جامعة السلطان قابوس
مجلة الآداب والعلوم الاجتماعية

Sultan Qaboos University
Journal of Arts & Social Sciences

الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان: دراسة حالة لطلبة الكلية التقنية بالمصنعة

سالم سعيد الكندي

أستاذ مساعد

قسم دراسات المعلومات - كلية الآداب والعلوم الاجتماعية

جامعة السلطان قابوس

salimsk@squ.edu.om

حليمه سليمان البلوشي

مدير مكتبة الكلية التقنية بالمصنعة

halima@act.edu.om

تاريخ الاستلام:٢٠١٩/٠٣/١١

تاريخ القبول للنشر: ٢٠٢٠/٠٢/١٠

الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان: دراسة حالة لطلبة الكلية التقنية بالمصنعة

سالم سعيد الكندي، وحليمه سليمان البلوشي

الملخص

هدفت الدراسة الحالية التعرف عن مستوى وعي الطلبة بالكليات التقنية بسلطنة عمان بأساليب الهندسة الاجتماعية من خلال الوقوف على مدى وعي الطلبة بمفاهيم التصيد، والبريد الاحتيالي وغيرها من الأساليب المتبعة للحصول على معلومات تتمتع بالخصوصية والسرية. كما تهدف إلى الكشف عن طبيعة السلوكيات والممارسات عند استخدام شبكات التواصل الاجتماعي والبريد الإلكتروني وكذلك الوسائل التنظيمية والتقنية للحد من الوقوع في شباك الهندسة الاجتماعية. ولتحقيق أهدف الدراسة الحالية، اتبعت الدراسة المنهج الكمي، متمثلًا في الاستبانة كأداة لجمع البيانات، وشمل مجتمع الدراسة جميع الطلبة (٢٩٠٨ طالبًا) في تخصصات الهندسة والدراسات التجارية وتقنية المعلومات بالكلية التقنية بالمصنعة باستثناء طلبة السنة التأسيسية. وصل عدد الاستبانات المسترجعة ٦٦٣ استبانة صالحة، وعليه يكون عدد الاستبانات الخاضعة للدراسة ٦٦٣ استبانة أي ما نسبته ١٩٪. تمثلت أهمية الدراسة في ندرة الدراسات المشابهة والتطبيقية التي تسلط الضوء على دراسة مدى وعي المجتمع الجامعي بمخاطر الهندسة الاجتماعية، بالإضافة إلى محدودية الدراسات العربية المماثلة التي تناولت الموضوع ذاته في تخصصات أخرى متنوعة، لذلك يؤمل أن تثري هذه الدراسة النتاج الفكري العربي في هذا المجال. أما الجانب التطبيقي فيتمثل في مساعدة إدارة الجامعات والكليات أو الجهات المعنية ببث الوعي لدى الطلبة، وأعضاء هيئة التدريس للوقوف على مثل هذه القضايا وتوضيح أهميتها وأهمية التصدي لمثل تلك الأساليب. أشارت نتائج الدراسة بشكل عام إلى ضعف مستوى دراية الطلبة بمفاهيم الهندسة الاجتماعية وأساليبها، كما أشارت النتائج أن ٥٥٪ بواقع ٣٥٤ طالبًا لم يسمعوا بالمصطلح نهائيًا، في حين ٤٥٪ على دراية بالمصطلح مع مستويات مختلفة من الاهتمام. وأن الغالبية من الطلبة لديهم وعي ببعض الممارسات التنظيمية والتقنية للوقاية من أساليب ومخاطر الهندسة الاجتماعية بطريقة غير مباشرة، إلا أن هذه النسب لا تتجاوز النصف في بعض الحالات، أي أنه لا يقل عن ٤٠٪ لهم ممارسات خاطئة عند استخدام البريد الإلكتروني ومواقع الشبكات مما يجعلهم عرضه للوقوع في شباك الهندسة الاجتماعية. خرجت الدراسة بمجموعة من التوصيات من أهمها: توعية المجتمع الجامعي بمفهوم الهندسة الاجتماعية وأساليبها، وتعزيز ثقافة الأمن السيبراني والهندسة الاجتماعية من بطرح مساقات تحاكي واقع ذلك، ثم تفعيل دور اختصاصي المعلومات في المسؤولية المجتمعية والوعي الرقمي.

الكلمات المفتاحية: الهندسة الاجتماعية، الوعي الرقمي، الوعي المعلوماتي، الخصوصية الرقمية، كليات التعليم التقني.

Awareness of Social Engineering Among Higher Colleges of Technology students: A Case Study of Al Musanna College of Technology

Salim Said Alkindi and Halima Sulaiman Darwish Al-Balushi

Abstract

The main objective of this study was to investigate the awareness of Social Engineering among Al Musanna College of Technology students in the Sultanate of Oman by identifying the students' awareness of the concepts of phishing, email fraud, and other social engineering techniques that use to obtain sensitive or confidential information. It also aimed to detect the nature of behaviors and practices when using social media, and the methods to avoid social engineering attacks. To achieve the objectives of the study, the current study followed the quantitative approach, represented in the questionnaire as a data collection tool. The study population consist of all students (2908) in Al Musanna College of Technology in three fields: engineering, business and information technology, excluding foundation year students. A total of 663 questionnaires were valid, the response rate to the survey was %19. The importance of this study that there are relatively few studies that highlight the unique of critical importance of teaching students how to avoid social engineering attacks, by introducing social engineering in such courses and provide students and faculty members with several workshops in order to educate them how to deal with such attacks. It also will create a new knowledge about level of students' awareness and attitudes about social engineering. The study found that the level of students' knowledge of the concepts and methods of social engineering is low.The results indicated that %55 of the students did not hear of this term definitively, while %45 knew the term with different levels of interest. The study also showed that majority of students were aware of some regulatory and technical practices that followed in order to avoid social engineering attacks, but these percentages do not exceed half in some cases, meaning that at least %40 have not demonstrate safe practices when using e-mail and/ or social media. The study came out with a set of recommendations, including raising the awareness of the university community about the concept of social engineering and its methods, educating students on the culture of cybersecurity and social engineering via courses, and activating the role of information specialist in social responsibility and digital awareness.

keywords: Social Engineering; Sultanate of Oman; Higher Colleges of Technology; Digital literacy; Information literacy.

المقدمة

لقد صاحب تطور وسائل الاتصال الحديثة وتكنولوجيا المعلومات والاتصالات، كتطور تقنيات حديثة في الأجهزة الذكية وظهور وسائل التواصل الاجتماعي، تسهيلات عديدة في نقل وتبادل المعلومات والمعرفة على مستوى الأفراد وكذلك مستوى المؤسسات والمنظمات. إلا أن كل تطور في مجالات التقنية الحديثة لا يخلو من كثير من المخاطر، فالتقنية أداة يمكن أن تشكل بطريقة إما لتحقيق أهداف إيجابية بمعنى تطويرية وتنظيمية لخدمة مجتمع ما أو تستخدم لأهداف غير ذلك، كما صاحب أيضًا هذا التطور ظهور كثير من الجرائم المعلوماتية على الشبكات، وظهور أنواع مختلفة من القضايا في الفضاء السيبراني (cyberspace)، ويعتبر مصطلح الأمن السيبراني (cybersecurity) من المصطلحات التي لاقت كثير من الانتباه في الفترة الأخيرة، لما لها من تأثير كبير على المؤسسات والأفراد بل على الدول. فلقد أصبحت التهديدات السيبرانية أحد التحديات الرئيسية التي تواجه كثير من دول العالم، مما يتحتم عليها مواجهتها، وخاصة مع تزايد الاعتماد على الإنترنت بشكل رئيس في مختلف المجالات، خاصة في الأمن القومي، مثل الشبكات العسكرية والبيانات المالية والمصرفية، وأمن المؤسسات بمختلف أنواعها، ومنها: البنوك والمؤسسات الاقتصادية والمنظمات وغيرها. فضلًا عن تزايد توجه الكثير من المؤسسات والمنظمات للتطبيقات المفتوحة وخدمات السحابة الإلكترونية وغير ذلك مما سهل عمل هذه المؤسسات.

يشير مصطلح الأمن السيبراني إلى مجموع الوسائل التقنية والتنظيمية والإدارية والتشريعية: لتعزيز حماية البيانات الشخصية وسريتها وخصوصيتها، ولضمان توفر عمل نظم المعلومات في الموسسات واستمراريته، وغالبًا ما يستخدم كثير من المتخصصين مصطلح الأمن السيبراني بشكل تبادلي مع مصطلح أمن المعلومات إلا أن في الحقيقة يوجد اختلاف بينهما؛ فقد تناول VanNiekerk (2013) وVon Solms تفاصيل مصطلح الأمن السيبراني وأمن المعلومات وأوجه الاختلاف بينهما، فقد أوضح الباحثان أن الأمن السيبراني يتجاوز حدود أمن المعلومات التقليدية ليشمل ليس فقط حماية موارد المعلومات، بل يشمل أيضاً الموجودات الأخرى في الفضاء السيبراني، بما في ذلك الشخص نفسه. ففي مجال أمن المعلومات يؤدي العامل البشري دورًا مهما في العملية الأمنية. في حين آن لهذا العامل في الأمن السيبراني بعد إضافي؛ أي قد يشكل الفرد أو الأشخاص أهدافًا محتملة للهجمات السيبرانية أو حتى التشارك ومن دون قصد في هجوم سيبراني. ويعرف الاتحاد الدولي للاتصالات (International Telecommunication Union, ITU) كما ورد في مختار، (٢٠١٣) الأمن السيبراني بأنه مجموعة الأدوات والسياسات، ومفاهيم الأمن، والضمانات الأمنية، ومناهج إدارة المخاطر، والإجراءات والتدريبات، وآليات الضمانات والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرية وأصول المؤسسات والمستخدمين، ويقصد بأصول المؤسسات: سلامة المعلومات (integrity)، والسرية (confidentiality) أي الحفاظ على القيود المصرح للوصول للمعلومات والإفصاح عنها، والتوافر (availability): ويعني ضمان الوصول للمعلومات في الوقت المناسب واستخدامها. في حين يرى Singh, and Vaish Keserwani (2014) أن أمن المعلومات (Information Security) يتمثل في حماية المعلومات ونظم المعلومات من الوصول غير المصرح به أو الاستخدام أو التعطيل أو التدمير، سواء في التخزين أو المعالجة أو النقل، والحرمان من الخدمة للمستخدمين المرخص لهم. كما يشمل أمن المعلومات تلك التدابير اللازمة لاكتشاف مثل هذه التهديدات وتوثيقها ومواجهتها، كما يتضمن مجموعة واسعة من إجراءات الأمان المادية مثل حماية أصول المعلومات الخاصة بالمؤسسة ضد الكوارث الطبيعية أو السرقة وهجمات الهندسة الاجتماعية.

وليس الهدف هنا التفصيل أو البحث في أوجه الاختلاف أو التشابه بين المصطلحين ولكن استعراض تأثير الهجمات السيبرانية (cyberattacks) على الأفراد والمؤسسات. فقلد أشار التقرير السنوي للأمن السيبراني بواسطة Cisco (2018) بأن سبعة من واقع عشر منظمات أفصحت بأن معدل هجمات الأمن السيبراني في تزايد في سنة ٢٠١٧، وأن معظم الهجمات بنسبة ٧٧٪ نجحت في اختراق المؤسسات عن طريق استخدام تقنيات بدون ملفات، كما أوضح نتائج التقرير أن ٦٩٪ من المؤسسات تعتقد بأن برامج مكافحة الفيروسات لا يمكنها إيقاف التهديدات السيبرانية، كما أشار التقرير أيضًا أن الإنفاق العالمي على الأمن السيبراني سيصل إلى ٩٦ مليار دولار في عام ٢٠١٨. كما قدرت قبل ذلك حكومة المملكة المتحدة أن الجريمة السيبرانية تكلف البلاد حوالي ٢٧ مليار جنيه إسترليني سنوياً، ووفقاً لبعض التقديرات، فإن التكلفة العالمية تبلغ ١ تريليون دولار سنوياً. وقد سهّلت موجة الجرائم هذه إلى حد كبير من خلال ظهور الاتصالات الإلكترونية، ولا سيما تلك التي تستخدم الإنترنت. (Tankard, 2011). فضلًا عن ارتفاع معدل استخدام الأجهزة الذكية ومواقع الشبكات الاجتماعية، فلقد سجلت شبكات التواصل الاجتماعي الفيسبوك(Facebook) وتويتر (twitter) وانستجرام (Instagram)، سناب شات (Snapchat) أكثر الشبكات الاجتماعية استخدامًا على مستوى العالم في نهاية نوفمبر ٢٠١٨ (Chaffey, 2018). كما سجلت أيضًا معدل استخدام كبير وخاصة على مستوى الدول العربية، ففي عمان أشار التقرير السنوي لاستخدام شبكات التواصل الاجتماعي (Arab Social Media Report,2017) أن نسبة استخدام الشبكات الاجتماعية في السلطنة على النحو الآتي: ٨٨٪ للفيس بوك (Facebook)، ٨٠٪ للواتساب (WhatsApp) ٤٠٪ لليوتيوب (YouTube) و انستجرام (Instagram)، و٣٦٪ لتويتر (twitter). ومع توسع دائرة الأمن السيبراني وارتباطه بكثير من التهديدات الإلكترونية كتعطيل الخدمة (Interruption of Service)عندما يقوم الخادم أو الجهاز بصورة تضر المستخدم النهائي الذي يتلقى هذه الخدمة، وإتلاف المعلومات وتعطيلها (Corruption or modification of information) أو التجسس على الشبكات، وتدمير أصول المعلومات؛ ظهر مصطلح الهندسة الاجتماعية

(social engineering) بشكله الجديد، والمقصود بشكله الجديد أن مصطلح الهندسة الاجتماعية مصطلح قديم، ويعود ظهور مصطلح المهندس الاجتماعي لمقالة للكاتب الهولندي Van Marken في عام ١٨٩٤ (socialeingenieurs) أي المهندسين الاجتماعيين. ويختلف أيضًا تعريف الهندسة الاجتماعية وفقًا للحقول المختلفة، أما الهندسة الاجتماعية من ناحية (الأمن security)، فتتمثل في الحصول على معلومات سرية عن طريق التلاعب/ أو خداع الناس. ويمكن تعريف الهندسة الاجتماعية كما ذكرها كيفن متنك (Kevin Mitnick) في كتابه (The Art Of Deception) بأنها استخدام الحنكة لخداع الشخص أي فن التلاعب بالآخرين، إذ يمكن من خلال ذلك أن يكشف عن معلومات سرية أو بإعطاء المهاجم الفرصة للوصول للمعلومات السرية التي قد تقع ضمن نطاق الخصوصية، وبالتالي فهي تتمثل في مجموعة من التقنيات المستخدمة لجعل الناس يؤدون عملا ما أو يفضون بمعلومات سرية (Mitnick, 2003). ويمكن تناول مفاهيم الهندسة الاجتماعية ومخاطرها وأساليبها في الصفحات القادمة.

زخر النتاج الفكري بمجموعة من الدراسات باللغة الانجليزية عن موضوع الهندسة الاجتماعية بشكلها القديم (مثال: May, 1980; Weinberg, 1966; Granger, 2001) كما تناولت أيضًا مجموعة من الدراسات موضوع الهندسة الاجتماعية إما من ناحية نظرية أو من ناحية توعية وثقافة تنظيمية دون التطرق إلى الجانب التطبيقي بها (مثال: Thornburgh, 2004; Abraham, Chengalur-Smith, 2010; Irani, Balduzzi, Balzarotti, Kirda and Pu, 2011). فلقد أوضح Hadnagy (٢٠١٠) في كتابه بعنوان "الهندسة الاجتماعية: فن القرصنة البشرية" تفاصيل الهندسة الاجتماعية وأساليبها، كما ظهرت كثير من الدراسات التي تعالج مفاهيم الهندسة الاجتماعية ومخاطرها، ومع ذلك فلقد أشار النتاج الفكري أن معظم مستخدمي الإنترنت ليس لديهم ثقافة معرفية بقضايا السرية على الإنترنت (Chitrey, Singh and Singh, 2012)، ولقد طبقت كثير من الدراسات بعض النظريات ومنها: دراسة Gulenko (2013) وخلصت إلى أن هنالك ضعف في ثقافة المستخدمين بمخاطر الهندسة الاجتماعية. وعند الحديث عن النتاج الفكري باللغة العربية فنجد ندرة في الدراسات التي تناولت موضوع الهندسة الاجتماعية بشكل تطبيقي من خلال الدراسات الميدانية. وتعد الدراسة الحالية على حد علم الباحث من الدراسات الأولى التي تجرى على طلبة الجامعات والكليات بشكل عام والكليات التقنية بسلطنة عمان بشكل خاص؛ للكشف عن مدى وعي الطلبة بمخاطر الهندسة الاجتماعية وطبيعة الممارسات الخاطئة على شبكة الإنترنت. وبناء على ذلك تسعى الدراسة إلى تحقيق الأهداف الآتية:

- الكشف عن مستوى معرفة الطلبة ودرايتهم بمفهوم الهندسة الاجتماعية وأساليبها
- طبيعة ممارسات الطلبة وسلوكياتهم على مواقع الإنترنت أو مواقع الشبكات الاجتماعية

ومن أهداف الدراسة المشار إليها أعلاه، تأتى أسئلة الدراسة على النحو الآتي:

١. ما مستوى وعي الطلبة بمخاطر الهندسة الاجتماعية وأساليبها؟
٢. ما طبيعة ممارسات الطلبة وسلوكياتهم على مواقع الإنترنت أو مواقع الشبكات الاجتماعية؟
٣. هل توجد فروق ذات دلاله إحصائية يعزى لمتغير الجنس والتخصص ومستوى معرفتهم بمخاطر الهندسة الاجتماعية؟
٤. هل توجد فروق ذات دلاله إحصائية يعزى لمتغير الجنس والتخصص وطبيعة ممارسات الطلبة على مواقع الإنترنت؟

تنبع أهمية الدراسة في ندرة الدراسات المشابهة والتطبيقية التي تسلط الضوء على دراسة مدى وعي المجتمع الجامعي بمخاطر الهندسة الاجتماعية، بالإضافة إلى محدودية الدراسات العربية المماثلة التي تناولت الموضوع ذاته في تخصصات أخرى متنوعة، لذلك يؤمل أن تثري هذه الدراسة النتاج الفكري العربي في هذا المجال. أما الجانب التطبيقي فيتمثل في مساعدة إدارة الجامعات والكليات أو الجهات المعينة ببث الوعي لدى الطلبة، وأعضاء هيئة التدريس للوقوف على مثل هذه القضايا وتوضيح أهميتها وأهمية التصدي لمثل تلك الأساليب، كما تكمن أهمية الدراسة التطبيقية في اقتراح بعض الأساليب أو الإجراءات التي من شأنها توعية الطلبة مفاهيم الهندسة الاجتماعية ومخاطرها على الأفراد والجماعات. وترتبط الدراسة بتخصصات أخرى مما قد تسهم النتائج في فتح أبواب أخرى لبحوث ذات العلاقة.

٢. الدراسات السابقة

يتناول قسم الدارسات السابقة النتاج الفكري وفقًا لمحورين أساسيين لتحقيق أهداف الدراسة، إذ يتناول المحور الأول مفهوم الهندسة الاجتماعية وأساليبها في حين يتناول المحور الثاني مجموعة الدراسات ذات العلاقة بالهندسة الاجتماعية ومدى وعي المستخدمين والممارسات الخاطئة على مواقع الإنترنت، ونظرًا لقلة النتاج الفكري حول مدى وعي الطلبة الهندسة الاجتماعية ستشكل الدراسات ذات العلاقة لخدمة أهداف الدراسة الحالية.

٢,١. مفهوم الهندسة الاجتماعية وأساليبها

لقد ورد تعريف الهندسة الاجتماعية في ٢٧ قاموس متخصص في قاعدة بيانات (Onelook)، ونجد بأن مفهوم الهندسة الاجتماعية يختلف وفقًا 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، كما تعرف أيضًا بأنها استخدام التخطيط المركزي في محاولة لإدارة التغيير الاجتماعي (Oxford Dictionaries). 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) (Dictionaries إلى استخدام أساليب الخداع للتلاعب بالأفراد بهدف الحصول على معلومات سرية 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. وعند الحديث عن مفهوم الهندسة الاجتماعية كما ورد في النتاج الفكري، فيعرفها Granger (2001) بأنها فن التلاعب بعقول الأفراد لكسب الثقة وتحقيق الغاية، وبالتالي فهي وسيلة ذكية للحصول على الرقم السري لمستخدم دون الحاجة لخرق النظام تقنيًا. ومهما أختلف مفاهيم الهندسة الاجتماعية، فالمغزى المراد تحقيقه هو الحصول على بيانات تتمتع بطابع عالي من الخصوصية والسرية، ويمكن النظر أيضًا للهندسة الاجتماعية من منظور معلوماتي؛ فيرى المتخصصون في مجال المعلومات بأن استخدام المصطلح مرتبط بالبيانات والمعلومات، فالوصول إلي البيانات ومعالجتها يكشف عن معلومات يستفاد منها لتحقيق غايات أخرى.

تختلف الأساليب والطرق التي يتبعها مستخدمو الهندسة الاجتماعية أو ما يطلق عليهم المهندسون الاجتماعيون في الوصول لمرادهم. تناول Granger (2001) مجموعة من أساليب الهندسة الاجتماعية ومنها:

(١) استخدام الهاتف في الخداع (Social Engineering by Phone) وتتمثل في اتصال هاتفي من المهندس الاجتماعي للضحية بهدف خلق سيناريو يفصح فيه المستخدم عن كلمة المرور أو إقناع الضحية بتحويل مبلغ أو ما شابه ذلك،

(٢) سلة المهملات أو بقايا المهملات (Dumpster Diving)وهي إحدى الطرق التي يستخدمها المهندس الاجتماعي؛ فسلة المهملات في المؤسسات والشركات قد تكون غنية بالمعلومات لما تحتويه من أوراق أو رسائل متلفة، أو أرقام هواتف أو مستندات وغير ذلك مما يشكل قيمه للمهندس لاستخدامها في عملية الخداع. وقد تناول E Frumento (2016) عدة طرق للهندسة الاجتماعية منها: أسلوب التصيد (Phishing) أو التصيّد الاحتيالي ويتمثل عندما يرسل المهندس الاجتماعي رسالة عن طريق بريد الكترونيً لشخص موثوق به، يطلب من الضحية رقمًا أو معلومة سرية يحتاجها المهندس لتحقيق هدف ما، وعادةً ما تتخذ تلك المصيدة في شكل بريد إلكتروني أو دردشة أو إعلان على الويب أو موقع ويب تم تصميمه لانتحال شخصية، رابط إلى صفحة ويب مزورة تبدو مشروعة أو غير ذلك بهدف سرقة كلمات المرور، وعادة ما يرسل المهندس الاجتماعي هذه الرسائل إلى أكبر عدد من الناس، ويأتي التصيد على طريقتين: الصيد بالرمح (Spear Phishing) وهي عندما يكون الضحية محدد مسبقًا من قبل المهندس الاجتماعي أي يملك المهندس الاجتماعي معلومات عن الضحية. والنوع الآخر يطلق عليه باسم (Vishing) أي voice Phishing أي رسالة صوتية تطلب من الضحية الاتصال بالبنك أو المصرف للتحقق من المعلومات. أما الطريقة الأخرى التي ذكرها المؤلف فيطلق عليها الفخ أوالطعم (Baiting) وفي مضمونه يشبه التصيد الاحتيالي، يتضمن تقديم شيء مثير لإغراء المستخدم النهائي، في مقابل معلومات تسجيل الدخول أو البيانات الخاصة. ويمكن أن يستخدم هذا الأسلوب على شكلين: الأول من خلال تنزيل مقاطع الموسيقى أو الأفلام أو غير ذلك ويتم ذلك بعرض بعض الروابط للمستخدم في مواقع لتنزيل مقاطع موسيقى معينة أو أفلام وبمجرد الضغط على الرابط يمكن تنزيل البرمجيات الخبيثة في جهاز المستخدم أو الضحية. أما الهيئة الأخرى فتتمثل في ان يضع المهندس الاجتماعي جهازا يحمل فيروسًا أو برنامجًا ضارًا، مثل فلاش، في مكان عام، يلتقطه الضحية المفترض ويدخله في الحاسوب، من دون أن يعلم بأنه ترك عمدًا. ومن الأمثلة على تلك البرامج التي تستخدم الطعم ما يطلق عليه أحصنة طروادة Trojan Horses. كما يستخدم المهندس طريقة أخرى يطلق عليها أسلوب (Pretexting) وهو عبارة عن سيناريو مخترع (Invented Scenario) يحدث عندما يخلق المهندس الاجتماعي إحساسًا بالثقة بينه وبين المستخدم النهائي عن طريق انتحال شخصية معينة قد يكون زميل عمل أو مسؤول عن الضحية في مكان العمل، وينتشر هذا النوع في الأيام الحالية عن طريق رسائل الاحتيال التي ترد عن طريق خدمة الواتساب. تناول أيضًا Hadnagy (2010) مجموعة من الأساليب التي يستخدمها المهندس الاجتماعي وهي نفس الأساليب المذكورة أعلاه بشي من التفصيل. وتعد أساليب التصيد بأنواعها المختلفة من أكثر الوسائل استخدامًا، فقد حلل Hadnagy محتوى أكثر من ١٠٠ رسالة بريد الكتروني تصيدية، وتتخذ طابع الاحتيال، وأسفرت نتائج التحليل أن أكثر الأساليب المستخدمة للتصيد رسائل التنبيه (alert) ورسال التحقق من الحساب (account verification) وعادة ما تأتي من البنوك أو المؤسسات التي يعمل بها الموظف.

ومع تطور تقنيات الويب وظهور الشبكات الاجتماعية والتطبيقات الذكية الاجتماعية، وتوجه كثير من الأفراد لاستخدامها فتحت أبوًابًا أخرى وطرق للخداع، فقد ذكر Chitrey, Singh and Singh (2012) مجموعة أساليب أخرى لاستخدام البرمجيات الخبيثة عن طريق الشبكات الاجتماعية والتطبيقات والبرامج الاجتماعية، البريد الإلكتروني، أحصنة طروادة، وغيرها. وأوضح Krombholz, Hobel, Huber and Weippl (2015) أن طبيعة خدمات الويب والإنترنت التي يستخدمها عمال المعرفة اليوم تمهد الطريق للهجمات الهندسية الاجتماعية المتطورة، وخاصة في ظل توجه الموظفين لاستخدام أجهزتهم الخاصة بما فيها الهواتف الذكية في بيئة العمل، فضلًا عن استخدام أدوات الاتصال والتعاون عبر الإنترنت فاستخدام شبكات التواصل الاجتماعي قد يؤدي لإنشاء نواقل هجوم جديدة لهجمات الهندسة الاجتماعية. لقد أظهرت الهجمات الأخيرة على شركات مثل New

York Times and RSA أن هجمات التصيد الاحتيالي المستهدفة هي خطوة تطورية فعالة لهجمات الهندسة الاجتماعية. كما أن انتشار استخدام شبكات التواصل الاجتماعي أدى أيضًا إلى استخدام أساليب أخرى من الهندسة الاجتماعية يطلق عليها (automated social engineering attack)، وتتم بشكل آلي باستخدام تقنيات الرد الآلي وغيرها (Huber, Kowalski, Nohlberg, Tjoa, 2009). ويؤكد أيضًا Abraham و Chengalur-Smit (٢٠١٠) علي أن انتشار استخدام التطبيقات والبرامج الاجتماعية بين مستخدمي الإنترنت وسيلة أخرى للوقوع في شباك الهندسة الاجتماعية من خلال تنزيل البرمجيات الخبيثة ضمن تلك التطبيقات. كما أشار أيضًا Irani, Balduzzi, Balzarotti, Kirda and Pu (2011) إلى نوع آخر من الهندسة الاجتماعية يطلق عليه الهندسة الاجتماعية العكسية (Reverse social engineering) فلقد أظهرت الأبحاث السابقة أن مستخدمي الشبكات الاجتماعية عبر الإنترنت يميلون إلى إظهار درجة أعلى من الثقة في طلبات الصداقة والرسائل المرسلة من قبل مستخدمين آخرين وهنا تتمثل هجمات الهندسة الاجتماعية المعكوسة في الشبكات الاجتماعية في خداع الضحية في الاتصال بالمهاجم نفسه نتيجة لتأسيس درجة عالية من الثقة بين الضحية والمهاجم إذ أن الضحية هو الكيان الذي أسس العلاقة.

ومهما تنوعت أساليب الهندسة الاجتماعية فالوصول للمعلومات السرية هو مطلب القائمين على الهندسة الاجتماعية، ويعمل أيضًا هؤلاء الأشخاص تحت ظروف معينة وفقًا لمجموعة من العناصر، فزعزعة أمن البلد وانتشار الشائعات، وضعف البنية التحية وقلة وعي المستخدمين كلها ظروف تساعد المهندس الاجتماعي من تحقيق أهدافه والوصول لمراده.

٢,٢. الوعي بمخاطر الهندسة الاجتماعية وأساليبها

تناولت كثير من الدراسات بطرق مختلفة مفاهيم الهندسة الاجتماعية ومدى وعي مستخدمي الإنترنت بمفاهيمها وإدراك مخاطرها، على مستوى الأفراد والمنظمات والمؤسسات. فمع تزايد فعالية الإجراءات الأمنية لحماية المعلومات الحساسة، يبقى الناس عرضة للتلاعب للإدلاء ببيانات أو معلومات سرية، وبالتالي يبقى العنصر البشري حلقة ضعيفة؛ الأمر الذي يجعل هجوم الهندسة الاجتماعية يستهدف هذا الضعف من خلال استخدام أساليب مختلفة للتلاعب بغية الحصول على معلومات حساسة (Mouton, Leenen, Venter, 2016)

فلقد أجرى Karakasiliotis, Furnell and Papadaki (2006) دراسة لتقييم مدى وعي مستخدمي الإنترنت بمخاطر الهندسة الاجتماعية وهجمات التصيد، استخدمت الدراسة الاستبانة كأداة لجمع البيانات تم نشرها على الويب، احتوت الاستبانة مزيجًا من ٢٠ رسالة بريد إلكتروني بشكل شرعي وغير شرعي (رسائل احتيال وتصيد) للمستخدمين، وطلب من المشاركين تصنيفها وشرح السبب المنطقي لقراراتهم. أظهرت نتائج الدراسة أن ١٧٩ وبنسبة ٣٦٪ تمكنوا من تحديد رسائل البريد الإلكتروني الشرعية أي الحقيقية غير الوهمية، مقابل ٤٥٪ نجحوا في التعرف على الرسائل غير الشرعية (الوهمية) (رسائل الاحتيال). ومع ذلك أيضًا لم يتمكن المشاركون الذين حددوا رسائل البريد الإلكتروني غير الشرعية بشكل صحيح من تقديم أسباب مقنعة لاختيارهم. وآعد Ekstedt (2016) و Flores دراسة حول تأثير العوامل التنظيمية والفردية على نية الموظفين في مقاومة مخاطر الهندسة الاجتماعية. تم توزيع استبانة على ٤٢٩٦ موظفًا من مجموعة متنوعة من المنظمات الموجودة في السويد. أظهرت النتائج أن مواقف المستخدمين من مقاومة الهندسة الاجتماعية لديها ارتباط قوي ومباشر مع نية مقاومة الهندسة الاجتماعية، كما أظهرت النتائج وجود علاقة قوية بين مواقف الأفراد التي تأثر على النية وثقافة أو الوعي بأمن المعلومات. أظهر الاختبارات أيضًا أن المواقف والمعتقدات المعيارية بثقافة أمن المعلومات تأثر على نية الموظفين في مقاومة الهندسة الاجتماعية. وبالتالي يمكن استنتاج أن كل من السلوك والمعتقدات المعيارية تلعب أدوارًا مهمة في حكم العلاقة بين ثقافة أمن المعلومات والنية لمقاومة الهندسة الاجتماعية. وبالتالي يمكن تلخيص نتائج الدراسة أن ثقافة أمن المعلومات تؤثر على موقف الموظفين تجاه مقاومة الهندسة الاجتماعية.

كما هدفت دراسة قام بها كل من Singh وChitrey, Singh (2012) لتطوير نموذج مقترح لفهم هجمات الهندسة الاجتماعية من خلال استبانة وزعت على تسعون مشاركًا في الهند، شملت خبراء مجال تكنولوجيا المعلومات مثل الاستشارات في مجال تكنولوجيا المعلومات وتطوير البرمجيات، الاستشارات الأمنية كما شملت أيضًا مجموعة من الطلبة في مختلف المنظمات والمؤسسات الصناعية ركزت الاستبانة على فهم سلوكيات المستخدمين من خلال معرفة مدى وعي الأفراد عينة الدراسة في الهند نحو الاستخدام الآمن والأخلاقي للحاسب الآلي وتطبيقات الإنترنت. كشفت نتائج الدراسة أن ٦١ ٪ من المشاركين في الاستبانة ليس لديهم ثقافة بمفاهيم السرية وتهديدات الهندسة الاجتماعية، ٩٠٪ يتفقون بأن لديهم مستوى عالي من الثقة لاستخدام مختلف الشبكات الاجتماعية والتطبيقات الاجتماعية وبالتالي فإن هذا المستوى العالي من الثقة الاجتماعية يجعلهم أكثر عرضة للهجمات القائمة على الهندسة الاجتماعية. كما جاءت نتائج دراستهم موافقة للنتاج الفكري فيما يتعلق بالقضايا المرتبطة بتكنولوجيا المعلومات، فيعتقد ٧٩ من المشاركين بأن معظم منتجات تكنولوجيا المعلومات بها ثغرات أمنية، ذكر ٦٤٪ من المشاركين أن معظم التقنيات الأمنية غير قادرة على كشف ومنع الهجمات القائمة على الهندسة الاجتماعية، ذكر ٩٣٪ من المشاركين أن بعض التقنيات المتاحة مثل تطبيق Google ومواقع الشبكات الاجتماعية ومنتديات النقاش والمدونات تستخدم بشكل كبير من قبل المهندسين الاجتماعيين كأداة لجمع المعلومات. كما أوضحت نتائج الاستبيان أن ٦١٪ من المشاركين قد واجهوا التصيّد الاحتيالي، ووجد ٥٢٪ منهم مرفقات روابط بالبريد الإلكتروني، ٤٦٪ هجمات من خلال الشبكات الاجتماعية عبر الإنترنت. بينما واجه

مشاركون آخرون هجمات من خلال النوافذ المنبثقة ,Vishing Botnets. و Dumpster Diving, Trojan Horse، ووافق ٧٦٪ من المشاركين على إن خدمة البريد الإلكتروني الوسيلة الأكثر تفضيلاً لشن الهجمات، بينما أوضح ٧٢٪ أن مصدرها الشبكات الاجتماعية و١٤٪ دعم خدمة الدردشة عبر IRC و٢٢٪ حدثت من استخدام الهاتف المحمول و٥٣٪ من خلال إعلانات منشورة على مواقع الويب. كما هدفت دراسة أخرى قام بها ,Bakhshi Furnell (2009) وPapadaki إلى التحقق من مستوى وعي الموظفين بالمنظمات التعاونية بالهندسة الاجتماعية بين الموظفين من خلال تجربة تستند على إرسال بريد الكتروني إلى ١٥٢ موظفاً تطلب منهم اتباع رابط معين إلى موقع ويب خارجي لتثبيت وتحديث برنامج. أظهرت النتائج أن ٢٣٪ من الموظفين قد تم خداعهم، مما يشير إلى أن العديد من المستخدمين يفتقرون إلى مستوى أساسي من الوعي الأمني الذي يعد مفيدًا لحمايتهم عبر الإنترنت.

وبشكل عام فلقد أوضحت نتائج الدراسات السابقة أن الوعي بكافة أنواعه، الوعي بأمن المعلومات والوعي الرقمي والمعلوماتي من أهم الوسائل التي قد تقلل من تهديدات الهندسة الاجتماعية. فلقد ذكرت دراسة Bullée, Montoya, Pieters, Junger and Hartel (2015) أن استخدام السلطة إحدى الوسائل التي يتبعها المهندس الاجتماعي في الإيقاع بالضحية، وتوصل أن التوعية تلعب دورًا هامًا في التقليل من مخاطر الهندسة الاجتماعية. كما تناول Mann (2017) في كتابه بعنوان قرصنة الإنسان: تقنيات الهندسة الاجتماعية والتدابير الأمنية المضادة، أهم الوسائل لمقاومة تلك التهديدات ومنها الوعي الرقمي. وذلك سعت كثير من المؤسسات لتوعية موظفيها بمخاطر الهندسة الاجتماعية من خلال عدة أساليب متنوعه، فلقد أشار Mataracioglu و(2011) Ozkan أن معهد UBITAK القومي لأبحاث علم الإلكترونيات والتشفير (UEKAE) التابع لأمن أنظمة المعلومات في تركيا قام بعمل مجموعة من الاختبارات على الوكالات العامة التركية في إطار "اختبارات أمن المعلومات" للتصدي لهجمات الهندسة الاجتماعية. شملت تلك الاختبارات الاتصال الهاتفي لمعاينة الموظفين من قبل المهندس الاجتماعي ومحاولة الاستيلاء على المعلومات الحساسة للموظفين عن طريق استغلال حسن نيتهم. ولقد كان الهدف من تلك الاختبارات معرفة إلى أي مدى موظفين المنظمات العامة التركية لديهم نقص في الوعي بأمن المعلومات وأنهم يهددون مبادئ أمن المعلومات في المنظمات التي يعملون بها. ولم يقتصر الأمر على المنظمات والمؤسسات بل أيضًا توجه كثير من مؤسسات المعلومات بما فيها المكتبات لتوعية الموظفين بمخاطر الهندسة الاجتماعية وخاصة أن المكتبات تتيح الوصول لعدد كبير من قواعد البيانات (Thompson, 2006)، كما تقوم كثير من المؤسسات باستخدام تمرين تطبيقي لتقييم ميل المستخدمين للرد على هجمات التصيد الإلكتروني في اختبار غير مُعلن عنه ,Dodge) (Ferguson, 2007 و Carver. لذلك أوصت كثير من الدراسات بضرورة توعية الأفراد والمؤسسات بمخاطر وتهديدات الهندسة الاجتماعية فقلد أوصى Abraham و Chengalur-Smit (2010) إلى أهمية قيام المنظمات بتخطيط برنامج شامل لأمن المعلومات، وتفعيل المسؤولية الاجتماعية المشتركة المطلوبة لمكافحة البرمجيات الخبيثة في الهندسة الاجتماعية. ومن ناحية أخرى أوضح Twitchell (2006) أنه ومع وجود عدد من التدابير المضادة للدفاع ضد هجمات الهندسة الاجتماعية، كتوعية وتعليم الموظفين، وإجراء عمليات المراجعة الأمنية، غيرها من التدابير التقنية والتنظيمية، إلا معظم مناهج المعلومات لا تتناول الهندسة الاجتماعية بشكل مباشر، وعليه يقترح Twitchell إن تعديل هذه المناهج لتشمل الهندسة الاجتماعية كموضوع قد يساعد الطلبة على الاستعداد بشكل أفضل لمواجهة تهديدات الهندسة الاجتماعية.

٣. منهجية الدراسة وإجراءاتها

اعتمدت الدراسة الحالية المنهج الكمي لتحقيق أهدافها، ويعرف المنهج الكمي على أنه طريقة لجمع وتحليل البيانات الكمية وتمثيلها احصائيًا لفهم مشكلة البحث وتحقيق الأهداف. ويعد استخدام المنهج الكمي في الدراسة الحالية الأمثل، إذ أنه يتيح فهم الوضع الحالي كميًا مما يشكل فهمًا أعمق لمشكلة الدراسة فيما يتعلق بقياس الواقع. وقد تم تحقيق المنهج الكمي في هذه الدراسة من خلال استخدام أداة الاستبانة لجمع البيانات.

تألف مجتمع الدراسة من جميع طلبة الكلية التقنية بالمصنعة للعام الأكاديمي ٢٠١٨- ٢٠١٩، والبالغ عددهم ٢٩٠٨طالبًا وطالبة في تخصصات الهندسة والدراسات التجارية وتقنية المعلومات، باستثناء طلبة السنة الدراسية الأولى؛ وذلك كونهم يدرسون البرنامج اللغة التحضيري (اللغة الانجليزية)، ولم ينخرطوا بعد في دراسة مقررات التخصص، يوضح الجدول (١) عدد الطلبة وفقًا للجنس والتخصصات العلمية.

تم توزيع الاستبانة على جميع أفراد مجتمع الدراسة، واستغرقت عملية التوزيع والتجميع من ١٠-١٥يومًا على فترات مختلفة لضمان الحصول على أكبر عدد ممكن من الاستجابات. ووصل عدد الاستبانات المسترجعة ٦٦٣ استبانة صالحة، وعليه يكون عدد الاستبانات الخاضعة للدراسة ٦٦٣ استبانة أي ما نسبته ١٩٪.

وقد تكونت الاستبانة من ثلاثة أجزاء: تمثل الجزء الأول في البيانات الشخصية، وتمثلت في: النوع، والسنة الدراسية، العمر، نوع الأجهزة المستخدمة في الولوج للإنترنت، متوسط عدد الساعات التي تستخدم فيها شبكات التواصل الاجتماعي أو المواقع الاجتماعية أسبوعيًا، حسابات الطلبة على مواقع الشبكات الاجتماعية. وتمثل الجزء الثاني في قياس مدى وعي الطلبة

جدول(١): توزيع مجتمع الدراسة وفقًا للتخصص العلمي والنوع

التخصص	ذكور	إناث	المجموع
الهندسة	٩٢٨	٤٧٧	١٤٠٥
تقنية المعلومات	٩٦	٥٨٠	٦٧٦
الدراسات التجارية	٣١٢	٥١٥	٨٢٧
المجموع	١٣٣٦	١٥٧٢	٢٩٠٨

مفاهيم الهندسة الاجتماعية وأساليبها. في حين شمل الجزء الثالث طبيعة الممارسات والسلوكيات التي يقوم بها الطلبة عند استخدام مواقع الشبكات الاجتماعية والبريد الإلكتروني، أو مواقع وتطبيقات أخرى. وللتأكد من صدق الأداة وثباتها تم توزيع الاستبانة على فئات مختلفة من المحكمين (أعضاء من هيئة التدريس في كلية الآداب والعلوم الاجتماعية، وتحديدًا من قسم دراسات المعلومات). وتم إجراء بعض التعديلات بناء على الملاحظات المسترجعة. تم تحليل نتائج الدراسة من خلال استخدام برنامج الاكسل إذ لا يتطلب تحقيق أهداف الدراسة استخدام اختبارات دقيقة، إذ قام الباحثون أولا بترقيم الاستبانات ثم ترميز البيانات التي تم جمعها، وإدخالها إلى الحاسب الآلي. وبعد ذلك تم تحديد قيمة الاختبارات المطلوبة وتمثيل البيانات إحصائيًا لتحقيق أهداف الدراسة.

٤. نتائج الدراسة ومناقشتها

يستعرض جدول (٢) استجابة أفراد مجتمع الدراسة للاستبانة، موزعًا على الجنس والتخصص والمرحلة العمرية، يتضح من الجدول أن نسبة استجابة أفراد مجتمع الدراسة لمتغير النوع متقاربة، إذ بلغت نسبة الذكور ٤١٪ بينما بلغت نسبة الإناث ٥٩٪، كما بلغت نسب استجابة مجتمع الدراسة وفقًا للتخصص ٣٩٪

جدول(٢): نسبة استجابة مجتمع الدراسة وفقًا لمتغير النوع، التخصص والعمر

النوع		
ذكر	٤١٪	٢٧١
أنثى	٥٩٪	٣٩٢
المجموع	١٠٠٪	٦٦٣
التخصص		
الهندسة	٣٩٪	٢٥٨
الدراسات التجارية	٣٢٪	٢١٠
تقنية المعلومات	٢٩٪	١٩٥
المجموع	١٠٠٪	٦٦٣
العمر		
١٨-٢٠	٣٢٪	٢٠٩
٢١-٢٣	٦١٪	٤٠٤
٢٤-٢٦	٦٪	٣٧
٢٧-٢٩	١٪	٥
٣٠ فأكثر	١٪	٨
المجموع	١٠٠٪	٦٦٣

جدول (٣): نسبة تكرار الولوج إلى الإنترنت وفقًا لنوع الجهاز المستخدم

	لم أستخدم أبدا،	نادرًا	بعض الأحيان	أحيانًا	دائمًا
١. الأجهزة اللوحية	٠	٢٦٪	٢٧٪	٢٥٪	٢١٪
٢. الهواتف الذكية	٠	٥٪	١١٪	١٥٪	٧٦٪
٣. جهاز الحاسب الشخصي أو الجهاز المحمول	٠	١٣٪	٢١٪	٣٤٪	٤٣٪
٤. الحواسيب الصغيرة أو حواسيب اليد	٠	٢٣٪	٢٧٪	٢٧٪	٢٦٪

للهندسة، ٣٢٪ للدراسات التجارية و٢٩٪ لتقنية المعلومات، وتعتبر هذا النسبة متوازنة وفقًا للمجموع الكلي لمجتمع الدراسة في كل تخصص. بينما كانت أكبر نسبة للاستجابة للفئة العمرية بين ٢١-٢٣ إذ بلغت ٦١٪، ومعظم هذه الفئة تتركز في السنة الدراسية الثانية والثالثة والرابعة.

يوضح جدول (٣) تكرار استخدام الطلبة للأجهزة الموضحة في الجدول في الولوج للإنترنت، إذ يشير الطلبة بنسبة ٧٦٪ استخدام الهواتف الذكية في الولوج إلى الإنترنت وبشكل دائم، وبنسبة ٤٣٪ استخدام الجهاز الشخصي أو المحمول بشكل دائم، كما تشير أيضًا النتائج أن كل أنواع الأجهزة تستخدم من قبل الطلبة في الولوج إلى الإنترنت، وتعتبر هذه النسب طبيعية لاتجاه كثير من الناس نحو استخدام الأجهزة الذكية في اتمام كثير من الوظائف واستخدام خدمات الويب ومنها الشبكات الاجتماعية.

كما تشير أيضا نتائج الدراسة أن ٢٪ فقط من الطلبة لا يملكون حسابًا على مواقع الشبكات الاجتماعية، في حين ٩٨٪يملكون حسابًا علي مختلف مواقع الشبكات الاجتماعية، ٣٣,٦٪ يميلون لاستخدام (Instagram)، تلي في المرتبة الثانية، (snapchat) (twitter) ثم (Facebook) بالترتيب. ومعظم الطلبة يقضون على الشبكات الاجتماعية من ٠-١٠ ساعات أسبوعيًا بواقع ٣٤٪، ١١-١٥ ساعة بواقع ٢٧٪. ولعل هذه النتائج متوقعه بالنسبة لطلبة الكلية إذ يحتل (Instagram) وسناب شات (snapchat) النسبة الأكبر من الاستخدام، إذ أن تقرير منظمة (Cisco) في ٢٠١٨، يشير أن الشبكات الفيس بوك، انستغرام، تويتر، وسناب شات تحتل أكثر نسبة استخدام على مستوى العالم، كما يشير التقرير السنوي لاستخدام شبكات التواصل الاجتماعي في ٢٠١٧ (Arab Social Media Report,2017) أن نسبة استخدام الشبكات الاجتماعية في السلطنة كالآتي: ٨٨٪ للفيس بوك (Facebook)، ٨٠٪ للواتساب (WhatsApp)، ٤٠٪ لليوتيوب (YouTube) وانستجرام (Instagram)، و٣٦ ٪ لتويتر (twitter)، كما أن نسبة الاستخدام لتلك الشبكات متقاربة عند متغير النوع والتخصص، ولا توجد فروق في الاستخدام ذات دلالة إحصائية تعزى لمتغير النوع والتخصص. إذ مع الانتشار الكبير لتلك الشبكات من خلال الهواتف الذكية ذللت كثير من الحدود الثقافية وجعلت العالم أكثر انفتاحًا.

يشير شكل (١) إلى قياس مدى معرفة الطلبة بمصطلح الهندسة الاجتماعية، إذ أشارت النتائج أن ٥٥٪ بواقع ٣٥٤ طالبًا لم يسمعوا بالمصطلح نهائيًا، في حين ٤٥٪ على دراية بالمصطلح مع مستويات مختلفة من الاهتمام، ٢٣٪ على دراية بها، ١٥٪ على دراية بها وليسوا مهتمين بمعرفة المزيد، ثم ٧٪ فقط على معرفة بها ومهتمين بمعرفة المزيد. ولعل عدم وضوح المصطلح أو التوعية بها في البيئة الأكاديمية تفسر أن أكثر من ٥٠٪ من الطلبة ليسوا على دراية بالمصطلح نفسه، مع عدم توجه الغالبية الأخرى الذين هم على علم بالمصطلح بمعرفة المزيد عنه، وهذا يدل على عدم معرفة ووعي الطلبة بخطورة الهندسة الاجتماعية والذي بدوره يؤثر على قابليتهم في معرفة المزيد عنه. ولا توجد فروق في الوعي بمعرفة المصطلح ذات دلاليه إحصائية تعزى لمتغير النوع

والتخصص. ويمكن أن يفسر عدم وجود فروق لمتغير النوع والتخصص أن المصطلح قد يكون جديدًا للطلبة، فضلًا عن عدم وجود توعية بمفهوم الهندسة الاجتماعية وأساليبها.

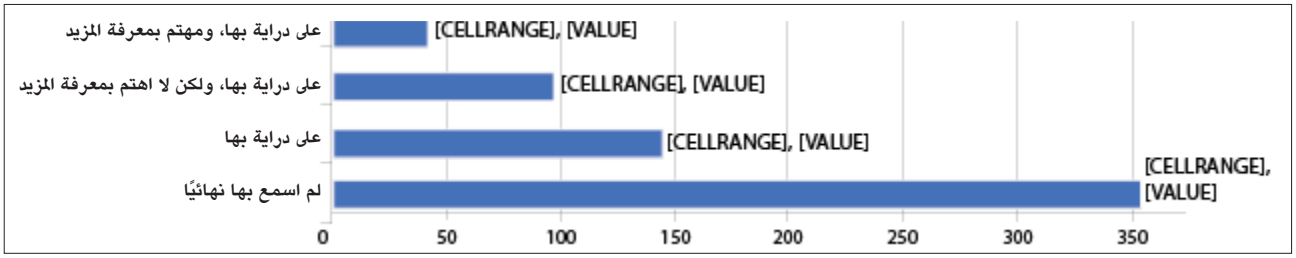
يشير شكل (٢) أيضًا إجابة مجتمع الدراسة على السؤال المتعلق بمعرفتهم بالبريد الإلكتروني الاحتيالي، إذا تشير النتائج أن ٧٠٪ من الطلبة لا يدركون ما هو البريد الكتروني الاحتيالي أو ليسوا متأكدين ما المقصود به، وهذا يعبر أيضًا عن قلة وعي الطلبة بالمصطلح، أو عدم وجود توعية أصلًا بهذا النوع من أساليب الاحتيال التي تأتي عن طريق البريد الإلكتروني.

كما يوضح الشكل رقم (٣) أن ٤٣٪ من الطلبة ليسوا على دراية بهجوم التصيد (Phishing attack) عبر البريد أو في مواقع الشبكات، وأن ٣٨٪ فقط على علم بذلك. وهذا قد يفسر أيضًا بنفس التفسير السابق وهي ضعف وعي الطلبة بأساليب الهندسة الاجتماعية، وتعتبر أساليب التصيد من الوسائل التي يستخدمها كثير من المهاجمين كما ورد في النتاج الفكري (E Frumento وآخرون، ٢٠١٦؛ Hadnagy، ٢٠١٠). كما تشير النتائج إلى عدم وجود فروق في دراية الطلبة بهجوم التصيد ذات دلالة إحصائية تعزى لمتغير النوع والتخصص.

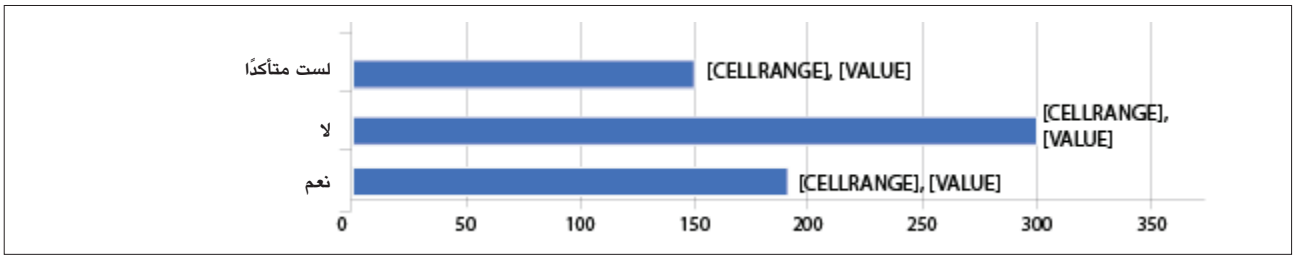
يبين شكل (٤) أن ٦٩٪ من الطلبة أفادو بأنهم لم يتعرض بريدهم الإلكتروني للاختراق، وهذه الاجابة تحمل على الشكل العام أي أن الطلبة لم يظهر لهم اختراق واضح للبريد الإلكتروني وهذا ما يعتقده كثير من الطلبة وقد يكون فعلا تصورًا واضحًا.

ولكن في المقابل تفيد اجابات الطلبة في شكل (٥)، أن ٤٩٪ أشاروا بأنهم وجودوا على جهازهم الآلي فيروس أو حصان طروادة، وهذا يفسر أيضًا الأساليب المختلفة التي يتبعها القراصنة أو المهندسين الاجتماعيين في الولوج إلى الأجهزة الخاصة بالمستخدمين،

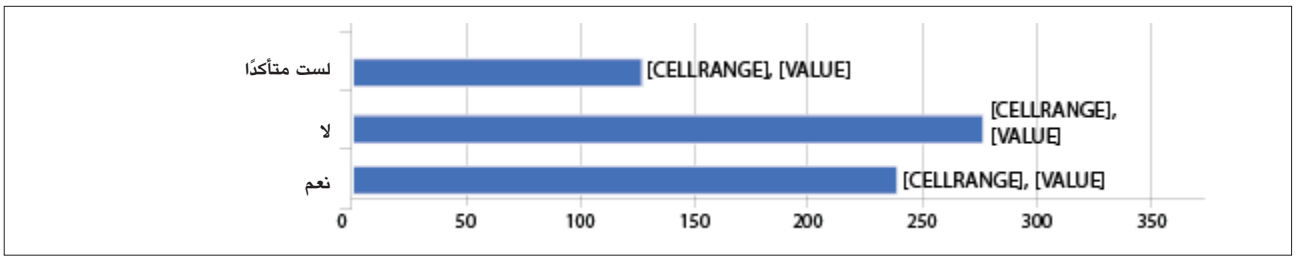
الشكل (١): هل أنت على دراية بمصطلح الهندسة الاجتماعية؟



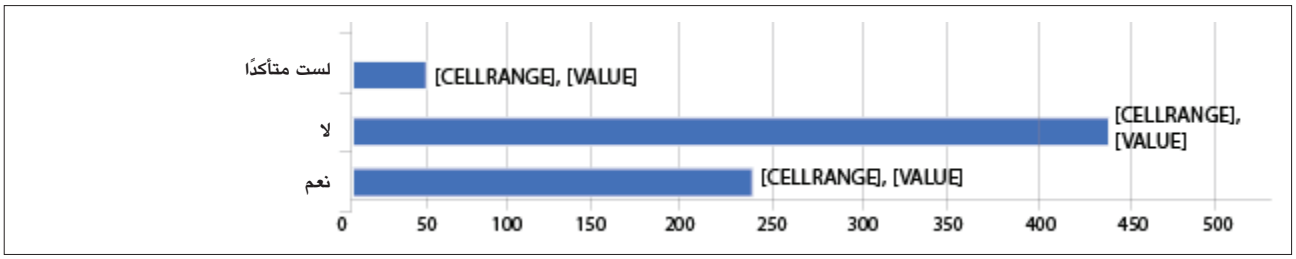
شكل (٢): استجابة مجتمع الدراسة حول معرفتهم بالبريد الإلكتروني الاحتيالي



شكل (٣): استجابة مجتمع الدراسة حول معرفتهم بهجوم التصيد



شكل (٤): استجابة مجتمع الدراسة حول مدى تعرض البريد الالكتروني للاختراق



ومن الصعب معرفة تعرض الحاسب الآلي للاختراق. إذ يشير E Frumentoوآخرون (٢٠١٦) أن أسلوب الطعم أو الفخ إحدى الأساليب المستخدمة للإيقاع بالضحية، وأن من أكثر البرامج التي تستخدم الطعم ما يطلق عليه أحصنة طروادة rojan Horses كما ذكر Singh (2012) و Chitrey, Singh مجموعة أساليب تستخدم ضمن الشبكات الاجتماعية والبريد الإلكتروني منها أحصنة طروادة، وغيرها. وتشير النتائج أيضًا إلى عدم وجود فروق في دراية الطلبة بهجوم التصيد ذات دلاليه إحصائية تعزى لمتغير النوع والتخصص.

كما يشر شكل (٦) أن ٤٧٪ من الطلبة تلقوا مكالمات هاتفية أو بريد إلكتروني يطلب منهم بياناتهم الشخصية، وهذا يدل على أن أساليب الهندسة الاجتماعية في تزايد، إذ أن حولي نصف الطلبة المنتسبين للكلية التقنية يحتمل أن يكونوا عرضة للتعرض لهذا النوع من الاحتيال، وهذا يدل أيضًا أن أسلوب التصيد بأنواعه المختلفة من أكثر الأساليب المتبعة في الاحتيال وهذا بدوره يتوافق مع دراسة Hadnagy (2010) التي استنتجت أن أكثر الأساليب المستخدمة في الاحتيال عبر البريد هو أسلوب التصيد، كما تتفق أيضًا مع دراسة Granger (2001) إذ أشار أن استخدام الهاتف في الخداع (Social Engineering by Phone) والتي تتمثل في اتصال هاتفي من المهندس الاجتماعي للضحية بهدف خلق سيناريو يفصح فيه المستخدم عن كلمة المرور أو إقناع الضحية بتحويل مبلغ أو ماشابه ذلك من الطرق المستخدمة في الايقاع بالضحية.

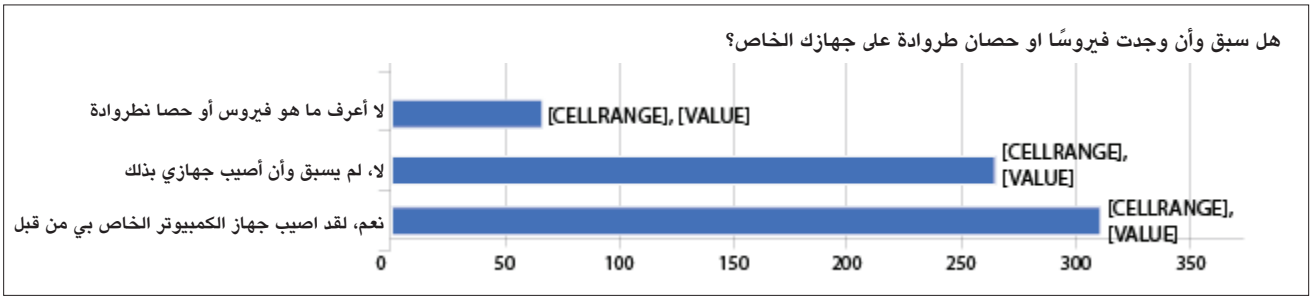
يستعرض جدول (٣) طبيعة الممارسات والسلوكيات التي يقوم بها الطلبة عند استخدام مواقع الشبكات الاجتماعية والبريد الإلكتروني، أو مواقع وتطبيقات أخرى. ومع أن النتائج في مضمونها تشير أن الغالبية من الطلبة لديهم وعي ببعض الممارسات التنظيمية والتقنية للوقاية من أساليب ومخاطر الهندسة الاجتماعية بطريقة غير مباشرة، إلا أن هذه النسب لا تتجاوز النصف في بعض الحالات، أي أنه لا يقل عن ٤٠٪ لهم ممارسات خاطئة عند استخدام البريد الإلكتروني ومواقع الشبكات مما يجعلهم عرضه للوقوع في شباك الهندسة الاجتماعية.

تشير النتائج أن ٦٨٪ من الطلبة يهتمون بموضوع الخصوصية إذ يقومون بضبط إعدادات الخصوصية على مواقع الشبكات الاجتماعية، و٦٢٪ لا يتيحون بياناتهم الشخصية على مواقع الشبكات، ٥٧٪ لا يشاركون معلوماتهم عن الأسرة والأصدقاء في مواقع الشبكات. وهذا يفيد بأن نسبة جيدة من الطلبة يتخذون بعض الاجراءات التي قد تضمن لهم خصوصيتهم على مواقع الشبكات الاجتماعية، ولا توجد فروق ذات دلالة إحصائية تعزى لمتغير النوع والتخصص فيما يتعلق بجميع العبارات في الجدول (٤).

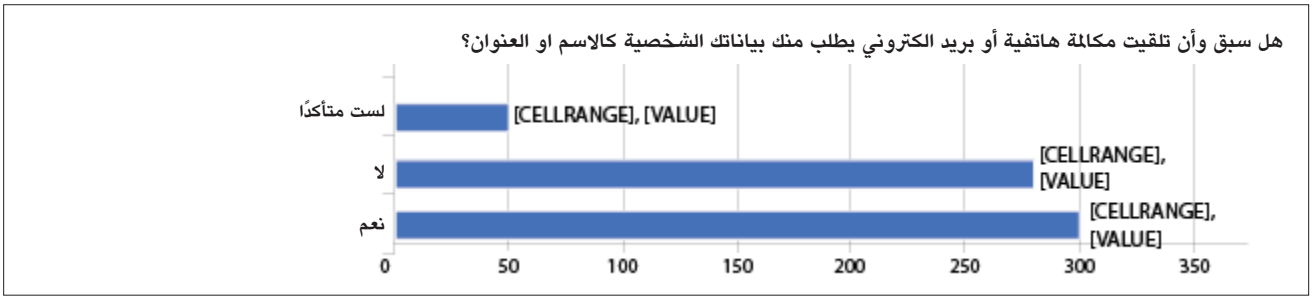
وتأتي إجابة الطلبة على عبارة "أقوم بقبول الأصدقاء على الشبكات الاجتماعية دون معرفتي بهم" بنعم، بواقع ٥٦٪ مما يعطي مؤشرًا أن الطلبة يقبلون الصداقات الواردة على الشبكات الاجتماعية بدافع الثقة، مما قد يكون مدخلًا آخرًا لما يسمى بالهندسة الاجتماعية العكسية، إذ أشار Irani وآخرون (٢٠١١) أن الأبحاث السابقة توصلت إلى أن مستخدمي الشبكات الاجتماعية عبر الإنترنت يميلون إلى إظهار درجة أعلى من الثقة في طلبات الصداقة والرسائل المرسلة من قبل مستخدمين آخرين وهنا تتمثل هجمات الهندسة الاجتماعية المعكوسة في الشبكات الاجتماعية في خداع الضحية في الاتصال بالمهاجم نفسه نتيجة لتأسيس درجة عالية من الثقة بين الضحية والمهاجم إذ أن الضحية هو الكيان الذي أسس العلاقة.

كما تشير النتائج أيضًا في جدول (٣) حرص الطلبة على اتخاذ الاجراءات التقنية لحماية الحاسب الآلي كتمكين وتثبيت جدران الحماية في جهاز الحاسب الآلي (٥٦٪)، وتحديث جدران الحماية (٦٠٪)، ومع ذلك لازال ٣٠٪ من الطلبة لا يهتمون بالإجراءات

شكل (٥) استجابة مجتمع الدراسة حول معرفتهم تعرض جهازهم الخاص لفيروس أو أحصنة طروادة



شكل (٤) استجابة مجتمع الدراسة حول مدى تعرض البريد الالكتروني للاختراق



التقنية لحماية الحاسب الآلي، كما أشارت النتائج أيضًا أن ٤٩٪ فقط من الطلبة لا يستخدمون نفس كلمات المرور لجميع حساباتي الشخصية أو للمؤسسة (الكلية أو الجامعة)، و٤٦٪ لا يستخدمون كلمات سهلة التذكر وليست متنوعة (رموز أو أرقام فقط) لكلمات المرور للبريد الإلكتروني أو مواقع الشبكات، ومع أن هذه من الاجراءات الاحترازية لتضييق الأمر على المخترقون من تخمين كلمات المرور أو الوصول إليها إلا أننا نجد نسبة لا تتجاوز ٥٠٪ من الطلبة الذين يقومون بعمل ذلك تجنبًا لسرقة كلمات المرور. وهذا مؤشرًا أيضًا يجب الوقوف عليه إذ أن هذه النسبة تستدعي النظر في مسائل التوعية. ومن الملاحظ أن مع اهتمام بعض الطلبة بالجوانب التقنية لحماية الأجهزة الخاصة من الاختراقات أو الهجمات الإلكترونية إلا أنه يبقى بث الوعي الرقمي مهم من أفراد المجتمع من الطلبة، إذ أن هذا الوعي ينقصه التنفيذ العملي من خلال معرفتهم بالجوانب التقنية الأخرى التي قد تعزز من حماية الحاسب الآلي وخاصة في ظل انتشار هجمات جديدة وأساليب حديثة للمهندسين الاجتماعيين كما ورد في النتاج الفكري، وقد تشمل التوعية تحديث جدران الحماية فمع وجود نسبة ٦٠٪ من الطلبة ممن يقومون بذلك يبقى نسبة ٤٠٪ ممن لا يقومون بذلك، وهذا ينطبق على بقية الإجراءات التقنية الأخرى كتحديث الرقم السري.

كما يلاحظ من الجدول (٣) أن ٣٤٪ من الطلبة يقومون بالنقر على الروابط التي تقودهم للأخبار عبر البريد الإلكتروني ومواقع الشبكات دون الرجوع للموقع نفسه، وكذلك بنفس النسبة من يقومون بالنقر على الروابط التي تصلهم عبر بريدهم الإلكتروني للدخول على مواقع الشبكات مثل الفيسبوك وتويتر دون الحاجة للرجوع للموقع نفسه. وهذه تعتبر من أشهر أساليب الطعم أو الفخ، الذي تبعها المهندس الاجتماعي للإيقاع بالضحية والحصول على كلمات المرور أو تنزيل برمجيات خبيثة على جهاز المستخدم. وبالتالي فإن عملية تلافي مثل هذه الإشكاليات أن يقوم المستخدم بالدخول على أي موقع أو شبكة اجتماعية من خلال الصفحة الرئيسية للموقع من خلال معرف الموارد الموحد (URL)، وليس من خلال ما يصل إلية عبر البريد الإلكتروني للدخول على الموقع. ويتعلق هذا الجانب بالوعي التنظيمي الذي يعزز فهم الطلبة لبعض الممارسات التي يعتقد البعض أنها غير مهمة أو قد لا تشكل خطرًا يسهل الهجمات الإلكترونية.

٥. التوصيات والدراسات المستقبلية

جدول (٣): طبيعة الممارسات والسلوكيات التي يقوم بها الطلبة عند استخدام مواقع الشبكات الاجتماعية والبريد الإلكتروني، أو مواقع وتطبيقات أخرى.

	العبارة	نعم	لا	لا ينطبق	نسبة الاستجابة
١	أقوم بتغيير إعدادات الخصوصية في ملفي الخاص على مواقع الشبكات الاجتماعية	٦٨٪	٢٦٪	٦٪	١٠٠٪
٢	أتيح بياناتي الشخصية على مواقع الشبكات الاجتماعية	٢٤٪	٦٢٪	١٤٪	١٠٠٪
٣	أشارك الآخرين معلومات عن الأسرة والأصدقاء	٢٣٪	٥٧٪	٢٠٪	١٠٠٪
٤	أقوم بقبول الأصدقاء على الشبكات الاجتماعية دون معرفتي بهم.	٥٦٪	٣٢٪	١١٪	١٠٠٪
٥	أقوم بحجب الرسائل التي تأتيني من أفراد لا أعرفهم على مواقع الشبكات الاجتماعية	٥٦٪	٣٢٪	١١٪	١٠٠٪
٦	أقوم بحذف ملفات الكوكيز من المواقع التي أقوم بزيارتها	٤٦٪	٣٦٪	١٨٪	١٠٠٪
٧	أقوم بحجب الإعلانات والدعايا التي تأتيني في البريد العشوائي	٥٨٪	٢٩٪	١٤٪	١٠٠٪
٨	أقوم بالرد على رسائل البريد الإلكتروني لأفراد لا أعرفهم	٢٨٪	٥٥٪	١٧٪	١٠٠٪
٩	أقوم بالرد على رسائل البريد الإلكتروني التي تحتوي على تعليمات لتحسين خدمة البريد الكتروني مع طلب للرقم السري.	٣٠٪	٥٥٪	١٥٪	١٠٠٪
١٠	أقوم بإعطاء رقمي السري في حالة طلب مني أحد ذلك	٢٢٪	٥٩٪	١٩٪	١٠٠٪
١١	أقوم بتمكين وتثبيت جدران الحماية في جهاز الحاسب الآلي الخاص بي	٥٦٪	٣١٪	١٣٪	١٠٠٪
١٢	أقوم بتحديث جدران الحماية على جهازي الخاص	٦٠٪	٢٩٪	١١٪	١٠٠٪
١٣	أستخدم نفس كلمات المرور لجميع حساباتي الشخصية أو للمؤسسة (الكلية أو الجامعة)	٣٩٪	٤٩٪	١٢٪	١٠٠٪
١٤	استخدم كلمات سهلة التذكر وليست متنوعة (رموز أو أرقام فقط) لكلمات المرور للبريد الإلكتروني أومواقع الشبكات	٤٣٪	٤٦٪	١٢٪	١٠٠٪
١٥	أقوم بتنزيل برامج مجانية دون التأكد من مصدرها	٣٩٪	٤٨٪	١٤٪	١٠٠٪
١٦	أقوم بتنزيل روابط ملفات الموسيقى التي تصلني عبر البريد الإلكتروني أو شبكات التواصل دون التأكد من مصدر الرابط.	٢٩٪	٥٥٪	١٦٪	١٠٠٪
١٧	أقوم بالنقر على الروابط التي تقودني للأخبار عبر البريد الإلكتروني ومواقع الشبكات دون الرجوع للموقع نفسه	٣٤٪	٥٥٪	١١٪	١٠٠٪
١٨	أقوم بالنقر على الروابط التي تصلني عبر بريدي للدخول على مواقع الشبكات مثل الفيسبوكوتويتر دون الحاجة للرجوع للموقع نفسه.	٣٤٪	٥٠٪	١٦٪	١٠٠٪

في ضوء النتائج التي توصلت إليها الدراسة فقد خلص الباحثون إلى مجموعة من التوصيات، من أهمها:

- **العمل على توعية مجتمع مؤسسات التعليم بمفهوم الهندسة الاجتماعية وأساليبها من خلال مجموعة من الورش والمحاضرات التي من شأنها رفع المستوى المعرفي والرقمي لديهم، والتنبيه من الممارسات أو السلوكيات الخاطئة عند استخدام الشبكات الاجتماعية أو البريد الإلكتروني، وذلك بالتعاون مع الجهات المعنية.**
- **العمل على دعم برامج ومهارات الوعي المعلوماتي لدى الطلبة وأعضاء هيئة التدريس وذلك من خلال التنسيق مع الجهات المتخصصة كقسم دراسات المعلومات بجامعة السلطان قابوس للرقي بمستوى الوعي المعلوماتي وتعزيز ثقافة المواطنة الرقمية لديهم التي تعتبر من الأساليب التنظيمية التثقيفية للحد من تلك السلوكيات.**
- **تدريس مساقات في الأمن السيبراني، وأخلاقيات المعلومات كمواد متطلبات للكلية في إطار بث الوعي المعلوماتي والرقمي لدى المجتمع الجامعي للحد من مخاطر الهندسة الاجتماعية وغيرها من المعضلات الأخلاقية على الشبكات الاجتماعية في ظل ثورة المعلومات والمعرفة.**
- **تفعيل دور اختصاصي المعلومات بمكتبات الكليات التقنية في المسؤولية المجتمعية، من خلال تبني برنامج توعوي متكامل للاختصاصيين بالتنسيق مع قسم دراسات المعلومات بجامعة السلطان قابوس، لرفع ثقافة ومهارات اختصاصي المعلومات ليفعل برامج التوعية الرقمية في الكليات التقنية.**

ومن خلال جملة النتائج والتوصيات تقترح الدراسة مجموعة من الدراسات المستقبلية منها:

- دراسة حول ثقافة الطلبة حول الخصوصية المعلوماتية.
دراسة عن دور الوعي المعلوماتي في التقليل من مخاطر الهندسة الاجتماعية وأساليبها تستهدف طلبة التعليم العام والتعليم العالي.
دراسة حول تعزيز ثقافة المواطنة الرقمية لدى الطلبة وأعضاء هيئة التدريس بالكليات التقنية، والوقوف على أهم تحديات تعزيز تلك الثقافة.

المراجع

مختار، محمد (٢٠١٣). Cybersecurity: هل ممكن أن تتجنب الدول مخاطر الهجمات الإلكترونية. استرجع بتاريخ ١١، ١١، ٢٠١٨ من:
file:///C:/Users/user/Desktop/مواضيع%20متفرقه/الأمن%20السيبراني/Social%20En.pdf.

Abraham, S., &Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, 196-183 ,(3)32.

Arab Social Media Report (2017). Social media and internet of things. Retrieved December 2018 ,2 from https://www.mbrsg.ae/getattachment/1383b88a-6eb476-9a-bae61903688099-4b/Arab-Social-Media-Report2017-

Bakhshi, T., Papadaki, M., &Furnell, S. (2009). Social engineering: assessing vulnerabilities in practice. Information management & computer security, ,(1)17 63-53.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., &Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of experimental criminology, 115-97 ,(1)11.

Chaffey,D. (2018). Global social media research summary 2018. Retrieved from https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

Chitrey, A., Singh, D., & Singh, V. (2012). A comprehensive study of social engineering based attacks in india to develop a conceptual model. International Journal of Information and Network Security, 45 ,(2)1.

Cisco (2018). Cisco 2018 Annual Cybersecurity Report. Retrieved from https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. Computers & Security, 80-73 ,(1)26.

E Frumento, E. (2016)The role of Social Engineering in evolution of attacks - Dogana Project. Project co-funded by the European Commission under the Horizon 2020 Programme.https://www.dogana-project.eu/.../D-2.1The-role-of-SE-in-the-evolution-of-attacks.pdf

Kumar, A., Chaudhary, M., & Kumar, N. (2015). Social engineering threats and awareness: a survey. European Journal of Advances in Engineering and Technology, 19-15 ,(11)2.

Mann, I. (2017). Hacking the human: social engineering techniques and security countermeasures. Routledge.

Mataracioglu, T., &Ozkan, S. (2011). User awareness measurement through social engineering. arXiv preprint arXiv:1108.2149.

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

May, G. A. (1980). Social engineering in the Philippines: The aims, execution, and impact of American colonial policy, 1913-1900. Greenwood Press.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 209-186 ,59.

Orgill, G. L., Romney, G. W., Bailey, M. G., &Orgill, P. M. (2004, October). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In Proceedings of the 5th conference on Information technology education (pp. 181-177). ACM.

Singh, A., Vaish, A., &Keserwani, P. K. (2014). Information Security: Components and Techniques. International Journal, 1)4).

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. Network security, 19-16 ,(8)2011.

Thompson, S. T. (2006). Helping the hacker? Library information, security, and social engineering. Information Technology and Libraries, 225-222 ,(4)25.

Thornburgh, T. (2004, October). Social engineering: the dark art. In Proceedings of the 1st annual conference on Information security curriculum development (pp. 135-133). ACM. Doi:1059524.1059554/10.1145

Flores, W. R., &Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. computers &security, 44-26 ,59.

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

Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, December, 18. Retrieved from https://s3.amazonaws.com/academia.edu.documents/04/33172114SocialEngineering

Gulenko, I. (2013). Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness. Information Management & Computer Security, 101-91 ,(2)21.

Hadnagy, C. (2010). Social engineering: The art of human hacking. John Wiley & Sons.

Huber, M., Kowalski, S., Nohlberg, M., &Tjoa, S. (2009, August). Towards automating social engineering using social networking sites. In Computational Science and Engineering, 2009. CSE'09. International Conference on (Vol. 3, pp. 124-117). IEEE.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011, July). Reverse social engineering attacks in online social networks. In International conference on detection of intrusions and malware, and vulnerability assessment (pp. 74-55). Springer, Berlin, Heidelberg.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011, July). Reverse social engineering attacks in online social networks. In International conference on detection of intrusions and malware, and vulnerability assessment (pp. 74-55). Springer, Berlin, Heidelberg.

Karakasiliotis, A., Furnell, S. M., &Papadaki, M. (2006). Assessing end-user awareness of social engineering and phishing.

Krombholz, K., Hobel, H., Huber, M., &Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 122-113 ,22. https://doi.org/10.1016/j.jisa.2014.09.005

Twitchell, D. P. (2006, September). Social engineering in information assurance curricula. In Proceedings of the 3rd annual conference on Information security curriculum development (pp. 193-191). ACM.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 102-97 ,38.

Weinberg, A. M. (1966). Can technology replace social engineering?.Bulletin of the Atomic Scientists, ,(10)22 8-4.