانات الدراسة

وفقاً للاستجابات التي تم الحصول عليها من افراد عينة الدراسة البالغ عددهم (٣٨٩) فرداً، فإن البيانات الوصفية للمستجيبين تنوعت بحسب البيانات العامة المدرجة في الاستبانة والمتمثلة في الجنس، والفئة العمرية، والمستوى التعليمي، ومستوى الوعي بالامن السيبراني. والجداول من (٣) إلى (٦) توضح التفاصيل الوصفية العامة كما يلي:

جدول ٣ :توزيع عينة الدراسة بحسب نوع الجنس

الجنس	العدد	النسبة المئوية
ذكر	٣١٦	% ٨١,٣
انثى	٧٣	% ١٨,٧
المجموع	٣٨٩	% ١٠٠

فالجدول (٣) يبين أن نسبة الذكور في عينة الدراسة بلغت (٨١,٣ %) في حين أن نسبة الإناث في نفس العينة قد بلغت (١٨,٧ %). وهذ التمثيل النوعي في الجنس لعينة الدراسة يتماشى مع الفروق النسبية بين الرجال والنساء لموظفي القطاع العام العاملين وفق سلم الموظفين العام التابع لوزارة الخدمة المدنية بالمملكة العربية السعودية إلى حدٍ ما، حيث أن عدد الموظفين من الرجال يزيد عن ثلثي الموظفين من النساء تقريباً (وزارة الخدمة المدنية بالمملكة العربية السعودية، ٢٠١٦).

جدول ٤: توزيع عينة الدراسة بحسب الفئة العمرية

الفئة العمرية	العدد	النسبة المئوية
٢١ – ٤٠ سنة	٢٣٤	% ٦٠,٣
٤١ – ٦٠ سنة	١٥٣	% ٣٩,٣
أكبر من ٦٠ سنة	٢	% ٠,٤
المجموع	٣٨٩	% ١٠٠

وبالنظر إلى الجدول (٤) نجده يوضح توزيع المستجيبين من عينة الدراسة، حيث أن نسبة المستجيبين الذين أعمارهم تقع بين (٢١ – ٤٠ سنة) بلغت (٦٠,٣ %)، ونسبة الذين أعمارهم تقع بين (٤١ – ٦٠ سنة) بلغت (٣٩,٣ %)، في حين أن هناك شخص واحد فقط يفوق عمره (٦٠ سنة) ضمن المستجيبين وبنسبة (٠,٤ %). وهذه النسب أيضاً تتوافق إلى حد ما مع بيانات وزارة الخدمة المدنية التي تتناول التوزيع النسبي للفئات العمرية لموظفي القطاع العام (وزارة الخدمة المدنية بالمملكة العربية السعودية، ٢٠١٦).

جدول ٥: توزيع عينة الدراسة بحسب المستوى التعليمي

المستوى التعليمي	العدد	النسبة المئوية
بكالوريوس	١٠٨	٪٢٧,٨٣
دبلوم فوق الجامعي	٣٢	٪٨,٢٥
ماجستير	١٩٣	٪٤٩,٦٣
دكتوراه	٥٦	٪١٤,٢٩
المجموع	٣٨٩	% ١٠٠

ومن خلال الجدول (٥) يتبين توزيع المستوى التعليمي للمستجيبين من افراد العينة، حيث كانت النسبة الأكبر من حملة الماجستير والبالغة (٤٩,٦٣ %)، ومن ثم تلتها شريحة حملة البكالوريوس بنسبة (٢٧,٨٣ %)، وباقي النسب المئوية توزعت بين المستويات التعليمية الأخرى. وتجدر الإشارة إلى أن نسبة حملة شهادتي البكالوريوس والماجستير تتوافق مع الترتيب النسبي للمستويات التعليمية لموظفي القطاع العام حيث كانتا النسبتين الأعلى على التوالي (وزارة الخدمة المدنية بالمملكة العربية السعودية، ٢٠١٦).

جدول ٦: توزيع عينة الدراسة بحسب مستوى الوعي بالأمن السيبراني

مستوى الوعي	العدد	النسبة المئوية
منخفض	١١٣	٪٢٩,٠٥
متوسط	١٧٨	٪٤٥,٧٦
مرتفع	٩٨	٪٢٥,١٩
المجموع	٣٨٩	% ١٠٠

أما الجدول (٦) الذي يوضح توزيع المستجيبين بحسب مستوى الوعي لديهم بالأمن السيبراني، ومن خلال ما تم الحصول عليه يتضح أن من هم في المستوى المنخفض من الوعي بلغت نسبتهم (٢٩,٠٥٪)، ومن هم في المستوى المتوسط (٤٥,٧٦٪) ومن هم في المستوى المرتفع من الوعي بلغت نسبتهم (٢٥,١٩٪)، وهنا تجدر الإشارة إلى أنه تم قياس مستوى الوعي لدى المستجيبين من خلال إجابتهم على أسئلة المحور الثاني "الإهتمام بالأمن السيبراني" وتقييمها وفق الجدول (١).

أما ما يتعلق بالمتغير المستقل: الوعي بالأمن السيبراني بمستوياته الثلاثة (منخفض، متوسط، مرتفع)، والمتغيرات التابعة: مستوى التعامل مع وسائل التحقق الرقمي من الهوية، ومستوى الاهتمام بالأمن السيبراني؛ فإن تحليل البيانات وفقاً للمنهج التحليلي يعتبر مناسباً. ويعتبر التحليل الإحصائي للبيانات المعملية (Parametric) مناسب لطبيعة الدراسة والبيانات التي تم تجميعها، حيث أنه توجد إفتراضات مسبقة على مجتمع الدراسة حول طبيعة دور الوعي بالأمن السيبراني في الحد من انعكاسات وسائل التحقق الرقمي من الهوية على المستخدمين. إضافة إلى كون البيانات التي تم تجميعها من عينة الدراسة تتسم بالتوزيع الطبيعي في مجملها. وعليه، فقد تم الإعتماد على تحليل التباين الأحادي، ومن ثم تمت مقارنة المتوسطات وفقاً لردود المستجيبين، والتقرير حول صحة قبول الفرضيات أو عدم صحة ذلك . وقد تم التحليل بواسطة استخدام برنامج الحزم الإحصائية الاجتماعية (SPSS).

٣. تحليل التباين الأحادي (One Way ANOVA)

يستخدم تحليل التباين الأحادي كإحدى إختبارات التحليل الإحصائي في لبيانات المعلملية للمقارنة بين ثلاثة مجموعات أو أكثر وفقاً لمتوسطاتها وإنحرافاتها المعيارية. وبإستخدام برنامج الحزم الإحصائية الاجتماعية (SPSS) تم إجراء الإختبار على المستجيبين من المستويات الثلاثة للمتغير المستقل الوعي بالأمن السيبراني (منخفض، متوسط، مرتفع). وقد كانت نتيجة التحليل الإحصائي كما هو مبين في الجدول ٧:

جدول ٧: نتيجة تحليل التباين الأحادي على عينة الدراسة

		مجموع مربعات الإنحراف	درجة الحرية	متوسط المربعات	ف	مستوى المعنوية
وسائل التحقق الرقمي من الهوية	بين المجموعات	٢٣,٤٠٧	٢	١١,٧٠٤	٢٣,٧٣٧	٠,٠٠٠
	داخل المجموعات	١٢٧,٧٠٢	٣٨٦	٠,٤٩٣		
	المجموع	١٥١,١١٠	٣٨٨			
الوعي بالأمن السيبراني	بين المجموعات	٣٨,٨٢٦	٢	١٩,٤١٣	٥١٥,٥١٩	٠,٠٠٠
	داخل المجموعات	٩,٧٥٣	٣٨٦	٠,٠٣٨		
	المجموع	٤٨,٥٧٩	٣٨٨			

ومن خلال الجدول رقم ٧ الذي يوضح نتيجة تحليل التباين الأحادي يمكن رفض فرضية العدم التي تنص على أنه "لا يوجد دور لبرامج التوعية بالأمن السيبراني في تحسين تعامل المستخدمين مع وسائل التحقق الرقمي من الهوية"، حيث أن قيم ف الناتجة عن المتغيرات التابعة هي أعلى من القيم المفترضة

لقبول فرضية العدم عند مستوى معنوية ٠,٠٠٠. وعليه، يمكن قبول الفرضية البديلة والمقارنة بين متوسطات إجابات المجموعات الثلاثة التي تمثل مستويات المتغير المستقل كما سيأتي في القسم التالي.

٤. إستخدام متوسطات الإجابات على عبارات المحاور

فيما يتعلق بالمحور الأول والمتمثل في وسائل التحقق الرقمي من الهوية، فإن تحليل الإستجابات التي تم الحصول عليها وفقاً لبرنامج الحزم الإحصائية الاجتماعية (SPSS) كما هو مبين في جدول (8) حيث يظهر القيم المتوسطة للفقرات وانحرافها المعياري، إضافة إلى المتوسط العام للمحور في كل مجموعة والمتوسط العام لكل فقرة. وقد أظهرت نتائج التقييم بأن المبحوثين في جميع المجموعات الثلاثة كانت القيم المتوسطة الأعلى لهم للفقرة الثانية التي تفيد بأنهم لا يتركون الحسابات أو الأنظمة مفتوحةً بدون تسجيل خروج عند المغادرة حتى في حال الرغبة للعودة إليها مرة أخرى ، فقد كانت النتيجة العامة لتقييم العبارة على مستوى المجموعات الثلاثة هي "مرتفع جداً" وبمتوسط إجابات عام (٤,٢٧) وإنحراف معياري (١,١٣٨). وبالمقابل فقد أظهرت نتائج التقييم بأن المبحوثين في جميع المجموعات الثلاثة كانت القيم المتوسطة الأدنى لهم للفقرة الخامسة التي تفيد بأنهم يكررون استخدام المعرفات الخاصة بهم (كلمات المرور على سبيل المثال) في أكثر من موقع وحساب إلكتروني. وهذا يدل على أنه وبالرغم من اختلاف مستويات التوعية، إلا أن هذا التصرف الذي لا يتوافق مع السياسات الأمنية يمارس من قبل مختلف المستخدمين بصرف النظر عن مستوى وعيهم الأمني. وقد كانت نتيجة التقييم العام للعبارة على مستوى المجموعات الثلاثة هي "منخفض"" وبمتوسط إجابات عام (٢,٣١) وإنحراف معياري (١,٣٤١). أما باقي الفقرات فقد تراوحت نتائج تقييمها العام بين "متوسط" و "مرتفع" بقيم متوسطة تتراوح بين (٣,٠٨) و (٣,٩٨)، ومتوسط إنحرافات معيارية تتراوح بين (١,٣٨٣) و (١,٢٧٦).

وبشكل مجمل، فإنه قد لوحظ وجود علاقة طردية بين متوسطات الفقرات ومستويات الوعي بين المجموعات، وهذا يعني بأنه كلما زاد مستوى الوعي يلاحظ ارتفاع القيمة المتوسطة للفقرة. وهذه النتيجة تتضح بجلاء من خلال المتوسطات العامة للمجموعات على كامل المحور (٣,٠٧، ٣,٤١، ٣,٨٠) لمجموعات مستوى الوعي المنخفض، والمتوسط، والمرتفع على التوالي.

جدول ٨: تقييم عبارات محور وسائل التحقق الرقمي من الهوية

المحور	كود العبارات (وفق الجدول ٢)	المجموعة الأولى (وعي منخفض)		المجموعة الثانية (وعي متوسط)		المجموعة الثالثة (وعي مرتفع)		متوسطات الفقرات	
		المتوسط	الإنحراف المعياري	المتوسط	الإنحراف المعياري	المتوسط	الإنحراف المعياري	المتوسط	الإنحراف المعياري
وسائل التحقق الرقمي من الهوية	١	٣,٦١	١,٣٥٠	٤,٠٦	١,٢٧٩	٤,٢٥	١,١١٧	٣,٩٧	١,٢٧٦
	٢	٣٤,١	١,٢٣٤	٥٤,١	١,٢٢٨	٤,٥٥	.,٨٨٣	٤,٢٧	١,١٣٨
	٣	٢,٦٧	١,٥٢٢	٣,٠٧	١,٤٦٩	٣,٦٧	١,٥٢٢	٣,١٤	١,٥٥٥
	٤	٢,٨٦	١,٤٢٤	٣,٦٤	١,٣٧٢	٣,٩٨	١,٢١٣	٣,٥٠	١,٤١٤
	٥	٢,٠٦	١,٣٠٦	٢,١٤	١,٣٢٢	٢,٧٢	١,٣١٣	٢,٣١	١,٣٤١
	٦	٢,٦١	١,٣٨٤	٣,٢٠	١,٣٥٤	٣,٤٣	١,٢٩٤	٣,٠٨	١,٣٨٣
	٧	٣,٢٨	١,٤٠٣	٣,٨٤	١,٢٨٤	٤,٠٨	١,١٤٧	٣,٧٣	١,٣٢١
	٨	٣,٣١	١,٥٦٥	٣,٢٣	١,٥٩٧	٣,٧٢	١,٥٥٣	٣,٤٢	١,٥٨٠
	متوسطات المجموعات	٣,٠٧	١,٣٩٩	٣,٤١	١,٣٦٣	٣,٨٠	١,٢٥٥	٣,٤٣	١,٣٧٦

أما فيما يتعلق بالمحور الثاني المتمثل في الاهتمام بالأمن السيبراني، فإن تحليل الإستجابات التي تم الحصول عليها وفقاً لبرنامج الحزم الإحصائية الاجتماعية (SPSS) كما هو مبين في جدول (٩) حيث يظهر القيم المتوسطة للفقرات وانحرافها المعياري، إضافة إلى المتوسط العام للمحور في كل مجموعة والمتوسط العام لكل فقرة. وقد أظهرت نتائج التقييم بأن المبحوثين في جميع المجموعات الثلاثة كانت القيم المتوسطة الأعلى لهم للفقرة التاسعة عشر التي تفيد بأنهم يمتثلون للسياسات الأمنية ويأخذونها على محمل الجد ويسعون لتطبيق بنودها، فقد كانت النتيجة العامة لتقييم العبارة على مستوى المجموعات الثلاثة هي "مرتفع جداً" وبمتوسط إجابات عام (٤,٦٤) وإنحراف معياري (٠,٨١٧). وبالمقابل فقد أظهرت نتائج التقييم بأن المبحوثين في جميع المجموعات الثلاثة كانت القيم المتوسطة الأدنى لهم للفقرة الثانية عشر التي تفيد بأنهم يعتمدون على الصلاحيات الافتراضية التي تكون معدة مسبقاً في البرمجيات والتطبيقات بالرغم من انها قد لا تتناسب مع الحاجة الفعلية للتعامل معها. وهذا يدل على أنه وبالرغم من اختلاف مستويات التوعية، إلا أن هذا التصرف الذي لا يتوافق مع السياسات الأمنية يمارس من قبل مختلف المستخدمين بصرف النظر عن مستوى وعيهم الأمني. وقد كانت نتيجة التقييم العام للعبارة على مستوى المجموعات الثلاثة هي "منخفض"" وبمتوسط إجابات عام (٢,٠١) وإنحراف معياري (١,١٦٣). أما باقي الفقرات فقد تراوحت نتائج تقييمها العام بين "منخفض" و "مرتفع جداً" بقيم متوسطة تتراوح بين (٢,٣١) و (٤,٥٦)، ومتوسط إنحرافات معيارية تتراوح بين (١,٤٤٧) و (٠,٩٦٨).

وكما لوحظ في المحور الأول، فإنه قد لوحظ وجود علاقة طردية بين متوسطات الفقرات ومستويات الوعي بين المجموعات في هذا المحور أيضاً، وهذا يعني بأنه كلما زاد مستوى الوعي يلاحظ ارتفاع القيمة المتوسطة للفقرة. وهذه النتيجة تتضح بجلاء من خلال المتوسطات العامة للمجموعات على كامل المحور (٣,١٣، ٣,٥٩، ٤,٠٧) لمجموعات مستوى الوعي المنخفض، والمتوسط، والمرتفع على التوالي.

جدول ٩: تقييم عبارات محور رسائل التحذير الأمني

المحور	كود العبارات (وفق الجدول ٢)	المجموعة الأولى (وعي منخفض)		المجموعة الثانية (وعي متوسط)		المجموعة الثالثة (وعي مرتفع)		متوسطات الفقرات	
		المتوسط	الإنحراف المعياري	المتوسط	الإنحراف المعياري	المتوسط	الإنحراف المعياري	المتوسط	الإنحراف المعياري
الإهتمام بالأمن السيبراني	٩	٣,٢٣	١,٥٠٠	٣,٧١	١,١٦٠	٤,١٦	١,٠٨٢	٣,٧٠	١,٣١١
	١٠	٣,٢٥	١,٣٦٦	٣,٦٨	١,٣٥١	٣,٨٢	١,٣٠٠	٣,٥٨	١,٣٥٦
	١١	٣,٠٩	١,٣٦١	٣,٩٠	١,٢٢٠	٤,٢٤	.,٩٩٤	٣,٧٤	١,٢٨٩
	١٢	١,٩٣	١,١٠٨	١,٩٤	١,١٩٥	٢,١٦	١,١٨٣	٢,٠١	١,١٦٣
	١٣	٣,٩٠	١,٣٥٦	٤,٢٨	١,٢٦٤	٤,٥٧	١,٠١٥	٤,٢٥	١,٢٤٥
	١٤	٣,٧١	١,٣٨٠	٤,٤١	.,٨٨٣	٤,٨٣	.,٣٧٨	٤,٣٢	١,٠٧٠
	١٥	٣,٦٩	١,٢٦٠	٤,٣٧	.,٩٩٠	٤,٧٥	.,٦١١	٤,٢٧	١,٠٧٩
	١٦	١,٨٠	١,١٧٠	٢,٠١	١,٢٠٦	٣,١١	١,٥٧٩	٢,٣١	١,٤٤٧
	١٧	٢,٠٣	١,٢١٥	٢,٨٧	١,٥٣٩	٤,٠٥	١,٢٤٩	٢,٩٩	١,٥٧٢
	١٨	٢,٠٦	١,٢٥٢	٢,٤٧	١,٣١٠	٣,٤٥	١,٥٦٨	٢,٦٦	١,٤٩٩
	١٩	٤,٣٠	١,٠١٣	٤,٧٤	.,٥٥٤	٤,٨٩	.,٤٩٠	٤,٦٤	.,٨١٧
	٢٠	٣,٨٠	١,٣٠٢	٣,٩٧	١,٢٩٨	٤,٧٥	.,٧٣١	٤,١٨	١,٢١٠
	٢١	٤,٠١	١,٣٦٨	٤,٧٥	.,٥٩٥	٤,٩١	.,٣٩١	٤,٥٦	.,٩٦٨
	٢٢	٢,٩٧	١,٢٥٢	٣,١٧	١,٤٠٨	٣,٢٨	١,٥٠١	٣,١٤	١,٣٩٢
	متوسطات المجموعات	٣,١٣	١,٢٧٩	٣,٥٩	١,١٥٥	٤,٠٧	١,٠٠٥	٣,٦٠	١,٢٤٤

وبشكل عام، تأتي نتيجة تقييم المحورين كنتيجة لحساب متوسطات الأوساط الحسابية، والإنحرافات المعيارية لفقرات كل محور لكل مجموعة. وقد أظهرت النتائج كلا المحورين كانت نتيجة تقييمهما "مرتفع" وبمتوسطات حسابية (٣,٤٣) و(٣,٦٠)، وإنحرافات معيارية (١,٣٧٦) و(١,٢٤٤)، ونسب

ممارسة إيجابية تراوحت بين (٦٨,٥٥ %) و(٧١,٩٥٪) وهذا يظهر في الجدول (١٠) كما يلي:

جدول ١٠: تقييم المحاوروفق متوسطات الإجابات على عبارات المحاور

المتغير الوسيط (المحور)	المتوسط الحسابي	الإنحراف المعياري	النسبة	التقييم
وسائل التحقق الرقمي من الهوية	٣,٤٣	١,٣٧٦	% ٦٨,٥٥	مرتفع
الإهتمام بالأمن السيبراني	٣,٦٠	١,٢٤٤	٧١,٩٥٪	مرتفع

ثاني عشر: نتائج الدراسة

في ضوء ما استفسرت عنه الدراسة الميدانية، والموجهات النظرية للبحث، فإن ثمة نتائج رئيسية أفرزتها الدراسة الراهنة لعل من أهمها:

١. فيما يتعلق بالسؤال الفرعي الأول (ما مستوى الوعي بالأمن السيبراني لدى المستخدمين بشكل عام؟)، فإن النتائج المرتبطة به تكشف بأنه ومن خلال تحليل محوري الدراسة بعباراتهما الاثنتان والعشرون وجد أن المستوى العام للوعي بالأمن السيبراني يعتبر مرتفعاً بمتوسط (٣,٥٢) من أصل (٥) ونسبة ممارسة إيجابية (٧٠,٢٥٪). حيث كانت نسبة الوعي في المحور الأول (٦٨,٥٥٪)، وفي المحور الثاني (٧١,٩٥٪).

٢. أما فيما يتعلق بالسؤال الفرعي الثاني (ما طبيعة السلوك الصادر من المستخدمين تجاه وسائل التحقق الرقمي من الهوية؟) فإن النتائج المرتبطة به تفيد بأن: هناك بعض التصرفات (إيجابية أو سلبية) التي تشرك جميع المجموعات الثلاثة في مستوى ممارستها بالرغم من اختلاف مستويات الوعي بين تلك المجموعات. وهذه النتيجة قد تقود إلى استنتاج هام وهو أن المستخدم قد يكون مجبراً على تلك التصرفات بصرف النظر عن مستوى الوعي لديه. الأمر الذي قد يلقي بالكرة في ملعب مختصي الأمن السيبراني ويحتم ضرورة مراجعة الأساليب المعمول بها في الوقت الراهن في حال كانت تلك التصرفات سلبية. إلا أنه وبشكل عام فقد لوحظ وجود علاقة طردية بين التصرفات السلوكية الصادرة من المستخدمين تجاه وسائل التحقق الرقمي من الهوية.

٣. من خلال الإستجابات التي تم الحصول عليها من المبحوثين وما نتج عن تحليل التباين الأحادي الذي نتج عنه رفض فرضية العدم وقبول الفرضية البديلة، إضافة على نتائج حساب المتوسطات والإجابة على الأسئلة الفرعية للدراسة: فإنه يمكن الإستنتاج بأن هناك علاقة طردية واضحة بين برامج التوعية بالأمن السيبراني وتعامل المستخدمين مع وسائل التحقق الرقمي من الهوية وفقاً للأطر والأساليب العلمية والأسانيد المرجعية التي تم تبنيها والعمل بمقتضياتها للوصول إلى النتيجة النهائية للدراسة.

ثالث عشر: الخلاصة والتوصيات

في ضوء ما تمخضت عنه الدراسة الحالية وسابقتها من نتائج، فإن الباحث يمكنه وضع مجموعة من التوصيات التي يمكن تفعيلها بغرض تحسين وتطوير دور برامج التوعية بالأمن السيبراني من أجل تحسين التفاعل مع وسائل التحقق الرقمي من الهوية. ويمكن إجمال تلك التوصيات فيما يلي:

١. يجب أن يكون المستخدم الطرفي (المستفيد النهائي) هو المرتكز الأساسي لعملية تطوير وسائل التحقق الرقمي من الهوية لضمان الحصول على الإنسجام والتناغم المرغوب بين المستخدم والأنظمة التي تعتمد على التقنية.

٢. يوصى بمراعاة الفروقات المجتمعية والبيئية والثقافية والخلفيات العلمية والمعرفية عند تصميم وسائل التحقق من الهوية، لما لتلك الفروق من أثر واضح على نجاعة وكفاءة وفاعلية تلك الوسائل.

٣. تعدد خيارات التحقق الرقمي من الهوية في نظام التحقق (على سبيل المثال: كلمات المرور النصية و كلمات المرور الرسومية والسمات الحيوية) يوفر حرية الإختيار للمستخدمين بما يتوافق مع رغبتهم وميولهم الشخصي، وبالتالي ضمان الإستخدام الطوعي لنظام التحقق الرقمي من الهوية.

٤. لرفع درجة إلتزام المستخدمين بإتباع الطرق السليمة والآمنة في التعامل مع أنظمة التحقق الرقمي من الهوية الرقمية، يفترض أن تكون أسس ومنطلقات التفاعل المهذب من أهم المرتكزات التي يتم الإعتماد عليها في تحقيق مبدأ احترام المستخدم في البيئة الرقمية.

٥. يوصى بإتباع برامج توعوية متدرجة تبدأ بإكساب المعرفة، ومن ثم التدريب، ومن ثم التشجيع، وانتهاءً بالمسؤلية والمسائلة (العقاب).

٦. هناك الكثير من أنظمة التحقق الرقمي المعلبة (المتوفرة تجارياً والجاهزة للإستخدام). وعليه، ينبغي التأكد من مدى ملائمة تلك الأنظمة وقابليتها للتطبيق والإستخدام في بيئة العمل المستهدفة قبل اعتمادها وتبني استخدامها.

المراجع ومصادر المعلومات

المراجع العربية:

[١] الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية (٢٠١٨). "تعريف الأمن السيبراني". الحساب الرسمي للهيئة على موقع التواصل الاجتماعي "تويتر. الرابط: https://twitter.com/NCA_KSA/status/1023917241870557184

[٢] رؤية المملكة العربية السعودية ٢٠٣٠م (٢٠١٦). "تقرير رؤية المملكة العربية السعودية ٢٠٣٠"

[٣] وزارة الخدمة المدنية بالمملكة العربية السعودية (٢٠١٧). " تقرير إنجازات وزارة الخدمة المدنية للعام المالي ١٤٣٧ هـ / ١٤٣٨ هـ"

[٤] برنامج التعاملات الإلكترونية الحكومية (يسر) (٢٠١٨). "تقرير مؤشر النضج للخدمات الحكومية". وزارة الاتصالات وتقنية المعلومات.

[٥] هوساوي، ياسر (٢٠١٩). " آليات تحقيق الأمن السيبراني وانعكاساتها على سلوك مستخدمي تقنية المعلومات من موظفي القطاع الحكومي". مؤتمر التنمية الإدارية في ضوء رؤية المملكة ٢٠٣٠. معهد الإدارة العامة.

المراجع الأجنبية:

[6] Bada, M., Sasse, A. M., & Nurse, J. R. (2019). "Cyber security awareness campaigns: Why do they fail to change behavior? ".

[7] Bahr, G. S., & Allen W. H. (2013) "Rational interfaces for effective security software: Polite interaction guidelines for secondary tasks." International Conference on Universal Access in Human-Computer Interaction. Springer, Berlin, Heidelberg.

[8] Gliem, J. A., & Gliem, R. (2003) "Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales." Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.

[9] Hausawi, Y. M. (2016) "Current trend of endusers' behaviors towards security mechanisms." International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer, Cham.

[10] Hausawi, Y. M. (2015) Towards a Usable-Security Engineering Framework for Enhancing Software Development. Diss.

[11] Hausawi, Y. M., Allen, W. H., & Bahr G. S. (2014) "Choice-based authentication: a usable-security approach." International Conference on Universal Access in Human-Computer Interaction. Springer, Cham.

[12] Heartfield, R., & Loukas, G. (2018) "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework." Computers & Security 76: 101127.

[13] Joseph, A. O., Kathrine, J. W., & Vijayan, R. (2014) "Cloud security mechanisms for data protection: a survey." International Journal of Multimedia and Ubiquitous Engineering 9.9: 8190.

[14] Kaur, T., Malhotra, V., & Singh, D. (2014) "Comparison of network security toolsfirewall, intrusion detection system and Honeypot." Int. J. Enhanced Res. Sci. Technol. Eng: 200204.

[15] Kitchin, R. (2014) "The data revolution: Big data, open data, data infrastructures and their consequences". Sage.

[16] Lazar, J., Feng, J. H., & Hochheiser, H. (2017) "Research methods in human computer interaction". Morgan Kaufmann.

[17] Liddell, T. M., & Kruschke, J. K. (2018) "Analyzing ordinal data with metric models: What could possibly go wrong?." Journal of Experimental Social Psychology 79: 328-348.

[18] Mayron, L. M., Hausawi, Y. M., & Bahr, G. S. (2013) "Secure, usable biometric authentication systems." International Conference on Universal Access in Human-Computer Interaction. Springer, Berlin, Heidelberg.

[19] Parker, F., Ophoff, J., Van Belle, J. P., & Karia, R. (2015). Security awareness and adoption of security controls by smartphone users. In 2015 Second international conference on information security and cyber forensics (InfoSec) (pp. 99-104). IEEE.

[20] Pfleeger, S. L., M. Sasse, A., & Furnham, A. (2014) "From weakest link to security hero: Transforming staff security behavior." Journal of Homeland Security and Emergency Management 11.4: 489510.

[21] Raja, K. B., et al. (2015) "Multimodal authentication system for smartphones using face, iris and periocular." Biometrics (ICB), 2015 International Conference on. IEEE.

[22] Rodionova, O. Y., Titova, A. V., & Pomerantsev A. L. (2016) "Discriminant analysis is an inappropriate method of authentication." TrAC Trends in Analytical Chemistry 78: 1722.

[23] Stallings, W. (2017) "Cryptography and network security: principles and practice". Upper Saddle River, NJ: Pearson.

[24] Fisher, L. A., Clark, J. R. A., & Baines, N. E. (2014) "Alert message control of security mechanisms in data processing systems." U.S. Patent No. 8,627,466.

[25] Bano, M., & Zowghi, D. (2015) "A systematic review on the relationship between user involvement and system success." Information and Software Technology 58: 148169.

[26] Cochran, W. G. (1977). Sampling techniques. John Wiley & Sons.

[27] De L., Michael, K.M., & Eds, J. B. (2007) "The history of information security: a comprehensive handbook". Elsevier.

[28] Department of Homeland Security. (n.d.). (2018) Retrieved from: https://www.us-cert.gov/security-publications.

[29] Hadlington, L. (2017) "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors." Heliyon 3.7: e00346.

[30] Herath, T., et al. (2014) "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service." Information systems journal 24.1: 6184.

[31] IBM. Security Concepts and Mechanisms. IBM Knowledge Center, (2018). Retrived from: https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009730_.htm.

[32] Israel, G. D. (1992). Determining sample size.

[33] Jain, A. K., Ross, A. A., & Nandakumar, K. (2011) "Introduction to biometrics". Springer Science & Business Media.

[34] Kelley, D. (2018) "Investigation of Attitudes Towards Security Behaviors." McNair Research Journal SJSU 14.1: 10.

[35] Ng, B. Y., Kankanhalli A., & Xu Y. C. (2009) "Studying users' computer security behavior: A health belief perspective." Decision Support Systems 46.4: 815825.

[36] Safa, N. S., Solms R. V., & Futcher L. (2016) "Human aspects of information security in organisations." Computer Fraud & Security 2016.2: 1518.

[37] SANS. Security Awareness Survey. (2017) SANS Awareness. Retrived from: https://www.sans.org/sites/default/files/201801/securityawarenesssurvey.pdf

[38] Sekaran, U., Bougie R. (2006) "Research Methods of Business A Skill Building Approach." John Wiley and Sonc, Inc.

[39] Sitová, Z., et al. (2016) "HMOG: New behavioral biometric features for continuous authentication of smartphone users." IEEE Transactions on Information Forensics and Security 11.5: 877892.

[40] Smith-Creasey, M., Albalooshi, F., & Rajarajan, M. (2018, August). Context Awareness for Improved Continuous Face Authentication on Mobile Devices. In 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) (pp. 644-652). IEEE.

[41] Stanton, J., et al. (2004) "Behavioral information security: two end user survey studies of motivation and security practices." AMCIS 2004 proceedings: 175.

[42] Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & Security, 88, 101640.

ملحق ١: استبانة دور التوعية بالأمن السيبراني في الحد من الأثر الإنعكاسي لوسائل التحقق الرقمي من الهوية على سلوك المستخدم العادي

الزميل العزيز،

في إطار دراسة وتحليل دور التوعية بالامن السيبراني على تعامل الموظفين مع وسائل التحقق الرقمي من الهوية، فإن الباحث يهدف إلى الوقوف على طبيعة العلاقة الثلاثية التي تربط بين الموظفين والتوعية وتلك الوسائل. وفي ضوء هذه الأهداف، فإن الدراسة تسعى إلى الإجابة على تساؤل رئيس مؤداه:

ما طبيعة العلاقة بين برامج التوعية بالأمن السيبراني وتعامل المستخدمين مع وسائل التحقق الرقمي من الهوية

وحيث انكم ضمن عينة ممثلة لمجتمع الدراسة، فإن الباحث يود منكم المشاركة مشكورين بتعبئة هذه الاستبانة الإلكترونية التي بين أيديكم. وبهذه الفرصة نشكر لكم سلفاً حسن تعاونكم. وفي حال وجود تساؤلات أو استفسارات يرجى التواصل مع الباحث عبر البريد الإلكتروني: Hawsawiy@ipa.edu.sa

ملاحظة:

يرجى تعبئة كامل الإستبانة وذلك بإختيار الخيار المناسب وذكر الدافع لإختيار ذلك الخيار في حال طلب ذلك.

يرجى التنبه إلى أن بعض الفقرات تمت صياغتها سلبياً بحكم طبيعة الدراسة البحثية.

الباحث

القسم الأول (المعلومات الأساسية): يهتم الباحث في هذا القسم بجمع بعض المعلومات المرتبطة بالمشارك وهي: الجنس، والفئة العمرية، والمستوى التعليمي، ومستوى الوعي بالامن السيبراني.

الكود	المتغير	الاختيارات			
١	الجنس	ذكر	أنثى		
٢	الفئة العمرية (بالسنوات)	٢١ - ٤٠	٤١ – ٦٠	> ٦٠	
٣	المستوى التعليمي	بكالوريوس	دبلوم فوق الجامعي	ماجستير	دكتوراه
٤	مستوى الوعي بالأمن السيبراني	منخفض	متوسط	مرتفع	

القسم الثاني (وسائل التحقق الرقمي من الهوية): يركز الباحث في هذا القسم على تجميع البيانات المرتبطة بتعاملهم مع وسائل التحقق الرقمي من الهوية الرقمية كإسم المستخدم وكلمة المرور والرقم السري والسمات الحيوية (بصمة الإصبع مثلاً)

الكود	العبارات	لا إطلاقاً ٥	نادراً ٤	محايد ٣	أحياناً ٢	دائماً ١	ملاحظات
١	اعطي معلومات الدخول الخاصة بي ككلمات المرور لشخص آخر بهدف تسهيل العمل						
٢	اترك الحساب أو النظام مفتوحاً بدون تسجيل خروج عند المغادرة للعودة إليه بدون دخول مرة أخرى						
٣	استخدم خاصية التذكر التلقائي الموجودة في المتصفحات لتجاوز مرحلة التحقق من معلومات الدخول						
٤	اقوم باستخدام لوحة المفاتيح لإدخال معلومات الدخول الخاصة بي أمام الآخرين						
٥	اكرر استخدام المعرفات الخاصة بي (كلمات المرور على سبيل المثال) في أكثر من موقع وحساب إلكتروني						
٦	لا أقوم بتغيير معلومات التحقق من الهوية الخاصة بي من فترة إلى اخرى						
٧	في اعتقادي ان بعض من حولي جديرين بالثقة في معرفة معلومات الدخول الخاصة بي						
٨	أقوم بكتابة أو تدوين معلومات الدخول الخاصة بي في مكان ما ليسهل استخدامها وتذكرها						

القسم الثالث (الإهتمام بالأمن السيبراني): يركز الباحث في هذا القسم على تجميع البيانات المرتبطة بمدى إهتمام المستخدمين بالأمن السيبراني وحرصهم على تحقيقه.

الكود	العبارات	لا إطلاقاً ١	نادراً ٢	محايد ٣	أحياناً ٤	دائماً ٥	ملاحظات
٩	اهتم بتطوير مهاراتي وزيادة معارفي بالآليات المناسبة لتحقيق الأمن السيبراني وطرق الوقاية من المشاكل السيبرانية						
١٠	أقوم بإعطاء أقل قدر ممكن من الصلاحيات للآخرين (بما يساعد على إنجاز المهام فقط)						
١١	أقوم بمراجعة الصلاحيات الافتراضية التي تكون معدة مسبقاً في الأجهزة وأقنعها بما يتناسب مع الحاجة الفعلية للتعامل معها						
١٢	لا اعتمد على الصلاحيات الافتراضية التي تكون معدة مسبقاً في البرمجيات والتطبيقات فهي قد لا تتناسب مع الحاجة الفعلية للتعامل معها						
١٣	أقوم بإخفاء محتويات شاشة الجهاز الذي اعمل عليه عند مغادرتي للمكان وذلك بإقفالها						
١٤	لا أقوم بإرسال بعض الوثائق والملفات إلى عناوين بريد إلكتروني غير البريد الذي اريد الإرسال له عن طريق الخطأ						
١٥	لا أقوم بطباعة بعض الوثائق على طابعات غير التي اريد الطباعة عليها عن طريق الخطأ						
١٦	لا أقوم باختيار أسئلة تذكر سهلة بهدف تبسيط استرجاع معرفات الدخول (كلمة المرور مثلاً) عند نسيانها						
١٧	لا أقوم بالدخول على حساباتي وحسابات العمل عن طريق الشبكات العامة بحجة إنجاز الأعمال في وقتها وضمان عدم التأخر في إنجازها						
١٨	لا استخدم أدوات التخزين المتنقلة (كالفلاش) لحفظ الوثائق المهمة بها بحجة أنها سهلة الحمل والإستخدام						
١٩	امتثل للسياسات الأمنية وآخذها على محمل الجد وأسعى لتطبيق بنودها						
٢٠	أقوم بالتواصل مع مسئولي أمن المعلومات فوراً في حال وجود حدث يستدعي ذلك						
٢١	أقوم بالتخلص من رسائل البريد الإلكتروني مجهولة المصدر دون فتحها						
٢٢	لا أقوم بتجريب بعض الأنظمة والتطبيقات الرقمية للوقوف على ايجابياتها وسلبياتها من باب حب الاستطلاع						