مجلة كلية التربية

دور الجامعات المصرية في توعية طلابها بمخاطر الهندسة الاجتماعية (دراسة ميدانية–جامعة أسيوط)

The Role of Egyptian Universities in Raising Awareness among Their Students about The Dangers of Social Engineering

(A field study – Assiut University)

اعداد

د. علي محمد يحي علي

مدرس أصول التربية

كلية التربية –جامعة أسيوط

مستخلص البحث:

هدف البحث إلى تقديم تصور مقترح لتفعيل دور الجامعة في توعية طلابها بمخاطر الهندسة الاجتماعية، وسبل مواجهتها، واستخدم البحث المنهج الوصفي، وقد تم استخدام الاستبانة كأداة للحصول على أراء أعضاء هيئة التدريس، ومعاونيهم؛ بلغ عددهم(٢٦١) عضوا ممثلا من كليات نظرية وعملية، وهي(التربية، التربية للطفولة المبكرة، التمريض، الزراعة)؛ لتعرف واقع دور الجامعة في توعية طلابها بمخاطر الهندسة الاجتماعية، من خلال الإدارة والمعلم الجامعي، والمقررات والأنشطة الجامعية، وتوصل البحث إلى ضعف دور الجامعة في تحقيق ذلك، ومن ثم قدم البحث تصوراً مقترحاً قد يفيد في تفعيل ممارسات الإدارة الجامعية في توعية طلابها بالهندسة الاجتماعية، وتفعيل دور أعضاء هيئة التدريس، وتجديد المقررات والابتكار في الأنشطة الطلابية؛ حتي تستطيع تأدية الدور المناط منها في تحقيق وعي الطلاب بمخاطر الهندسة الاجتماعية وغيرها من صور الهجمات السيبرانية.

الكلمات مفتاحية: الأمن السيبراني– الجامعات المصرية –الهندسة الاجتماعية.

The Role of Egyptian Universities in raising awareness among Their Students about the Dangers of Social Engineering (a field study - Assiut University)

Abstract:

The research aimed to present a proposed vision to activate the role of the university in raising awareness of its students about the dangers of social engineering, and ways to confront it. The research used the descriptive approach, and the questionnaire was used as a research tool to obtain the opinions of faculty members and their assistants; their number reached (261) members representing theoretical and practical colleges, namely (Education, Early Childhood Education, Nursing, Agriculture); to know the reality of the university's role in raising awareness of its students aboutthe dangers of social engineering, through the administration and university teacher, university courses and activities. The research concluded that the university's role in achieving this is weak, and then the research presented a proposed vision that may be useful in activating university administration practices in raising awareness of its students about social engineering, activating the role of faculty members, renewing courses and innovating in student activities; so that it can perform the role assigned to it in achieving student awareness of the dangers of social engineering and other forms of cyber-attacks.

Keywords: Cybersecurity, Egyptian universities, social engineering.

أولا: الإطار العام للبحث:

مقدمة:

لقد أصبحت التقنية أكثر اختراقاً لحياتنا اليومية، وأصبحنا نعتمد عليها في كل صغيرة وكبيرة، وأصبحت الشبكة هي المسيطر الأكبر على حياتنا؛ فهناك الكثير من البرامج والتقنيات والأقفال المادية والتقنية، وكم من كبير من الأمن البشري يحيط بالمؤسسات؛ وذلك لتحقيق الأمن المعلوماتي لها، ولكنها على الرغم من ذلك فإنها مازالت غير آمنة، وما زال الأمن المحيط به وهماً بإمكانهم اجتيازه عن طريق الخيط الأضعف في أمن المعلومات" الإنسان" عن طريق التحايل عليه، واستغلال طبيعته البشرية التعاونية لأغراضهم الخاصة، وهو ما يسمى "بالهندسة الاجتماعية" التي باتت اليوم أساساً لمعظم الهجمات الإلكترونية مجهولة المصدر ومعقدة التعقيب.

وتدور الهندسة الاجتماعية حول سيكولوجية الإقناع، التي يتم استهداف العقل البشري من خلالها، ويتمثل هدفها في كسب ثقة الأشخاص ليتخلوا عن حذرهم، بالإفصاح عن بيانات سرية أو شخصية، يستخدمها المهندس الاجتماعي في اختراق الحسابات وتنفيذ عمليات القرصنة؛ مما يعرضهم للابتزاز وإلحاق الضرر بهم. (عبد الرحمن، ٢٠٢٢، ١٥٥٣)

ونتيجة لإتاحة هذه التقنية والاستخدام المكثف للتكنولوجيا ووسائل الإعلام الاجتماعية في أوساط الطلبة الجامعيين؛ يجعلهم أكثر المجموعات عرضة للانتهاكات وللتهديد والإذلال والتهكم اللفظي والاعتداء المعنوي والإحراج من أي شخص عبر شبكات التواصل الاجتماعي، مما يجعل الهندسة الاجتماعية من أبرز التحديات على المجتمعات والأفراد؛ إذ يعد خداع البشر مهمة أسرع وأكثر كفاءة من اختراق شبكات الحاسب الآلي، واختراق الأمن الإلكتروني (Wang et al., 2021, 15).

ولأن دور الجامعة قد تطور واتسع في العصر الحديث ولم يعد مجرد تخريج عدد من المهندسين والأطباء والمعلمين وغيرهم، بل أصبحت قائدة لخطى التطور والتقدم؛ بما تكشفه من حقائق وما تسهم فيه من حلول للمشكلات الراهنة والمستقبلية، وتسهم في مواجهة تحديات العصر ومتطلباته ونشر المعرفة وتوسيع أفاقها، وهو ما

يفرض عليها أدواراً مضاعفة في توعية طلابها بثقافة الأمن المعلوماتي، ومخاطر الهندسة الاجتماعية، وكيفية الوقاية منها، وهو ما أكدته العديد من الدراسات والأدبيات، مثل دراسة (Mangold, 2016) والتي أكدت على ضرورة إكساب الطلاب الجامعيين الوعي، وزيادة معرفتهم بمفاهيم بالأمن السيبراني، وأوصت بإقامة الدورات التدريبية الخاصة بالأمن السيبراني، وإقامة المعسكرات السيبرانية لتلبية الطلب المتزايد على المختصين في الأمن السيبراني.

ودراسة محمد (٢٠١٦) التي بينت أن للمؤسسات التعليمية دوراً كبيراً في تحقيق الأمن داخل المجتمعات، والتصدي للجرائم الحديثة: كجرائم الإرهاب الإلكتروني، التي تعد من أبرز سلبيات التطور الهائل في الجرائم المعلوماتية، ولهذه المؤسسات أيضا دور وقائي في درء الفساد وارتكاب الجريمة، وذلك بغرس الأخلاق، والقيم، والسلوك، والمنهج الصحيح في نفوس طلبتها،

واتفقت هذه الدراسات مع دراسة (Lehto, 2018) التي أشارت إلى أنه: على الجامعات تطبيق الأمن السيبراني؛ لحماية البيانات والمعلومات والوثائق المهمة التي تخزن في أجهزتها، وأهمية تدريس الأمن السيبراني في الجامعات؛ لأهميته في حماية الأفراد والمؤسسات من المخاطر المختلفة وخاصة الهندسة الاجتماعية.

وتزامن مع هذه الدراسة دراسة العريشي، الدوسري (٢٠١٨) التي أكدت أن دور الجامعة في تعزيز أمن المعلومات في المجتمع يمكن تحقيقه من خلال تنمية الفكر الثقافي بأهمية أمن المعلومات، والاسهام في توعية المجتمع بالمخاطر السيبرانية وتهديداتها، وكذلك دراسة Wijayanto & Prabowo (2020) التي أكدت على أن الحاجة إلى الوعي بالأمن السيبراني وتطبيقاته وبرامجه أصبحت أكثر إلحاحاً؛ في ظل الظروف التي تواجه العالم.

ودراسة (Redman,S.& Joiner (2020التي أكدت أن تنمية الوعي بمفاهيم الأمن السيبراني، ومخاطر الهندسة الاجتماعية يكون بإعداد مقرر يدرس مبادئ الأمن السيبراني.

ومما سبق يتضح أن الهندسة الاجتماعية شكلت تهديدا خطيرا لأمن الفضاء الإلكتروني، وأدت لحدوث تداعيات كثيرة على الفئة المستهدفة من الشباب وخاصة الجامعي؛ وللحماية من هجمات الهندسة الاجتماعية ، فإنه من الضرورة معرفة ماهية الهندسة الاجتماعية؛ حيث يستغل المهاجمون عدم معرفة الضحية بالرقمنة، وكيفية تجنب المخاطر عند التعامل مع الانترنت، وبالتالي فهناك حاجة ماسة لتعزيز الوعي المعرفي بمفهوم الهندسة الاجتماعية، ومخاطرها، وأساليبها، واستراتيجيات الحماية منها، وهنا يظهر أهمية دور الجامعة في توعية طلابها بذلك وتوعيتهم بالأمن السيبراني بصفة خاصة من خلال التدريس، والبحث العلمي، وخدمة المجتمع، وأن تعمل على نشر المعرفة وإثراء المهارات العلمية في أمن المعلومات؛ بهدف مكافحة الانتهاكات والهجمات التي تسببها أساليب الهندسة الاجتماعية، كما يجب على أعضاء هيئة التدريس توعية الطالب وتحذيرهم من التهديدات الإلكترونية.

مشكلة البحث:

أن القيم التي يكتسبها الشباب الجامعي لم تعد مرجعيتها مؤسسات التنشئة الاجتماعية لوحدها، بل رافقتها وسائل الاتصال الرقمي، وهو ما زاد لديهم حالة عدم الاستقرار بين القيم الموروثة والقيم المكتسبة، فأصبح للشباب مؤسسات افتراضية مختلفة تشارك وبقوة في تنشئتهم الاجتماعية؛ مما يهدد مرجعيتهم من حيث العلاقات الأسرية والاجتماعية وانتشار ظاهرة العزلة. والمتتبع للمشهد الحالي يرى جليا اعتماد المؤسسات، والدوائر العامة والخاصة على تكنولوجيا المعلومات، ناهيك عن وجودها بين الأسر والمجتمعات، وقد ظهر بشكل واضح أفراد مبدعون في مجال الانترنت والتكنولوجيا، لكن منهم من وظف إبداعه لغايات مخالفة للمبادئ والقوانين الدولية والعامة، وهي ما عرف فيما بعد بالقرصنة الإلكترونية أو الهاكر، والذي يطلق عليه اليوم: الجريمة الإلكترونية، والإرهاب الإلكتروني، وغيرها، وظهور أنماط جديدة لها على المستويات: الوطنية، والإقليمية، والعالمية، فزادت معاناة دول العالم من النشاطات الإرهابية، وزادت خطورة هذه النشاطات الإجرامية إلى درجة فاقت قدرات الدول قاطبةً على المواجهة، بما في ذلك الدول الكبرى بوعلي(٢٠١٩، ١٨٤) . مما استوجب على

الدول وكافة مؤسساتها حماية مواطنيها ومؤسساتها المختلفة من هذا النوع من الجرائم، ومن هؤلاء الأشخاص المستغلين إتقانهم للكفاءات التكنولوجية في الإضرار بغيرهم ممن لا يملكون مهارات التعامل مع التكنولوجيا، أو يفقدون الوعي بخطورة الجرائم الإلكترونية، وكيفية التعامل معها.

كذلك المتتبع لحال الطلبة الجامعيين يجد أنهم ليسوا على دراية بمصطلح الهندسة الاجتماعية على الرغم من تعرضهم لأساليبها ومخاطرها؛ وذلك نتيجة لما يشهده العالم المعاصر من تطورات سريعة في تقنيات المعلومات والاتصالات أفرزت تقنيات وتطبيقات رقمية وأجهزة مختلفة سهلت سرعة عمليات التواصل والوصول بين أفراد مجهولين رقميين قد يشكلون خطراً على الجيل فكراً وسلوكاً، وفى ظل تعذر مراقبة الأجيال وما يطلعون عليه فيها من مواقع مشبوهة وخطيرة أو يتبنون أفكارا وسلوكيات تخالف تعاليم الدين وقيمه وأخلاقه وتتعارض مع الثوابت المجتمعية والوطنية تأتى أهمية تعرفهم على كيفية مواجهة مخاطر الفضاء السيبراني.

وقد أجرى الباحث دراسة استكشافية لآراء بعض طلاب كليات جامعة أسيوط العملية والنظرية، حول معرفتهم بمصطلح الهندسة الاجتماعية، والإجراءات التي تتخذها الجامعة لتوعيتهم بمخاطرها، وطرق الوقاية منها، اتضح من خلالها ضعف وجود مقررات دراسية اجبارية أو اختيارية تقدم معلومات عن الهندسة الاجتماعية، وأساليبها ومخاطرها، والأمن السيبراني، أو المخاطر والهجمات السيبرانية، كما لا توجد منتديات أو لقاءات لتعريف الطلاب بمخاطر الهندسة الاجتماعية وأنواعها، كما أن الأنشطة الطلابية التي تقام في الجامعة أنشطة تقليدية نمطية تخلو من أي ممارسات أو مسابقات تنافسية عن أفضل الطرق للتعامل الآمن مع الانترنت والتصدي للمهندسين الاجتماعيين وهجمات التصيد والانتحال التي يمارسوها.

وجاءت دراسة الكندي؛ البلوشي(٢٠٢١، ٧٢) لتؤكد ضعف مستوى دراية الطلبة بمفاهيم الهندسة الاجتماعية وأساليبها، وأن الغالبية من عينة الدراسة لديهم وعي ببعض الممارسات التنظيمية والتقنية للوقاية من أساليب ومخاطر الهندسة الاجتماعية بطريقة غير مباشرة. وكذلك دراسة جعفر(٢٠٢٣، ٨٣) التي أوضحت ارتفاع نسب

المتأثرين بأساليب الهندسة الاجتماعية من الطلبة الجامعيين؛ على الرغم من ادراكهم لأهمية أمن المعلومات.

ودراسة العمري؛ العمري(٢٠٢٤،٣) التي أكدت على ضعف وعي عينة الدراسة من الطلبة بكلية التعليم التكنولوجي بمفهوم الهندسة الاجتماعية، بينما كان لديهم وعي بحماية بياناتهم ومعلوماتهم الشخصية في مواقع التواصل.

ودراسة صالح؛ أحمد(٢٠٢٥،٨٤) التي أكدت تعرض العديد من الأسر للهجمات الإلكترونية، وأن أكثر أشكال هجمات الهندسة الاجتماعية الرقمية هي اتصال هاتفي يطلب بعض البيانات الشخصية، يليه سرقة الأموال من حساب أحد أفراد الأسرة، وارسال روابط خبيثة عبر الواتساب والفيسبوك.

ما يجعلنا نلمس تأثر الأجيال بالتقنيات الرقمية في العالم الافتراضي، حيث يستمدون منها بعض الأمور السلبية والثقافات الخاطئة؛ كتعرضهم للجرائم والاحتيال الإلكتروني والابتزاز والقرصنة والتنمر وسرقة البيانات، وعرض ما يتعارض مع القيم وغيرها، والتي تمثل جميعها أساليب للهندسة الاجتماعية. لذا تبرز أهمية تعرف دور الجامعات المصرية في توعية طلابها بالهندسة الاجتماعية ومخاطرها.

تساؤلات البحث:

لتحقيق الهدف الرئيس التي يسعي البحث لتحقيقه، والمتمثل في معرفة دور الجامعات المصرية في توعية طلابها بمخاطر الهندسة الاجتماعية، لا بد من الإجابة عن التساؤلات التالية:

- ما الإطار الفكري للهندسة الاجتماعية؟
- ما الإطار الفكري لدور الجامعات المصرية في توعية طلابها بمخاطر الهندسة الاجتماعية؟
- ما واقع دور جامعة أسيوط في توعيها طلابها بمخاطر الهندسة الاجتماعية؟
- ما التصور المقترح لتفعيل دور الجامعات المصرية في توعية طلابها بمخاطر الهندسة الاجتماعية؟

أهداف البحث:

يسعى البحث الحالي إلى تحقيق العديد من الأهداف أهمها ما يلي:

– توضيح الإطار المفاهيمي والفكري للهندسة الاجتماعية.

– عرض الإطار الفكري لدور الجامعة في إذكاء الوعي بالمخاطر التي تسببها الهندسة الاجتماعية كأحد صور التهديدات السيبرانية.

– الكشف عن واقع دور جامعة أسيوط في تحقيق الأمن السيبراني لدى طلابها.

– تقديم تصور مقترح لتفعيل دور جامعة أسيوط في توعية طلابها بمخاطر الهندسة الاجتماعية.

أهمية البحث:

تتضح أهمية البحث الحالي من:

أ– أهمية نظرية وتتمثل في:

– تقديمه إطار فكرى ومفهومي عن الهندسة الاجتماعية ومخاطرها.

–توضيحه لدواعي الاهتمام بدور الجامعة في توعية طلابها بمخاطر الهندسة الاجتماعية، وكيفية تفعيل دورها في تحقيق الأمن السيبراني لدى منسوبيها ومؤسساتها التعليمية؛ باعتباره الدرع الواقي لمخاطر الهندسة الاجتماعية.

–استجابة للعديد من التوصيات للمؤتمرات والأدبيات السابقة؛ بضرورة الاهتمام بتوعية الشباب الجامعي بمخاطر الفضاء الإلكتروني، والانتهاكات التي تحدث فيه.

ب– أهمية تطبيقية وتتمثل في:

– تقديمه رؤية مقترحة قد تفيد صانعي القرار والإدارة الجامعية في إعادة النظر في خطط الجامعة فيما يخص البرامج والمقررات الدراسية والأنشطة الطلابية وأعضاء هيئة التدريس؛لتفعيل دورها في تحقيق البيئة الآمنة رقمياً ومعلوماتياً للأشخاص والمؤسسات.

منهج البحث وأدواته:

استخدم البحث المنهج الوصفي لمناسبته لطبيعة البحث الحالي، لتعرف التأطير النظري للهندسة الاجتماعية، وأسبابها، وتداعياتها على الطلاب، وكذلك لتعرف متطلبات تحقيق دور الجامعة في توعية طلابها من الهندسة الاجتماعية باستخدام

الأمن السيبراني، معتمدة على الاستبانة كأداة لجمع البيانات وتحليلها لتعرف واقع دور جامعة أسيوط في توعية طلابها بالهندسة الاجتماعية.

حدود البحث:

تتمثل حدود البحث الحالي فيما يلي:

يقتصر البحث الحالي في حده الموضوعي على دور جامعة أسيوط في توعية طلابها بمخاطر الهندسة الاجتماعية، وفى حده البشري على عينة من أعضاء هيئة التدريس ومعاونيهم ببعض الكليات النظرية والعملية بكليات جامعة أسيوط وهي (التربية، التربية للطفولة المبكرة، التمريض، الزراعة) وذلك في الفترة الزمنية خلال الفصل الدراسي الثاني من العام الجامعي ٢٠٢٤/٢٠٢٥م.

مصطلحات البحث الاجرائية:

- الهندسة الاجتماعية:

وتعرف الهندسة الاجتماعية اجرائيا بأنها: تلك الهجمات التي يقوم بها المخترقين مستخدمين فيها مجموعة من الأساليب التي تمكنهم من الحصول على المعلومات التي يريدونها من الضحايا، والتي تعتمد في تطبيقها على الخداع والتلاعب بالعقول، وتعد الهندسة الاجتماعية أحد انواع الجرائم السيبرانية.

-الأمن السيبراني:

يُعرف الأمن السيبراني اجرائيا بأنه" الحماية من الكشف عن المعلومات أو سرقة أو إتلاف أنظمة الحاسوب وشبكات الانترنت، لدي طلبة الجامعات، من أجل المحافظة على الأجهزة سواء الشخصية أم العامة، والبرامج والبيانات الإلكترونية من أي تعطيل أو سوء توجيه من الهاكرز أو محترفي الجرائم الإلكترونية، أثناء حصولهم على الخدمات التي تقدمها الجامعات

خطوات السير في البحث:

تم تقسيم خطوات السير في البحث إلى المحاور التالية:

أولا: الإطار العام للبحث:

ثانيا: الإطار النظري للبحث، ويشتمل على:

– الإطار الفكري للهندسة الاجتماعية ومخاطرها على الطلبة الجامعيين.

– دور الجامعة في توعية طلابها بمخاطر الهندسة الاجتماعية.

ثالثا: الإطار الميداني للبحث، ويشمل تحليل واقع دور الجامعة في توعية طلابها بمخاطر الهندسة الاجتماعية من وجهة نظر أعضاء هيئة التدريس، وتقديم تصور مقترح لدور الجامعة في توعية طلابها بالهندسة الاجتماعية ومخاطرها وسبل مواجهتها.

ثانيا: الإطار النظري للبحث:

١–الإطار المفاهيمي للهندسة الاجتماعية:

يعد مصطلح الهندسة الاجتماعية (Social Engineering) مصطلح قديم جديد، حيث ظهر مصطلح الهندسة الاجتماعية في مقالة للكاتب الهولندي Van Markenعام ١٨٩٤، حيث ذكر مصطلح المهندسين الاجتماعيين، وورد تعريف الهندسة الاجتماعية في ٢٧ قاموس متخصص في قاعدة بيانات(One look) ونجد بأن مفهوم الهندسة الاجتماعية يختلف وفقا للتخصصات العلمية وطبيعة السياق المستخدم، فمصطلح الهندسة الاجتماعية في العلوم السياسية مرتبط بقضايا التأثير على مواقف الأفراد والجماعات أو استخدام مختلف الأساليب للتأثير على مواقف معينة وسلوكيات اجتماعية على نطاق واسع.

أما عن مفهوم الهندسة الاجتماعية عند الحديث عن الأمن أو أمن المعلومات، فتتمثل في خداع الناس أو التلاعب بهم للإفصاح عن معلومات تتمتع بالسرية أو الخصوصية. ففي سياق أمن المعلومات يشير المصطلح كما ورد في قاموس Oxford Dictionariesإلى استخدام أساليب الخداع للتلاعب بالأفراد بهدف الحصول على معلومات رسمية أو شخصية يمكن استخدامها لأغراض احتيالية. ويربط قاموس (Free On-Line Dictionary of Computing) مصطلح الهندسة الاجتماعية بعمليات الاحتيال والخداع للحصول على معلومات سرية باستخدام مجموعة من الأساليب وتقنيات مختلفة. (الكندي؛ البلوشي، ٢٠٢٠، ٧٤–٧٥)

كما يعرف مفهوم الهندسة الاجتماعية بأنه عمليات التنكر والحيل الاجتماعية والثقافية والنفسية التي يستخدمها بعض الأفراد لمساعدة القائمين بالتهكير في اقتحام الأنظمة الكمبيوترية (Bullee & Junger ,2021, 3)

كما تعرف الهندسة الاجتماعية: أنها استخدام المهاجم لحيل نفسية؛ كي يخدع مستخدمي الحاسوب؛ ليمكنوه من الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيه (الحنيطي، ٢٠٢١، ٢٨)

والهندسة الاجتماعية هي فن التأثير على الأفراد؛ من أجل الحصول على معلومات سرية مثل: كلمات المرور، والعناوين، والتفاصيل المصرفية، إلخ.. من خلال استغلال نقاط الضعف البشرية، بدلا من استخدام نقاط ضعف التكنولوجية، وتستغل هذه الهجمات نقاط الضعف البشرية مثل: المشاعر، والثقة، والعادات لكسب رضا الناس، والمعلومات أو البيانات السرية، وعلى الرغم من أن هذا أقل تقدما من استراتيجيات الهجوم السيبراني الأخرى، فإن وسائل التواصل الاجتماعي الهندسية يمكن أن تسبب ضرراً جسيماً للضحية (Chetioui,2022, 657) .

وقد برز مفهوم الهندسة الاجتماعية في البداية كفكرة لتنظيم وتأسيس مجتمع منظم وفعال، بشكل منهجي، وهو ما يشبه آلة منظمة، يمكنها حمل أجيال نحو معدلات الازدهار والرفاهية والوفرة المتزايدة باستمرار. فكانت الفكرة باختصار، هي بناء منزل مواطن يشبه الآلة، من خلال طريقة تطبيق العلوم الاجتماعية، أي الهندسة الاجتماعية، فكان يستخدمها السياسيون ويسترشدون بها في عملية صنع القرار بمعرفة الخبراء؛ سواء في اكتشاف المشكلات التي يجب معالجتها، أو صياغة الحلول، وتطوير طرق مبتكرة لتنفيذ الحلول بشكل فعال، وفي هذا المعنى لم تكن الهندسة الاجتماعية مجرد مسألة حرفية حكومية، ولكنها أيضا مسألة تتضمن الاحتراف وتوحيد معايير الرعاية والمراقبة الفردية من أجل الحصول على معلومات تسهم في تحقيق أغراض معينة تسهم في تشكيل المجتمع والتحكم في شئونه-Bengt, et. al., 2012, 12) 13)

بعد ذلك بدأت تتضح الهندسة الاجتماعية واستخداماتها المختلفة التي قد تضر بالبشر، فالهندسة الاجتماعية تعتمد على أساليب عديدة للاحتيال كالكذب على الناس من أجل الحصول على المعلومات، كما أنها قد تستهدف معرفة كيفية الحصول على الأشياء مجانا، وغيرها من أساليب التلاعب بالأشخاص لأداء أعمال أو إفشاء معلومات سرية، وعلى الرغم من أنها تشبه خدعة الثقة أو الاحتيال البسيط إلا أن المصطلح ينطبق عادة على الخداع لغرض جمع المعلومات أو الاحتيال أو الوصول إلى نظام الكمبيوتر.

فقد تمارس الهندسة الاجتماعية وجها لوجه بطرقها وأساليبها الذكية، وقد لا يواجه المهاجم الضحية وجها لوجه، وذلك عن طريق استخدام التقنيات الحديثة. ومما سبق نستنتج أن مفهوم الهندسة الاجتماعية يدور حول كيفية الحصول على معلومات سرية أو الاحتيال على الآخرين، باستخدام الخداع والتلاعب بالأفكار، والمغزى المراد تحقيقه منها هو الحصول على بيانات تتمتع بطابع عالي من الخصوصية والسرية، وهي مرتبطة باستخدام الأدوات التقنية الحديثة؛ وذلك لكثرة استخدامها، ولكونها الأسرع في التواصل، كذلك لصعوبة التعرف على المهندس الاجتماعي.

أنواع هجمات الهندسة الاجتماعية:

تعد هجمات الهندسة الاجتماعية من أهم أنماط الهجمات التي تعترض تحقيق الأمن أثناء التعامل مع الشبكة العنكبوتية وتقسم إلى:

أولا هجمات تعتمد على العامل التقني: (إبراهيم، وآخرون، ٢٠٢٢، ٤٠٦-٤٠٧)

أ) التصيد: ويعد الشكل الأكثر شيوعاً من بين هجمات الهندسة الاجتماعية، ويعتمد على استغلال الخطأ البشرى؛ للحصول على البيانات أو نشر البرامج الضارة، أو إرسال مواقع عبر البريد الإلكتروني تحيل إلى روابط ويب ضارة. ويشتمل هذا النمط على أنماط اخرى كالتصيد الاحتيالي Phishing: ويقصد به هجمات التصيد التي تتم عبر حسابات خدمة العملاء المزيفة على وسائل التواصل الاجتماعي، واختراق البريد الإلكتروني: وفى هذا النوع يتم إرسال رسائل نصية عبر البريد الإلكتروني بزعم أنها من كبار الموظفين أو من جهات معينة؛ للتسلل إلى الأعمال.

ب) التصيد الاحتيالي عبر الرسائل القصيرة Phishing SMS: وتستخدم الرسائل النصية القصيرة على أنها من كيانات شرعية موثوقة، بالإضافة إلى بعض التقنيات الأخرى، لتجاوز المصادقة الثنائية، وقد يقومون بتوجيه الضحايا إلى مواقع الويب الضارة على هواتفهم، كما يمكن أيضا استخدام صورة أخرى من هذا النمط وهي الرسائل المسجلة، حيث يتم إخبار المستلمين بأن حساباتهم المصرفية قد تعرضت للاختراق، ومن ثم يتطلب منهم إدخال البيانات عبر لوحة مفاتيح الهاتف، وبالتالي يمكن الوصول إلى حساباتهم المصرفية.

ج) الاصطياد Baiting: وهذا النوع يتم استخدامه في العالمين الرقمي والحقيقي، ويختلف عن سابقيه في الوسيلة، حيث يعتمد على ترك محركات الأقراص (USB) في مناطق عامة؛ وذلك بغرض جذب فضول الأفراد، وبمجرد توصيلها بجهازه يتم تنزيل البرامج الضارة على القرص الصلب، ومن ثم تبدأ هذه البرامج بممارسة عملها أيا كانت طبيعتها سواء أكانت برامج تجسس أو غيرها مرسلة البيانات مباشرة إلى المتسلل؛ ومن ثم إتاحة الفرص له بالوصول إلى مواقع الويب والحسابات.

وقد يأتي الاصطياد الرقمي في صورة إعلانات مغرية، أو عناصر مجانية يكون الهدف من ورائها توجيه المستخدمين إلى مواقع الويب التي تؤدى إلى تنزيل البرامج الضارة، كما يتم إخفاء برامج التجسس، والبرامج الضارة في صورة تحديثات برامج أو برامج تقليدية (Phoenix nap, 2020)

د) المقايضة: يقدم هذا النوع من الهجمات كخدمة فنية في المقابل للحصول على المعلومات، ويتمثل التهديد الشائع في قيام المهاجم بانتحال شخصية ممثل لتكنولوجيا

هـ) التتبع Tailgating: ويستخدم خاصية الرجوع إلى الخلف والوصول إلى المناطق المحظورة، فقد ينتحل شخصية موظف التوصيل أو غيره ممن قد يحتاجون إلى وصول مؤقت.

و) التصيد بالرمح: وهو أكثر أشكال الهجمات تعقيداً، حيث يتعرف المهاجم على الضحية وينتحل شخصية شخص يعرفه ويثق به. (Taylor,2020)

ثانيا: هجمات معتمدة على العامل البشري:

وهذه الهجمات تعتمد على الإنسان، وتتم من الإنسان إلى الأخر، دون تدخل التقنية، وتتم كالتالي: (إبراهيم، ٢٠١٩، ١١٨)

أ- الإقناع: عن طريق التحدث مع الشخص المطلوب استدراجه، وتشجيعه على الإفصاح بالمعلومات سواء كانت سرية أو لها علاقة بهدف المخترق؛ وذلك من خلال ترك انطباع جيد لدى الضحية باستخدام أساليب عدة للإقناع؛ كي يتمكن المخترق من الحصول على المعلومات التي يريدها.

ب- الهندسة الاجتماعية المعاكسة: تتم عن طريق الإيحاء للضحية بأنك شخص مهم، أو ذو صلاحيات عليا؛ يستخدم المهندس الاجتماعي طريقة يطلق عليها أسلوب (Pretexting)وهو عبارة عن سيناريو مخترع (Invented Scenario) يحدث عندما يخلق المهندس الاجتماعي إحساسا بالثقة بينه وبين المستخدم النهائي عن طريق انتحال شخصية معينة، قد يكون زميل عمل أو مسؤول عن الضحية في مكان العمل.

ج- الانتحال: وغالبا ما يتم عن طريق الهاتف؛ فهو لا يستدعي الحضور وجها لوجه.

د- التجسس والتصنت: وتستخدم عند مراقبة الضحية حين كتابة معلومات مهمة، أو التصنت عليها عند إجراء مكالمة هاتفية، والحصول على معلومات مهمة.

ومع تطور تقنيات الويب وظهور الشبكات الاجتماعية والتطبيقات الذكية الاجتماعية، وتوجه كثير من الأفرادً لاستخدامها فُتحت أبوابا أخرى وطرق للخداع.

ثالثا: الهندسة الاجتماعية عن طريق مشاهير التواصل الاجتماعي:

يسعى الكثير من مشاهير التواصل الاجتماعي في شتّى منصات وبرامج التواصل الاجتماعي إلى الوصول إلى أكبر شريحة ممكنه من المتابعين، بهدف كسب الثقة بشكل يجعلهم مقبولين اجتماعيا وبالتالي يصبح تأثيرهم بشكل أكبر على هذه الفئة سواء بشكل مباشر أو غير مباشر، ويمكن القول بأن لبرامج التواصل الاجتماعي تأثيرا على هندسة المجتمع وإحداث العديد من التغيرات في كافة المجالات سواء في الجانب الاجتماعي، أو الثقافي، أو التأثير في سلوكيات أفراد المجتمع وذائقتهم واهتماماتهم،

وذلك من خلال ما يتم عرضه في هذه البرامج والمنصات.(العمري، العمري، ٢٠٢٤، ١٧-١٨)

ويشير (الحارثي؛ بن نحيت، ٢٠١٧) أن الشهرة عبر مواقع التواصل الاجتماعي حدث أو موقف طارئ لا يتطلب موهبة أو تخطيط أو مال ولا يرتبط بفئة عمرية أو نوع محدد، فربما بمجرد الخروج عن المألوف اجتماعيا، قد تكون حديث المجالس والبرامج الإعلامية ومحط أنظار أفراد المجتمع الذي تعيش فيه. وقد لا يكون هدف المشاهير في مواقع التواصل الاجتماعي الشهرة في بداية الأمر، كما أن الشهرة ليس لها طريقة محددة أو أسلوب واضح؛ فهي تعتمد على قبول المجتمع للموقف أو الفعل المُشاهد. ومن خلال متابعة التواصل الاجتماعي يتضح بأن قبول أفراد المجتمع للشخص المشهور في برامج التواصل الاجتماعي يجعلهم يتقبلون منه سلوكياته ومشكلاته والحديث عن تفاصيل حياته؛ بهدف كسب ثقة المتابعين وتحقيق أعلي قدر من المشاهدات.

ونلاحظ مما سبق تعدد الصور والأساليب التي يستخدمها المهندس الاجتماعي للإيقاع بفرائسه من الفضاء الرقمي، والذي أصبح هو الشغل الشاغل لمعظم فئات أفراد المجتمع؛ لاسيما فئة الشباب الأكثر استخداما واحتكاكا بأدوات التواصل الاجتماعي، وبطبيعة الخصائص المميزة لعمرهم يتأثرون بما يرونه على هذه الوسائل، وبالتالي يكون لها من التأثيرات التي تحتاج إلى تعامل مناسب؛ لتخطي هذه التأثيرات.

أسباب حدوث جرائم الهندسة الاجتماعية:

هناك العديد من الأسباب التي أدت إلى انتشار هذا النوع من الجرائم والانتهاكات، ويمكن إجمالها في الأسباب والدوافع الآتية:(البداينة، ٢٠١٨، ١٤-١٦)

- **أسباب اقتصادية:** تأتى هذه الدوافع في مقدمة الأسباب التي أدت لارتفاع معدلات هذه الجرائم، حيث يعد التربح السريع والحصول على المال من أبرز دوافع جرائم الابتزاز الالكتروني، بالإضافة الى ارتفاع معدلات الفقر والبطالة، وشعور الشباب بالفراغ، مع زيادة مشاعر الكراهية وعدم الانتماء لأسرهم ومجتمعاتهم.

- **أسباب أخلاقية ودينية:** تعرض المجتمع المصري لخلل قيمي وديني كبير خاصة في العقد الأخير، وهو الأمر الذي تسببت فيه وسائل الإعلام والدراما عندما روجت لنماذج البلطجة والعنف، في ظل عدم وجود رقابة على ما تقوم بتقديمه، وغياب الوازع الديني.
- **أسباب اجتماعية:** وتكمن بالأساس في تدهور مستوى التربية للأفراد وغياب الرقابة على الأبناء وتركهم فريسة لمحتويات الإنترنت المليئة بالمفاهيم المغلوطة. كذلك قد يكون البحث عن التقدير وإظهار التفوق من أهم أسباب هذه الجرائم فبعض الجرائم الإلكترونية التي يرتكبها صغار السن، وذلك من باب التحدي، وإظهار تفوقهم على وسائل التكنولوجيا.
- **أسباب تقنية:** تتسم الجرائم الإلكترونية بعدد من السمات أبرزها أنها لا تحتاج إلى وجود الجاني في موقع الجريمة ولا تستخدم أدوات الجرائم التقليدية وإنما تتم عن بعد وتتطلب فقط معرفة الجاني بالتكنولوجيا الحديثة والمتقدمة، ولا تتطلب مواجهات مع رجال الأمن ويصعب الإيقاع بمرتكبيها، وهذه السمات تمثل إغراء كبيرا حتى للأشخاص العاديين لارتكاب هذه النوعية من الجرائم.

وتضيف دراسة (فاروق، علي، ٢٠١٥) الأسباب التالية:

- **حب التعلم:** حيث يعتقد المهاجم أن أجهزة الحاسوب والأنظمة هي ملك للجميع وأن المعلومات ليست حكرا على أحد، وعلى الجميع الاستفادة منها.
- **الرغبة الشخصية:** قد تكون بسبب المشاكل التي يواجها المهاجم أو لظروف البيئة المحيطة به؛ حيث تزرع بداخله رغبة الانتقام، ووجود مثل هذه الأنظمة الإلكترونية تسهل القيام برغباته، فيعبث بمحتوياتها إلى درجة التخريب، أو يكون بدافع التحدي وإثبات الجدارة أمام الأخرين بقدرته على اختراق أنظمة الحاسوب والمساس بها.
- **التسلية واللهو:** فكثير من المهاجمين يعتبرون عملهم هذا مجرد وسيلة للتسلية والمرح.

ومما سبق يتضح تعدد أسباب الهندسة الاجتماعية، والتي منها أسباب أخلاقية تتمثل في غياب الوازع الديني، وأسباب تقنية؛ نتيجة لانتشار التقنية وتطورها بشكل

واسع مع سهولة استخدامها، وأسباب اقتصادية تتعلق بالحالة الاقتصادية للمجتمعات وما يصاحبها من تدهور لحال المؤسسات الاقتصادية، وصعوبة توفير فرص عمل لكثير من الشباب، ومنها ما يتعلق برغبة المهندس الاجتماعي بالكسب السريع غير المشروع، نتيجة لانتشار البطالة، والفراغ الفكري، وسهولة الاستهواء، وسيطرة التقنية الحديثة، بالإضافة إلى غياب دور الأسر في توجيه الأبناء وارشادهم إلى خطورة هذه الممارسات؛ والتي تتنافي مع القيم والأخلاق التي تميز المجتمع، وتكسبه طابعه الخاص به.

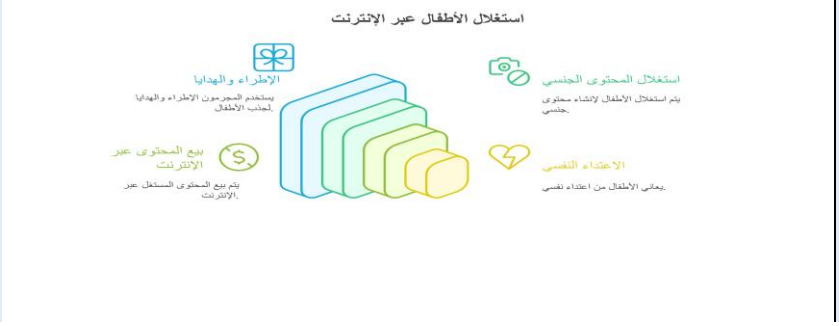
تداعيات الهندسة الاجتماعية:

أحدثت شبكة الإنترنت وأجهزة الكمبيوتر والهواتف المحمولة وغيرها من أشكال التكنولوجيا ثورة في كل جانب من جوانب الحياة، وبالرغم من مميزاتها التي لا تحصى، إلا أنها وفرت فرصاً عديدة للمجرمين لارتكاب أشكال مختلفة من أساليب الهندسة الاجتماعية، قد تتعدى التأثيرات السلبية والخطيرة لهذا النوع من الجرائم الأشخاص، فتؤثر بشكل كبير على بناء الأسرة والمجتمع، بل وقد تشكل تهديدا للدولة ومؤسساتها، ويمكن إجمال هذه التأثيرات والتداعيات على المستويات التالية، والتي من أهم مخاطرها ما يلي:(العمري، العمري، ٢٠٢٤، ١٨-٢٠)

- **على مستوى الفرد:** يُمثل الأطفال أو المراهقين نسبة كبيرة من ضحايا عمليات الابتزاز الإلكتروني، حيث يتعامل الأطفال مع الأجهزة الرقمية واللوحية بشكل يفوق تعاملهم مع أسرهم وذويهم، وهو ما يجعلهم فريسة سهلة أمام الجناة من مستخدمي هذه الأجهزة بشكل إجرامي والذين يقومون بإرسال طلبات الصداقة إلى هؤلاء الأطفال مستخدمين أساليب الإطراء وتقديم الهدايا لاستدراجهم واستغلالهم في تصوير محتويات جنسية يقومون باستغلالها وبيعها على الإنترنت. كما أنهم في أغلب الحالات يقومون أيضا باستدراج هؤلاء الأطفال بهدف الاعتداء عليهم وإيذائهم نفسيا، فضلا عن اختطاف الأطفال والمتاجرة بهم وبيع أعضائهم أو استخدامهم لأغراض جنسية من جانب الجناة، وفى حالة كون الضحية من الأشخاص الناضجين فإن تأثير عمليات الابتزاز الإلكتروني تُحدث بهم أثارا نفسية وعضوية

هائلة، فغالبا ما يقوم المبتز بتركيب صور أو مقاطع الضحية بشكل مسيء وغير لائق يسبب له الحرج والخجل ويطلب الجاني مقابل مادى أو جنسي من أجل عدم نشر هذه الصور أو المقاطع، ويعيش المجنى عليه ضغطا نفسيا وعصبيا غير محتمل خشية أن يقوم هذا الجاني بنشر هذه المادة في محيط عمله أو أسرته أو على وسائل التواصل الاجتماعي، مع خوفه من الاتصال بالأجهزة المعنية فيقوم الجاني بنشر المحتوى المسيء فورا، وهو ما أدى للجوء بعض الضحايا إلى الانتحار.

شكل توضيحي لتأثيرات أساليب الهندسة الاجتماعية على الأفراد



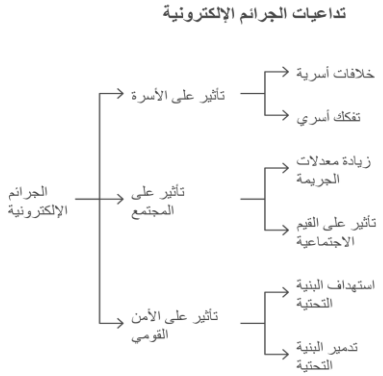
شكل (١) توضيح لتأثيرات الهندسة الاجتماعية على الأفراد (من إعداد الباحث)

- **على مستوى الأسرة:** قد تنال الجرائم الإلكترونية من العلاقات الأسرية وتكون سببا في نشأة الخلافات بين أفراد الأسرة مما يؤدي إلى التفكك الأسري، وذلك بسبب الكثير من النتائج التي تُسببها تلك الجرائم كالتّشهير ببعض الأفراد ونشر الأخبار الكاذبة وسرقة الملفات الخاصة بالأفراد ونشرها في الإنترنت ووسائل التواصل الاجتماعي المختلفة، لقد أصبحت سمعة الأشخاص محل تهديد من قبل القراصنة الذين قد يستهدفون بزيف صورهم ومقاطعهم الزوج أو الزوجة أو الأبناء، وحتى بعد التيقن من خداع هؤلاء وزيف المحتوى الذى يبتزون به الضحية تحدث لا محالة فجوة في العلاقة بين الزوجين أو بين الآباء والأبناء، خاصة مع غياب ثقافة التعامل مع هذا النوع من الجرائم والنقص الشديد في المعلومات حول طبيعتها

وطرق التعامل مع مرتكبيها، ولقد شهد المجتمع مؤخرا انهيار عدد كبير من الأسر بسبب هذا النوع من الانتهاكات الإلكترونية.

- **على مستوى المجتمع:** أصبحت الجرائم الإلكترونية تُشكل خطرا على النسق القيمي للمجتمع المصري ولعل أبرز تداعياتها السلبية هو زيادة معدلات الجريمة خاصة أن هذه الجريمة تتسم بعدد من الصفات تجعلها أمرا سهلا للأشخاص العاديين الذين يتمتعون بقدرة مميزة للتعامل مع تكنولوجيا الانترنت المستحدثة، خاصة وأن الضحية عادة ما يفتقر إلى آليات التعامل مع هذه التكنولوجيا ويخشى إبلاغ الجهات المختصة فيستجيب لطلبات الجاني والذي في أغلب الأحيان يطلب مبلغا ماديا كبيرا ، فيقوم المجنى عليه بسرقة هذا المبلغ – إذا لم يتوافر لديه – أو ارتكاب جريمة أخرى تمكنه من الحصول على المبلغ المطلوب، فيصبح الأمر كسلسلة من الجرائم ترتكب بداية من عملية دنيئة للابتزاز الإلكتروني.
- **استهداف الأمن القومي وتدمير البنية التحتية للدولة:**(Darcili &Celic, 2022, 274) بفضل التقدم التكنولوجي في السنوات الأخيرة، أصبحت البنية التحتية الحيوية أكثر أهمية في الحياة الاجتماعية الحديثة، وتعد الإدارة الآمنة والفعالة للبنية التحتية علامة على التطور الاجتماعي للدولة، حيث أصبح الاعتماد على الشبكة العنكبوتية أكثر من أي وقت مضى أمر غاية في الأهمية، فضمان أمن البنية التحتية يعتمد بشكل كبير على تقنيات الشبكات، وبناء على ذلك، فإن توفير الأمن السيبراني للبنية التحتية الحيوية للدولة، يعد مرادفا للأمن القومي، فحماية البنية التحتية ومكافحة الهجمات السيبرانية يعد من الأمور المهمة لأنه يمثل خدمات عامة وأساسية لكافة أفراد المجتمع.

وفيما يلي شكل توضيحي بأهم تداعيات أساليب الهندسة الاجتماعية:



شكل (٢) توضيح لأهم تداعيات الهندسة الاجتماعية على المجتمع
(من إعداد الباحث)

وبما أن الهندسة الاجتماعية تعد ظاهرة متزايدة في العصر الرقمي، حيث تؤثر بشكل كبير على الأفراد والمجتمعات، فإن أهمية توعية الطلبة في كافة المراحل التعليمية بتأثيرات الهندسة الاجتماعية في الفضاء الرقمي تتمثل في تمكينهم من فهم هذه الظاهرة، وتحديد الطرق المناسبة للتعامل معها. فالتوعية تساهم في تعزيز الوعي الرقمي لديهم، وتمكينهم من اتخاذ قرارات مدروسة ومسؤولة في استخدام الفضاء السيبراني.

وتعزيز الوعي الرقمي لدى الطلبة وتمكينهم من فهم كيفية استغلال الشركات والمؤسسات للبيانات الشخصية والمعلومات الحساسة لتوجيه السلوكيات، والتأثير على القرارات الشخصية، وأن الفضاء الرقمي ليس مجرد منصة للتواصل والترفيه، بل هو أيضا مجال للتلاعب والتحكم والتأثير الاجتماعي، لن يتأتى إلا من خلال المؤسسات التربوية، وخاصة الجامعة؛ ذلك أن طلبة الجامعة هم أكثر الفئات استخداما للتقنيات الحديثة، وهم الأكثر رغبة في الاستكشاف لكل ما هو جديد وبالتالي، فهم الأكثر عرضة للتعرض لأساليب الهندسة الاجتماعية السائدة والمصاحبة لوسائل الاتصال

الحديثة والتقنيات الرقمية التي يستخدموها، وفيما يلي عرض لدور الجامعة في توعية طلابها بالهندسة الاجتماعية ومخاطرها.

المحور الثاني: دور الجامعة في توعوية طلابها بالهندسة الاجتماعية ومخاطرها:

تعد مؤسسات الجامعات من أهم المؤسسات الايدولوجية الرئيسة للدولة، ويبرز دورها في اعداد أجيال على أسس معلوماتية تستطيع أن تسهم في رقي المجتمع، وتحقيق متطلبات سوق العمل، ومحاربة السلوكيات التي تعوق عمليات التنمية الاجتماعية والاقتصادية؛ ويمتد إلى الاستشراف والتنبؤ بالآليات والأدوات التي تستخدم في الهندسة الاجتماعية، وكافة الجرائم السيبرانية، لذا سيتناول هذا المحور عرض دور الجامعات في توعية طلابها بالجرائم السيبرانية ومنها الهندسة الاجتماعية، ولتحقيق ذلك فإنه يجب الاعتماد على العمل المخطط والواضح، وذلك من خلال استخدام استراتيجيات الحماية والتحصين والتي تتمثل فيما يلي: (محمود، مجاهد، ٢٠٢٢، ١٤٥١)

- **استراتيجية الحماية:** ويقصد بها العمل بشكل مسبق لمواجهة التهديدات والمخاطر التي تحيط بالمجتمعات والأفراد، سياسيًا، واقتصاديًا، واجتماعيًا، وثقافيا، وأخلاقيًا، وهو ما يتطلب من الدولة وضع معايير واستخدام كافة مؤسساتها لمواجهة انعدام الأمن بطريقة شاملة ووقائية لا تقتصر على ردود الأفعال تجاه التهديدات؛ بل تعمل بشكل وقائي وتكشف ثغرات البنية الأساسية للدولة.
- **استراتيجية التمكين:** ويقصد بها مساعدة الأفراد على اكتساب القدرة على التصرف والتخطيط سواءً لصالحهم أو لصالح بقية أفراد المجتمع، وجعلهم يمتلكون القدرة على المطالبة باحترام حقوقهم وحرياتهم والتصدي للكثير من المخاطر التي تواجه المجتمع على كافة الأصعدة السياسية والاقتصادية والاجتماعية والثقافية والأخلاقية وإيجاد الحلول لها، الأمر الذي يتطلب المشاركة الجادة من مؤسسات الدولة المختلفة للنهوض بكل ما من شأنه تعزيز هذه القدرات.

وفيما يلي نعرض كيفية تحقيق دور الجامعة في ذلك من خلال تحقيق الأمن السيبراني فيها:

❖ تحقيق الأمن السيبراني في الجامعات المصرية للحد من مخاطر الهندسة الاجتماعية:

لكون التعليم أصبح مرتبطا بشبكة الانترنت ارتباطا وثيقا، فلا يوجد عضو هيئة تدريس أو طالب إلا واستخدم الانترنت في عمليتي التعليم والتعلم، إضافة إلى قضائهم أوقات طويلة في مجال الترفيه والتسلية، وهذا يعنى أن الجميع معرض لمواجهة مخاطر الانترنت، وهذا يعكس أهمية تعزيز ثقافة الأمن السيبراني لحمايتهم وحماية معلوماتهم وتوعيتهم بمخاطر الانترنت والهندسة الاجتماعية، وغيرها من صور الجرائم الإلكترونية.

أولا: مفهوم الأمن السيبراني:

نظراً لما يتسم به العصر الحالي من تغير سريع وانفجار معرفي مستمر، والتقدم العلمي، والتطور التكنولوجي، وبعض التغيرات العصرية والمتمثلة في العولمة، والثورة المعلوماتية، مع اختراع الانترنت، والتي أحدث انفتاح واسع على حريات جديدة، وشجع على ذلك تأثيرات بقاء هوية المرء مجهولة، والتألف السيبراني، والمشاركة الجماعية على الهواء، وعدم الشعور بالإحراج، والتصعيد، كل هذه التغيرات وغيرها أوجبت الاهتمام بأمن وسلامة المعلومات والأجهزة الحاسوبية الشخصية أو الخاصة بالمؤسسات، وذلك من خلال الأمن السيبراني الذى يعد الآلية التي تعتمد على الحاسوب لحماية المعدات والمعلومات والخدمات من الوصول غير القانوني وغير المصرح به.

ويعرف الأمن السيبراني Cybersecurity بأنه: النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى مكان عليه بأسرع وقت ممكن بحيث لا تتوقف حركة العمل. (السمحان، ٢٠٢٠، ٩)

كما يعرف بأنه: كل الممارسات التقنية التي تقوم بحماية الشبكات والأجهزة من أي نوع من أنواع الاختراقات أو الهجمات السيبرانية. (Alshingiti & Abdulrazzaq, 2023,1763)

ويشير مفهوم الأمن السيبراني إلى: حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استغلال غير مشروع. (هيئة الاتصالات وتقنية المعلومات، ٢٠٢٠، ٥). وبالتالي قد يعبر عن التدابير المتخذة لحماية الكمبيوتر أو الشبكة من الوصول غير المصرح به للحفاظ على أمن وسلامة المعلومات المخزنة داخلها بالأمن السيبراني، كما يتضمن التدخلات الفنية التي تحمى البيانات ومعلومات الهوية والأجهزة من الوصول غير المصرح به، أو الضرر بما في ذلك أمن الأصول في الفضاء الإلكتروني.

كما تعرفه المطيري (٢٠٢١، ٦٤٠) بأنه: تنظيم وجمع للموارد والعمليات والهياكل المستخدمة لحماية أصول محددة في الفضاء السيبراني والأنظمة التي تدعم الفضاء الإلكتروني من الأحداث التي لا تتوافق بحكم القانون مع حقوق الملكية الفعلية، وتقع مسؤولية الأمن السيبراني على جميع الأفراد، حيث يتعين على كل مستخدم اتخاذ قرارات مستنيرة حول كيفية وصولهم إلى بياناتهم الخاصة وتخزينها.

ومن التعريفات السابقة للأمن السيبراني نجد أنه يسعي للحفاظ على موارد المؤسسات وممكناتها، والعمليات الحيوية بها، ويمتد أثره إلى المورد البشري؛ مثل خلال التدريب والوعي بأنظمته وكيفية عمله، من أجل الحفاظ على المؤسسات من عمليات السطو والاحتيال السيبراني الذي يحدث عند التعامل غير الآمن على الانترنت.

أنواع الأمن السيبراني:

في ضوء التعريفات المتنوعة السابقة للأمن السيبراني، يمكن تحديد أنواع مختلفة له، تتمثل فيما يلي: (triada network ,2019,2)

- **أمن الشبكات** *(*Network Security*)* وفيه تتم حماية أجهزة الحاسوب من الهجمات التي قد يتعرّض لها داخل الشبكة وخارجها، ومن أبرز التقنيات

المُستخدمة لتطبيق أمن الشبكات جدار الحماية الذي يعمل واقيًا بين الجهاز الشخصي والأجهزة الأخرى في الشبكة، بالإضافة إلى أمن البريد الإلكتروني.

- **أمن التطبيقات (Application Security)** وفيو تتم حماية المعلومات المتعمقة بتطبيق على جهاز الحاسوب، كإجراءات وضع كممات المرور، وعمليات المصادقة، وأسئلة الأمان التي تضمن هوية مستخدم التطبيق.
- **الأمن السحابي (Cloud Security)** تُعرف البرامج السحابية بأنّها برامج تخزين البيانات وحفظها عبر الإنترنت، ويلجأ الكثير إلى حفظ بياناتهم عبر البرامج الإلكترونية عوضًا عن برامج التخزين المحمية، ممّا أدى إلى ظهور الحاجة إلى حماية تلك البيانات، فتعنى البرامج السحابية بتوفير الحماية اللازمة لمستخدميها.
- **الأمن التشغيلي (Operational Security)** وهو إدارة أخطار عمليات الأمن السيبراني الداخلي، وفيه يوَظَّف خبراء إدارة المخاطر لإيجاد خطة بديلة في حال تعرض بيانات المستخدمين لهجوم إلكتروني، ويشمل كذلك توعية الموظفين وتدريبهم على أفضل الممارسات لتجنب المخاطر.

أهمية الأمن السيبراني:

إدراكاً لأهمية مفهوم الأمن السيبراني، والدعوات المستمرة بضرورة تحقيق متطلباته بالجامعات لمواجهة الجرائم السيبرانية؛ حيث يعد الأمن السيبراني مجالا لأى مواجهة أو دفاع عن الهجوم السيبرانية، فهو يحمى البيانات والبنية التحتية من أي هجمات سيبرانية، وخاصة عندما حدث هجوم تقنى في العقد السابق، وأصبح مصدر قلق للحكومة والعامة والقطاعات الخاصة؛ لذا يجب التصدي لمثل هذه الهجمات ومعالجتها بشكل ذكى ومبتكر، وفى ظل مواكبة التطور التكنولوجي والتحول الرقمي كان لابد من مواجهة العقبات والمعوقات الإلكترونية، بما يتناسب مع أهمية المعلومات لكل فرد أو مؤسسة وحماية هذه المعلومات من أهم هجوم إلكتروني قد يؤثر سلبا على المؤسسات المختلفة، ومنها الجامعات.(الشايع، ٢٠١٩، ٥٩)

ومع ازدياد الجرائم الناتجة عن الهندسة الاجتماعية، وزيادة هيمنة تكنولوجيا المعلومات والاتصالات على النسق العام للحياة، وزيادة النصب والاحتيال، والقرصنة،

مع اعتماد الحياة المعاصرة في معظم مجالاتها على التكنولوجيا الرقمية، ووقوع العديد من المؤسسات حول العالم ضحية لأحد أشكال المخاطر والانتهاكات من الأضرار المادية والنفسية والمعنوية التي تؤثر على المؤسسات التعليمية والتربوية، وهذه الأضرار تكسب الأمن السيبراني أهمية خاصة.

ومما يزيد أهمية الأمن السيبراني تعرض الأفراد بمختلف المؤسسات إلى الانتهاكات والمخاطر السيبرانية، دون أن يكون لديهم دراية بتلك المخاطر والانتهاكات ومدى خطورتها على التصفح الآمن للإنترنت، وتتجلى أهمية الأمن السيبراني في قدرته على مقاومة التهديدات المتعمدة، وغير المتعمدة، والاستجابة والتعافي، وبالتالي التخلص من الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدامها، وذلك لأنه يتميز بالآتي: (الهيئة الوطنية للأمن السيبراني، ٢٠١٨)؛ (البار؛ السميري، ٢٠١٩، ١٢):

١–ضمان الوصول المنطقي إلى الأصول المعلوماتية والتقنية للمؤسسة؛ وذلك لمنع الوصول غير المصرح به، وتقييد الوصول لما هو مطلوب لإنجاز الأعمال.

٢–قدرته على حماية أنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين (طلاب–أعضاء هيئة التدريس– اداريين)، والبني التحتية للمؤسسة الجامعية، وكذلك القدرة على حماية البريد الإلكتروني من الهجمات السيبرانية.

٣–القدرة على حماية وإدارة أمن الشبكات.

٤–ضمان حماية أجهزة المؤسسة الجامعية المحمولة بما في ذلك أجهزة الحاسب المحمول، والهواتف الذكية، والأجهزة الذكية اللوحية، وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال المؤسسة، وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في المؤسسة.

٥– السرية وسلامة البيانات والمعلومات ودقتها، وتوافرها وفق السياسات والإجراءات التنظيمية للجامعات.

مما سبق نلاحظ أن تميز الأمن السيبراني بالسرية، وضمان حماية أجهزة الجامعة، وبيانات المنسوبين، وأنظمة معالجة المعلومات، يجعله من أهم الأساسيات

التي يجب أن تمتلكها الجامعة لحماية طلابها من الهجمات السيبرانية، وخاصة هجمات التصيد والاحتيال والنصب، أو الهجمات التي تستهدف إلحاق الضرر بالأجهزة والشبكات، وتأمين الجامعات لمتطلباته يعد خط دفاع قوي ضد أي هجمات مشابهة؛ مما يوفر الأمن النفسي للطلبة وجميع منسوبي الجامعة.

أهداف الأمن السيبراني:

يوجد مجموعة من الأهداف للأمن السيبراني في الجامعات تتمثل في (المنيع، ٢٠٢٢، ١٦٣):

١-توفير بيئة آمنة تتمتع بقدر من الموثوقية في مجتمع المعلومات.

٢-تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات.

٣-التصدى لهجمات وحوادث أمن المعلومات التي تستهدف الجامعة وكلياتها

٤-توفير المتطلبات اللازمة للحد من الجرائم السيبرانية التي تستهدف المستخدمين.

٥-مقاومة البرمجيات الخبيثة وما تستهدفه من إحداث أضرار بالغة بالمستخدمين وأنظمة المعلومات.

٦-الحد من التجسس والتخريب الإلكتروني على مستوى الكليات والجامعة.

٧-التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة بأنواعها وسد الثغرات في أنظمة المعلومات.

ومما سبق يتضح أن الأمن السيبراني يركز في أهدافه على حماية المعلومات من الاختراق أو الاستيلاء عليها؛ وكذلك حماية الأشخاص من خلال تأمين الطلاب والاداريين في الجامعة لبياناتهم الشخصية، وأجهزتهم الشخصية، مما يساعد في المحافظة علي سلامة بيانات الطلاب وجميع منسوبي الجامعة، وكذلك الأجهزة والأدوات من المهندسين الاجتماعيين، وهذا يسهم في استقرار المؤسسة الجامعية، وحماية معلوماتها، ومعلومات العاملين بها، وبالتالي تحقيق الأمان النفسي لهم، وما يترتب على ذلك من تحقيق رفعة للمؤسسة.

عناصر الأمن السيبراني:

هناك ثلاثة عناصر للأمن السيبراني، تتكامل هذه العناصر معاً؛ حتى توفر الحماية المطلوبة، وفى حال فقد أياً منها سيكون هناك خلل أمنى في الجانب الذي يغطيه هذا العنصر، وللمحافظة على أمن البيانات والمعلومات في النظام يجب أن تتوافر فيه العناصر التالية (البار والمرحبي، ٢٠٢٠، ٢):

١-السرية (Confidentiality):وتعنى منع الوصول إلى المعلومات، إلا من الأشخاص المصرح لهم فقط، سواء عند تخزينها، أم معالجتها، أم عند نقلها عبر وسائل الاتصال، وكذلك تحديد صلاحية التعديل والحذف والإضافة.

٢-التكامل وسلامة المحتوى (Integrity): المقصود بها أن تكون المعلومة صحيحة عند إدخالها، وكذلك أثناء تنقلها بين الأجهزة في الشبكة، والتأكد أنه لم يمسها أي تغيير، وذلك باستخدام مجموعة من الأساليب والأنظمة.

٣-التوافر والإتاحة (Availability): وتعنى بقاء المعلومة متوفرة للمستخدم، وإمكانية الوصول إليها في أي وقت، وعدم تعطل ذلك نتيجة لخلل في أنظمة إدارة قواعد المعلومات والبيانات، أو وسائل الاتصال.

مما سبق نجد أن توافر هذه العناصر وتكاملها كفيل بتحقيق الأمن السيبراني، وتحقيق أمن المؤسسة الجامعية بما فيها من مكونات مادية وبشرية؛ وذلك من خلال حفظ وتأمين المنشأة ضد الهجمات السيبرانية، بوجود آليات دفاع وحماية، ومن خلال تحقيق الوعي اللازم لمنسوبي الجامعة بتأمين حساباتهم الشخصية، واستخدام كلمات مرور قوية، وعدم فتح أي روابط غير معروفة المصدر، وعدم الإدلاء ببياناتهم الشخصية لأي شخص أو جهة غير موثوقة.

متطلبات تحقيق الأمن السيبراني في الجامعات المصرية:

مع زيادة مخاطر الهندسة الاجتماعية التي تتزايد باستمرار، والتي تستهدف فئات الشباب الجامعي، باعتبارهم مورد التنمية البشرية، وتكوين الكفاءات للدولة، يستوجب على الجامعات وكل الجهات المعنية بحمايتهم؛ من خلال وضع خطط

استراتيجية لضمان الأمان والسلامة الرقمية والشخصية لمنسوبي الجامعات، وذلك يتطلب ما يلي:

١- مختصين في مجال الأمن السيبراني: (أحمد، فتحي، ٢٠٢٠، ٤٥٤)

وهم العنصر البشري المعني بإدارة الأمن السيبراني في الجامعة؛ حيث بحكم كفاءته في مهامه المتعلقة بالمجال الأمني، فدوره مثل الجندي يحتاج إلى تدريبات دورية؛ لتحديث معارفه، يحتاج إلى برامج حماية محدثة، وهو ما يسهم في الحفاظ على أمن وبنية الجامعة التحتية.

٢- قيادة واعية داعمة: (الشوابكة، ٢٠١٩، ١٧٢)

تحقيق الأمن السيبراني في الجامعة يستوجب قيادة واعية مسؤولة عن عمل الفرق المكلفة بالأمن السيبراني على جميع مؤسسات الجامعة، تستطيع ترشيح منسوبيها ممن تتوافر فيهم الشروط للحصول على البرامج التدريبية، وتوفر بيئة إلكترونية آمنة للتواصل، ومن خلال حثهم على تحسين البيئة الثقافية، والتنظيمية، والتقيد بضوابط الأمن السيبراني التي تسنها الجامعة وتضع ضوابطها، مشجعة علي تعرف كل جديد عن التقنيات التكنولوجية الحديثة، ووسائل الأمن الضرورية لها.

٣- تقنيات وأدوات ضمان الأمن السيبراني:(Zec& kajtazi, 2015,231)

وتتمثل متطلبات تحقيق الأمن السيبراني في الجانب التقني في الجامعات فيما يلي:

- توفير جدار حماية على شبكة الانترنت، وتوفير برامج مكافحة الفيروسات.
- رفع مستوي أمان كلمات المرور بتطبيق شروط كلمات المرور الآمنة.
- تحديث البرامج وأنظمة التشغيل؛ لسد الثغرات ومعالجة المشكلات المتعلقة بها.
- عمل النسخ الاحتياطي للبيانات دوريا؛ لاسترجاعا في حال فقدان البيانات أو تعطل الأجهزة عن العمل. وذلك من خلال الاستعانة بالأفراد والشركات المتخصصة؛ وذلك لبناء قدرة دفاع الكتروني قوية، تستطيع كشف الدخيل علي نظام الجامعة المعلوماتي، ومواجهة التهديدات المكتشفة والمحتملة، والحد من خطورتها.

٤- الدعم المالي والتخطيط من الإدارة العليا للجامعة:

حيث تقوم الجامعة بتقييم شامل للمؤسسة الجامعية، ونظامها وتحديد نقاط ضعفها، والتي تستوجب الدعم المالي، والتخطيط لمكونات المادية للجامعة، مثل الحواسيب والوسائل التقنية، والمعامل الرقمية، بالإضافة إلى المورد البشري الذي يعتبر الحلقة الأضعف في عملية الهندسة الاجتماعية. (البار، السميري، ٢٠١٩، ١٤)

وإجمالا لما سبق يمكن توعية طلاب الجامعات بمخاطر الهندسة الاجتماعية وسبل مواجهتها من خلال الآتي:(بنوان، وآخرون، ٢٠١٦، ١٧٢-١٧٣)

- إدخال مادة الثقافة القانونية في المناهج الدراسية، بحيث تكون هذه المادة عامة على جميع الطلاب، وتتناول هذه المادة في بعض أجزائها الجوانب القانونية والتشريعية للجرائم الإلكترونية.
- يمكن دراسة الموضوعات المتعلقة بالقضايا المرتبطة بالملكية الفكرية، وتوعية الطلاب بها في مختلف الكليات.
- تدريس مقررات حول الجرائم الإلكترونية وسبل مواجهتها في مناهج التعليم قبل الجامعي والجامعي ومجالات التخصص الفني والقانوني، والاجتماعي، والنفسي، والاقتصادي.
- استحداث مادة حول أخلاقيات استخدام الانترنت" وإدراجها ضمن المناهج التعليمية للتوعية وإكساب الأطفال والشباب اتجاهات إيجابية تجاه استخدام الإنترنت والتطبيقات الإلكترونية.
- الاهتمام بتدريس بعض الموضوعات مثل ثقافة السلام، واحترام الآخرين، وثقافة الحوار، والتسامح، والأخلاقيات والقيم ودورها في بناء المجتمع.
- طرح بعض المقررات التي يمكن أن تكون اختيارية بين مجموعة من المقررات مثل مقرر أمن المعلومات، والأمن السيبراني والشبكات.
- إنشاء دبلوم متخصصة للدراسات العليا في الملكية الفكرية، أو في الأمن المعلوماتي، وهي من مجالات الدراسة الجديدة التي يحتاج سوق العمل إليها.

- الاهتمام بابتعاث الطلاب وخاصة في مراحل الدراسات العليا؛ للتعرف على الخبرات المتنوعة للجامعات في هذا المجال.
- عقد ندوات في مجال أمن المعلومات، وكيفية حماية المعلومات والبيانات الخاصة بالمؤسسات الصناعية والتجارية من القرصنة.
- إجراء بعض البحوث المشتركة بين الجامعة وبعض القطاعات الإنتاجية الخاصة بالجرائم الإلكترونية، من حيث ماهيتها، والقوانين الخاصة بها، والمجرمون وأنواعهم، وخصائصهم...الخ.
- التعاون مع وزارة الاتصالات في إعداد المؤتمرات الخاصة بالجرائم المعلوماتية وتأثيرها السلبي على الشباب وقيم المجتمع.
- إسهام بعض أعضاء هيئة التدريس في تصميم بعض البرامج التي يكون هدفها تطهير الإنترنت من المواقع الإرهابية.
- إنشاء مركز معلوماتي تابع للجامعة، فالأمن المعلوماتي هو جزء حيوي من الأمن القومي.

وانطلاقا من العرض السابق لأهم المتطلبات الواجب على الجامعات توفيرها لتحقيق الأمن السيبراني لمنتسبيها وتأمينهم وتوعيتهم من مخاطر الهندسة الاجتماعية، لزم التعرف على واقع دور جامعة أسيوط في توعية طلابها بمخاطر الهندسة الاجتماعية؛ وذلك لصياغة تصور مقترح لتحقيق دورها في توعية وحماية طلابها من مخاطر الهندسة الاجتماعية، وذلك في الجانب الميداني التالي.

ثالثا: الإطار الميداني للبحث: ويقسم إلى تحليل واقع دور الجامعة في توعية طلابها بالهندسة الاجتماعية، ثم وضع تصور مقترح لتحقيق/ تفعيل دورها.

أولا– تحديد الهدف من الاستبانة:

قام الباحث بدراسة ميدانية بهدف تعرف واقع دور جامعة أسيوط في توعية طلابها بمخاطر الهندسة الاجتماعية.

ثانيا– أداة الدراسة الميدانية وخطوات إعدادها:

أ– مرحلة إعداد أداة البحث:

من خلال اطلاع الباحث على الدراسات السابقة والأدبيات التربوية المتعلقة بمجال الدراسة؛ تم تكوين الصورة الأولية للاستبانة من أربعة محاور رئيسة، وقد تكون كل محور من مجموعة عبارات يمكن توضيحها على النحو التالي:

جدول (١)

محاور الاستبانة وعباراتها

كما اختار الباحث مقياسًا ثلاثيًا؛ وذلك لمناسبته لموضوع الاستبانة، وقد كانت البدائل التي تحدد استجابة عينة البحث على درجة التواجد/التحقق على النحو التالي:

المحور		عدد العبارات
المحاور	الأول: واقع دور الإدارة الجامعية	(٨)
	الثاني: واقع دور عضو هيئة التدريس	(٨)
	الثالث: واقع دور المقررات الاكاديمية	(٦)
	الرابع: واقع دور الأنشطة الطلابية	(٥)

(متواجد– متواجد لحد ما– غير متواجد).

ب–تقنين أداة البحث:

١– تحديد صدق الاستبانة:

اعتمد الباحث على نوعين من الصدق:

ا– صدق المحتوى: وذلك بعرضها في صورتها المبدئية على مجموعة من خبراء التربية، وذلك بغرض إبداء الرأي والتأكد من الآتي:

١– مدى انتماء العبارة للمحور الرئيس.

٢– دقة الصياغة والوضوح اللغوي.

٣– إضافة أو حذف أو استبدال ما يرونه مناسباً من عبارات.

وقد جاءت معظم آراء السادة المحكمين بالإجماع على صلاحية الاستبانة وصدقها في قياس ما أعدت من أجله بعد إجراء مجموعة تعديلات اندرجت تحت الآتي:

- إعادة صياغة بعض المفردات إما لعدم وضوحها أو لطولها، أو لأن بعض المفردات مركبة.
- نقل أو استبدال بعض المفردات من مكانها وذلك لعدم أهميتها في مواضعها.

٢- صدق الاتساق الداخلي: بعد تصميم وإعداد الاستبانة في صورتها النهائية والتأكد من الصدق الظاهري لها تم تطبيقها ميدانيًا، وتم حساب معامل الارتباط بيرسون لمعرفة الصدق الداخلي للاستبانة؛ حيث تم حساب معامل الارتباط بين درجة كل محور من محاور الاستبانة بالدرجة الكلية للاستبانة، كما هو موضح بالجدول التالي:

جدول رقم (٢) معامل الارتباط للعبارات في علاقتها بمجمل المحور ومجمل الاستبانة

م	ارتباط العبارة بالمحور	ارتباط العبارة بإجمالي الاستبانة
	المحور الأول: دور الإدارة الجامعية	
١	0.73	0.31
٢	0.69	0.51
٣	0.69	0.33
٤	0.65	0.52
٥	0.37	0.33
٦	0.58	0.29
٧	0.71	0.45
٨	0.71	0.35
	المحور الثاني: أعضاء هيئة التدريس	
١	0.68	0.37
٢	0.59	0.30
٣	0.46	0.29
٤	0.49	0.32
٥	0.47	0.54
٦	0.87	0.32
م	ارتباط العبارة بالمحور	ارتباط العبارة بإجمالي الاستبانة
٧	0.58	0.31
٨	0.69	0.51
	المحور الثالث: المقررات الجامعية	
١	0.69	0.33
٢	0.71	0.52
٣	0.37	0.33
٤	0.73	0.29
٥	0.65	0.45
٦	0.71	0.35
٧	0.68	0.37
	المحور الرابع: الأنشطة الطلابية	
1	0.49	0.30
2	0.46	0.29
3	0.34	0.32
4	0.47	0.54
5	0.78	0.32

ومن الجدول السابق رقم (٢) يتضح أن معامل الثبات بالنسبة للمحاور والاستبانة ككل مرتفعة؛ وبناء على هذه النتيجة، فإن مستوى الثبات لمحتوي الاستبانة ملائم، ويدل على صلاحية الاستبانة للتطبيق.

ثالثاً: عينة الدراسة الميدانية:

تم اختيار عينة الدراسة الميدانية من بعض أعضاء هيئة التدريس ومعاونيهم من كليات جامعة أسيوط وهي (التربية– التربية للطفولة المبكرة– التمريض– الزراعة) والجدول التالي يوضح ذلك:

جدول رقم (٣)

خصائص عينة البحث الميداني

الكلية		المجتمع الأصلي	العينة	النسبة %
كليات نظرية	كلية التربية	١٦٨	٩٣	%٥٥.٣
	كلية التربية للطفولة المبكرة	٣٨	١٨	%٤٧.٣
كليات عملية	كلية التمريض	٢١٠	٦٣	%٣٠
	كلية الزراعة	٣٥٣	٨٧	%٢١.٨
المجموع		٧٦٩	٢٦١	%٣٤

رابعاً: المعالجة الإحصائية

تمت المعالجة الإحصائية للنتائج على النحو التالي:

أ: بالنسبة لنسب متوسط الاستجابة ودرجة التحقق:

١- تم حساب تكرارات استجابات عينة البحث تحت درجات الموافقة (متواجد /متواجد لحد ما/غير متواجد)

٢- أعطيت درجات اعتبارية/وزنية لكل بديل من البدائل الثلاثة السابقة على النحو الآتي:(٣ متواجد، ٢ متواجد لحد ما، ١ غير متواجد) لكل عبارة من عبارات الاستبانة

٣- تم ضرب مجموع تكرارات الاستجابات في الدرجة الاعتبارية لبدائل الاستجابات لكل عبارة على حدة.

٤- تم حساب الوزن النسبي لكل عبارة من عبارات الاستبانة على حدة عن طريق جمع حاصل ضرب التكرارات في الدرجة الوزنية من خلال المعادلة:

الوزن النسبي = مج ك ١ x ٣ + مج ك ٢ x ٢ + مج ك٣ x 1

حيث إن:

ك ١= عدد التكرارات تحت البديل الأول (درجة التواجد/التحقق: متواجد).

ك ٢= عدد التكرارات تحت البديل الثاني (درجة التواجد/التحقق: متواجد لحد ما)

ك ٣= عدد التكرارات تحت البديل الثالث (درجة التواجد/التحقق: غير متواجد).

٥- تم حساب نسبة متوسط الاستجابة من خلال قسمة الوزن النسبي على عدد أفراد العينة مضروباً في عدد البدائل المتاحة كالتالي:

$$\text{نسبة متوسط شدة الاستجابة} = \frac{\text{مج ك١ x ٣ + مج ك٢ x ٢ + مج ك٣ x ١}}{\text{عدد أفراد العينة x٣}}$$

٦- حساب نسبة متوسط شدة الاستجابة النظرية لعبارات الاستبانة بالمعادلة:

$$\text{نسبة متوسط شدة الاستجابة النظرية} = \frac{\text{الدرجة الوزنية لأكبر بديل – الدرجة الوزنية لأقل بديل}}{\text{عدد احتمالات الاستجابة}}$$

$$= \frac{٣ - ١}{٣} = ٠.٦٦٧$$

٧- حساب الخطأ المعياري لمتوسط شدة الاستجابة من خلال القانون(٩).

$$\text{خ.م} = \sqrt{\frac{\text{أ} \times \text{ب}}{\text{ن (أفراد العينة)}}}$$

حيث إن: (أ) نسبة متوسط شدة الاستجابة النظرية للعبارة = ٠.٦٦٧

(ب) باقي النسبة من الواحد الصحيح = ٠.٣٣، (ن) أفراد العينة.

ج- تعيين حدي الثقة لنسبة متوسط شدة الاستجابة لكل مؤشر طبقا للقانون:

حدود الثقة = نسبة متوسط شدة الاستجابة ± ١,٩٦ × الخطأ المعياري (خ. م)

حدود الثقة: الحد الأعلى=٠.٦٤ (إيجابي التحقق)

الحد الأدنى: أقل من أو= ٠.٥٦ (سلبي التحقق)

ما بين قيم الحدين: (متوسط التحقق)

- **-تحليل نتائج الدراسة الميدانية وتفسيرها:**

جدول رقم (٤) استجابات أفراد العينة على محاور الاستبانة كلها

المحاور	عينة الدراسة ن=٢٦١		درجة التحقق
	و	ت	
المحور الأول: واقع دور إدارة الجامعة	0.56	2	+
المحور الثاني: واقع دور عضو هيئة التدريس	٠.٧٤	1	+
المحور الثالث: واقع المقررات الجامعية	0.55	3	-
المحور الرابع: واقع الأنشطة الطلابية	o.48	4	-
الاستبانة ككل	0.59	–	–

(و) تعني قيمة الوزن النسبي (ت) تعني ترتيب العبارة (–) درجة التحقق السلبية (+) درجة التحقق إيجابية

يتضح من الجدول السابق (٤) أن استجابات أفراد العينة ككل على أبعاد الاستبانة بلغ وزن نسبي (٠.٥٩) بدرجة تحقق صغيرة، والذي يؤكد ضعف توافر المتطلبات لجامعة أسيوط لتحقيق دورها في توعية طلابها بمخاطر الهندسة الاجتماعية، وقد جاء المحور الأول والثاني بدرجة تحقق صغيرة (٠.٥٧، ٠.٥٩)، بينما أظهرت استجابات أفراد العينة ضعف تحقق المحورين الثالث والرابع.

-استجابات أفراد العينة لكل محور من محاور الاستبانة على حده:

أ-المحور الأول: واقع دور الإدارة الجامعية في تحقيق الوعي بمخاطر الهندسة الاجتماعية لدى طلابها:

جدول رقم (٥) استجابات أفراد العينة حول عبارات المحور الأول: واقع دور الإدارة الجامعية

م	العبارات	عينة الدراسة ن=٢٦١		درجة التحقق
		و	ت	
١	توفر الكوادر البشرية المؤهلة لتقديم الدعم الفني	٠.٧٤	١	+
٢	توفر برامج تدريبية عن التعامل الآمن على الإنترنت بالشراكة مع المجتمع	٠.٥٥	٤	+
٣	تُفعل ضوابط وعقوبات لممارسي الهندسة الاجتماعية	٠.٥٠	٨	-
٤	تزود منتسبيها ببرامج حماية للبيانات والمعلومات محدثة باستمرار	٠.٥١	٧	-
٥	تتواجد وحدة خاصة بإدارة مخاطر الأمن السيبراني	٠.٥٣	٥	-
٦	توفر ميزانية لتأمين البنية التحتية الرقمية	٠.٥٨	٢	+
٧	استغلال وسائل الإعلام الجامعية والمنصات الرقمية لنشر محتوى ثقافي توعوي عن الهندسة الاجتماعية ومخاطرها	٠.٥٦	٣	+
٨	تتبادل الخبرات مع جامعات عربية وأجنبية في مجال الأمن السيبراني	٠.٥٢	٦	-
مجموع		٠.٥٦		

(و) تعني قيمة الوزن النسبي (ت) تعني ترتيب العبارة (–) درجة التحقق السلبية

توضح نتائج الجدول السابق رقم (٥) أن الوزن النسبي لاستجابات أفراد العينة كلها بلغ(٠.٥٦) بدرجة تحقق صغيرة، مما يوضح ضعف اهتمام الإدارة الجامعية بمخاطر الهندسة علىجتماعية، حيث جاءت العبارة (١) في المرتبة الأولى بوزن نسبي بلغ (٠.٧٤) بدرجة تحقق مرتفعة، ويشير ذلك إلي توفر الكوادر الفنية المؤهلة للدعم الفني للأجهزة، وذلك مرجعه إلى تحول معظم قاعات التدريس في الجامعة إلى التدريس الرقمي، واستخدام منصات عديدة لتقديم المقررات الدراسية مثل: Thinqe, Teams، وغيرها، بينما جاءت العبارة (٦) بوزن نسبي (٠.٥٦) بدرجة تحقق صغيرة؛ وذلك مرجعه وجود التجهيزات من الحواسيب والأجهزة في قاعات وفصول التدريس والمعامل، وبالنسبة للعبارة(٧) التي جاءت بوزن نسبي (٠،٥٨) ودرجة تحقق صغيرة، فذلك لأن استغلال وسائل الاعلام الجامعية والمنصات الرقمية لنشر محتوي ثقافي وتوعوي ازداد مؤخرا مع اهتمام الجامعة بالإعلان عن حصادها الشهري والسنوي علي موقع الجامعة.

بينما لم تحصل باقي العبارات(٢، ٣، ٤، ٥، ٨) على درجة تحقق، حيث حصلت على وزن نسبي أقل من الحد الأدنى(٠.٥٦)، حيث ضعف الشراكة مع مؤسسات المجتمع بشكل عام ، وبالتالي ضعفها في مجال توفير برامج تدريبية عن التعامل الآمن على الانترنت لمنسوبي الجامعة، وكذلك لا يوجد تفعيل لسياسات وعقوبات ممارسة الهندسة الاجتماعية؛ والذي قد يكون مرجعه عدم وجود وحدة خاصة بإدارة مخاطر الأمن السيبراني في الجامعة، والتي يكون عليها تأمين الأجهزة الشخصية للطلاب والعاملين بالجامعة وأعضاء هيئة التدريس ومعاونيهم، وتأمين أجهزة الجامعة ببرامج حماية من الفيروسات، والتحديث المستمر لأنظمة وبرامج التشغيل، بالإضافة إلي ضعف التعاون وتبادل الخبرات مع جامعات مناظرة محلية أو عربية أو دولية في مجال الأمن السيبراني.

ب–المحور الثاني: واقع دور عضو هيئة التدريس الجامعي:

جدول رقم (٦)

استجابات أفراد العينة حول عبارات المحور الثاني: واقع دور عضو هيئة التدريس الجامعي في توعية الطلاب بالهندسة الاجتماعية ومخاطرها:

م	العبارات	عينة الدراسة ن=٢٦١		درجة التحقق
		و	ت	
١	**ينمي معارف الطلاب في مجالات التكنولوجية الرقمية الحديثة والأمن المعلوماتي**	٠.٥٦	٧	+
٢	**يشجع الطلاب على الاستفادة من المتغيرات التكنولوجية والتقنية الحديثة**	٠.٦٨	٦	+
٣	**يعمل على اكساب الطلاب مهارات وأخلاقيات المواطنة الرقمية.**	٠.٧٤	٤	+
٤	**يوعى الطلاب بمفهوم الهندسة الاجتماعية**	٠.٤٠	٨	-
٥	**يتواصل باستمرار مع الطلاب لمناقشة أي تغيرات أو انحرافات أخلاقية لدى البعض.**	٠.٧١	٥	+
٦	**يقدم القدوة الحسنة أمام طلابه في الحفاظ على الأخلاق والتمسك بالتقاليد والقيم الأصيلة**	٠.٩٨	١	+
٧	**يوعي الطلاب بأهمية التحقق من مصادر التعلم، والروابط الضارة عند تصفح الانترنت**	٠.٩٤	٢	+
٨	**يستخدم أساليب تدريسية تنمي القدرة على النقد والتحليل لدى الطلاب**	٠.٩٤	٢	+
	مجموع	٠.٧٤		

(و) تعني قيمة الوزن النسبي (ت) تعني ترتيب العبارة (–) درجة التحقق السلبية

يتضح من الجدول السابق رقم (٦) أن المحور في مجمله متحقق بدرجة عالية، حيث حصل على إجمالي وزن نسبي (٠.٧٤) حيث يبذل أعضاء هيئة التدريس قصارى جهدهم لتوعية الطلاب وتثقيفهم بالمتغيرات المعاصرة، وجاءت العبارة (٦) بوزن نسبي (٠.٩٨) ودرجة تحقق مرتفعة؛ كون المعلم الجامعي قدوة حسنة لطلابه في الالتزام والتمسك بالتقاليد والقيم الأصيلة، وهو من أهم الواجبات على أعضاء هيئة التدريس ومعاونيهم.

وحصلت العبارتين (٧، ٨) على وزن نسبي (٠.٩٤) في المرتبة الثانية في التحقق، حيث يرغب عضو هيئة التدريس من طلابه تحري الدقة في المعلومات ومن مصادر الحصول عليه، كون المعلومات أصبحت متدفقة بطريقة واسعة وسريعة،

وكذلك يشجعهم على التعلم من خلال التنويع في استخدام وسائل ومعينات تساعدهم على النقد والتحليل وعدم الانسياق وراء ما ينشر على صفحات المواقع الإلكترونية، أو التعامل مع الأشخاص الغرباء، أو الدخول على روابط ضارة بدافع الفضول والاستكشاف.

وجاءت العبارة (٣) بوزن نسبي (٠.٧٤) ودرجة تحقق مرتفعة، حيث يعمل عضو هيئة التدريس على اكساب الطلاب مهارات وأخلاقيات المواطنة الرقمية من وجهة نظره من خلال تعريفهم بحقوقهم وواجباتهم الرقمية، وتوعيتهم بالمخاطر التي قد يتعرضوا لها عند التعامل على الانترنت.

وجاءت العبارة (٥) بوزن نسبي (٠.٧١) ودرجة تحقق مرتفعة، حيث يعمل عضو هيئة التدريس على التواصل المستمر مع طلابه من خلال المناقشات التي تتم في المحاضرات أو السكاشن العملي عندما تكون طبيعة المادة التعليمية تستلزم ذلك، أو وفقا للأحداث الشائعة التي تستلزم النقاش مع الطلاب.

وجاءت العبارتين (١، ٢) بوزن نسبي (٠.٥٦، ٠.٦٨) ودرجة تحقق مرتفعة، حيث يطلب عضو هيئة التدريس من طلابه الاستفادة من المتغيرات التكنولوجية والتقنية الحديثة من خلال التكليفات والتقييمات التي تعتمد على التقنيات الحديثة.

بينما جاءت العبارة(٤) بوزن نسبي (٠.٤٠) وهي درجة منخفضة بالنسبة للتحقق، حيث لا يقوم عضو هيئة التدريس باستخدام هذا المفهوم بشكل صريح وإنما يوعي الطلاب بشكل عام، حيث عدم استخدام هذا المفهوم بشكل كبير، وإنما يتم استخدام مصطلحات مثل، الجرائم الإلكترونية، الهجمات السيبرانية، النصب، انتحال الشخصية وغيرها، وهذه النتيجة تتفق مع دراسة (الكندي؛ البلوشي، ٢٠٢١، ٧٢) التي تؤكد ضعف مستوى دراية الطلبة بمفاهيم الهندسة الاجتماعية وأساليبها، وأن الغالبية منهم لديهم وعي ببعض الممارسات التنظيمية والتقنية للوقاية من أساليب ومخاطر الهندسة الاجتماعية بطريقة غير مباشرة.

ج-المحور الثالث: واقع دور المقررات الجامعية:

جدول رقم (٧)

استجابة أفراد العينة حول واقع دور المقررات الجامعية في توعية طلاب الجامعة بالهندسة الاجتماعية ومخاطرها

م	العبارات	عينة الدراسة ن=٢٦١		درجة التحقق
		و	ت	
١	محتوى يعزز الهوية الثقافية للطلاب الجامعيين	٠.٥٨	٣	+
٢	موضوعات عن الهندسة الاجتماعية ومخاطرها	٠.٤٢	٦	-
٣	مناسبة محتوى المعرفة الرقمية المتضمنة في المقررات الدراسية قدرات وامكانيات الطلاب واختلافاتهم.	٠.٧٢	١	+
٤	تتضمن المقررات الدراسية محتوى عن الآثار الناتجة عن التعامل غير الآمن على الانترنت	٠.٥٢	٤	-
٥	تؤكد المقررات الدراسية على أهمية الحقوق والواجبات الرقمية عند استخدام الوسائل التكنولوجية الحديثة	٠.٦٢	٢	+
٦	تتضمن المقررات الدراسية موضوعات عن الصحة والسلامة الرقمية مثل (السلامة السيبرانية-المواطنة الرقمية...	٠.٥٢	٤	-
	مجموع	٠.٥٥		

(و) تعني قيمة الوزن النسبي (ت) تعني ترتيب العبارة (-) درجة التحقق السلبية

يتضح من نتائج الجدول السابق (٧) عدم تحقق هذا المحور، حيث حصل على وزن نسبي (٠.٥٥) أقل من الحد الأدنى (٠.٥٦)، مما يدل على ضعف تضمين مفهوم الهندسة الاجتماعية في المقررات الدراسية الجامعية، أو أي موضوعات ذا صلة بهذا المفهوم، وقد جاءت العبارة (٥) بدرجة تحقق متوسطة بلغت (٠.٦٢)، حيث وجود بعض المقررات الدراسية التي تؤكد على أهمية الحقوق والواجبات الرقمية عند استخدام الوسائل التكنولوجية الحديثة، والتي أضيفت حديثا كمقررات ثقافية في بعض الكليات.

وجاءت العبارة (٣) بدرجة تحقق مرتفعة ووزن نسبي (٠.٧٢)، حيث يتم التدرج في تقديم المعرفة الرقمية، لتكون مناسبة لقدرات وامكانيات الطلاب واختلافاتهم الفردية.

وكذلك جاءت العبارة (١) بدرجة تحقق متوسطة حيث بلغ الوزن النسبي لها (٠.٥٨) التي تؤكد وجود محتوى يعزز الهوية الثقافية للطلاب الجامعيين، وخاصة في الكليات النظرية، تبعا لطبيعة المواد المقدمة فيها.

د-المحور الرابع: واقع الأنشطة الطلابية في توعية الطلاب بالهندسة الاجتماعية ومخاطرها:

جدول رقم (٨) استجابات أفراد العينة حول واقع الأنشطة الطلابية في توعية الطلاب بالهندسة الاجتماعية ومخاطرها

م	العبارات	عينة الدراسة ن= ٢٦١		درجة التحقق
		و	ت	
١	تتضمن الأنشطة ندوات تثقيفية عن مخاطر الهندسة الاجتماعية ودور الأمن السيبراني في مواجهتها	٠.٤٦	٣	-
٢	يتم تدعيم المكتبات الجامعية بكل الوسائل اللازمة لتوعية الطلاب بمخاطر الجرائم الإلكترونية، وسلبيات التعامل غير الآمن مع التكنولوجيا الرقمية	٠.٤٩	٥	-
٣	تتضمن الأنشطة مسابقات حول التصدي للهندسة الاجتماعية وأساليبها	٠.٤٨	١	-
٤	تقدم دورات تدريبية وأدلة توعوية للمتعلمين لحماية بياناتهم وأجهزتهم الشخصية	٠.٤٥	٤	-
٥	تقوم الجامعة بحملات إعلامية توعوية ضد الشائعات وهجوم الاصطياد والانتحال الإلكتروني.	٠.٥٣	٢	-
	مجموع	**٠.٤٨**		

(و) تعني قيمة الوزن النسبي (ت) تعني ترتيب العبارة (-) درجة التحقق السلبية

يتضح من الجدول السابق (٨) ضعف تحقق هذا المحور، حيث حصل على إجمالي وزن نسبي للمحور ككل(٠.٤٨)، وذلك مرجعه؛ أن الأنشطة الطلابية الجامعية نمطية مرتبطة بمناسبات وفاعليات معينة تقام سنويا في الجامعة، كما ارتبط عند الكثير من الطلاب أن المكتبات الجامعية لتحصيل المادة العلمية ذات الصلة بالتخصصات التي يدرسوها، وبالتالي لا يوجد بها الوسائل أو الأنشطة التي تزيد وعيهم فيما يخص الهندسة الاجتماعية والمفاهيم المرتبطة بها، كما أن دور الجامعة في القيام بحملات ضد الشائعات وأساليب الاصطياد والانتحال مازال ضعيفا ؛ ذلك لأن الهجمات التي

تحدث نتيجة للهندسة الاجتماعية تكون سريعة وتعتمد على ضعف العنصر البشري، وخوفه من التصريح بذلك.

ومن خلال العرض السابق لنتائج الدراسة الميدانية لواقع دور جامعة أسيوط في توعية طلابها بمخاطر الهندسة الاجتماعية، اتضح ضعف دورها في تحقيق ذلك؛ حيث دور الإدارة الجامعية جاء بدرجة تحقق صغيرة، فلا يوجد وحدة لإدارة المخاطر السيبرانية بالجامعة، أو اهتمام بتقديم برامج توعوية لمنسبين الجامعة من الطلاب والأعضاء والعاملين، سواء من جانب الجامعة ومؤسساتها، أو بالتعاون مع مؤسسات المجتمع، والجامعات المناظرة محليا وعربيا ودوليا، وتحقق دور عضو هيئة التدريس في تحقيق التوعية للطلاب، ولكن بطريقة غير مباشرة، وبالنسبة للمقررات الجامعية، والأنشطة فلم تحقق الدور المتوقع منها في توعية الطلاب بالهندسة الاجتماعية ومخاطرها؛ لذا سيقوم الباحث بوضع تصور مقترح لتحقيق دور جامعة أسيوط في التوعية بالهندسة الاجتماعية باستخدام الأمن السيبراني، وذلك فيما يلي:

❖ التصور المقترح لتفعيل دور جامعة أسيوط في توعية طلابها بمخاطر الهندسة الاجتماعية:

من منطلق أن الهدف الرئيس للبحث يتمثل في تفعيل دور الجامعات المصرية لتنمية وعي طلابها بالهندسة الاجتماعية ومخاطرها وسبل مواجهتها، وفي ضوء ما توصل إليه البحث بإطاره النظري والميداني من نتائج، يقدم البحث تصورًا مقترحًا يتكون من مصادر التصور، منطلقات التصور، وأسس التصور، وأهداف التصور، ومضمون التصور، وذلك على النحو التالي:

مصادر التصور المقترح:

يستمد هذا التصور من المصادر التالية:

١- نتائج الدراسة الحالية، والذي اعتمد على محورين، هما:

- تحليل وتفسير نتائج استبانة الجانب الميداني التي تم تطبيقها على عينة ممثلة من أعضاء هيئة التدريس ببعض الكليات العملية وهي (التمريض، الزراعة)، وبعض الكليات النظرية وهي (التربية، والتربية للطفولة المبكرة).

- الإطار النظري للهندسة الاجتماعية كأحد صور الجرائم والتهديدات السيبرانية، ومتطلبات تحقيق الأمن السيبراني في الجامعة.

٢- الدراسات والبحوث السابقة وما انتهت إليه من نتائج وتوصيات ومقترحات.

هدف التصور المقترح:

يهدف التصور إلى تحقيق دور الجامعة في توعية طلابها لمخاطر الهندسة الاجتماعية وسبل مواجهتها باستخدام الأمن السيبراني.

مرتكزات التصور المقترح ومنطلقاته:

نتيجة لإتاحة التقنيات الرقمية الحديثة، والاستخدام المكثف للتكنولوجيا ووسائل الإعلام الاجتماعية في أوساط الطلبة الجامعيين؛ مما يجعلهم أكثر المجموعات عرضة للانتهاكات وللتهديد والإذلال والتهكم اللفظي والاعتداء المعنوي والإحراج من أي شخص عبر شبكات التواصل الاجتماعي.

كذلك لطبيعة هذه المرحلة الشديدة الأهمية من عمر الشباب وهي مرحلة التعليم الجامعي، وما يصاحبها من حب استكشاف وفضول لتعرف المجهول، وبالإضافة إلى سهولة الإغواء الفكري، والتقني، بكل صوره عبر الانترنت بسبب ضعف خبرة الطلاب، وضعف توعيتهم، او بسبب مهارة المهندسين الاجتماعيين؛ مما يجعل الهندسة الاجتماعية من أبرز التحديات على المجتمعات والأفراد؛ إذ يعد خداع البشر مهمة أسرع وأكثر كفاءة من اختراق شبكات الحاسب الآلي، واختراق الأمن الإلكتروني.

أيضا أهمية الجامعة كمؤسسة تربوية يقع على عاتقها توعية والحفاظ على منتسبيها من أخطار الهجمات السيبرانية بكل أنواعها؛ لما تمتلكه من مقومات على مستوى التدريس والتعليم، والبحث العلمي، وتقديم خدمات للمجتمع، الأمر الذي يفرض عليها أن تكون قدر ثقة المجتمع فيها. والتي يحتم عليها إعداد نوعية من الأفراد على قدر كاف من التعليم والثقافة، حتى يتسنى لهم الوعي بالمخاطر المحيطة بهم، ومواجهتها.

ويرتكز التصور على مجموعة من المرتكزات تتمثل فيما يلي:

- الاستفادة من التطور التكنولوجي والرقمي في نشر الوعي: من خلال استخدام المنصات الرقمية ووسائل التواصل الاجتماعي لتوسيع دائرة التأثير على الطلاب وعلى أسرهم، وكافة مؤسسات المجتمع.
- تلبية للدعوات المستمرة لتحقيق الشراكة بين الجامعات ومؤسسات المجتمع، والجامعات ذات الخبرة في مجال تحقيق الأمن السيبراني، وزيادة وعي الطلاب بمخاطر الهجمات والجرائم السيبرانية.
- تفعيل دور الجامعة، وإعادة الريادة لأدوارها الأساسية التي تواكب الاتجاهات الحديثة في توعية منسوبي الجامعة بكافة فئاتهم بالمخاطر المحيطة بهم، من خلال الاستفادة من ممكنات الجامعة مثل: تنظيم الأنشطة الثقافية، الندوات، ورش العمل، والبرامج التوعوية التي تركز على هذه القضايا، بما يتناسب مع متطلبات العصر وتطلعات الطلبة.

أسس التصور المقترح:

يرتكز هذا التصور المقترح على مجموعة من الأسس لتفعيل دور جامعة أسيوط في توعية طلابها بمخاطر الهندسة الاجتماعية وسبل مواجهتها، وهذه الأسس تتمثل في:

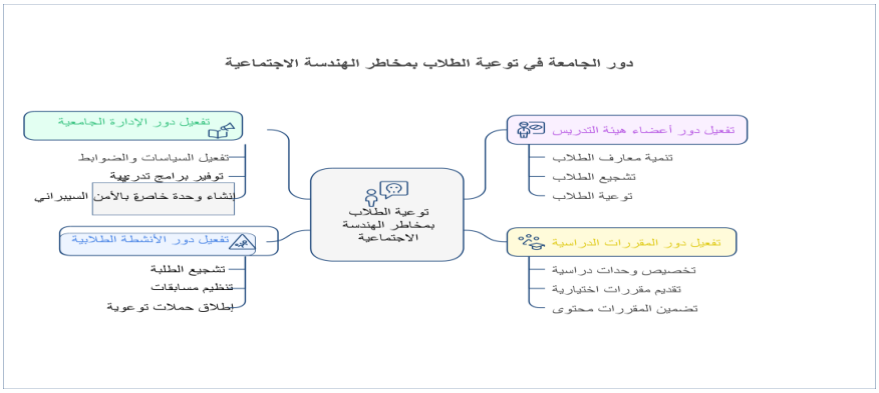
- أساس أمني: يتمثل في تأمين وحماية بيانات ومعلومات الطلبة الجامعيين، وأجهزتهم الشخصية، وحماية ممتلكات الجامعة ومعلوماتها من أي اختراق غير مصرح به من الأشخاص المخترقين، وبالتالي تنمية وعيهم بالأمن السيبراني وتحقيق السلامة الرقمية على الانترنت، مما يزيد من ثقتهم بأمنهم الشخصي وأمن الجامعة الرقمي.
- أساس ثقافي معرفي: يتمثل في تعزيز المحتوى الثقافي والتعليمي الذي يتناول الهوية الثقافية والأمن الفكري والمعلوماتي ضد أي انحرافات أو تهديدات سيبرانية أثناء التعامل في الفضاء الإلكتروني.
- أساس اجتماعي: يتمثل في اعتبار الطلاب الجامعي هم القوة الفاعلة في أي مجتمع، وبالتالي ضرورة توعيتهم بالمخاطر التي تحيط بهم، والمتعلقة باتصالهم المستمر واليومي بالأجهزة الرقمية سواء للتعليم أم للتسلية والترفيه، والتي تحدث

نتيجة لجهلهم بأساليب التصيد والاحتيال الإلكتروني التي يستخدمها المهندسون الاجتماعيون للحصول على بياناتهم أو افسادها وإلحاق الضرر بأجهزتهم الشخصية أو الأجهزة في الجامعة.

- أساس تنظيمي وإداري: من خلال وضع آليات واضحة داخل الجامعة لتوعية الطلاب الجامعي بمخاطر الهندسة الاجتماعية والمخاطر الأخرى السيبرانية، مثل وجود وحدة لإدارة المخاطر السيبرانية، وعقد العديد من البرامج التدريبية وورش العمل التي تساعد الطلاب وجميع منسوبي الجامعة في مواجهة مخاطر الهندسة الاجتماعية.
- أساس رقمي: من خلال استغلال الوسائل التكنولوجية الحديثة ومنصات التواصل الاجتماعي لنشر الوعي بماهية الهندسة الاجتماعية ومخاطرها، وسبل مواجهتها، واستخدام كل وسائل الاتصال المتاحة في القيام بحملات توعية؛ تتناسب وهذا الخطر السيبراني.
- أساس تشاركي: وذلك عن طريق تشجيع الشراكات مع الجامعات المحلية والدولية وبعض الجهات الحكومية ذات الصلة، والقطاع الخاص لتنظيم فعاليات مشتركة تسهم في رفع وعي الطلاب بمخاطر الهندسة الاجتماعية، وتعزز من دور الجامعة في تحقيق ذلك.

مضمون التصور المقترح:

يتضمن التصور المقترح مجموعة من الممارسات الضرورية لتحقيق دور الجامعة في توعية طلابها بمخاطر الهندسة الاجتماعية، وسبل مواجهتها، وذلك من خلال تفعيل جوانبها الأربعة، والشكل التالي يوضح ذلك:



شكل (٣) توضيح لدور الجامعة في توعية الطلاب بمخاطر الهندسة الاجتماعية (من اعداد الباحث)

١- تفعيل دور الإدارة الجامعية، من خلال:

- تفعيل السياسات والضوابط لحفظ الأمن السيبراني داخل الجامعة
- توفير برامج تدريبية عن التعامل الأمن على الانترنت لمنسوبي الجامعة.
- تفعيل ضوابط وعقوبات صارمة لممارسي الهندسة الاجتماعية.
- إنشاء وحدة خاصة بإدارة مخاطر الأمن السيبراني.
- استغلال وسائل الإعلام الجامعية والمنصات الرقمية لنشر محتوى ثقافي توعوي، وتوفير منصات حوار مفتوحة بين الطلاب حول ماهية الهندسة الاجتماعية ومخاطرها وسبل مواجهتها.
- توفير البنية التحتية والدعم المالي مثل:

- تجهيز قاعات ومعامل الكليات وبأحدث الأجهزة وبرامج التشغيل المحدثة باستمرار، وتدعيمها ببرامج حماية ودفاع ضد الفيروسات.

- تخصيص ميزانية مستقلة لتأمين البنية التحتية الرقمية للوحدات الإدارية والأكاديمية في الجامعة.
- توفير الدعم الفني من الكوادر البشرية المؤهلة في جميع الوحدات الإدارية والأكاديمية في الجامعة.

- تبادل خبرات وبناء شراكات مع جامعات محلية ودولية في مجال الأمن السيبراني وعقد بروتوكولات تعاون بين الجامعات والجامعات المناظرة في الدعم التوعوي من خلال ندوات أو ورش عمل أو زيارات ميدانية لأهم الُمنشآت ذات التأمين السيبراني العالي.
- الشراكة مع مؤسسات المجتمع المحيط في تقديم دورات وندوات توعوية لمنسوبي الجامعة عن مخاطر الهندسة الاجتماعية، وسبل مواجهتها، وكذلك تقديم الدعم المادي.

١- تفعيل دور أعضاء هيئة التدريس، من خلال:

- تنمية معارف الطلاب في مجالات التكنولوجية الرقمية الحديثة والأمن المعلوماتي.
- تشجيع الطلاب على الاستفادة من المتغيرات التكنولوجية والتقنية الحديثة.
- العمل على اكساب الطلاب مهارات وأخلاقيات المواطنة الرقمية.
- توعية الطلاب بمفهوم الهندسة الاجتماعية.
- التواصل المستمر مع الطلاب لمناقشة أي تغيرات أو انحرافات أخلاقية لدى البعض.
- تقديم القدوة الحسنة أمام طلابه في الحفاظ على الأخلاق والتمسك بالتقاليد والقيم الأصيلة.
- توعية الطلاب بأهمية التحقق من مصادر التعلم، والروابط الضارة عند تصفح الانترنت.
- استخدام أساليب تدريسية تنمي القدرة على النقد والتحليل لدى الطلاب.

٢- **تفعيل دور المقررات الدراسية، وذلك من خلال:**

- تخصيص وحدات دراسية ضمن المقررات العامة والتخصصية عن ماهية الهندسة الاجتماعية ومخاطرها وسبل مواجهتها.
- تقديم مقررات اختيارية عن: الصحة والسلامة الرقمية- المواطنة الرقمية- الهوية الثقافية في مقابل الهجمات السيبرانية...
- تكليف الطلاب بتقديم عروض توضيحية أو مشاريع بحثية مرتبطة بمواجهة الهندسة الاجتماعية في تخصصاتهم المتنوعة.
- تضمين المقررات محتوى يعزز الهوية الثقافية للطلاب الجامعيين.
- تضمين المقررات مواد عن الثقافة القانونية فيما يخص الجرائم الإلكترونية، خاصة أساليب الهندسة الاجتماعية.

٣- **تفعيل دور الأنشطة الطلابية، من خلال:**

- تشجيع الطلبة على انشاء برامج دفاع سيبرانية أو تطبيقات وجدران حماية لكشف الفيروسات والهجمات السيبرانية، ومنع حدوثها، ومكافأتهم على ذلك.
- تنظيم مسابقات حول سبل التصدي للهندسة الاجتماعية وأساليبها المختلفة.
- إطلاق حملات توعوية عبر الفعاليات التي تقيمها الجامعة عن الشائعات وهجمات التصيد، والانتحال، والتنمر السيبراني، وغيرها.
- تدعيم المكتبات الجامعية بكل الوسائل اللازمة لتوعية الطلاب بمخاطر الجرائم الإلكترونية، وسلبيات التعامل غير الآمن مع التكنولوجيا الرقمية.
- تشجيع الطلبة على إنشاء مدونات أو مجلات ثقافية رقمية داخل الجامعة للتوعية بالقضايا المجتمعية المعاصرة.

قائمة المراجـــــع

أولا: مراجع عربية:

إبراهيم، مها أحمد. (٢٠١٩). الهندسة الاجتماعية وشبكات التواصل الاجتماعي، وتأثيرها على المجتمع العربي، المجلة الدولية لعلوم المكتبات والمعلومات، *الجمعية المصرية للمكتبات والمعلومات والارشيف*، ٣ (١)، ١٩٥ -٢١٨.

أحمد، عبد الرحمن؛ فتحي، محمد. (٢٠٢٠). استراتيجية مقترحة لتحويل جامعة المنيا إلى جامعة ذكية في ضوء توجهات التحول الرقمي، *مجلة جامعة الفيوم للعلوم التربوية والنفسية*،١٤ (٦)، ٤٠٣-٥٢٨.

بنوان، هبة إبراهيم الشحات؛ والمنوفي، محمد إبراهيم؛ الجندي، ياسر مصطفى. (٢٠١٦). الجامعة وتنمية وعى طلابها بالجرائم الإلكترونية في ضوء التطور التقني والمعلوماتي، *مجلة كلية التربية، جامعة كفر الشيخ*، ١٦ (٣)، ١٤٩-١٨٠.

البار، عدنان مصطفي؛ السميري، عيسى. (٢٠١٩). أساسيات الأمن السيبراني، الرياض، دار كنترولي للنشر.

البار، عدنان مصطفي؛ المرحبي، خالد علي (٢٠٢٠). *أمن المعلومات والأمن السيبراني*، ورقة علمية، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز، السعودية.

البداينة، ذياب موسي. (٢٠١٤). الجرائم الإلكترونية: المفهوم والأسباب، ورقة مقدمة في الملتقي العلمي: الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية المنعقدة في الفترة من ٢/٤-٢٠١٤/٩، كلية العلوم الاستراتيجية، عمان، الأردن، ١-٢٨.

ترجمة ومعني الهندسة الاجتماعية في قاموس الكل عربي انجليزي .Almaany Retrieved https://cutt.ly/qBTCEBp

التويجري، صالح عبد العزيز. (٢٠٢٢). العوامل ذات العلاقة بالتحولات السلبية لمتابعة مشاهير السناب شات: دراسة ميدانية على طلاب جامعة الإمام محمد بن سعود الإسلامية من وجهة نظر أعضاء هيئة التدريس، *الجامعة الإسلامية، المدينة المنورة*، (٩)، ٢٢٥ – ٢٧٥.

جعفر، ميادة كاظم. (٢٠٢٣). تأثيرات أساليب الهندسة الاجتماعية على اختراق معلومات الطلبة الجامعيين في مواقع التواصل الاجتماعي: دراسة تطبيقية على عينةٍ من الطلبة الجامعيين، *مجلة جامعة الاسراء الجامعة للعلوم الاجتماعية والانسانية، بغداد*، ٥ (٩)، ٤٧٣-٥٠٣.

الجمل، حازم حسن أحمد. (٢٠٢٠). الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠، مجلة البحوث الأمنية، كلية الملك فهد الأمنية، *مركز الدراسات والبحوث، السعودية*، ٣٠ (٧٧)، أغسطس، ٢٤٣ – ٣٢٨.

الحارثي، سعيد؛ بن نحيت، زياد. (٢٠١٧). *صناعة النجومية*، مكتبة الملك فهد الوطنية.

الحنيطي، ماجد محمد (٢٠٢١). *تكنولوجيا الصراعات الدولية المعاصرة*، دار الآن، الأردن.

زرنير، آمال. (٢٠٢٠). أثر حروب الجيليلن الرابع والخامس في إدامة الصراع بدول المنطقة العربية: سوريا وليبيا أنموذجا، مجلة العلوم الاجتماعية، مجلس النشر العلمي، جامعة الكويت، ٤٨(٤)، ٢٣-٢٨.

صالح، أمنية محمد البكري؛ أحمد، إيمان أحمد سيد. (٢٠٢٥). استراتيجيات الحماية من الهندسة الاجتماعية وعلاقتها بالحد من مهددات الأمن الأسري لدى عينة من ربات الأسر، *مجلة البحوث في التربية النوعية، جامعة المنيا*،١١ (٥٧)، ٨٣-١٣٢.

السمحان، منى عبد الله. (٢٠٢٠). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. *مجلة كلية التربية، جامعة المنصورة*، ١١١ ، ٣-٣١.

الشايع، خالد. (٢٠١٩). *الأمن السيبراني مفهومه وخصائصه وسياساته*، القاهرة، الدار العالمية للنشر والتوزيع.

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

العمري، صالح محمد حسن؛ العمري، عبد الرحمن عبد الله. (٢٠٢٤) الآثار الاجتماعية للهندسة الاجتماعية في الفضاءِ الرقمي على المُجتمع السعودي: د راسة وصفية على عينة من طلبة جامعة الملك عبد العزيز بجدة، المجلة الدولية للتصاميم والبحوث التطبيقية، *جمعية تكنولوجيا البحث العلمي والفنون*، ٣ (٨)، ١-٤٣.

فاروق، علي؛ علي، خديجة. (٢٠١٥). القرصنة الإلكترونية في الجزائر وأثرها على المستخدم، مكتبة عين الجامعة، متاح على الرابطhttps://ebook.univeyes.com/34400

فوزي، إسلام. (٢٠٢٢). الأمن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سوسيولوجي، المجلة الاجتماعية القومية، *المركز القومي لبحوث الاجتماعية والجنائية، القاهرة*، ٥٦(٢) مايو، ٩٩-١٣٩.

الكندي، سالم سعيد، البلوشي، حليمة سليمان. (٢٠٢٠)، الوعي بثقافةِ الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عُمان، *مجلة العلوم والآداب الاجتماعية- جامعة السلطان قابوس*، ١١ (٢)، ٧٠-٨٦.

محمد، سماح. (٢٠١٦). دور المؤسسات التربوية في مواجهة الإرهاب الإلكتروني. *مجلة كلية التربية، جامعة كفر الشيخ – كلية التربية*، ١٦ (١)، ٢٨١-٣٤٣.

محمود، أحمد محمود؛ مجاهد، نهي عادل (٢٠٢٢). التربية الإعلامية كآلية لتمكين طلاب الجامعة من مواجهة حروب الجيل الخامس، وتحقيق الأمن الإنساني، المجلة المصرية لبحوث الإعلام، ٨٠، كلية الإعلام، جامعة القاهرة.

المطيري، عبد الاله (٢٠١٨). دور الإعلام الجديد في التوعية من الجرائم الإلكترونية، رسالة ماجستير (جامعة نايف العربية للعلوم الأمنية)، كلية العوم الاجتماعية.

المنتشري، فاطمة يوسف، حريري، رنده (٢٠٢٠) درجة وعى معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، المجلة العربية للتربية النوعية، *المؤسسة العربية للتربية والعلوم والآداب، القاهرة*، (١٤)، ٩٥-١٤٠.

المنيع، الجوهرة عبد الرحمن إبراهيم. (٢٠٢٢). متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠، *المجلة العلمية لكلية التربية، جامعة أسيوط*،٣٨ (١)، يناير، ١٥٦-١٩٤.

الهيئة الوطنية للأمن السيبراني. (٢٠١٨). الضوابط الأساسية للأمن السيبراني Retrieved . https://ega.ee/wp-content/uploads/2024/12/Essential-Cybersecurity-Controls.pdf

ثانيا: مراجع أجنبية:

Alshingiti Z., Alaqel R., Al-Muhtadi J., Haq Q.E.U., Saleem K Faheem., M.H (2023)., A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN, Electronics 12 (1) 1 Art. no.Jan

Bengt, Larson et, al .(2012): transformation of the swidsh with Ferris State from social engineering to governance, US, *PALGRAVE MACMILLAN*.

Bullee, Jan-Willem, &Junger, Marianne. (2021), Social Engineering, Linkoping University, Linkoping, Sweden

Chetioui, K., et al. (2022). Overview of social engineering attacks on social

Coughlin, T.M. (2017). Cybersecurity Education for Adolescents and Non-Technical Adults. *Master's Thesis*. An Academic Publisher. USA. 11(1)

Daricili, A. B., & Celik, S. (2022). National Security 2.0: The Cyber Security of Critical Infrastructure. PERCEPTIONS: *Journal of International Affairs, 26*(2), 259-276

https://doi.org/10.1016/j.jisa.20٢٤.09. 05

Krombholz, K., Hobel, H., Huber, M., &Weippl, E.(2015). Advanced social engineering attacks. *Journal of Information Security and applications*, 122-113 ,22.

Lehto, M. (2018): Cyber security education and research in the Finland's universities and universities of applied sciences. Cyber security an threats: Concepts, methodologies, tools, and applications, IGI Global, pp 248-267.

Mangold, L.V. (2016): An Analysis of Knowledge Gain in Youth Cybersecurity Education Programs

Nakama, D., & Paullet, K. (2018). The Urgency for Cybersecurity Education: The Impact of Early College Innovation in Hawaii Rural Communities. *Information Systems Education Journal, 16*(4), 41-52.

networks. *Procedia Computer Science*, (198), Leuven, Belgium, P.P657.

Phoenix nap. (2019). phoenix nap. Retrieved from 17 Types of Cyber Attacks to Secure Your Company From in 2024: https://phoenixnap.com/blog/cyber-security-attack-types

Redman, S. & Joiner, K. F. (2020): Improving General Undergraduate Cyber Security Education: A Responsibility for All Universities? Creative Education, 11(12), pp 2541 –2558.

Taylor, H. (2020, 22 Jan). What Are Cyber Threats and What to Do About Them. Retrieved from prey: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

Triada network, (2019). "Different types of cyber security", triada network,

Wijayanto, H., & Prabowo, I. A. (2020): Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Journal Sisfokom (Sistem Informasi dan Komputer)*, *9*(3), pp 395-399

Zec, M. & Kajtazi, M. (2015). Examining How IT Professionals in SmesTake Decisions About Implementing Cyber Security Strategy،P aper Presented at Ecime 2015 - 9th European Conference, UK, September 2122 ,2015، Retrieved from: Https://Www.Researchgate.Net/ Publication/ 338149057_Examining_How_IT_Professionals_In_Smes_Take_Decisions_About_Implementing_Cyber_Security_Strategy.