ترجمة وتكيف مقياس الأمن النفسي السيبراني في البيئة العربية: دراسة تقويمية

المستخلص:

هدفت الدراسة إلى ترجمة وتكيف مقياس الأمن النفسي السيبراني في البيئة العربية: دراسة تقويمية، ولعينة مكونة من535 فرداً تنوعت حسب الجنس إلى (87.1%) من الاناث، (12.9%) من الذكور ، وتراوحت أعمارهم في المدى من (15 إلى 60)، وحسب الحالة الاجتماعية (86.4%) متزوج و(13.1%) أعزب، وحسب الجنسية (96%) مصري، (4%) جنسيات عربية أخرى، على حسب الوظيفة (70.3%) يعملوا و(29.7%) لا يعملوا، على حسب عدد الساعات التي يقضوها على الانترنت من 3-4 ساعات (40.2)، من 5-6 ساعات (23%)، ومن7-9ساعات (19.4%)، ومن 10-15ساعة (9.3%)، أما أخري (8%) وكانت اجابتهم (عشر دقائق-ساعة ونصف-أكثر من 15ساعة). اعتمدت الدراسة على تصميم الدراسات المستعرضة من خلال تطبيق القائمة المعدلة للمشكلات النفسية والسلوكية من خلال لينك الكتروني تم إرساله للطلاب، في الفترة من 20/9/2022 الي الفترة من 2/2/2023، وتم استخدام التكرارات ومعامل ارتباط المفردة بالدرجة الكلية، والفا بعد استبعاد المفرة، بينما تم استخدام التحليل العاملي الاستكشافي والتوكيدي، وتم تحليل البيانات باستخدام SPSS(28) و MPLUS(7) ، وفي حالة الاعتماد على معيار معامل الارتباط بين المفردة والدرجة الكلية (يزيد عن 0.50), وكذلك تشبع المفردة بالعامل (يزيد عن 0.63) فأنه يجب استبعاد المفردة الأولي في البعد الأول، والمفردة السابعة في البعد الثاني، وفي البعد الثالث المفردتان الاولي والأخيرة، وهؤلاء المفردات كانت لهم أقل قيم لثبات المقياس بعد استبعادهما بالتالي الصيغة المختصرة تتكون من 28 مفردة. وعند تقدير الثبات اوميجا يتضح أن الفا للنسخة المختصرة للمقياس في ضوء النسخة الأولي كانت قيمة المعامل ألفا= 0.888 ,وقيمة المعامل اوميجا = 0.913.

الكلمات المفتاحية: الأمن النفسي السيبراني- نظرية الاستجابة للمفردة – الهندسة الاجتماعية- الخصوصية الرقمية – السلوكيات على السوشيال ميديا والأداء النفسي على الانترنت.

Translating and adapting the cyber psychological security measure in the Arab environment: an evaluation study

Abstract:

The study aimed to Translating and adapting the cyber psychological security measure in the Arab environment: an evaluation study, and for a sample of 535 individuals that varied according to gender to (87.1%) of females, (12.9%) of males, and their ages ranged from (15 to 60), according to Marital status (86.4%) are married and (13.1%) are single, and by nationality (96%) are Egyptian, (4%) are other Arab nationalities, by occupation (70.3%) are working and (29.7%) are not working, according to the number of hours They spend on the Internet from 3-4 hours (40.2%), from 6-5 hours (23%), from 7-9 hours (19.4%), and from 10-15 hours (9.3%). As for others (8%), their answer was (ten). Minutes - an hour and a half - more than 15 hours. The study relied on the design of retrospective studies through the application of the modified questionnaire for psychological and behavioral problems using an electronic link that was sent to the students. This was conducted from September 20, 2022, to February 2, 2023, the frequencies and the item correlation coefficient were used with the total score and the saturation of the items with the general factor and alpha after excluding the item. The data were analyzed using SPSS (28) and MPLUS (7). the difficulty parameter from 0.051 to 1.478. The item with a factor (more than 0.63), then it is necessary to exclude the first item in the first dimension, and the seventh item in the second dimension, and in the third dimension the first and last items, and these items had the lowest values of the stability of the scale after their exclusion, so the abbreviated formula consists of 28 items, when estimating the omega

stability of the two versions, it becomes clear that alpha is for the abbreviated version of the scale in the light of the first version The value of the coefficient alpha = 0.888, the value of the coefficient of omega = 0.913.

Key words: cyber psychological security- Social engineering- Digital privacy- Social media behaviors and online psychological performance.

مقدمة:

علم النفس هو الدراسة المتعلقة بالسلوك الفردي والعقل البشري، والتي تشرح قضايا متنوعة ومتعلقة بالتجارب الفردية، وبالفكر البشري، كما تهدف دراسات علم النفس إلى استخدام طرق وأدوات بحث مختلفة لتحليل الحالة العقلية وقدرات الفرد، وتشمل أبعاده علم النفس التطبيقي علم النفس الإكلينيكي وعلم النفس التعليمي وعلم نفس المستهلك وعلم النفس التنظيمي وعلم النفس الاجتماعي وعلم النفس الرياضي، كما أن هناك مجال آخر سريع الظهور هو علم النفس السيبراني. (Ahuja, & Alavi, 2017)

وأصبح علم النفس السيبراني هو مجال للدراسة أو البحث للعلماء وعلماء النفس لأنه مرتبط بالعقل والسلوك البشري بسبب الإنترنت ومشاركة وسائل التواصل الاجتماعي .إلى جانب ذلك، فهو مجال ناشئ فإزداد العالم في التحول إلى التكنولوجيا الرقمية، وإزداد اعتماد الإنسان على التكنولوجيا، ووفقًا للإحصائيات الأن اعتبارًا من يناير 2023، كان هناك 5.16 مليار مستخدم للإنترنت في جميع أنحاء العالم، وهو ما يمثل 64.4 في المائة من سكان العالم، ومن هذا الإجمالي، كان 4.76 مليار، أو 59.4 في المائة من سكان العالم، من مستخدمي وسائل التواصل الاجتماعي، وترك التحول الهائل إلى الرقمنة تأثيرًا كبيرًا على كيفية عمل الناس وتفاعلهم في عصر لتكنولوجيا.

وكما يعد علم النفس السيبراني والسلوك والشبكات الاجتماعية هو العلم الأساسي لفهم التأثير الاجتماعي والنفسي لممارسات الإنترنت وتطبيقاته والشبكات الاجتماعية في العصر الرقمي الواقع الافتراضي والذي يهتم بتأثيرات التقنيات التفاعلية على السلوك والمجتمع، سواء كانت إيجابية أو سلبية. Wiederhold, (2014)

وكما أنه أحد المجالات الناشئة للدراسات النفسية (Suler, 2004) حيث يدرس العلماء وعلماء النفس علاقة وتأثيرات عالم الإنترنت على العقل البشري بسلوكياتهم الإيجابية أو السلبية (Elhai, & Rozgonjuk, 2020)

وركزت معظم الدراسات البحثية المتعلقة بموضوع علم النفس السيبراني من خلال تأثير الإنترنت، وخاصة منذ ظهور وسائل التواصل الاجتماعي وتأثيرها على نفسية الأفراد والجماعات، ومع ذلك، مل مجال علم النفس السيبراني جميع التفاعلات الرقمية التي تؤثر على علم النفس البشري، مثل الواقع الافتراضي والواقع المعزز والذكاء الاصطناعي والألعاب عبر الإنترنت والحوسبة المحمولة.

وفي دراسة (2019) Singh, & Singh, تم لفت الانتباه إلى السلوكيات البشرية والأجهزة الرقمية وإلى أيضًا أهمية علم النفس السيبراني لرفاهية الصحة العقلية وعلم النفس الإكلينكي من خلال عالم

الانترنت، فهو العلم الذي يهتم بدراسة العقل والسلوك من منطق التفاعل بين الإنسان والتكنولوجيا التي أصبحت مسيطرة على العالم، كما أنه يضم كافة الظواهر النفسية المرتبطة بتكنولوجيا الاتصالات وتقنياتها، بما تشتمل عليه من هواتف وألعاب ووسائط رقمية وواقع افتراضي يكون له أثر في تغير السلوكيات والأفكار.

مشكلة الدراسة:

على الرغم من الطبيعة النفسية الجوهرية للعديد من هجمات الأمن السيبراني، لا تزال الابحاث عن دور علم النفس في الأمن السيبراني محدودًا، في الواقع، حتى الأبحاث في الهندسة الاجتماعية يتم إجراؤه غالبًا من تخصص الحوسبة بدلاً من علم النفس الاجتماعي .فإن الحاجة إلى نهج نفسي اجتماعي يقترح حقيقة أن حوادث الأمن السيبراني واسعة النطاق – وناشئة عن دوافع متنوعة مثل المكاسب المالية والاحتجاجات السياسية / الأيديولوجية – وغالبًا ما يتم تحريضها من قبل الجماعات، على عكس الأفراد الذين يتصرفون بمفردهم، على سبيل المثال، Anonymous، واحدة من أكثر مجموعات الهاكرز شهرة، ليست مجموعة متماسكة تعمل بالتعاون، ولكنها مصطلح شامل لأولئك الذين تتطابق أهدافهم مع أهداف هذه المجموعة.(Thackray, et al., 2016)

وفي عام 2016 بدأ الاعتراف بعلم النفس في المؤلفات الأكاديمية للأمن السيبراني، وظهرت أهمية علم النفس في مجال الأمن السيبراني (Thackray,et al.,2016) فغالبية البحوث النفسية التي تم إجراؤها حتى الآن في الأمن السيبراني تركز على الوقاية والتخفيف من استراتيجيات وحوادث الأمن السيبراني والقليل منها ركز على دوافع الجناة، يمكن لعلم النفس تقديم الكثير في المساعدة على فهم دوافع الجناة أو المحتالين. (Ghosh, & Turrini, 2010)

ونظرًا لأن مجال علم النفس السيبراني لا يزال نسبيًا في مهده، فعلماء النفس في وضع جيد لإبلاغ هذا التخصص المبتكر من خلال التعاون متعدد التخصصات، مثل التفاعل بين الإنسان والحاسوب، علوم الحاسب والهندسة وعلم النفس، وسوف يزدهر مجال علم النفس السيبراني بشكل متزايد عندما يستمر تطوير التكنولوجيا واستخدامها.

ومع نمو التقنيات الجديدة والتفاعل المتزايد المتصل داخل عالمنا، ظهر مجال علم النفس السيبراني باعتباره تخصص فريد .فهذا التخصص هو فهم العمليات النفسية المتعلقة بجميع الجوانب لخصائص السلوك البشري المترابط تقنيًا (Atrill–Smith et al., 2019)، علاوة على ذلك، هناك اعتراف بمفهوم علم النفس السيبراني من خلال الجمعيات المهنية، مثل American Psycho–logical Association (APA)، وكذلك من خلال المجلات والمؤتمرات الجديدة، والبرامج الأكاديمية الناشئة .على هذا النحو، فإن مصطلح

cyberpsychology لقد أصبح يشمل مجالات متنوعة من والتطبيقات التي يتم عرضها من خلال عدسة علم النفس والعلوم السلوكية

ولقد انفجرت التكنولوجيا والسلوك البشري من خلال عدسة علم النفس، وما يتصل بذلك من مجال علم النفس السيبراني، ولقد غير الإنترنت التفاعلات الاجتماعية وأنماط الاتصال وحتى هوياتنا، فمجال علم النفس السيبراني اهتم بشكل أساسي بمتغيرات الشخصية، والعمليات الإدراكية، والأداء العاطفي، والاستجابات السلوكية، ويتم ذلك من خلال سلوك الاشخاص على الإنترنت وشخصيتهم.

وعلى الرغم من كم الإيجابيات التي حققتها التكنولوجيا المعلوماتيية قد صاحبتها إنعاكسات سلبية خطيرة نتيجة سوء الاستخدام، وكما أن مصطلح الامن النفسي السيبراني لاقى انتباه العديد من الباحثين في الفترة الاخيرة، وذلك لكثرة التهديدات والتحديات السيبرانية، كما انها أصبحت تواجهة الدول أيضا بل العالم، وذلك بسبب الاعتماد الرئيسي على الانترنت واستخداماته، وفضلاً عن توجه العديد من المؤسسات والمنظمات للتطبيقات المفتوحة وخدمات السحابة الالكترونية.

ولقد أشار التقرير السنوي للأمن السيبراني بواسطة Cisco(2018) بأن سبعة من واقع عشرة منظمات أصحت بأن معدل هجمات الأمن السيبراني تزايد في عام 2017، وإن(77%) من الهجمات نجحت في اختراق المؤسسات، وأكدت على أن برامج مكافحة الفيروسات لا يمكنها لإيقاف التهديدات السيبرانية.

وأشار (Thackray,et al.,2016) إلى كيف يمكن الاستخدام الأفضل لعلم النفس للمساعدة في منع الحوادث السلبية للأمن السيبراني؟ ويتم ذلك:

1- عن طريق تحسين الأمن السيبراني ويكون ذلك مرتبط بالتوعية المناسبة .كما قال لي Lee Hadlington _عالم النفس المعتمد والأستاذ المساعد في علم النفس السيبراني في De Montfort University_ "الأمر كله يتعلق بالوعي العام – وهو نهج شامل للأمن السيبراني".
2- كيف نفكر هو جزء أساسي من الأمن السيبراني، وطريقة تفكيرنا تتغير باستمرار فيما يتعلق بالأمن السيبراني، كما تتشكل هذه العقليات من خلال العديد من العوامل، بما في ذلك كيفية تفسيرنا وتجهيزنا لتهديدات الأمن السيبراني، وما إذا كنا نعتقد أننا يمكن أن نقع ضحية لهجوم، وكيف ندرك ما يفكر فيه المهاجمون، ولماذا يفعلون ما يفعلونه، وما هي الادوات النفسية التي يستخدموها يتم لسحبهم ولخداعهم للضحايا.

3- قديماً، كان يُنظر إلى الأمن السيبراني على أنه مشكلة تقنية، كانت حلول البرمجيات والأجهزة أساسية لها. ومع ذلك، في السنوات الأخيرة، انتقل التركيز من الجانب التقني إلى الجانب البشري للأمن السيبراني. يُنظر إلى الناس أكثر فأكثر على أنهم "الحلقة الأضعف"، أو يشار إليهم بإخلاص باسم PEBCAK (توجد مشكلة بين الكرسي ولوحة المفاتيح) ويوضح أن المستخدم النهائي المعني هو مصدر المشكلة، يتم استخدام المصطلح عندما تكون المشكلة التي يتم معالجتها خطأ أساسي للمستخدم.

وبدلاً من محاولة حل المشكلات البشرية بالحلول التكنولوجية، فإن الحل الأفضل هو النظر إلى المعرفة العلمية الحالية والعمل مع الخبراء في علم النفس، كما يمكن للمعرفة في مجال علم النفس إنشاء حملات توعية أكثر فاعلية، من خلال تدريب الناس على اكتشاف الهجمات الإلكترونية الاجتماعية من خلال استخدام المعرفة الموجودة في مجال علم النفس المعرفي، كما تؤدي عمليات التعاون إلى تحسين الأمن السيبراني الفردي، وكذلك المنظمات تصبح أكثر أمانًا، والمجتمع (دوليا) يعمل بشكل أفضل.

فهناك حاجة قوية لحل مشكلات الأمن السيبراني على هذا المستوى، قادمًا من خلفية البرمجة، يهدف إلى أن علماء الكمبيوتر يقوموا بحل نقاط الضعف في بنية البرنامج. مثل، أن يطلب البرنامج كلمة مرور قوية.

ولتحقيق ذلك، يعد العمل مع علماء النفس أمرًا أساسيًا حيث يتم تدريبهم على وصف وفهم وحل مشكلات السلوك البشري؛ من خلال جلب علماء النفس إلى مجال الأمن السيبراني، يمكنهم تطبيق النظريات النفسية وأفضل الممارسات الحالية على مشاكل الأمن السيبراني، بالإضافة إلى تطوير نظريات نفسية جديدة حول تفاصيل الهجمات الإلكترونية والمرونة الإلكترونية.

فأصبح علم النفس السيبراني مجالًا مهمًا في علم النفس، وأصبح دوره في منع الهجمات الإلكترونية موضوعًا مهما وخصوصاً عند مناقشة استراتيجيات الدفاع السيبراني؛ يقترح خبراء من معهد [3] SANS ""SysAdmin, Audit, Network, and Security"، وهو معهد تدريب وأمان معترف به يركز على تطوير مهارات الأمان والحماية في مجالات مثل إدارة الأنظمة، والتدقيق، بأن استخدام علم النفس الطب الشرعي لتحديد هوية المجرمين الذين يقفون وراء هجوم إلكتروني من خلال دراسة العملية والتقنيات والمهارات والإجراءات والتقنيات التي يستخدمها مجرمو الإنترنت أثناء الهجوم .نظرًا لأن أجهزة الحوسبة والإنترنت لها تأثير مثير للإعجاب على حياتنا، سواء في المنزل أو في العمل، فقد أصبح استخدام علم النفس السيبراني لفهم كيفية تأثير التقنيات الناشئة على حياة الناس مجالًا مهمًا في عصر المعلومات اليوم.

وعليه فإن الدراسة الحالية تركز على الكشف عن بنية الأمن النفسي السيبراني، والدراسة الحالية تحاول الوصول الي رؤية حول طبيعة البناء لدي عينة من المجتمع العربي اخذة في الاعتبار الكشف عن البنية العاملية للمقياس، كما اهتمت بالتحليل السيكومتري لمقياس الامن النفسي السيبراني، **وفي ضوء ما سبق يهتم البحث الحالي بالإجابة على الاسئلة التالية:**

1- ما المؤشرات السيكومترية لمفردات مقياس الأمن النفسي السيبراني؟

2- ما البنية العاملية لمقياس الأمن النفسي السيبراني؟

أهداف الدراسة:

1. حساب المؤشرات السيكومترية الوصفية لمفردات مقياس الأمن النفسي السيبراني المتمثل في:
   أ- التكرارات والنسب المئوية لبدائل الاستجابات للمفردات.
   ب- مؤشرات جودة المفردات لمقياس الأمن النفسي السيبراني.
2. الكشف عن البنية العاملية لمقياس الامن النفسي السيبراني في ضوء التطبيق على عينة الدراسة.
3. التحقق من البناء المفترض لمقياس الامن النفسي السيبراني من خلال التحليل العاملي التوكيدي.
4. التحقق من ثبات البناء العاملي لمقياس الامن النفسي السيبراني.
5. الصيغة المختصرة لمقياس الأمن النفسي السيبراني؛ وما جودتها السيكومترية.

أهمية الدراسة:

1. بناء مقياس للأمن النفسي السيبراني، حيث أنه لا يوجد في البيئة العربية والأجنبية – في حدود علم الباحثة- مقياس له، وندرة تحدث الدراسات عن هذا المصطلح لأنه مصطلح جديد نسبياً.
2. بناء وتكييف وتقويم مقياس الأمن النفسي السيبراني، للإعتماد عليه في تشخيص الأمن النفسي السيبراني.
3. ودراسة أحد المفاهيم النفسية الجديدة – نسبيًا – في تخصص علم النفس. حيث أنه يهدف إلى دراسة الأفراد والمجتمعات والتقنيات الرقمية والجوانب النفسية وتفاعلاتهم.
4. تقيم كيفية استخدام الناس للتكنولوجيا للتفاعل في الفضاء السيبراني وكيف تؤثر هذه التفاعلات على حياتهم في العالم الحقيقي أو العالم الغير المتصل.
5. نتائج هذه الدراسة تفتح المجال للباحثين في تناول الأمن النفسي السيبراني في سياق معرفي.

مصطلحات الدراسة:

- **الأمن النفسي السيبراني: cyber psychological security**

هو مجال جديد – نسبيًا – في تخصص علم النفس، ومصطلح ليس شائعا، ويعتبر بمثابة مظلة كبيرة تغطي موضوعات فرعية تتدرج تحته و يجب دراستها ، حيث أنه يهدف إلى دراسة الأفراد والمجتمعات والتقنيات الرقمية والجوانب النفسية وتفاعلاتهم، كما أنه يقيم كيفية استخدام الناس للتكنولوجيا للتفاعل في الفضاء السيبراني وكيف تؤثر هذه التفاعلات على حياتهم في العالم الحقيقي أو العالم الغير المتصل، فهو يدرس التغييرات في السلوك البشري بسبب الاستخدام المفرط للإنترنت ووسائل التواصل الاجتماعي، وهناك ثلاثة أبعاد مرتبطة به وهما: هجمات الهندسة الاجتماعية، السلوكيات علي السوشيال ميديا والأداء النفسي على الانترنت ، انتهاك الخصوصية الرقمية. (آلاء نور الدين، 2023)

الإطار النظري:

يصبح الفرد أسيراً لما يتعرض له في الفضاء السيبراني من أفكار وصور ذهنية وانطباعات، فيوفر الإنترنت مكانًا فريدًا للتعبير عن الذات البديلة، خاصة لأولئك الذين يعانون من القلق الاجتماعي، ويشعرون بالقدرة على التعبير عن الجوانب الذاتية الخفية على الإنترنت، هذا الوسيط يعطي الأفراد فرصة لمشاركة عواطفهم وأفكارهم وبياناتهم وما يعجبهم وما يكرهون وأشياء أخرى تحدث في حياتهم، كما يتخذ العديد من الأشخاص هذه الوسيلة ، فقط لاشتقاق المتعة من التجربة و للتواصل مع الآخرين، وهنا تتبلور أهمية علم النفس السيبراني في تحليل التفاعل بين الافراد والتكنولوجيا ومردود ذلك على الافكار والسلوك. (سعيد، 2022)

أشار (Khera, 2018) من منظور الأمن السيبراني، قد يعتقد الكثير من الناس أن تكنولوجيا المعلومات لا علاقة لها بعلم النفس .بينما في الواقع، هم مرتبطون جدًا. على سبيل المثال، يظل استغلال الأشخاص نفسياً للحصول على معلومات حساسة (على سبيل المثال، بيانات الحساب البنكية) هو الأداة الأساسية التي يستخدمها المجرمين الإلكترونين للحصول على وصول غير مصرح به إلى أنظمة تكنولوجيا المعلومات.

وأكد في مقال نشرة (Khera, 2018) في Haking Media أنه يمكن لعلماء النفس رفع مستوى الوعي العام حول مخاطر الأمن السيبراني وبالتالي تشجيعهم على أن يصبحوا أكثر وعياً بالخصوصية من خلال استخدام الحملات المستهدفة عبر شبكات التواصل الاجتماعي وغيرها من القنوات الإعلامية التقليدية مثل التلفزيون والصحف.

فأصبح هناك حاجة إلى علم النفس السيبراني؛ لأن حياة البشر محاطة بالتكنولوجيا والهواتف الذكية والترفيه الرقمي ووسائل التواصل الاجتماعي التي أصبحت تسيطر علينا، فهو مرتبط بالعقل والسلوك البشري بسبب الإنترنت ومشاركة وسائل التواصل الاجتماعي حتى تطبيقات الهاتف المحمول أصبحت تتبع وتترقب

الأفراد ورغباتهم مثل تتبع الوسائط الاجتماعية وتطبيقات اللياقة، فهي جعلت الانسان معتادًا عليها. وبالتالي لا توجد إمكانية للعيش بدون هاتف ذكي وإنترنت مثل ما حدث في مواقف (COVID19) حيث حدث إغلاق عالمي، وحدث تباعد اجتماعي، فجاءت المنصة الرقمية لإنقاذ حياة الناس وترك العالم يسير على الطريق الصحيح وسط الإغلاق على سبيل المثال، بدأت الفصول الافتراضية، وتم تقديم العمل من المنزل، وتم التدريب عبر الإنترنت. إلى جانب ذلك، ازداد شراء البقالة عبر الإنترنت مقارنة بالعام الماضي .

فعلم النفس السيبراني هو مزيج من النتائج الإيجابية والسلبية. ترتبط التأثيرات السلبية بالاضطرابات النفسية مثل الأرق والعدوانية والقلق وما إلى ذلك، بالإضافة إلى أنها يمكن أن تؤثر أيضًا على العلاقات الشخصية والاجتماعية مع العائلة والأصدقاء.

أصبح الأفراد يتفاعلون بشكل متزايد مع العالم من خلال الإنترنت التكنولوجيا في العديد من مجالات حياتهم، والبحث عن السلوك عبر الإنترنت، يشمل تصرفات الاشخاص في الفضاء الإلكتروني وعلاقته بالشخصية والعلاقات عبر الإنترنت، وغالبًا ما يتصرف الأشخاص بشكل مختلف في الفضاء الإلكتروني عن غيره.، كما أن إلغاء القيد عبر الإنترنت هو مصطلح يستخدم لوصف خفض القيود النفسية في البيئات الاجتماعية عبر الانترنت (Joinson, 2007; Suler, 2004, 2016)، ينعكس ذلك في خفض القيود السلوكية في الفضاء السيبراني.

دور علم النفس في تعزيز الأمن السيبراني

استخدام علماء النفس فهم السلوك البشري في الفضاء السيبراني، يمّكن علماء النفس من إدخال الثقافة والسلوك والتحولات نحو مستوى أعلى من الأمان لكل فرد وللمستويات الجماعية أيضاً من خلال:

1- تحديد المواقف الاجتماعية التي يكون فيها الأفراد يظهروا ميل أعلى للخصم من خلال مشاركة المعلومات الخاصة بهم على المواقع غير الرسمية، على سبيل المثال، وجدت الدراسة أن الناس أكثر عرضة للكشف المعلومات الشخصية والسرية في الإعدادات، مثل المحادثة غير الرسمية أو على الشبكات مواقع التواصل الاجتماعية. (John, Acquisti, & Loewenstein, 2011)

2- تحديد الأنماط الإجرامية والأنشطة الخبيثة من خلال مراقبة الانحرافات عن المعايير السلوكية، والتفاعل مع مزودي التكنولوجيا لتطوير أنظمة أمنية قادرة على اكتشاف مثل هذا الأنشطة، مع الأخذ بعين الاعتبار التشويه النفسي الذي يؤثر على قرارات الخصوصية.(Morewedge,et al.,2005)

3- استشارة المشرعين والمجموعات التوجيهية بشأن التأثير النفسي والاجتماعي للجرائم الإلكترونية من أجل رفع مستوى التشريع إلى مستوى يضاهي مستوى الجرائم غير الافتراضية. كما وجد أن التشريعات المجزأة (أي تباين التشريعات عبر البلدان) هي أحد العوامل الرئيسية التي تعيق مكافحة الجريمة السيبرانية.(UNODC, 2013)

4- زيادة الوعي العام بمخاطر الأمن السيبراني لتعديل تصور الناس، وبالتالي سلوكهم تجاه الخصوصية .من الضروري أن يتواصل علماء النفس مع الجمهور من خلال وسائل الإعلام الرئيسية والشبكات الاجتماعية(Wiederhold, 2014)

5-فهم تأثير الجرائم الإلكترونية على سلوك الضحايا خلال مراحل الإيذاء .وجد الباحثون أن ضحايا الجرائم الإلكترونية يمرون بثلاث مراحل عند قيامهم بالتفاعلات الاحتيالية: ما قبل التجريم (الانفصال أو التفريق)، ومن ثم (فترة الانتقال)، وما بعد الحدي (التأسيس). كما يجب على علماء النفس فهم أعراض ومخرجات كل مرحلة من أجل تحسين ممارسات العلاج والحفاظ عليها. (Burgard, & Schlembach, 2013)

في الماضي ، كان المتخصصين في الأمن السيبراني يعملون على إقناع قادة الأعمال بأن تهديد هجوم الأمن السيبراني حقيقي لأي منظمة، كما بدأ العديد من المديرين التنفيذيين يعيشون في حالة من الإنكار (أو الجهل المتعمد) لسنوات ، معتقدين أن الأمن السيبراني كان شئ تسالي، كما يتضح من الاتجاهات السائدة في الإنفاق على الأمن السيبراني، ولكن يبدو أنها طريقة التفكير تغيرت، وفقًا لموقع Statista.com، تضاعف الإنفاق على الأمن السيبراني في الولايات المتحدة أكثر من الضعف منذ عام 2010 من 27.4 مليار دولار إلى حوالي (66) مليار دولار في عام 2018. وتزعم Gartner أن في 2018 كان أقرب إلى (100) مليار دولار وتتوقع أنه في عام 2019، سيتجاوز الإنفاق الأمريكي من (120) مليار دولار.

وهناك علاقة بين تخصص الحوسبة وعلوم الكمبيوتر وعلم النفس، ساعد علماء النفس في الكثير من تقديم العديد من الطرق لفهم الطريقة التي تعمل بها أنظمة الكمبيوتر وتم تطويرها واستخدامها بناءً علي ذلك، ولكن أيضًا فهم أجهزة الكمبيوتر ساعد علماء النفس على نمذجة الإدراك البشري وعمل التدريبات البشرية للتأقلم مع التطور، قام علماء النفس بتتبع وبحث تطوير وتأثير أجهزة الكمبيوتر فكان ذلك مفيد لطلاب النظم التقنية الآمنية والأمن السيبراني؛ لانهم بحاجة إلى فهم العناصر المعرفية والاجتماعية والنفسية والفروق الفردية بين الاشخاص، وتساعدهم أيضا في النظر للقدرات والقيود للكمبيوتر وللمستخدمين ويساعدهم على تصميم أنظمة كمبيوتر أكثر فعالة (قابلة للاستخدام) لجميع أنماط المستخدمين (Suler, 2016)

وأكد في مقال نشره Khera (2018) في Hakin9 Media أنه يتم استخدام علم النفس لتعزيز الأمن السيبراني وفي فهم سلوك المستخدمين في الفضاء السيبراني ولتطوير وتعزيز سلوكيات الدفاع عن الأمن السيبراني لكل من الأفراد والمؤسسات من خلال:

- استخدام علم النفس، يمكن فهم كيف ينظر الناس إلى المخاطر عبر الإنترنت وما الذي يحفزهم على أن يصبحوا أكثر وعياً بالأمان، على سبيل المثال، يمكن لعلماء النفس تحديد المواقف الاجتماعية المحادثات غير الرسمية مثل التحدث على وسائل التواصل الاجتماعي أو محادثة غير رسمية خارج العمل) عندما يميل الناس إلى الكشف عن معلومات حساسة.
- استخدام علم النفس، يمكن تحديد أنماط الأنشطة الإجرامية والأنشطة الخبيثة الأخرى ذات الصلة عبر الإنترنت واستخدامها لاحقًا من قبل موفري الأمن لتعزيز الحلول الأمنية لوقف الهجمات الإلكترونية قبل أن تتطور وتصبح تهديدًا.

وأصبح هناك انتظام في الهجمات الإلكترونية وأصبحت أكثر وضوحا في الأخبار وفي الحياة اليومية. في عام 2017، تم الإبلاغ عن أكثر من (1,600) خرق للبيانات في الولايات المتحدة. وهذا يصل إلى أكثر من أربعة محوالات في اليوم وذلك فقط الانتهاكات المبلغ عنها، نظرا لأن متطلبات الإخطار تختلف حسب الولاية. أصبحت تأثيرات الهجمات الإلكترونية وحجمها مذهلة لدرجة أننا لم نعد بحاجة إلى إقناع الناس بأن التهديدات الإلكترونية حقيقية. (Thackray, et al., 2016)

وأشار مكتب الأمم المتحدة المعني بالمخدرات والجريمة(UNODC, 2013) أنه أصبح 70% من سكان العالم يؤيدوا استخدام الانترنت، ويعتبر العامل البشري هو الحلقة الأضعف للأمان في الفضاء السيبراني، وكما يعد علم النفس له دور حاسم في التخفيف من هذا الخطر، من خلال تبصره في الطبيعة البشرية، كما إن تحويل التركيز من التكنولوجيا إلى علم النفس أمر منطقي لأنه حتى أنظمة الأمان الأكثر تعقيدًا تظل غير قادرة على منع الناس من الوقوع ضحية للهندسة الاجتماعية ، أو المخاطرة بخسارة مالية واجتماعية، ويعد ضروري أيضا بسبب التكلفة العالية للجرائم الإلكترونية على المجتمعات والحكومات.

وفي دراسة نشرتها مؤسسة Norton Internet Security estimated (2013) ذكرت أن الجرائم الإلكترونية تكلف أفرادًا، وشركات، وحكومات أكثر من 100 مليار دولار في عام 2012، كما سلطت الضوء أيضًا على الزيادة كانت بنسبة (200٪) في التكلفة لكل ضحية مقارنةً بالعام السابق، وذكرت دراسة Kirwan (2011) أن تأثير الجريمة السيبرانية، يتجاوز الضرر المالي؛ فتعاني الضحايا أيضا من أعراض

مشابهة لأعراض اضطراب ما بعد الصدمة (PTSD)، وجد Acquisti (2004) في دراسته ارتفاع في خطر الإيذاء الثانوي بين الأشخاص المقربين للضحايا.

وأكد Kirwan (2011) في دراسة أن الأفراد في وضع غير سار عندما يواجهوا الجرائم الإلكترونية. وعندما لا يتم تقديم معلومات كافية لاتخاذ القرارات المثلى في الخصوصية، يمكن للضحية ان تقع تحت تأثير الخصم نتيجة للتفاؤل الذي يمنحه لها الجاني، ولكن حتى في الحالات التي تكون فيها المعلومات كافية ومتاحة.

وأشار Mumford, (2009) في دراسته أن دور علماء النفس مهم في منع الهجمات الإلكترونية، وقالت عالمة علم النفس Anita D'Amico أمام لجنة فرعية في الكونغرس، أنه يجب علينا معالجة جميع الاختلافات العديدة ومعرفة الأدوار التي نلعبها نحن البشر في الأمن السيبراني، من خلال معرفة الأمن مثل جدران الحماية للبيانات الخاصة، وأنظمة كشف التسلل ومراقبة الشبكات كما .يجب علينا أيضًا تثقيف مطورى البرامج ومساعدة صانعى السياسات وجميع المستخدمين الذين يتواطأون عن غير قصد مع المهاجمين.

ولذلك هناك حاجة متزايدة لمنع وتخفيف تأثير حوادث الأمن السيبراني، وكان هذا هو محور غالبية الأبحاث النفسية حتى الآن .لكننا نحتاج أيضًا إلى فهم ما يحفز الناس على الانخراط في الجريمة الإلكترونية ..في هذا البحث نناقش المساهمات التي يمكن أن تقدمها البحوث النفسية الاجتماعية والنظرية للأمن السيبراني، وكيف يمكن تمكين الأفراد لاتخاذ قرارات مستنيرة بشأن مشاركتهم في حوادث الأمن السيبراني.

واشار Ancis (2020) أن علم النفس السيبراني هو مرتبط بمجالات أساسية تم تحديدها، بما في ذلك الاتجاهات في أخلاقيات علم النفس السيبراني والبحث والتدريب والتطبيق .وهي تشمل (أ) السلوك والشخصية عبر الإنترنت؛ (ب) استخدام وسائل التواصل الاجتماعي والأداء النفسي؛ (ج) الألعاب .(د) علم النفس التخاطر؛ و (هـ) الواقع الافتراضي (VR)، الذكاء الاصطناعي (AI) نشأت هذه المجالات الخمسة من مراجعة الادبيات بما في ذلك النصوص المركزة بشكل خاص على علم النفس والإنترنت، والمقالات والمجلات التي فحصت العلاقة بين التكنولوجيا والسلوك البشري من خلال عدسة علم النفس من خلال مؤتمرات APA السابقة للتكنولوجيا والعقل والمجتمع

وكما أشار Khera (2018) أن هناك ثلاثة أبعاد مرتبطة بالأمن النفسي السيبراني وهي: هجمات الهندسة الاجتماعية، التنمر الالكتروني، الخصوصية الرقمية.

- **هجمات الهندسة الاجتماعية:**

هي نوع من الهجمات الإلكترونية التي تستخدم الحيل النفسية عبر الهاتف أو باستخدام جهاز كمبيوتر لإقناع شخص ما بالكشف عن معلومات سرية عن نفسه أو عن المنظمة التي يعمل بها Khera (2018).

و من وجهة نظر الامن النفسي السيبراني تتمثل في الحصول على معلومات عن الأشخاص عن طريق التلاعب او خداع الأشخاص، ويمكن تعريفها كما ذكر Mitnick, & Simon, (2003) بأنها استخدام الحنكة لخداع الأشخاص أي فن التلاعب بالآخرين، إذا يمكن من خلاله الكشف عن معلومات سرية، او بإعطاء المهاجم الفرصة للوصول لتلك المعلومات

وتناول Granger (2001) أن هناك مجموعة من أساليب الهندسة الاجتماعية يتناولها المهندسون الاجتماعيون للوصول لمرادهم منها: استخدام الهاتف في الخداع عن طريق خلق حوار في اتصال هاتفي للحصول على معلومات، سلة المهملات أي ما يرمي في سلة المهملات الالكترونية يكون عني بالمعلومات التي تفيدهم بعمل الهجمات.

أحد الأمثلة على الهندسة الاجتماعية التي سيواجهها الكثير منا هو رسائل البريد الإلكتروني الهاكر، والتي تحاول خداع المستلم لفتح رابط أو مرفق يقوم بتثبيت برامج ضارة على أجهزة الكمبيوتر الخاصة بالمستلم، وتعتمد رسائل البريد الإلكتروني المخادعة هذه على العديد من مبادئ علم النفس الاجتماعي وعلم نفس المستهلك وتغيير السلوك، لخداعهم بسهولة والوصول للمعلومات التي يريدها الهاكر على سبيل المثال، الإلحاح إذا لم يتصرف المتلقي بسرعة .قد تكون عمليات الاحتيال هذه ناجحة في بعض الوقت.

وكما ذكر Khera (2018) أن هناك أنواع مختلفة أيضا من هجمات الهندسة الاجتماعية؛ الشكل الأكثر شيوعًا هو هجمات التصيد الاحتيالي، في التصيد الاحتيالي، يتظاهر المهاجم بأنه كيان موثوق به (على سبيل المثال، بنك أو خدمة وسائط اجتماعية أو مزود خدمة الإنترنت) ويحاول إقناع المستخدم بفتح بريد إلكتروني أو رسالة فورية؛ بعد ذلك يطلب منه النقر فوق رابط أو تنزيل مرفق يحتوي على برامج ضارة .إذا نقر المستخدم على الرابط الضار، فسيتم نقله إلى موقع ويب ضار يحتوي على مجموعة أدوات استغلال تقوم بمسح جهازه بحثًا عن خدمات ضعيفة أو نظام تشغيل غير مصحح .أو عندما يقوم الضحية بتثبيت برنامج ضار (مثل برامج الفدية أو برامج السرقة) على جهازه ثم يتم إرسال رسائل للبريد الإلكتروني خادعة، على سبيل المثال، يرسل المهاجم عددًا كبيرًا من رسائل البريد الإلكتروني إلى عدد كبير من المستخدمين، على أمل أن ينقر القليل منهم على الرابط الضار أو يكشف عن معلومات حساسة (على سبيل

المثال، بيانات اعتماد الحساب وتفاصيل بطاقة الائتمان)، ما يجعل هجمات الهندسة الاجتماعية ناجحة هو الاعتماد على التلاعب النفسي لكسب ثقة الضحية لتسليم المعلومات الحساسة.

- **الخصوصية الرقمية** Digital privacy

يقترح عالم الشبكات المعاصر العديد من الفرص لأجهزة التحكم عن بعد لسهولة التواصل بين المستخدمين، كما تشترط أنشطة الشبكة بإنشاء ملفات تعريف شخصية و تحميل المعلومات الشخصية التي تسهل الوصول إليها من قبل المستخدمين الآخرين وتتطلب ضرورة تحديث قواعد حماية البيانات و الخصوصية الرقمية لجميع المستخدمين) (Romansky, 2014) ، ولا تزال هناك مخاوف من الخصوصية تشكل مصدر قلق أساسي لمستخدمي الإنترنت، ومع ذلك ، فشل هذا القلق في التفكير في الواقع من خلال تشجيع مستخدمي الإنترنت على اتباع سلوك حماية الخصوصية، و يحاول الخبراء استخدام أساليب البحث في علم النفس السيبراني للعثور على إجابات لأسئلة مختلفة تتعلق بالخصوصية عبر الإنترنت:(Khera, 2018)

لماذا يميل مستخدمو الإنترنت إلى الكشف عن كميات كبيرة من البيانات الشخصية عبر الإنترنت على الرغم من مخاوفهم المتعلقة بالخصوصية؟

1. كيف يؤثر عمر مستخدمي الإنترنت على سلوك الخصوصية عبر الإنترنت .على سبيل المثال، يكشف المراهقون عن المعلومات الشخصية أكثر من الأشخاص الأكبر سنًا.
2. إلى أي مدى يحمي مستخدمو الإنترنت خصوصيتهم على الإنترنت؟ وما الأساليب – والأدوات – التي يستخدمونها لأداء ذلك عمليًا (على سبيل المثال، تثبيت مانع الإعلانات، وتصفح الإنترنت باستخدام الوضع الخاص الامن لمتصفح الويب).

المنهجية والإجراءات:

أولاً: تصميم الدراسة: اعتمدت الدراسة على تصميم الدراسات المستعرضة من خلال تطبيق القائمة المعدلة للمشكلات النفسية والسلوكية من خلال لينك الكتروني تم إرساله للطلاب، في الفترة من 20/9/2022 الي الفترة من 2/2/2023

ثانياً: المشاركون: تم الحصول على عينة متاحة على الانترنت من خلال طرح مقاييس الدراسة على صيغة Google form وتم ارسالها إلى العديد من الأفراد وكذلك التنبيه عليهم لإرسالها إلى اخرين حيث يكون التطبيق إلكترونياً على التليفون من خلال لينك مرسل له، بلغ عدد المشاركون(535) ممن طبقوا ، تنوعت حسب الجنس إلى (87.1%) من الاناث ، (12.9%) من الذكور ، وتراوحت أعمارهم في المدى من (15 إلى 60)، وحسب الحالة الاجتماعية (86.4%) متزوج و(13.1%) أعزب، وحسب الجنسية (96%)

مصري، (4%) جنسيات عربية أخرى، على حسب الوظيفة (70.3%) يعملوا و(29.7%) لا يعملوا، على حسب عدد الساعات التي يقضوها ع الانترنت من 3-4 ساعات (40.2)، من 6-5 ساعات (23%)، ومن7-9ساعات (19.4%)، ومن 10-15ساعة (9.3%)، أما أخري (8%) وكانت اجابتهم (عشر دقائق-ساعة ونصف-أكثر من 15ساعة)

ثالثا: المقياس وكيفية بنائة: خطوات بناء مقياس للامن النفسي السيبراني:

1- مر المقياس بمجموعة من الخطوات حتى وصل إلى صورته النهائية وهي الاطلاع على:

2- التعريفات المختلفة للامن النفسي السيبراني

3- الاطلاع على التراث البحثي في الدراسات الذي اهتم بدراسة الامن النفسي، الامن السيبراني.

4- وفي حدود علم الباحثة لا يوجد مقياس في البيئة العربية ولا البيئة الأجنبية للامن النفسي السيبراني، ولكن تم الاطلاع على مقالات ومؤتمرات ناقشن الامن النفسي السيبراني ومنها تم استخلاص الابعاد وبناءاً على ذلك أعدت الباحثة مقياس للأمن النفسي السيبراني مكون من ثلاثة أبعاد (الهندسة الاجتماعية- الخصوصية الرقمية - السلوكيات علي السوشيال ميديا والأداء النفسي على الانترنت)

5- صياغة تعريف إجرائي للامن النفسي السيبراني وهو: هو مجال جديد - نسبيًا - في تخصص علم النفس، ومصطلح ليس شائعا، ويعتبر بمثابة مظلة كبيرة تغطي موضوعات فرعية تندرج تحته و يجب دراستها ، حيث أنه يهدف إلى دراسة الأفراد والمجتمعات والتقنيات الرقمية والجوانب النفسية وتفاعلاتهم، كما أنه يقيم كيفية استخدام الناس للتكنولوجيا للتفاعل في الفضاء السيبراني وكيف تؤثر هذه التفاعلات على حياتهم في العالم الحقيقي أو العالم الغير المتصل، فهو يدرس التغييرات في السلوك البشري بسبب الاستخدام المفرط للإنترنت ووسائل التواصل الاجتماعي، وهناك ثلاثة أبعاد مرتبطة به وهما: هجمات الهندسة الاجتماعية، السلوكيات علي السوشيال ميديا والأداء النفسي على الانترنت ، انتهاك الخصوصية الرقمية.

6- ومن المؤتمرات والمقالات والدراسات التي أشارت إلى مصطلح الامن النفسي السيبراني وأبعاده: دراسة دراسة (2019) Singh & Singh، الجمعية المهنية American Psycho-logical Association (APA)، دراسة (2019) ,.Atrill-Smith et al، مقال نشره (2018) Khera في Hakin9 Media

7- يعد علم النفس السيبراني مجال للدراسة أو البحث للعلماء وعلماء النفس، فهو مجال ناشئ، فلا يوجد إلا اتفاق على المكونات الجوهرية للمفهوم، ومن ثم تبدو المنطقة البحثية التي تناولها بنية هذا المفهوم في حالة دينامية، وذلك لأن فهم الظواهر النفسية سياقها الثقافي والبيئ الذي يحدث فيها السلوك الإنساني بحاجة إلى مراجعة شمولية أبعاده، وربما إضافة جوانب لهذا التصور تتناسب مع البيئة العربية.

8- في ضوء ما سبق تم صياغة مقياس الامن النفسي السيبراني مكون من ثلاثة أبعاد (هجمات الهندسة الاجتماعية، السلوكيات علي السوشيال ميديا والأداء النفسي على الانترنت، انتهاك الخصوصية الرقمية)، بحيث يشمل البعد الاول 10 مفردات، والبعد الثاني 10 مفردات، والبعد الثالث 12 مفردة.

9- وتم استخدام تصنيف ليكرت (Likert) ثلاثي التدرج (نعم، إلى حد ما، لا) ويختار الاستجابة التي تتوافق رأيه، وتقدر الاستجابة (نعم) ب (2)، و(إلى حد ما) ب (1)، و (لا) ب (0).

10- صياغة مجموعة من التعليمات التي تتناسب مع طبيعة المقياس.

11- إعداد مفتاح تصحيح، حيث يحصل الشخص على ثلاث درجات للاستجابة المرتفعة (نعم)، وأثنان درجة للاستجابة (إلى حد ما)، ودرجة واحدة للاستجابة (لا) ومن ثم تكون الدرجة الكلية للمقياس (96)، والصغرى (32).

12- محكات انتقاء المفردة في المقياس، وضعت عدة محكات لاستبقاء المفردة في المقياس؛ أهمها: التأصيل النظري للمفردة وارتباطها بمظاهر الامن النفسي السيبراني؛ والخصائص الاحصائية السيكومترية وهي أن الالتواء لا يزيد عن 3، والتفرطح لا يزيد عن 7، ومعامل الارتباط المصحح لا يقل عن0.40، ومعامل صدق (تشبع المفردة بالعامل) لا يقل عن0.40 عامر (2019)، وبلغ ثبات الإتساق الداخلي المعامل الفا للمقياس0.884، وهذا يدل على التجانسية العالية بين المفردات لقياس الامن النفسي السيبراني.

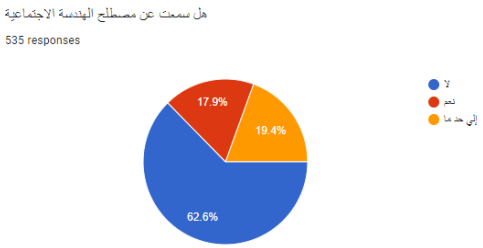
التحليل الاحصائي:

تم تحليل البيانات بإستخدام برنامج SPSS(28) لتقدير مؤشرات جودة المفردة، واستخدام برنامج MPLUS (7) لتقدير التحليل العاملي التوكيدي، تقدير التكرارات والنسب المئوية لكل إستجابة، إذا كان متوسط المفردة (معامل الصعوبة) يميل إلى القيمة المتوسطة فانها تكون ذات أهمية في المقياس ، القيمة المرتفعة للإنحراف المعياري مقارنة بالإنحراف المعياري لبقية المفردات فإن هذا يشير إلى أن المفردة استطاعت الكشف عن مدى أوسع من الفروق الفردية بين الافراد، إذا اقتربت قيمة الإلتواء والتفرطح من الصفر فأن توزيع بيانات المفردة تتمتع بالإعتدالية، يفضل أن يكون معامل الارتباط بين المفردة والدرجة الكلية (معامل التمييز) 0.70 فأكثر وأيضًا قيمة معامل الإرتباط المصحح 0.30 فأكثر، أما في التحليل العاملي تشبع المفردة بالعامل 0.63 فأكثر(معامل التمييز)، معامل الشيوع للمفردة يكون0.50 فأكثر، و معامل الثبات الإتساق الداخلي المعامل الفا كرونباخ والمعامل اوميجا لـ (McDonald, 1999). وتم حساب المتوسط الموزون weighted mean كمعيار للحكم وبالاعتماد على مجموع الإجابات عن كل فقرة من فقرات القائمة.

نتائج الدراسة

النتائج الخاصة بالسؤال الأول: ما المؤشرات السيكومترية لمفردات **مقياس الأمن النفسي السيبراني؟** للتحقق من هذا السؤال تم إجراء التحليلات الأتية:

- في البداية عند سوال العينة عن سماعه عن مصطلح الهندسة الاجتماعية كما هو موضح بالشكل (1)، فكانت إجابتهم لا بنسبة (62.6%)، وإلى حد ما (19.4%)، أما نعم فكانت بنسبة (17.9%)

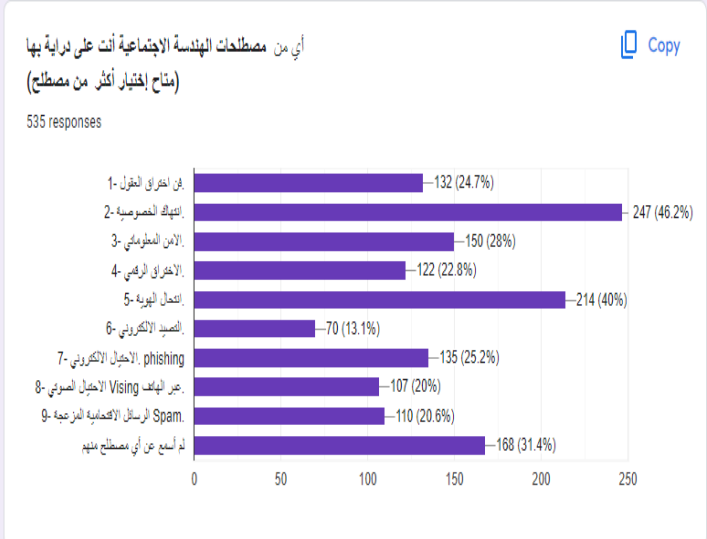


شكل (1) استجابات العينة

- فتم سؤال العينة سؤال تفصيلي أكثر عن معرفته بأي من مصطلحات الهندسة الاجتماعية هو على دراية بها كما هو موضح في شكل (2):

1. فن اختراق العقول. (24.7%)
2. انتهاك الخصوصية. (46.2%)
3. الامن المعلوماتي. (28%)
4. الاختراق الرقمي. (22%)
5. انتحال الهوية. (40%)
6. التصيد الالكتروني. (13%)
7. الاحتيال الالكتروني.Phishing (25%)
8. الاحتيال الصوتي Vising عبر الهاتف. (20%)

9. الرسائل الاقتحامية المزعجة Spam. (20.6%)
10. لم أسمع عن أي مصطلح (31.4%)



شكل (2) استجابات العينة

ومن خلال التحليل السابق اتضح لنا ان 31.4% في البيئة العربية لم يسمعوا عن أي مصطلح من مصطلحات هجمات الهندسة الاجتماعية، وهذه تعتبر نسبة مرتفعة بسبب عدم الوعي، وذلك أدى إلى ارتفاع نسبة الاحتيال الالكتروني.

أ- التكرارات والنسب المئوية لبدائل الاستجابات للمفردات وهي كالأتي:

الجدول (1): التكرارات والنسب المئوية لمفردات مقياس **الامن النفسي السيبراني** (N=535)

المفردات	لا	إلى حد ما	نعم	المفردات	لا	إلى حد ما	نعم
A1	171 (32.0)	52 (9.7)	312 (58.3)	S7	63 (11.8)	53 (9.9)	419 (78.3)
A2	120 (22.4)	72 (13.5)	343 (64.1	S8	40 (7.5)	64 (12.0)	431 (80.6)

المفردات	لا	إلى حد ما	نعم	المفردات	لا	إلى حد ما	نعم
A3	109 (20.4)	58 (10.7)	312 (58.3)	S9	47 (8.8)	70 (13.1)	418 (78.1)
A4	90 (16.8)	56 (10.5)	389 (72.7)	S10	65 (12.1)	58 (10.8)	412 (77.0)
A5	100 (18.7)	53 (9.9)	382 (71.4)	D1	308 (57.6)	94 (17.6)	133 (24.9)
A6	82 (15.3)	57 (10.7)	396 (74.0)	D2	12 (2.2)	61 (11.4)	462 (86.4)
A6	137 (25.6)	74 (13.8)	324 (60.6)	D3	66 (12.3)	126 (23.6)	343 (64.1)
A8	48 (9.0)	38 (7.1)	449 (83.9)	D4	16 (3.0)	76 (14.2)	443 (82.8)
A9	64 (12.0)	67 (12.5)	404 (75.5)	D5	19 (3.6)	103 (19.3)	413 (77.2)
A10	88 (16.4)	69 (12.9)	378 (70.7)	D6	168 (31.4)	159 (29.7)	208 (38.9)
S1	80 (15.0)	48 (9.0)	407 (76.1)	D7	24 (4.5)	40 (7.5)	471 (88.0)

المفردات	لا	إلى حد ما	نعم	المفردات	لا	إلى حد ما	نعم
S2	69 (12.9)	52 (9.7)	414 (77.4)	D8	222 (41.5)	151 (28.2)	162 (30.3)
S3	103 (19.3)	62 (11.6)	370 (69.2)	D9	140 (26.2)	233 (43.6)	162 (30.3)
S4	33 (6.2)	40 (7.5)	462 (86.4)	D10	150 (28.0)	213 (39.8)	172 (32.1)
S5	63 (11.8)	58 (10.8)	414 (77.4)	D11	123 (23.0)	246 (46.0)	166 (31.0)
S6	113 (21.1)	158 (29.5)	264 (49.3)	D12	139 (26.0)	220 (41.1)	176 (32.9)

يتضح من الجدول (1) أن معظم المفردات استطاعت الكشف عن مستويات مختلفة من انتهاك الخصوصية الرقمية والسلوكيات علي السوشيال ميديا والأداء النفسي على الانترنت ولكن كانت أكثر التكرارات للاستجابات على "نعم", وكشف ذلك على أن المفردات كانت أكثر فعالية في الكشف عن مستويات مرتفعة من التعرض للهجمات وانتهاك الخصوصية الرقمية على مواقع التواصل الاجتماعي، حيث كانت أكثر المفردات قدرة على الكشف عن المستوي المرتفع من هجمات الهندسة الاجتماعية " تعرضت للاحتيال من خلال رمي أوراق مهمة في سلة المهملات"، أما بالنسبة لانتهاك الخصوصية الرقمية " حيث كانت أكثر المفردات قدرة على الكشف عن المستوي المرتفع هي " تعرضت لسرقة حسابي البنكي بسبب شرائي من مواقع التواصل الاجتماعي" بينما أكثر مفردة كشفت عن المستويات المنخفضة من هجمات الهندسة الاجتماعية هي" تعرضت للاختراق من خلال طلب كلمة المرور الخاصة بك" "، أما بالنسبة لانتهاك الخصوصية الرقمية " حيث كانت أكثر المفردات قدرة على الكشف عن المستوي المنخفض" مواقع التواصل الاجتماعي يخترق الخصوصية لمستخدميه، أما بالنسبة للبعد الأخير (السلوكيات علي السوشيال ميديا والأداء النفسي على الانترنت) كانت الفقرات (D1,D8,D9,D10,D11,D12) كشفت عن المستويات

المنخفضة والمتوسطة للسلوك على الانترنت والسوشيال ميديا، **وبحساب المتوسط المرجح او الموزون weighted mean** كمعيار للحكم وبالاعتماد على مجموع الإجابات عن كل فقرة من فقرات القائمة، والذي بلغ (368) وبقوة نسبية (82%) وفي المجمل يتضح وجود درجة معقولة من التناسب في تكرارات الاستجابات الثلاثة لمفردات المقياس وعليه لا يمكن اختصار بدائل الإستجابة الثلاثة إلى عدد أقل من الاستجابات، مما يدعم جودة تصميم بدائل الاستجابات لمفردات القائمة.

ب-مؤشرات جودة المفردات

جدول (2) مؤشرات جودة المفردات لمقياس الامن النفسي السيبراني

المفردة	المتوسط	SD	الالتواء	التفرطح	المفردة	المتوسط	SD	الالتواء	التفرطح
1	1.73	0.91	0.54	-1.58	9	1.30	0.62	1.85	2.0
2	1.58	0.83	0.90	-0.94	10	1.35	0.68	1.67	1.20
3	1.51	0.81	1.09	-0.57	1	1.6729	0.84773	0.680	-1.269
4	1.44	0.76	1.33	0.046	2	2.8411	0.42288	-2.71	.9742
5	1.47	0.79	1.23	-0.26	3	2.5178	0.70523	-1.12	-0.12
6	1.41	0.74	1.43	0.35	4	2.7981	0.47047	-2.31	2.669
7	1.65	0.86	0.73	-1.24	5	2.7364	0.51538	-1.827	2.487
8	1.25	0.60	2.24	3.46	6	2.0748	0.83577	-0.141	-1.555
9	1.36	0.68	1.61	1.03	7	2.8355	0.47705	-2.937	.6702
10	1.45	0.76	1.27	-0.071	8	1.8879	0.84054	0.214	-1.553
1	1.38	0.73	1.53	0.61	9	2.0411	0.75090	-0.067	-1.221

2	1.35	0.69	1.66	1.12	10	2.0411	0.77544	−0.071	−1.332
3	1.50	0.79	1.14	−0.45	11	2.0804	0.73125	−0.126	−1.121
4	1.19	0.56	2.62	5.63	12	2.0692	0.76492	−0.118	−1.281
5	1.34	0.67	1.71	1.33					
6	1.71	0.79	0.54	−1.19					
7	1.33	0.67	1.75	1.48					
8	1.26	0.58	2.06	2.95					

يتضح من الجدول (2) في ضوء المتوسط أن كل المفردات تقترب من الدرجة (1) مما يدل على أن المفردات استطاعت الكشف عن مستويات مرتفعة من هجمات الهندسة الاجتماعية وانتهاك الخصوصية الرقمية، ما عدا المفردة "الاولي" تعرضت للاختراق من خلال طلب كلمة المرور الخاصة بك"فكان متوسطها يعبر عن الإستجابة بدرجة متوسطة وهي (إلى حد ما) .

وتنوعت الإنحرافات المعيارية للمفردات فكأن أعلى إنحراف معياري للمفردة" الاولي " مما يدل على جودتها في كشف مستويات متنوعة من هجمات الهندسة الاجتماعية، بينما كان أقل إنحراف معياري للمفردة" الثامنة " في انتهاك الخصوصية الرقمية وهي" تعرضت للتصيد من خلال عدم إلغائي لخاصية التتبع الجغرافي على مواقع التواصل الاجتماعي "مما يدل على انها أقل مفردة تنوعت عليها استجابات الافراد.

وفي ضوء مؤشري الالتواء والتفرطح يتضح تمتع كل درجات المفردات بالتوزيع الاعتدالي حيث لم تتخطى قيمة (2−,2) وفقا لـ (2013) Field، ما عدا المفردة الثامنة في البعد الأول هجمات الهندسة الاجتماعية فقد ابتعدت قليلًا عن الاعتدالية, وفي البعد الثاني انتهاك الخصوصية الرقمية " المفردتان الرابعة والثامنة فقد ابتعدتا قليلًا عن الاعتدالية، وفي البعد الثالث فقد أبتعد المفردات الثانية والرابعة والسابعة قليلا عن الاعتدالية.

النتائج الخاصة بالسؤال الثاني: الكشف عن البنية العاملية لمقياس الامن النفسي السيبراني في ضوء التطبيق على عينة الدراسة

تم تقدير معامل ثبات الاتساق الداخلي الفا كرونباخ للمقياس وبلغت قيمته 0.884 بينما بلغت قيمة المعامل اوميجا 0.931

جدول (3) معامل الارتباط والتشبع والشيوع لكل مفردة

المفردة	معامل الارتباط	معامل الارتباط المصحح	الفا بعد إستبعاد المفردة	التشبع	الشيوع
1	.134**	0.063	0.888	.134**	0.229
2	.561**	0.499	0.879	.561**	0.683
3	.605**	0.552	0.878	.605**	0.504
4	.616**	0.566	0.877	.616**	0.554
5	.613**	0.566	0.878	.613**	0.599
6	.563**	0.510	0.879	.613**	0.540
7	.596**	0.548	0.878	.613**	0.506
8	.619**	0.566	0.877	.619**	0.672
9	.667**	0.634	0.877	.667**	0.581
10	.666**	0.628	0.877	.666**	0.530
1	.626**	0.580	0.877	.626**	0.509
2	.549**	0.499	0.879	.549**	0.556
3	.670**	0.632	0.877	.670**	0.654
4	.615**	0.565	0.878	.615**	0.684
5	.634**	0.604	0.878	.634**	0.640
6	.628**	0.587	0.878	.628**	0.585
7	.402**	0.338	0.883	.206**	0.404
8	.670**	0.634	0.877	.670**	0.657
9	.661**	0.629	0.877	.661**	0.631
10	.644**	0.608	0.878	.644**	0.628

المفردة	معامل الارتباط	معامل الارتباط المصحح	الفا بعد إستبعاد المفردة	التشبع	الشيوع
1	.695**	9950.	0.884	.369**	0.329
2	0.052	0.013	0.886	0.052	0.519
3	.526**	0.875	0.887	.526**	0.814
4	.515**	0.760	0.887	.516**	0.616
5	.295**	0.195	0.887	.297**	0.375
6	.426**	0.716	0.884	.426**	0.679
7	.117**	0.335	0.887	.116**	0.457
8	.947**	0.267	0.883	.945**	0.680
9	.046**	0.435	0.882	.046**	0.645
10	. 875**	0.235	0.883	.876**	0.583
11	. 816**	0.216	0.883	.816**	0.721
12	.373**	0.309	0.883	.373**	0.666

يتضح من جدول (3) وبواسطة إجراء تحليل المكونات الأساسية لمفردات المقياس وكانت قيمة كايز ماير ولكين 0.950 والذى يجب أن لا يقل عن (0,5) حسب محك كايزر، مما يدل على مناسبة معاملات الارتباطات بين المفردات للتحليل, وبعد تحقق شروط التحليل العاملى تم استخدام التحليل العاملى الاستكشافى بطريقة المكونات الأساسية (Principle components) لاستجابات الطلاب عن مفردات المقياس،وفي ضوء مؤشري معامل ارتباط المفردة بالدرجة الكلية ومعامل الارتباط المصحح (معامل ارتباط المفردة بالدرجة الكلية مستبعدة منه درجة المفردة) يتضح أن معامل الارتباط لكل المفردات 0.5 تقريبا ماعدا المفردة الاولي في البعد الأول، والمفردة السابعة في البعد الثاني، وفي البعد الثالث المفردتان الاولي والأخيرة، بينما زادت قيم معامل الارتباط المصحح لكل المفردات عن 0.50 مما يدل على الارتباط المرتفع للمفردات بالبناء العام للأمن النفسي السيبراني.

.وفي ضوء نتائج التحليل العاملي فأن تشبعات كل المفردات زادت عن المعيار الذي وضعه(Commery & Lee, 1992) وهو 0.63 حيث يعبر عن تشبع جيد جدًا بالعامل العام او البناء التحتي مما يدل على قدرة تمييزية مرتفعة للمفردات ما عدا المفردة الاولي في البعد الأول، والمفردة الثانية والأخيرة في البعد

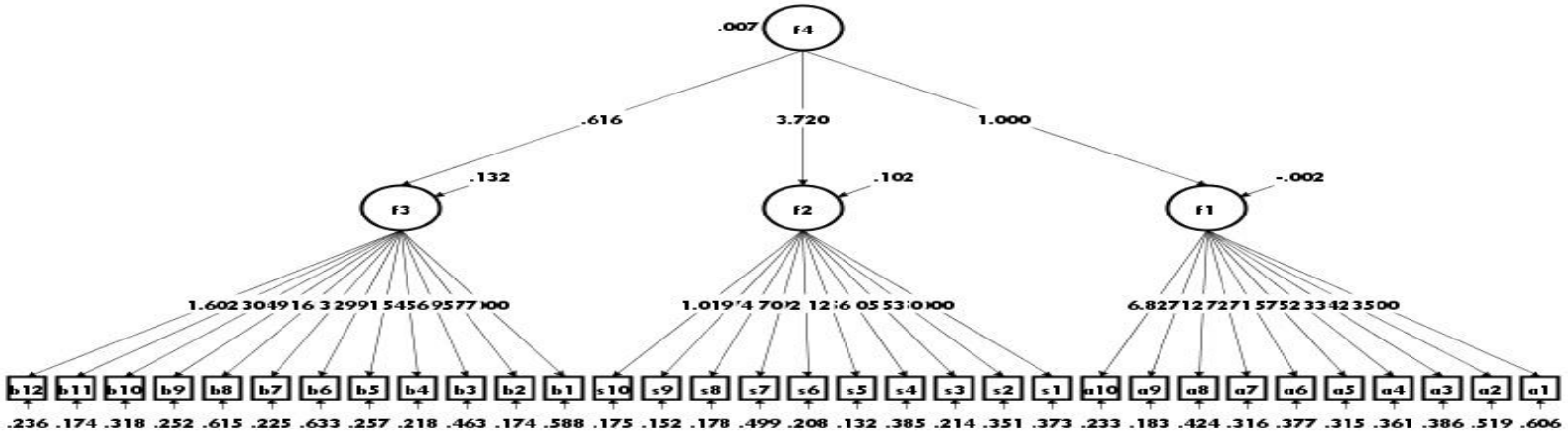
الثالث، فقد كانت لهما قدرة تمييزية متوسطة. وبالنسبة لقيم الشيوع فتجاوزت لكل المفردات 0.50 بمعني أن البناء التحتي فسر 50% من تباين كل المفردات ما عد المفردتين الاولي في البعد الأول، والأخيرة في البعد الثاني.

وقد تم حساب قيمة الجذر الكامن (Eigen value)، ونسبة التباين المفسر (Explained variance)، وكذلك التباين المفسر التراكمي لكل عامل من العوامل، وهذا أفاد أن معامل الارتباط بين كل زوج من المفردات لا يساوي صفر, وأعطي التحليل قبل التدوير ثلاثة عوامل، فبلغ الجذر الكامن للعامل الأول 9.022 وفسر 45.1% من تباين مصفوفة الارتباطات, بينما بلغ الجذر الكامن للعامل الثاني 1.421 وفسر 7.107% من تباين مصفوفة الارتباطات بين المفردات, بينما بلغ الجذر الكامن للعامل الثالث 1.145 وفسر 5.727% من تباين مصفوفة الارتباطات بين المفردات وتشبعت كل المفردات بالعامل الأول حيث تراوحت قيمة معامل التشبع من 0.61 حتي 0.75 ,

النتائج الخاصة بالسؤال الثالث: التحقق من البناء المفترض لمقياس الامن النفسي السيبراني من خلال التحليل العاملي التوكيدي.

- تم إختبار نموذج التحليل العاملي التوكيدي ثلاثي **العامل:**

التحقق من الصدق العاملي التوكيدي للبناء الاصلي الذي افترضه Pekurn et al. (2005)، للتحقق من هذا تم اجراء التحليل العاملي التوكيدي للمفردات 32في برنامج MPLUS (7) واتضح ان مؤشرات حسن المطابقة هي كاي تربيع= 956.513, df=170,p=0.00 ومؤشر RMSEA=0.093 ومؤشر TLI=0.833 ومؤشر CFI=0.851 وكان لهذا النموذج أقل قيمة لمؤشر المعلومات الاكيكي Akaike مما يؤكد تفوق هذا النموذج أ.



شكل (3): شكل المسار لنموذج التحليل العاملي التوكيدي ثلاثي الرتبة لمقياس الامن النفسي السيبراني

النتائج الخاصة بالسؤال الرابع: التحقق من ثبات البناء العاملي لمقياس الامن النفسي السيبراني.

ويتمثل ذلك من إجراءات النمذجة بالمعادلة البنائية ويتم عن طريق النسبة بين تباين الدرجة الحقيقية المشتقة من بارامترات النموذج المقدر إلى مجموع التباينات والتباينات المشتركة في النموذج عن طريق معامل أوميجا، كما أن أوميجا تمثل معاملا ثبات الاتساق والتجانس الداخلي للبنية العاملية والمشتقة من تقديرات CFA **(Yang & Green, 2011); Viladrich, Angulo–Brunet & Doval, 2017)**

جدول (4) قيم ثبات البنية CR، ونسب التباين المستخلص AVE، لكل عامل من القائمة، ومعامل ثبات أوميجا وألفا

	λ	λ²	λ² e=1−	CR	AVE	omega	α
العامل الأول	0.58	0.34	0.66	0.6	0.7	0.978	0.978
العامل الثاني	0.65	0.43	0.57				
العامل الثالث	0.67	0.45	0.55				

ونلاحظ من جدول (4) أن قيمة CR ثبات البنية للابعاد الستة بلغت قيمتها 0.6، كما أن قيم التباين المستخلصAVE أكثر من 0.5 وهي نفسك المحك المحدد، مما يشير إلى أن ثبات التجانس الداخلي لبنية القائمة يعبر عنه بالتباين المستخلص، وقيم نسب التباين المستخلص تمثل دالة في الصدق التمايزي لابنية القائمة الفرعية. (Scrima, 2015)

النتائج الخاصة بالسؤال الخامس: الصيغة المختصرة لمقياس الامن النفسي السيبراني؟ وما جودتها السيكومترية.

الصيغة المختصرة للمقياس يتضح لنا من خلال التحليلات في جدول(2 ,1) وفي حالة الاعتماد على معيار معامل الارتباط بين المفردة والدرجة الكلية (يزيد عن 0.50), وكذلك تشبع المفردة بالعامل (يزيد عن 0.63) فأنه يجب إستبعاد المفردة الاولي في البعد الأول، والمفردة السابعة في البعد الثاني، وفي البعد الثالث المفردتان الاولي والأخيرة، وهؤلاء المفردات كانت لهم أقل قيم لثبات المقياس بعد إستبعادهما بالتالي الصيغة المختصرة تتكون من 28 مفردة، وعليه فيمكنا تقدير الثبات اوميجا، يتضح أن الفا للنسخة المختصرة للمقياس كانت قيمة المعامل ألفا= 0.888 ,وقيمة المعامل اوميجا = 0.913 ، ولكن علينا الاخذ في الاعتبار ان تلك الصيغة المختصرة لها اقتصادية في عدد المفردات واختصار للوقت التطبيق.

التعليق على النتائج:

تناول البحث الحالي ترجمة وتكيف مقياس الامن النفسي السيبراني في البيئة العربية : دراسة تقويمية، وسعى البحث لتقنين ذلك المقياس، وقد تم استخدام عدد مناسب من الافراد، وكما تم تقدير الخصائص السيكومترية في ضوء مؤشرات معامل إرتباط المفردة بالدرجة الكلية وكذلك معامل الإرتباط المصحح, وثبات المقياس بعد إستبعاد المفردة ، فيتضح أن معامل الارتباط لكل المفردات (0.5) تقريبا ماعدا المفردة الاولي في البعد الأول، والمفردة السابعة في البعد الثاني، وفي البعد الثالث المفردتان الاولي والأخيرة، بينما زادت قيم معامل الارتباط المصحح لكل المفردات عن 0.50 مما يدل على الارتباط المرتفع للمفردات بالبناء العام للأمن النفسي السيبراني، وأيضًا تم حساب نتائج التحليل العاملي الاستكشافي حيث عبر عن تشبع جيد جدًا بالعامل العام او البناء التحتي مما يدل على قدرة تمييزية مرتفعة للمفردات، أما بالنسبة لقيم الشيوع فتجاوزت لكل المفردات 0.50 بمعني أن البناء التحتي فسر 50% من تباين كل المفردات ما عد المفردتين الاولي في البعد الأول، والأخيرة في البعد الثاني.

وأسفرت نتائج البحث عن توافر شروط سيكومترية مقبولة بل ومرتفعة وفقا للشروط الموضوعة، حيث يتوفر في المقياس شرطي أحادية البعد والاستقلال الموضعي، وذلك حقق صدق المفهوم أو البناء.

وأشارت نتائج السؤال الأول إلى أن معظم المفردات استطاعت الكشف عن مستويات مختلفة من للهجمات وانتهاك الخصوصية الرقمية و السلوكيات علي السوشيال ميديا والأداء النفسي على الانترنت، هذا وأشارت نتائج دراسة Granger, (2001) أن صاحب تطور وسائل الاتصال الحديثة وتكنولوجيا المعلومات والاتصالات، إلى ظهور تقنيات حديثة في الاجهزة الذكية، كما أدى ذلك إلى سهولة نقل وتبادل المعلومات والمعارف، وتطور التقنية الحديثة لا يخلو من المخاطر، لإنها أداة تتشكل بطرق متعددة إما لتحقيق أهداف إيجابية لخدمة المجتمع والاشخاص، أو لظهور الجرائم المعلوماتية في الفضاء السيبراني، وهذا ما سعي البحث إلى إبرازه والتحقق منه.

وبحساب المتوسط المرجح او الموزون mean weightedكمعيار للحكم وبالاعتماد على مجموع الإجابات عن كل فقرة من فقرات القائمة، والذي بلغ (368) وبقوة نسبية (82%) وفي المجمل يتضح وجود درجة معقولة من التناسب في تكرارات الاستجابات الثلاثة لمفردات المقياس وعليه لا يمكن اختصار بدائل الاستجابة الثلاثة إلى عدد أقل من الاستجابات، مما يدعم جودة تصميم بدائل الاستجابات لمفردات القائمة.

وبالتحقق من مؤشرات جودة المفردات وقد تم تقدير معامل ثبات الاتساق الداخلي الفا كرونباخ للمقياس وبلغت قيمته 0.884 بينما بلغت قيمة المعامل اوميجا 0.931

وفي ضوء مؤشري معامل ارتباط المفردة بالدرجة الكلية ومعامل الارتباط المصحح (معامل ارتباط المفردة بالدرجة الكلية مستبعدة منه درجة المفردة) يتضح أن معامل الارتباط لكل المفردات 0.5 تقريبا، بينما زادت قيم معامل الارتباط المصحح لكل المفردات عن 0.50 مما يدل على الارتباط المرتفع للمفردات بالبناء العام للأمن النفسي السيبراني، أما التشبعات لكل المفردات زادت عن 0.63 حيث يعبر عن تشبع جيد جدًا بالعامل العام او البناء التحتي مما يدل على قدرة تمييزية مرتفعة. أما بالنسبة لقيم الشيوع فتجاوزت لكل المفردات 0.50 بمعني أن البناء التحتي فسر 50% من تباين كل المفردات ما عد المفردتين الاولي في البعد الأول، والأخيرة في البعد الثاني.

هذا وأكدت الدراسات Suler, (2004)، Elhai & Rozgonjuk, (2020) على ظهور علم النفس السيبراني هو مجال جديد – نسبيًا – في تخصص علم النفس، وأنه ليس مصطلحًا شائعًا يستخدمه الناس حيث أنه يهدف إلى دراسة الأفراد والمجتمعات والتقنيات الرقمية والجوانب النفسية وتفاعلاتهم، كما أنه يقيم كيفية استخدام الناس للتكنولوجيا للتفاعل في الفضاء السيبراني وكيف تؤثر هذه التفاعلات على حياتهم في العالم الحقيقي أو العالم الغير المتصل. كما انه بمثابة مظلة كبيرة تغطي الموضوعات الفرعية التي يجب دراستها ، والتي تندرج تحت علم النفس السيبراني .وبالتالي ، من المهم معرفة ما هو علم النفس السيبراني

وأهميته في السنوات القادمة، وأصبح دوره في منع الهجمات الإلكترونية موضوعًا مهما وخصوصا عند مناقشة استراتيجيات الدفاع السيبراني، كما أصبح استخدام علم النفس السيبراني لفهم كيفية تأثير التقنيات الناشئة على حياة الناس مجالًا مهمًا في عصر المعلومات اليوم.

وتم إجراء التحليل العاملى على إجابات أفراد العينة عن مفردات مقياس الامن النفسي السيبراني، وذلك لمعرفة عدد العوامل التى يزيد قيم الجذر الكامن لها عن الواحد الصحيح، وقد تحقق شروط التحليل العاملى تم استخدام التحليل العاملى الاستكشافى بطريقة المكونات الأساسية (Principle components) لاستجابات الطلاب عن مفردات المقياس، وعند الكشف عن مؤشرات حسن المطابقة والتحقق من الصدق العاملي التوكيدي للبناء الاصلي الذي افترضه Pekurn et al. (2005)، للتحقق من هذا تم اجراء التحليل العاملي التوكيدي للمفردات 32في برنامج MPLUS(7) ، واتضح ان مؤشرات حسن المطابقة هي كاي تربيع= 956.513, df=170,p=0.00 ومؤشر RMSEA=0.093 ومؤشر TLI=0.833 ومؤشر CFI=0.851 وكان لهذا النموذج اقل قيمة لمؤشر المعلومات الاكيكي مما يؤكد تفوق هذا النموذج.

في العديد من الحالات، قد يكون من الصعب التمييز بين حادثة التنمر عبر الإنترنت وحادثة تتعلق بالأمن السيبراني .كما هو الحال مع عدد من حوادث الأمن السيبراني، فإن بعض المتنمرين عبر الإنترنت يحددون دافعهم الأساسي ببساطة أنهم يجدونها مضحكة كما أن لتأثير عدم الكشف عن الهوية وحجب الهوية ونزع الشخصية أهمية خاصة في مثل هذه الحوادث.(Slonje, & Smith, 2008)

في محاولة لتعزيز ثقافة الوعي الأمني بين الموظفين، كان هناك تحول في التفكير، تركز هذه الطريقة الجديدة على تعليم الشخص المناسب في الوقت المناسب بالطريقة الصحيحة للتحريض على التغيير في السلوك .أوضحأ" :Lee–Yow أن تتمثل الخطوة الأولى في تدريب cyberconIQ الذي نستخدمه في فهم ملفك الشخصي "مثل. هل تميل إلى اتباع القواعد أم أنك ربما قليلا من المجازفة؟ & ,Corradini (Corradini, 2020).

توصيات البحث المقترحة:

1- في ضوء نتائج البحث الحالي توصي الباحثة بأهمية الاخذ بنتائج المقياس المعد، حيث انه الفريد من نوعة في البيئة العربية والاجنبية، ولما يتصف به من شروط الصدق والثبات، كما تم التأكد من ذلك في ضوء افتراضات النظرية الحديثة في القياس النفسي.

2- التوسع في استخدام نماذج راش وغيرها من نماذج نظرية الاستجابة للمفردة، لما يتوفر بها من شروط تحقق قدر عالي من الدقة والموضوعية لادوات القياس.

يجب توظيف معلومات وظيفة المفردات في نظرية الإستجابة المفردة للوصول إلى صيغة مختصرة للمقياس من خلال سلوك منحنى وظيفة المفردات ومدي اقترابها أو ابتعادها عن البناء التحتي للمفهوم، وأيضًا مدي تماثل سلوك منحنيات معلومات المفردات.

المراجع:

سعيد، خالد. (2022). أثر علم النفس السيبراني ودوره في اكتشاف الأفكار اللاعقلانية من وجهة نظر المختصين في علم النفس بمدينة الرياض. مجلة الجامعة العراقية، 54(2)،400-413، مسترجع من http://mandumah.search.com/Record/1273635

عامر، عبد الناصر. (2019). *بناء الاختبارات والمقاييس النفسية: الأسس والتطبيقات. الرياض*: مكتبة العبيكان الرقمية.

عامر، عبد الناصر. (2023). التقويم السيكومتري للمقاييس النفسية باستخدام نظرية الاختبار الكلاسيكية و نظرية الاستجابة المفردة والوظيفة التمييزية للمفردات: مقياس الخوف من جائحة كورونا(COVID-19). مجلة الدراسات والبحوث التربوية بالكويت، العدد السابع.

Acquisti, A. (2004, May). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce* (pp. 21-29).

Ahuja, V., & Alavi, S. (2017). Cyber psychology and cyber behaviour of adolescents-the need of the contemporary era. *Procedia computer science*, *122*, 671-676.

Allen, M., & Yen, W. (2002). Introduction to measurement theory. Long Grove, IL: Waveland Press. (Original work published 1979).

Ancis, J. R. (2020). The age of cyberpsychology: An overview. *Technology, Mind, and Behavior*.

Attrill-Smith, A., Fullwood, C., Keep, M., & Kuss, D. J. (Eds.). (2019). *The Oxford handbook of cyberpsychology*. Oxford University Press.

Barnes, L. L., & Wise, S. L. (1991). The utility of a modified one-parameter IRT model with small samples. *Applied Measurement in Education*, *4*(2), 143-157.

Burgard, A., & Schlembach, C. (2013). Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet. *International Journal of Cyber Criminology*, *7*(2).

Cisco (2018). Annual Cybersecurity Report.Retrieved from https://www.cisco.com/c/dam/m/digital/elqcmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=

Comrey, A., & Lee, H. (1992). *A first course in factor load analysis (2nd ed.).* New York, NY: Erlbaum.

Corradini, I., & Corradini, I. (2020). Redefining the approach to cybersecurity. *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology*, 49-62.

De Ayala, R. J. (2022). *The theory and practice of item response theory* (2nd.ed). New York, NY: Guilford.

DeVellis, R. F. (2017). *Scale development: Theory and applications* (4th.ed*)*. Los Angeles: SAGE Publications, Inc

Edelen, M. O., & Reeve, B. B. (2007). Applying item theory (IRT) modeling to questionnaire development, evaluation, and refinement. *Quality of Life Research*, *16*, 5-18. doi:10.1007/s11136-007-9198-0

Edwards, M. C. (2009). An introduction to item response theory using the need for cognition scale. *Social and Personality Compass*, *3*, 507-529. doi:10.1111/j.1751-9004.2009.00194.x

Elhai, J. D., & Rozgonjuk, D. (2020). Editorial overview: Cyberpsychology: reviews of research on the intersection between computer technology use and human behavior. *Current opinion in psychology*, *36*, iv-vii.

Embretson, S. E., & Reise, S. P. (2000). *Item response theory for psychologists.* New York, NY: Psychology Press.

Field, A. (2013). *Discovering statistics using SPSS (4th.ed).* Sage Publications.Ltd.

Ghosh, S., & Turrini, E. (Eds.). (2010). *Cybercrimes: A multidisciplinary analysis*. Springer Science & Business Media.

Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. *Security Focus, December*, *18*.

Hambleton, R. K., Swaminathan, H., & Rogers, H. J. (1991*). Fundamentals of item response theory.* Newbury Park: Sage.

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research*, *37*(5), 858-873.

Joinson, A. N. (2007). Disinhibition and the Internet J. Gackenbach (Ed.), Psychology and the internet: Intrapersonal, interpersonal and transpersonal implications.

Keepers, G. A. (1990). Pathological preoccupation with video games. *Journal of the American academy of child & adolescent psychiatry*, *29*(1), 49-50.

Khera, V. (2018). *A study of cybersecurity for telecommunication services concerning smartphone users in Thailand* (Doctoral dissertation, Murdoch University).

Kirwan, G. (Ed.). (2011). The Psychology of Cyber Crime: Concepts and Principles: Concepts and Principles.

Lord, F., Novick, M., & Birnbaum, A. (1968). *Statistical theories of mental test scores*. England: Oxford, Addison-Wesley.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Morewedge, C. K., Gilbert, D. T., & Wilson, T. D. (2005). The least likely of times: How remembering the past biases forecasts of the future. *Psychological Science*, *16*(8), 626-630.

Mumford, G. (2009). Preventing cyber-attacks. www.apa.org/monitor/2009/09/cyber-attacks.aspx (Dec. 17, 2013)

Nunnally, J. C,& Bernstein, I. H. (1994). *Psychometric theory (3rd. ed*). New York, NY: McGraw-Hill.

Romansky, R. (2014, September). Digital privacy in the network world. In *Proceedings of the International Conference on Information Technologies (InfoTech-2014)* (pp. 18-19).

Samejima, F. (1969). *Estimation of latent ability using a response pattern of graded scores* (Psychometric Monograph No. 17, Part 2). Richmond, VA: Psychometric Society.

Samejima, F. (1997). *Graded response model. In Handbook of modern item response theory* (pp. 85-100). New York, NY: Springer.

Singh, A. K., & Singh, P. K. (2019). Recent Trends, Current Research in Cyberpsychology: a literature review. *Library Philosophy and Practice*, NA-NA.

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying?. *Scandinavian journal of psychology*, *49*(2), 147-154.

Suler, J. (2004). The online disinhibition effect. Cyberpsychology & Behavior, 7(3), 321-326. https://doi.org/10.1089/1094931041291295

Elhai, J. D., & Rozgonjuk, D. (2020). Editorial overview: Cyberpsychology: reviews of research on the intersection between computer technology use and human behavior. *Current opinion in psychology*, *36*, iv-vii.

Suler, J. R. (2016). Psychology of the digital age: Humans become electric. Cambridge University Press. https://doi.org/10.1017/CBO9781316424070

Taylor, J., McAlaney, J., Hodge, S., Thackray, H., Richardson, C., James, S., & Dale, J. (2017, April). Teaching psychological principles to cybersecurity students. In *2017 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1782-1789). IEEE.

Thackray, H., McAlaney, J., Dogan, H., Taylor, J., & Richardson, C. (2016). Social psychology: An under-used tool in cybersecurity.

UNODC. (2013) Comprehensive study on cybercrime. www.unodc.org/documents/organized crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed Dec. 16, 2022).

van Marken, Jacob C. (1894) 'Sociale ingenieurs,' in: *Delftsche Corps-Almanak*, pp. 155-170.

Wang, W. E. I. (2001). Internet dependency and psychosocial maturity among college students. *International journal of human-computer studies*, *55*(6), 919-938.

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

Wynn, R., Jonkman, M., Iverson, D., Munt, M., Milefsky, G. S., Evans, J., ... & Pinto, E. (2012). Copyright© 2012 Hakin9 Media Sp. z oo SK.

Young, K. S., & Case, C. J. (2004). Internet abuse in the workplace: new trends in risk management. *CyberPsychology & Behavior*, *7*(1), 105-111.

Young, K. S., & Rogers, R. C. (1998). The relationship between depression and Internet addiction. *Cyberpsychology & behavior*, *1*(1), 25-28.

ملحق (1)

السيد الفاضل المحترم/

السلام عليكم ورحمة الله وبركاته

يقوم الباحث بدراسة للامن النفسي السيبراني لعينة في المجتمع العربي والمقياس مكون من عدة مفردات او عبارات وامام كل عبارة ثلاثة بدائل للاستجابة، اختار البديل الذي يتناسب معك. وبيانات هذه المقاييس تتسم بالسرية التامة وتستخدم لاغراض البحث العلمي

ارجو مساعدتي في الإجابة ع المقاييس

- **تفاصيل شخصية**

1) العمر:

- 20-15
- 25-20
- 30-25
- 40-30
- 50-40
- 60-50
- 70 فأكثر

2) النوع:

- ذكر
- أنثى

حالتك الاجتماعية:

- متزوج
- أعزب
- مطلق
- أرمل

3) جنسيتك:

- مصري
- سعودي
- مغربي
- تونسي
- جزائري
- أخري

إذا كانت إجابت على الجنسية ب أخري ، إذكر ما هي جنسيتك

4) **التعليم:**

- أقل من 12 عاما من الدراسة
- تعليم ثانوي
- تعليم فني
- بكالوريوس
- ماجستير
- دكتوراه

5) **هل أنت تعمل:**

- نعم
- لا

6) **حدد راتبك الشهري:**

- 2000-1000
- 3000-2000
- 4000-3000
- 7000-5000
- 10000-8000
- أكثر من 10000
- أخري

7) **كم عدد الساعات التي تقضيها على الانترنت؟**

- 3 ساعات-4 ساعات

- 5 ساعات–6 ساعات
- 7 ساعات–9 ساعات
- 10 ساعات –15 ساعة
- أخري

إذا كانت كانت إجابتك ب أخري، إذكر عدد الساعات؟

8) هل لديك حساب فيس بوك؟

- نعم
- لا

9) أكثر مواقع Social Media التي تستخدمها

متاح اختيار أكثر من موقع

- Facebook
- Twitter
- Instagram
- Linked in
- VK
- Tik tok
- أخري
- أذكرهم

الامن النفسي السيبراني

هل سمعت عن مصطلح الهندسة الاجتماعية؟

- نعم
- لا

➢ **مصطلحات الهندسة الاجتماعية:**

(متاح اختيار أكثر من مصطلح)

1– فن اختراق العقول.

2- انتهاك الخصوصية.
3- الامن المعلوماتي.
4- الاختراق الرقمي.
5- انتحال الهوية.
6- التصيد الالكتروني.
7- الاحتيال الالكتروني.phishing
8- الاحتيال الصوتي Vising عبر الهاتف.
9- الرسائل الاقتحامية المزعجة Spam.

- **هجمات الهندسة الاجتماعية:**

1- تعرضت للاختراق من خلال طلب كلمة المرور الخاصة بك.
2- تعرضت للاختراق من خلال طلب تحميل برمجيات معينة على أجهزتك الخاصة.
3- تعرضت للاحتيال من خلال رسائل البريد الالكتروني عن طريق طلب التحقق من معلوماتك المسجلة في بنكك الخاص.
4- تعرضت للاحتيال عن طريق رسائل آلية تطلب منك ادخال رقم بطاقتك الائتمانية.
5- تعرضت للاحتيال من خلال اتصال هاتفي من شخص يدعي انه موظف في البنك ويطلب التحقق من بياناتك.
6- تعرضت للاختراق من رسائل Spam كتهنئة من صديق.
7- تعرضت لسرقة كلمة المرور الخاصة بك ومعلومات مهمة.
8- تعرضت للاحتيال من خلال رمي أوراق مهمة في سلة المهملات.
9- تعرضت للاختراق من خلال اتاحة معلوماتك المهنية وبريدك الالكتروني على مواقع التواصل الاجتماعي.
10- تعرضت للاحتيال من خلال الرد على رسائل على مواقع الفيس بوك لاشخاص لم اعرفهم.

- **انتهاك الخصوصية الرقمية:**

1- تعرضت لسرقة الهوية الرقمية (عمل أكونت بصوري ومعلوماتي الشخصية) من خلال الفيسبوك
2- تعرضت للتصيد الالكتروني والترصد من خلال الفيس بوك
3- تعرضت لاختراق معلوماتي على موقع الفيس بوك وسرقه الصفحة الشخصية.
4- تعرضت لسرقة حسابي البنكي بسبب شرائي من مواقع الفيس بوك

5- تعرضت لتطبيق مزيف على الفيس بوك واكتشفت انه يسرق بياناتي عند إدخالها.
6- موقع الفيس بوك يخترق الخصوصية لمستخدميه.
7- تعرضت للسرقة من خلال استخدام الإعلانات التي تظهر لك على الفيس بوك.
8- تعرضت للتصيد من خلال عدم إلغائي لخاصية التتبع الجغرافي على الفيس بوك
9- تعرضت لسرقة بياناتي من خلال استخدامي للتطبيقات الاجتماعية مثل (شكلك بعد30 سنه- شكل شريك حياتك) المنشورة على الفيسبوك.
10- تعرضت لسرقة حسابي بسبب دخولي على حسابي من أجهزة غير شخصية.

- **السلوكيات على السوشيال ميديا والأداء النفسي على الانترنت**

1- أمتلك مهارة لحل مشكلاتي من الادوات الرقمية مثل (عرض مشكلتي على جروبات فيس بوك)
2- أتحمل مسؤولية سلوكي عند استخدام الانترنت
3- أفعل إجراءات إلكترونية تشعرني بالأمان عند الاتصال بالأنترنت
4- استخدم التكنولوجيا بما يناسب تقاليدي
5- أحافظ على معلوماتي الخاصة والوظيفية
6- عند نشر أي معلومات رقمية عني سيؤثر ذلك على شخصيتي
7- أعرف كيفية الالتزام بالآداب الرقمية (أي لا أقوم بأعمال مخله) عند استخدام التكنولوجيا
8- عند نشر أي معلومات رقمية عني سيؤثر ذلك على وظيفتي
9- من السهل بالنسبة لي البحث عن وظيفية على مواقع سوشيال ميديا
10- أفضل البحث على مواقع سوشيال ميديا فيما يتعلق بالجانب المهني
11- السوشيال ميديا أداه فعاله للبحث عن وظيفية
12- في المستقبل، أذا كنت أرغب إذا كنت أرغب في البحث عن وظيفية سوف أستخدم موقع السوشيال ميديا