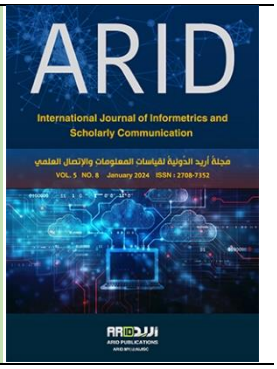
ARID Journals

ARID International Journal of Informetrics and Scholarly Communication (AIJISC)
ISSN: 2708-7352

Journal home page: http://arid.my/j/aijisc



مَجلةُ أُريد الدَّوليةُ لقياسات المعلومات و الإتصال العلمي

العدد 8 ، المجلد 5 ، كانون الثاني 2024 م

Social Engineering in Social Media Networks and Its Impact on Digital and Societal Security in the Sultanate of Oman: An Exploratory Study

Ahmed Maher Khafaga Shehata[1]*

Bushra Saif Al-Hadhrami[2]

1- Department of Information Studies - Sultan Qaboos University – Oman

2- Omani Studies Center-Sultan Qaboos University-Muscat-Sultanate of Oman

الهندسة الاجتماعية في شبكات التواصل الاجتماعي وتأثيرها على الأمن الرقمي والمجتمعي في سلطنة عمان: دراسة استكشافية

أحمد ماهر خفاجة شحاتة[1]*

بشرى سيف الحضرمي[2]

1- قسم دراسات المعلومات- كلية الاداب و العلوم الاجتماعية- جامعة السلطان قابوس – عمان

2- مركز الدراسات العمانية - جامعة السلطان قابوس - مسقط - سلطنة عمان

*a.shehata@squ.edu.om

arid.my/0005-6016

https://doi.org/10.36772/arid.aijisc.2024.583

ARTICLE INFO
Article history:
Received 3/10/2023
Received in revised form 9/11/2023
Accepted 2/12/2023
Available online 15/01/2024

ABSTRACT

Social engineering within social media networks presents a growing concern for public safety in the Sultanate of Oman. The risks associated with such attacks primarily arise from human vulnerabilities rather than technical failures. Consequently, this research conducted an in-depth examination of the ramifications of social engineering and the responses of Omani society to these threats, revealing their significant implications at the national level. Social engineering poses a substantial risk to public security by exploiting users into disclosing sensitive information, thereby necessitating enhanced security protocols to protect personal identities and financial assets. Utilizing a descriptive analytical approach, the study administered a questionnaire to a sampled population, comprising five sections related to demographic profiles, awareness of social engineering, its social and psychological impacts, proficiency in countering such schemes, and the various forms of social engineering attacks. The findings highlighted disparities in Omani societal attitudes towards social engineering, evident across gender, age, educational attainment, and occupational categories. This underscores the need to develop tailored security strategies that account for these variations to enhance protective measures. The study advocates for increasing digital literacy among Omani citizens and developing skills to combat social engineering tactics. These recommendations should form essential components of a cohesive national strategy aimed at strengthening digital security. Moreover, the research emphasizes the importance of exploring technological solutions to address social engineering challenges and enhance digital literacy. It stresses the necessity of collaborative efforts across sectors to cultivate a secure digital environment in the Sultanate of Oman, while highlighting the importance of continuous improvement and the implementation of comprehensive strategies to effectively counter social engineering threats.

Keywords: Social engineering, phishing, social networks, digital scams, digital security.

الملخص

الهندسة الاجتماعية هي مجموعة من التقنيات والأساليب النفسية التي تهدف إلى التلاعب بالأفراد وخداعهم للحصول على معلومات سرية أو القيام بأفعال معينة. وتعتمد هذه الممارسات على استغلال نقاط الضعف البشرية مثل: الثقة والفضول والخوف، بدلاً من استهداف نقاط الضعف التقنية في الأنظمة الأمنية. تمثل الهندسة الاجتماعية في شبكات التواصل الاجتماعي تحديًا متزايدًا للأمان العام في سلطنة عمان. ولعل مكمن الخطر في ذلك النوع من الهجمات اعتمادها في المقام الأول على الخطأ البشري وليس أخطاء الحاسب الآلي. نتيجة لذلك قامت الدراسة الحالية بتحليل متعمق لآثار الهندسة الاجتماعية واستجابة المجتمع العماني لها، حيث أظهرت النتائج أن هذه الظاهرة تشكل تهديدًا كبيرًا على المستوى الوطني. يظهر تأثير الهندسة الاجتماعية البارز على الأمان العام من خلال استهداف المستخدمين لاستخراج المعلومات الحساسة، مما يتطلب تعزيز التدابير الأمنية لحماية الهويات الشخصية والحسابات المصرفية. تبنت الدراسة المنهج الوصفي التحليلي من خلال توزيع استبانة على عينة الدراسة. اشتملت الاستبانة خمسة أقسام تتعلق بالخصائص الديموغرافية، والوعي بالهندسة الاجتماعية، والتأثير الاجتماعي والنفسي، ومهارات مكافحة الهندسة الاجتماعية، وأنواع هجمات الهندسة الاجتماعية. أبرزت نتائج الدراسة وجود تفاوت في اتجاهات المجتمع العماني تجاه الهندسة الاجتماعية استنادًا إلى: الجنس، العمر، المستوى التعليمي، والفئة الوظيفية. يبرز ذلك أهمية تصميم استراتيجيات أمان مخصصة تأخذ في اعتبارها هذه الاختلافات لتحسين فعالية الحماية .نتيجة لذلك أوصت الدراسة بضرورة زيادة الوعي الرقمي لدى المجتمع العماني وتطوير مهارات مكافحة الهندسة الاجتماعية. يجب أن تكون هذه التوصيات جزءًا من خطة وطنية متكاملة لتعزيز الأمان الرقمي. كما أظهرت الدراسة أهمية استكشاف سبل استخدام التكنولوجيا لمواجهة تحديات هندسة الاجتماع وتحسين التوعية الرقمية. كما أوضحت الدراسة أهمية تكامل الجهود بين القطاعات المختلفة لضمان بيئة رقمية آمنة في سلطنة عمان، مع التأكيد على أهمية التحسين المستمر وتبني استراتيجيات شاملة لمكافحة الهندسة الاجتماعية.

الكلمات المفتاحية: الهندسة الاجتماعية، التصيد الاحتيالي، الشبكات الاجتماعية، الأمن الإلكتروني، الاحتيال الرقمي، الوعي الرقمي.

المقدمة

يشهد خلال السنوات القليلة الماضية تزايدت هجمات الهندسة الاجتماعية بشكل سريع في على شبكة الإنترنت، وعلى الأخص من خلال صفحات منصات التواصل الاجتماعي مثل واتساب، فيسبوك، وتويتر. ولعل الهدف الرئيس من تلك الهجمات هو التلاعب بالأفراد والمؤسسات لإفشاء بيانات قيمة وحساسة لصالح أشخاص يهدفون في المقام الأول إلى الربح المالي. ويمكن القول بأن الهندسة الاجتماعية تمثل خطرًا كبيرًا على مستخدمي الشبكة العنكبوتية في العالم أجمع، حيث تتحدى أمان جميع الشبكات بغض النظر عن قوة وسائل الحماية وأنظمة التشفير وأنظمة كشف التسلل وأنظمة برامج مكافحة الفيروسات. حيث تعتمد الهندسة الاجتماعية في المقام الأول على الخطأ البشري وليس أخطاء الحاسب الآلي؛ لذلك، فهي الحلقة الأضعف في سلسلة الأمان. تؤثر تلك التقنيات التي تتم من خلال التفاعلات البشرية على الشخص نفسياً من أجل الإفصاح عن معلومات سرية مثل رقم الحساب البنكي، الأرقام السرية للحسابات، تواريخ الميلاد أو أي معلومات أخرى يمكن استخدامها للاحتيال أو لكسر الإجراءات الأمنية. بسبب هذا، تعد هجمات الهندسة الاجتماعية أقوى الهجمات لأنها تهدد جميع الأنظمة مهما بلغت قوتها ودرجة الأمان بها.

لا يوجد دولة في منأى عن هجمات الهندسة الاجتماعية، ولكن يمكن القول إن الولايات المتحدة كانت الدولة الأولى استهدافًا من قبل معظم هجمات الهندسة الاجتماعية ولديها أعلى تكلفة للهجوم، تليها ألمانيا واليابان. التكلفة التقديرية لهذه الهجمات في الولايات المتحدة كانت 121.22 مليار دولار (Salahdine & Kaabouch, 2019). وتعتبر الشركات الأمريكية مستهدفة بشكل كبير حيث تتعامل هذه الشركات مع بيانات دولية ذات قيمة كبيرة، وعندما يتم اختراق هذه الشركات، فإنها تؤثر بشكل كبير على الاقتصاد؛ وبهذا أصبحت الهندسة الاجتماعية تمثل تهديدًا خطيرًا في فضاء الإنترنت، وهي وسيلة فعالة لمهاجمة أنظمة المعلومات.

وتستهدف الهندسة الاجتماعية الحصول على بيانات تسمح بالدخول إلى حسابات الأشخاص والتحكم في الأصول المالية الخاصة بهم وإجراء تحويلات لحسابات أخرى أو حتى إجراء عمليات شراء من مواقع دولية. ذلك النوع من الهجمات يمثل تحديًا أمام السلطات الأمنية حيث أن نجاح أو فشل تلك الهجمة يعتمد في المقام الأول على مدى وعي الشخص المستهدف بأنه قد يعطي بيانات سرية لطرف ثالث يهدف إلى إساءة استغلال تلك البيانات (Mouton et al., 2016).

ويمكن تعريف الهندسة الاجتماعية بأنها فن دفع المستخدمين إلى اختراق أنظمة المعلومات بنفسهم بدلاً من الهجمات التقنية على الأنظمة، يستهدف المهندسون الاجتماعيون البشر بدلا من الآلات بإمكانية الوصول إلى المعلومات، ويتلاعبون بهم عن طريق إيهامهم بأنهم يقومون باستخدام مواقع موثوق فيها لإفشاء معلومات سرية أو حتى لتنفيذ هجماتهم الخبيثة من خلال التأثير والإقناع.

عادة ما تكون إجراءات الحماية التقليدية مثل برامج الحماية من الفايروسات غير فعالة ضد هذا النوع من الهجوم (Krombholz et al., 2015).

ومن ذلك المنطلق، ونتيجة تزايد هجمات الهندسة الاجتماعية سعت الدراسة الحالية إلى التعرف على الوعي بالهندسة الاجتماعية في سلطنة عمان والآثار الاجتماعية المترتبة على ذلك النوع من الهجمات وتأثيره على المجتمع العماني.

مشكلة الدراسة

تمثل هجمات الهندسة الاجتماعية مشكلة في العالم أجمع حيث أصبح مستخدم الإنترنت التقليدي هو من يساعد قراصنة الإنترنت على سرقة البيانات والحصول على معلومات قد تكون حساسة. التحول من هجمات الإنترنت التقليدية التي كانت تستهدف نظم الشركات والمؤسسات، بني على أن الحلقة الأضعف في تلك النظم هو الإنسان حيث إنه أكثر عرضة للوقوع في الخطأ. ولذلك تعمل تلك الهجمات على التحايل على العقل البشري وإيهامه أن يقوم بإعطاء معلومات عادية لأشخاص موثوقين أو لصفحات إنترنت تابعة لشركات يقوم بالتعامل معها بشكل دوري. ولعل المستخدم العربي وخاصة العماني لشبكة الإنترنت ليس في منأى عن هجمات الهندسة الاجتماعية حيث يتعرض سنويا المستخدمون في سلطنة عمان للاحتيال من خلال تلك الهجمات مما يؤدي إلى خسائر مادية ومعنوية كبيرة (الكندي، 2020).

ولعل مكمن الخطر من الهجمات الاجتماعية هو قلة وعي أفراد المجتمع بالهندسة الاجتماعية وأساليبها والأخطار التي يمكن أن تنجم عنها، مما قد يتسبب في وقوع أولئك الأفراد فريسة لهجمات الهندسة الاجتماعية. ونتيجة لذلك هناك حاجة ملحة لتعريف مستخدم الإنترنت في سلطنة عمان بمخاطر الهندسة الاجتماعية وكيفية تجنب تلك الهجمات من خلال برنامج ثقافي لرفع الوعي المعلوماتي لدى المستخدمين وتعزيز قدرتهم على التعامل مع تلك المخاطر والتقليل من ضحايا الهندسة الاجتماعية.

أهداف الدراسة

تسعى الدراسة إلى تحقيق الأهداف الآتية:

1. التعرف على مستوى الوعي لدى المجتمع العماني حول مفاهيم الهندسة الاجتماعية.
2. تحديد مدى إدراك المجتمع العماني لمهارات التصدي لهجمات الهندسة الاجتماعية.
3. التعرف على الآثار الاجتماعية والنفسية التي يعتقد المجتمع العماني أن الهندسة الاجتماعية تخلفها.
4. تحديد أنواع الهجمات التي يدركها أفراد العينة والتي تستخدم الهندسة الاجتماعية.

5. التعرف على اتجاهات المجتمع العماني حول الهندسة الاجتماعية باختلاف المتغيرات الديموغرافية (الجنس، العمر، التعليم، الفئة).

فرضيات الدراسة

في ضوء أهداف مشكلة وأهداف وأسئلة الدراسة وتحليل الدراسات السابقة، جرى استخلاص وصياغة مجموعة فروض لاختبارها على عينة من **المنتسبين لجامعة السلطان قابوس خلال الفترة من يونيو 2023 حتى ديسمبر 2023.**

- **الفرضية الأول:** هناك اختلاف في اتجاهات المجتمع العماني حول الهندسة الاجتماعية بناءً على الجنس.
- **الفرضية الثانية:** هناك اختلاف في اتجاهات المجتمع العماني حول الهندسة الاجتماعية بناءً على الفئات العمرية.
- **الفرضية الثالثة:** هناك اختلاف في اتجاهات المجتمع العماني حول الهندسة الاجتماعية بناءً على مستوى التعليم.
- **الفرضية الرابعة:** هناك اختلاف في اتجاهات المجتمع العماني حول الهندسة الاجتماعية بناءً على الفئة الاجتماعية.

الدراسات السابقة

يتناول قسم الدراسات السابقة النتاج الفكري الخاص بالهندسة الاجتماعية من خلال ثلاثة محاور رئيسة هي الوعي بمخاطر الهندسة الاجتماعية، آليات التصدي لهجمات الهندسة الاجتماعية، وأثر الهندسة الاجتماعية على الأفراد. ونظرًا لقلة النتاج الفكري العربي حول وعي الأفراد بهجمات الهندسة الاجتماعية، ستسخدم الدراسات السابقة لخدمة أهداف الدراسة الحالية.

الوعي بمخاطر الهندسة الاجتماعية

يميل العديد من الأشخاص عبر استخدامهم للإنترنت ووسائل التواصل الاجتماعي إلى أن يكونوا أحرارًا في مشاركتهم لمعلوماتهم الخاصة التي يرونها غير ضارة، ولكن المهندسين الاجتماعيين ينظرون إليها بشكل مختلف تمامًا (Alexander & Wanner, 2016). وهذا ما أكدت عليه دراسة .Algarni et al (2017) بأن هجمات الهندسة الاجتماعية تشكل خطرًا أمنيًا، وتعد شبكات التواصل الاجتماعي هي المصدر الأكثر شيوعًا لهذه الهجمات، وعلى الرغم من أن المنظمات تدرك مخاطر الهندسة الاجتماعية، إلا أنها تواجه قلة فهم ووعي من قبل المجتمع بهذه التهديدات، وهذا ما أكدته نتائج الدراسة التجريبية إلى أن قلة الوعي التكنولوجي والرغبة في التسلية هي من أهم الأسباب للوقوع ضحية الهندسة الاجتماعية.

وتؤكد العديد من الدراسات التي أجريت أن معظم مستخدمي الحاسوب لديهم نقص في المعرفة بأمن المعلومات بسبب عدم كفاية الوعي. وقد ثبت أيضًا أن المؤسسات الأكاديمية والحكومات على حد سواء تبذل جهودًا لتوفير الوعي الأمني لتعزيز فهم الجمهور

لمخاطر وتهديدات الأمن السيبراني (Arachchilage & Love, 2014). وهذا ما أثبتته دراسة محمد (2017) التي هدفت إلى التعرف على مدى وعي مستخدمي شبكات التواصل الاجتماعي في المجتمع العربي تجاه الهندسة الاجتماعية، والتي أجريت على 336 مستخدمًا، وأظهرت النتائج قلة إدراك مجتمع الدراسة بمفهوم الهندسة الاجتماعية والتصيد الإلكتروني، في حين كانت النتائج إيجابية حول سلوك مجتمع الدراسة تجاه حماية معلوماتهم الشخصية على حسابات التواصل الاجتماعي. وأيضا توصلت دراسة عبد الرحيم (2020) التي أجريت على 600 مبحوث من الجمهور في جمهورية مصر بأن نسبة 80.8% من المبحوثين قد شاركوا في تطبيقات الهندسة الاجتماعية عبر موقع (فيس بوك)، وهذا يوضح قلة الوعي بالهندسة الاجتماعية، وانخفاض ثقافة الخصوصية الرقمية، ومن أبرز أسباب استخدام الجمهور لهذه التقنيات التسلية والترفيه.

كما هدفت دراسة .Alsulami et al (2021) إلى معرفة مدى الوعي بالهندسة الاجتماعية في قطاع التعليم بالمملكة العربية السعودية، ولتحقيق هذا الهدف تم توزيع استبانة على 465 طالبا، وعضو هيئة تدريس، وموظفا في المؤسسات التعليمية، وأظهرت النتائج أن 66% ليس لديهم المعرفة بالهندسة الاجتماعية، وتشير النتائج إلى وجود اختلافات كبيرة بين المشاركين الذين لديهم معرفة مسبقة بالهندسة الاجتماعية وأولئك الذين لا يمتلكون هذه المعرفة من حيث ممارساتهم الأمنية للتصدي لمثل هذه الهجمات. وأيضا أعد Almutairi& Alghamdi(2022) دراسة حول دور وأثر الهندسة الاجتماعية في الأمن السيبراني، والتي هدفت إلى التأكد من مستوى الوعي بالهندسة الاجتماعية، وقد تم توزيع استبانة على 508 موظف من مؤسسات مختلفة تقع في مدينة الرياض بالمملكة العربية السعودية، وأظهرت النتائج أن 63.4% من العينة ليس لديهم فكرة عن مفهوم الهندسة الاجتماعية، و67.3% ليس لديهم الوعي عن تهديدات الهندسة.

أما في سلطنة عمان فقد كشفت نتائج دراسة الكندي والبلوشي (2020) عن طريق الاستبانة التي تم توزيعها على 2908 طالب في تخصصات مختلفة من طلبة كلية التقنية بالمصنعة، عن درجة منخفضة من فهم الطلاب لمبادئ وممارسات الهندسة الاجتماعية، حيث لم يسمع 55 % من مجموع الطلبة المستجيبين (663) عن كلمة الهندسة الاجتماعية مطلقًا، و45 % كانوا على دراية بالمصطلح ولكن بمستويات متفاوتة من الاهتمام. علاوة على ذلك، فإن غالبية الطلاب على دراية بالعديد من الأساليب التنظيمية والتقنية التي يمكن استخدامها لتجنب مخاطر الهندسة الاجتماعية، وإن كانت في بعض الظروف لا تتجاوز هذه الأرقام النصف، مما يعني أن 40٪ منهم على الأقل لديهم عادات سيئة، وهم عرضة لمخاطر الهندسة الاجتماعية عند استخدام البريد الإلكتروني، ومواقع الشبكات الاجتماعية. وتتفق دراسة الكلباني والعزرية (2022) مع الدراسة السابقة، التي طبقت على عينة من موظفي وطلبة جامعة التقنية والعلوم التطبيقية بالرستاق، إلى وجود ضعف معرفي بمصطلح الهندسة الاجتماعية، وضعف الوعي باختراعات البرامج الخبيثة، وعدم القدرة على تمييز المواقع المزيفة، في حين أن الموظفين واعون بأهمية عدم مشاركة

الأقرباء والأصدقاء بالرقم السري للبطاقة المدنية أو الحساب البنكي. في حين أن دراسة الجنيبية (2023) أظهرت وجود مستوى وعي مرتفع لدى العاملين في المكتبات الأكاديمية بسلطنة عمان بالمفاهيم والأساليب المرتبطة بالهندسة الاجتماعية، مثل مفهوم التصيد الاحتيالي وانتحال الهوية، وعلى الرغم من أن 60% لم يكونوا على دراية بمصطلح الهندسة، وقد يعزى السبب لعدم استخدام المصطلح بشكل كبير، كما أظهرت النتائج أن العاملين لديهم وعي تقني عالٍ بالممارسات المرتبطة بشبكات التواصل الاجتماعي، والمواقع الإلكترونية والبريد الإلكتروني، ويعزى السبب إلى أن العاملين في المكتبات الأكاديمية لديهم وعي معلوماتي وخبرة ومهارة وتعامل مستمر مع هذه التقنيات.

آليات التصدي لهجمات الهندسة الاجتماعية

يعتبر منع هجمات الهندسة الاجتماعية والحماية منها مهما للغاية لجميع مستخدمي أجهزة الحاسب والهواتف، ولا يوجد دليل قاطع على منع هذه الهجمات، ولكن تم تصميم العديد من الأدوات والتقنيات لتقليل هذه الهجمات وجعل المنظمات والأفراد أقل عرضة للخطر، وفي محاولة لترويض وتقليل احتيال الهندسة الاجتماعية على الشركات والمؤسسات ينصح بوضع بروتوكولات شاملة وسياسات واضحة (Chen et al., 2015). وتعتبر الهندسة الاجتماعية هي أحد أهم الاهتمامات الرئيسة من قبل الحكومات؛ بسبب استغلال أحد أهم مواردها، ألا وهي الموارد البشرية، إذ يستغل المهندسون الاجتماعيون نقاط الضعف النفسية للأفراد، مما يشكل تهديدات خطيرة للأمن السيبراني، وللبنية التحتية الرقمية، وتوجد هناك العديد من أشكال الهجمات، مثل استهداف الملكية الفكرية، والبيانات السرية، والموارد المالية؛ لذا يجب أن تستعد المؤسسات لأي نوع من هذه الهجمات من خلال برامج توعوية مثل المؤتمرات وحملات التوعية، وورش عمل، والمحاضرات (Mashtalyar et al., 2021). وقد اتفقت أغلب الدراسات على أهمية التدريب ونشر الوعي من قبل المؤسسات. إذ لا يمكن إيقاف الهجمات باستخدام تقنيات أمنية فقط؛ لأن المهندس الاجتماعي قادر على أن يخترق النظام الأمني بكل سهولة، وإن كان قويا، لذلك هناك حاجة ماسة لتدريب الأشخاص على الوعي بالأمن السيبراني (Chetioui et al., 2022). إذ إن جرائم الهندسة التي يمارسها المهندسون ليست بسبب المعرفة التقنية، ولكن بسبب استغلال نقاط الضعف البشرية، لذلك لا توجد طريقة مضمونة للحماية منها بسبب وجود العامل البشري، لذا لا بد من أن يمتلك الموظفون في مختلف المؤسسات معرفة بمفهوم الهندسة، وعلى المنظمات أن تزيد من مستوى وعي الموظفين بالتهديدات المحتملة من الهندسة الاجتماعية، وتثقيفهم بالسياسات والإجراءات الأمنية من خلال عمل المحاضرات، وعلى المنظمة أن تنشئ سياسات أمنية واضحة وعمل خطة زمنية تشمل مجموعة من الأهداف وتقييما دوريا للمخاطر (Aldawood et al., 2020). وأيضا كشفت دراسة Fuertes et al. (2022) أن المؤسسات تنفق ملايين الدولارات الأمريكية من أجل تطبيق معايير الأمان من خلال الأجهزة والبرمجيات، وعلى الرغم من ذلك فإن إحدى الطرق الأكثر فعالية للتخفيف من هجمات الهندسة الاجتماعية

هي تعليم وتدريب الأشخاص الأكثر عرضة لمثل هذه الهجمات؛ إذ إن نقاط الضعف البشرية هي الأكثر خطورة. وقد أشارت دراسة Salahdine & Kaabouch(2019) إلى قائمة من الإجراءات والخطوات الدفاعية لهجمات الهندسة الاجتماعية، تتمثل في التثقيف والتدريب في المجالات الأمنية، وزيادة الوعي الاجتماعي بهجمات الهندسة، وتوفير تقنيات كشف وتجنب هذه الهجمات، وتعلم كيفية الحفاظ على المعلومات السرية، وتعليم الأمن السيبراني من أجل تنمية المهارات للتصدي لمثل هذه الهجمات. لذا يجب على المنظمات محاربة هجمات الهندسة الاجتماعية من خلال وضع سياسات وإجراءات تحديد الأدوار والمسؤوليات لجميع المستخدمين وليس فقط الأفراد في المجال الأمني، وعلى المنظمة التأكد من أن هذه السياسات يتم تنفيذها بشكل صحيح، وأن يقدم التدريب المنتظم لكل نوع من هجمات الهندسة الاجتماعية (Hasan et al., 2010). كما أوضح أحمد (2014) بأن المؤسسات لها دور في نشر الوعي للعاملين من خلال توضيح قوانين وطرق الحماية من الهندسة الاجتماعية، عن طريق تثقيف الموظفين بمجال أمن المعلومات والاختراقات، وتدريبهم على عدم إفشاء معلومات سرية، وإتلاف أجهزة الكمبيوتر القديمة والمستندات التي تحتوي على معلومات حساسة.

وبجانب أهمية التدريب ونشر الوعي من قبل المنظمات والمؤسسات، فإن التطوير المعرفي لأفراد المجتمع بآليات محاربة هجمات الهندسة لا تقل أهمية عما سبق. إذ أظهرت دراسة Cusack& Adedokun (2018) أن العديد من المنظمات تميل إلى استخدام الحلول التدريبية وزيادة الوعي من خلال التحذيرات حول هجمات الهندسة الاجتماعية، التي لم تعد فاعلة على الأرجح لأن معظم التدريبات حول الهندسة الاجتماعية تعتمد على اكتشاف التهديدات الإلكترونية مثل هجوم التصيد الاحتيالي وتجنب تنزيل البرامج الضارة التي يمكن أن تكون سهلة الإدارة. لذا من المهم بأن يكون الأفراد على دراية بتقنيات الهندسة الاجتماعية، إذ يمكن أن يساعد الوعي بحماية الأشخاص من الاحتيال، وضرورة فهم كيفية عمل الهندسة الاجتماعية، وأنواع الهجمات المستخدمة، والمعرفة بأساليب الهندسة في الحفاظ على أمن المعلومات الحساسة (Brody et al., 2012). وأكدت نتائج دراسة Alsulami et al. (2021) بأن المستخدمين الذين لديهم وعي بمخاطر الهندسة الاجتماعية لديهم أساليب وممارسات أمان معلوماتية مثل الحذر عند فتح البريد الإلكتروني والمرفقات، وملاحظة المحاولات المشبوهة من المهندسين الاجتماعيين، وتحميل برامج مكافحة الفيروسات، وهذا يدل على أهمية التوعية والتدريب فيما يتعلق بالهندسة الاجتماعية وممارسات أمن المعلومات. وقد اتفقت دراسة الكلباني و العزرية (2022) مع الدراسة السابقة إلى أن أهم تقنيات الحماية والتصدي لهجمات الهندسة الاجتماعية التوعية والتثقيف، ووضع لوائح تنظيمية وسياسات أمنية من قبل المؤسسات مثل تغيير كلمة المرور بين فترة وأخرى، وعدم استخدام الذاكرة الخارجية الشخصية، وتنصيب برامج جدران الحماية ومكافحة الفيروسات، وشراء البرامج المرخصة. وأشار عبد المنعم (2021) بأن الإدراك وزيادة الوعي لأفراد المجتمع هي مفتاح مواجهة الهندسة الاجتماعية، من خلال تقديم حملات للتوعية

بمفهوم الهندسة الاجتماعية ومخاطرها، وأيضا للمعلمين دور في توجيه ومساعدة الطلاب ونشر الوعي بكيفية الوقاية منها، والاهتمام بتنمية الذكاء الوجداني، وتطوير مهارات إدارة العقل والبشر، ومهارات التفكير الناقد.

أثر الهندسة الاجتماعية على الأفراد

الهندسة الاجتماعية هي فن التلاعب بنقاط الضعف البشرية من أجل تحقيق هدف ضار **(**Mouton et al., 2014**)**. وتواجه الشبكات الاجتماعية اليوم بشكل كبير تحديات متزايدة بسبب هجمات الهندسة الاجتماعية، والسبب في ذلك يرجع إلى اعتماد هذه الهجمات على التلاعب بالأفراد وباستغلال عواطفهم من أجل اختراق الأنظمة والحصول على المعلومات بغض النظر عن قوة أنظمة وبرامج الحماية لمحاربة هذه الهجمات (Tulkarm, 2021)**.** ونظرا لتزايد هجمات الهندسة الاجتماعية في السنوات الأخيرة، فقد زاد الضرر الناتج عن هذه الهجمات، والتي بدورها أثرت بشكل كبير على الأفراد والمنظمات، إذ يعتبر العامل البشري أحد الأسباب الرئيسة لهذه الهجمات (Alsulami et al. , 2021). فقد أصبحت الهندسة الاجتماعية تشكل تهديدا اجتماعيا في المجتمعات الافتراضية من خلال وسائل التواصل الاجتماعي، وقد تأثرت العديد من الحكومات والشركات والأفراد بهذه الهجمات، وتسببت بأضرار عاطفية ومالية (Chetioui et al., 2022)**.** وهذا ما أكدته دراسة .Fuertes et al(2022) إلى أن هجمات الهندسة الاجتماعية التي وقعت في الفترة من 2011 إلى 2020، والتي جرى حصرها من الدراسات والمقالات المنشورة، تسببت في خسائر مالية، وألحقت الضرر بسمعة الأفراد والشركات، وتعد الشبكات الاجتماعية والبريد الإلكتروني من أهم المصادر الأساسية التي نشأت منها هذه الهجمات.

وقد أظهرت دراسة روميصاء و لويزة (2021) التي هدفت إلى دراسة أثر الهندسة الاجتماعية في مواقع التواصل الاجتماعي على طلبة قسم الإعلام الآلي وتكنولوجيا المعلومات بجامعة قاصدي مرباح ورقلة بالجزائر أن 28.3% ظهرت عليهم آثار اجتماعية نتيجة تعرضهم للابتزاز، كما تعرضوا لتشويه السمعة، ومن الآثار النفسية التي خلفتها الهندسة الاجتماعية القلق بنسبة 30%، ثم تليها الخوف بنسبة 21.7%، وأقل نسبة كانت للاكتئاب 13.3%، والتفكير بالانتحار 3.3%، أما فيما يتعلق بالآثار المادية، فقد أظهرت الدراسة أن 51.7% من الحالات لم تخلف الهندسة الاجتماعية عليهم أي أثر مادي، في حين أن 33.3% أثرت عليهم إذ تعرضوا للنصب (مبلغ مالي)، و11.7% تعرضوا للإفلاس المالي، وأقل نسبة 3.3% سببت الهندسة لهم الديون.

وأشارت دراسة .Hussain et al(2023) أن فئة البالغين في الولايات المتحدة الأمريكية هم أكثر عرضة لعمليات الاحتيال؛ بسبب انخفاض مستوى قدراتهم العقلية والجسدية، كما يتخذ البالغون إجراءات دفاعية أقل ضد هجمات الهندسة الاجتماعية والأمن السيبراني، ويثقون بالأشخاص بشكل أسرع، وأيضا يتعرض كبار السن لخطر الوقوع مرتين لهجمات الاحتيال والتصيد، وتسبب

هذه التقنيات مشاكل في الصحة العقلية والجسدية، والنفسية مثل القلق والاكتئاب والوحدة. وأيضا أشارت دراسة Chuang (2021) أن تقنية الحيل الرومانسية (Romance Scams) هي إحدى تقنيات الهندسة الاجتماعية، وتتمثل في إقامة علاقات افتراضية من خلال مواقع الويب وشبكات التواصل الاجتماعي لخداع الضحايا وابتزاز الأموال، ويتأثر الشباب وبالأخص النساء من هذه التقنية، وغالبا ما يعاني ضحاياها من التوتر واليأس والعصبية واضطراب ما بعد الصدمة، وحتى الأفكار الانتحارية. واتفقت دراسة عبد المنعم (2021) مع الدراسة السابقة بأن الهندسة الاجتماعية تؤثر على الكثيرمن الأفراد وتكبدهم خسائر مالية وفقدانا للسمعة، كما تصل في بعض الأحيان إلى حد الانتحار.

سبب موضوع أمن المعلومات قلقًا للمنظمات في العقود الماضية، فقد تم تطوير تقنيات لمواجهة الهجمات الأمنية، ولكن الحلقة الأضعف للمنظمات هي العنصر البشري، وتشكل الهندسة الاجتماعية تهديدًا للمنظمات والأفراد، وأفضلُ دفاع ضد هجمات الهندسة الاجتماعية هي تقنية استخدام حدسك UYCS (Use Your Common Sense)، وهي تعتمد على تثقيف الأفراد حول أنواع الهجمات والتدابير الاحترازية، مثل عدم الإفصاح عن المعلومات السرية عبر شبكات التواصل الاجتماعي والبريد الإلكتروني والهاتف لأي مجهول، وعدم النقر على أي مرفقات مشبوهة عبر البريد الإلكتروني، وعدم النقر على الروابط المشبوهة، والتحديث المستمر لبرامج مكافحة الفيروسات بالإضافة إلى ذلك جرى تطوير برامج لمكافحة بعض تقنيات الهندسة مثل نظام كشف التسلل Intrusion detection systems(IDS)، ونظام الحماية Intrusion Prevention System (IPS)، بالإضافة إلى تدريب المستخدمين على بعض الأدوات التي يستخدمها المتسللون مثل The Social Engineer Toolkit (SET)، وأخيرًا لتحقيق ثقافة أمنية واسعة يجب تدريب ورفع الوعي للأفراد لصد هجمات الهندسة الاجتماعية (Chinta et al., 2016). وقد أشارت دراسة Aldawood & Skinner (2018) إلى أن مجموعة عمل مكافحة التصيد الاحتيالي (APWG) تعتبر أحد الأمثلة على المنظمات غير الربحية التي تعمل على توفير تدريب على مكافحة التصيد الاحتيالي لزيادة الفهم العام والوعي بأمن المعلومات، كما يعد فريق الاستعداد لطوارئ الحاسوب في الولايات المتحدة مثالاً آخر يقدم نصائح مجانية على موقعه على الويب حول الاختراقات الأمنية الشائعة لمستخدمي الحاسوب الذين يفتقرون إلى معرفة الأسس الأمنية للحاسب الآلي.

وقد كشفت دراسة Salahdine & Kaabouch (2019) استراتيجيات لكشف الهجمات وإجراءات الوقاية، وقد قارنت بين التقنيات المستندة على الإنسان والتقنيات المستندة على الحاسوب، فالتقنيات البشرية تتمثل في التعليم والتدريب ورفع الوعي، ومن إيجابياتها سهولة التدريب، وتقليل عدد الضحايا، ولكن هناك أوجه قصور وهي التأثر العاطفي، والثقة، وأن القرارات نسبية وتتغير، أما بالنسبة للتقنيات التي تعتمد على الحاسوب فهي تتمثل في البرامج والأنظمة، وهي فعالة ودقيقة، ولكن باهضة الثمن،

وأيضا تواجه قصورًا في الفهم البشري لها. ومن هذه البرمجيات أدوات مكافحة التصيد (McAfee filter, Microsoft filter, and Web sense)، برامج التنبيه والمسح (برامج مكافحة الفيروسات)، استخدام تقنيات الذكاء الاصطناعي، تدريب وتعليم الآلة (Machine learning-based)، وتقييم المخاطر التي تتمحور حول الهندسة الاجتماعية Social Engineering Centered Risk Assessment (SERA). ومن جهة أخرى فقد أوصى **Sandouka et al.,** (2009) بأهمية تبني تقنيات الذكاء الاصطناعي (**AI**) للتصدي لهذه الهجمات؛ لأن الذكاء الاصطناعي لديه القدرة على الرد على نطاق واسع من الهجمات بطريقة الوقت الحقيقي ويمكن أن يزيد من الأمن التنظيمي. كما أوصت دراسة Twitchell (2006) بوضع ثلاثة أنواع من الدفاع موضع التنفيذ ضد هجمات الهندسة الاجتماعية وهي التعليم والتدريب والتوعية (ETA)؛ وذلك لتحقيق سياسة النسخ الاحتياطي والتدقيق.

منهج الدراسة وأدواتها

تطلبت هذه الدراسة الوصول إلى فهم شامل لمستوى الوعي والإدراك لدى المجتمع العماني حول الهندسة الاجتماعية، وتحديد تأثيراتها الاجتماعية والنفسية، إلى جانب فحص أنواع الهجمات المدركة وتحليل اتجاهات المجتمع بناءً على متغيرات ديموغرافية. لتحقيق هذه الأهداف، تبنت الدراسة المنهج الوصفي التحليلي الذي يشمل استعراض وتحليل المصادر الأدبية المتاحة، بما في ذلك الكتب، والمقالات العلمية، والأبحاث السابقة المنشورة في مجلات ومؤتمرات مختصة بموضوع الهندسة الاجتماعية.

بالإضافة إلى ذلك، جرى تصميم استبانة لجمع البيانات من عينة من المنتسبين لجامعة السلطان قابوس خلال الفترة من يونيو 2023 حتى ديسمبر 2023. اشتملت الاستبانة خمسة أقسام تتعلق بالخصائص الديموغرافية، والوعي بالهندسة الاجتماعية، والتأثير الاجتماعي والنفسي، ومهارات مكافحة الهندسة الاجتماعية، وأنواع هجمات الهندسة الاجتماعية.

اعتمد الباحثون على استخدام الاختبارات الإحصائية باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية Statistical Package for Social Sciences (SPSS) وذلك لمعالجة البيانات المستقاة من استمارات الاستبانة واستخراج النتائج المتعلقة بمحاور الدراسة المختلفة. حيث جرى تحليل استجابات أفراد العينة وحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية، بالإضافة إلى إجراء اختبار T للعينات المستقلة وتحليل التباين الأحادي One-way ANOVA لفحص الفروق ذات الدلالة الإحصائية وفقاً لمتغيرات الدراسة. واختبار توكي اللاحق لتوضيح الاختلافات بين الأزواج وتقديم مؤشرات لحجم التأثير وقد مَكّن استخدام البرنامج الإحصائي SPSS من تحليل البيانات واستخلاص النتائج بدقة وموضوعية للتحقق من معنوية فروض الدراسة.

أساليب جمع البيانات

اعتمد الفريق البحثي لجمع البيانات على مصدرين:

1. **المصادر الأولية:**

جرى جمع البيانات الأولية من خلال استبانة قام الباحث بتطويرها من أجل تحقيق أغراض الدراسة، حيث تم توزيعها على عينة من المنتسبين لجامعة السلطان قابوس خلال الفترة من يونيو 2023 حتى ديسمبر 2023.

2. **المصادر الثانوية:**

اعتمد الفريق البحثي على الدراسات والأدبيات السابقة العربية منها والأجنبية ذات الصلة بموضوع الدراسة، كما جرى الاعتماد على الكتب والرسائل العلمية، وكذلك التقارير والدوريات والمجلات العلمية إضافةً إلى مواقع الإنترنت.

مجتمع الدراسة

يعنى بمجتمع الدراسة جميع الأفراد الذين يشملون موضوع مشكلة الدراسة، حيث يضم كافة المنتسبين لجامعة السلطان قابوس خلال الفترة من يونيو 2023 حتى ديسمبر 2023.

عينة الدراسة

وهي تعد طريقة من آليات البحث وجمع المعلومات وذلك يتم عن طريق أخذ عينة من مجموعة محددة، حيث يتم الانتقال من الجزء إلى الكل أو التوصل إلى أخذ تصور كامل عن المجتمع من خلال الأفراد. وقد اعتمد الباحثون على أسلوب العينة العشوائية البسيطة لتحديد عينة من المنتسبين لجامعة السلطان قابوس خلال الفترة من يونيو 2023 حتى ديسمبر 2023.

أداة جمع البيانات

جرى بناء أداة الدراسة لتشمل 38 عبارة، منها 6 عبارات للمتغيرات الديموغرافية للعينة، و32 عبارة وفق مقياس ليكرت Likert الخماسي بإعطاء الأوزان النسبية لكل فئة كالتالي (1: غير موافق بشدة، 2: غير موافق، 3: محايد، 4: موافق، 5: موافق بشدة) والذي يمكن تقسيمه إلى فئات حسب المتوسط الحسابي لكل عبارة كما في جدول (1). وتنقسم الاستبانة إلى أربع محاور: المحور الأول: الوعي بالهندسة الاجتماعية، المحور الثاني: مهارات التصدي لهجمات الهندسة الاجتماعية، المحور الثالث: الآثار الاجتماعية والنفسية التي خلفتها الهندسة الاجتماعية، المحور الرابع: أشكال الهجمات باستخدام الهندسة الاجتماعية.

جدول (1): مقياس ليكرت الخماسي

الفئة	الاتجاه
من 1 إلى 1.79	منخفض جدا
من 1.80 إلى 2.59	منخفض
من 2.60 إلى 3.39	متوسط
من 3.40 إلى 4.19	مرتفع
من 4.20 إلى 5	مرتفع جدا

مناقشة النتائج

تم عرض نتائج تحليل بيانات الدراسة ومناقشتها تبعًا لتسلسل محاور وأسئلة الاستبانة. ويشمل الجزء الأول أسئلة عامة تتعلق بالخصائص الديموغرافية لعينة الدراسة:

البيانات الديموغرافية

شكلت نسبة الذكور (45.6%)، بينما شكلت الإناث (54.4%) من العينة، ويوضح هذا التوزيع التوازن النسبي بين الجنسين في العين. كما جاءت الفئة العمرية الأكثر تمثيلاً في الدراسة هي الفئة من 16-20 عاماً بنسبة (18.1%)، يليهم الفئة من 45 عاماً فأكثر بنسبة (15.9%)، بينما كانت الفئة الأقل تمثيلا في العينة هي من 26-30 عاماً بنسبة (9.9%). أما من حيث المؤهل العلمي، فقد شكل حملة درجة البكالوريوس النسبة الأكبر وهي (51.6%)، يليهم حملة الماجستير بنسبة (25.3%) ثم الدكتوراه بنسبة (13.7%)، بينما يمثل حملة الدبلوم النسبة الأقل بواقع (9.3%) من إجمالي أفراد العينة. كما جاءت فئة الموظفين في المرتبة الأولى من حيث طبيعة العمل بنسبة (53.3%) يليهم طلبة الجامعات بنسبة (36.3%) ثم أعضاء هيئة التدريس بنسبة (10.4%).

جدول (2): الخصائص الديموغرافية لعينة الدراسة

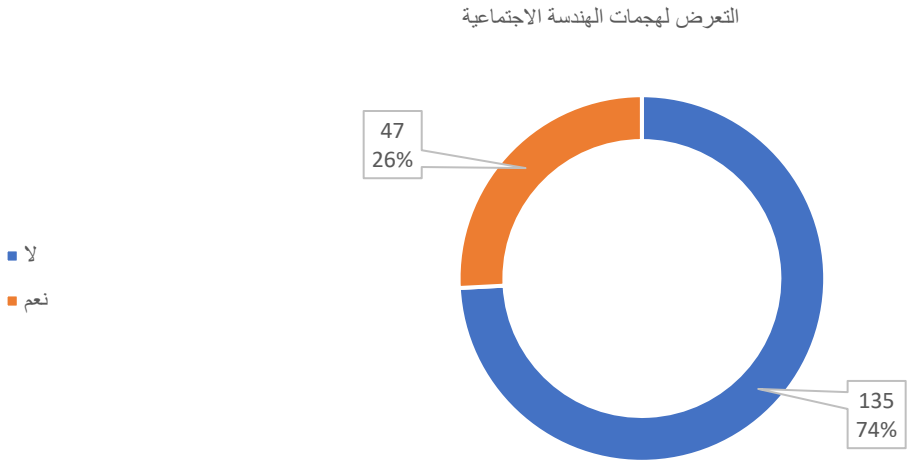
المتغير	الفئات	التكرار	النسبة المئوية
الجنس	ذكر	83	45.6
	أنثى	99	54.4
العمر	20-16	33	18.1
	25-21	25	13.7
	30-26	18	9.9
	35-31	26	14.3
	40-36	26	14.3
	45-41	25	13.7
	-45	29	15.9
المستوي التعليمي	دبلوم	17	9.3
	بكالوريوس	94	51.6
	ماجستير	46	25.3
	دكتوراه	25	13.7
الفئة الوظيفية	طالب	66	36.3
	موظف	97	53.3
	عضو هيئة تدريس	19	10.4

المحور العام للدراسة

التعرض لهجمات الهندسة الاجتماعية

وفقًا للرسم البياني1: يظهر أن 26% فقط من المشاركين في الاستطلاع، بمعدل 47 شخصًا، أفادوا بأنهم تعرضوا لهجمات الهندسة الاجتماعية. في المقابل، 74%، أو 135 شخصًا، ذكروا أنهم لم يتعرضوا لهذه الهجمات. هذه الأرقام تشير إلى وجود فجوة كبيرة في الوعي بالهندسة الاجتماعية وتأثيرها. من المحتمل أن بعض المشاركين الذين أجابوا بـ "لا" قد تعرضوا بالفعل لهجمات الهندسة الاجتماعية دون أن يدركوا ذلك، نظرًا لطبيعة هذه الهجمات المعقدة والخفية.

هذه الهجمات غالبًا ما تتخفى في صورة رسائل بريد إلكتروني مضللة، مكالمات هاتفية موهومة، أو حتى التفاعلات الشخصية، مما يجعلها صعبة الكشف.

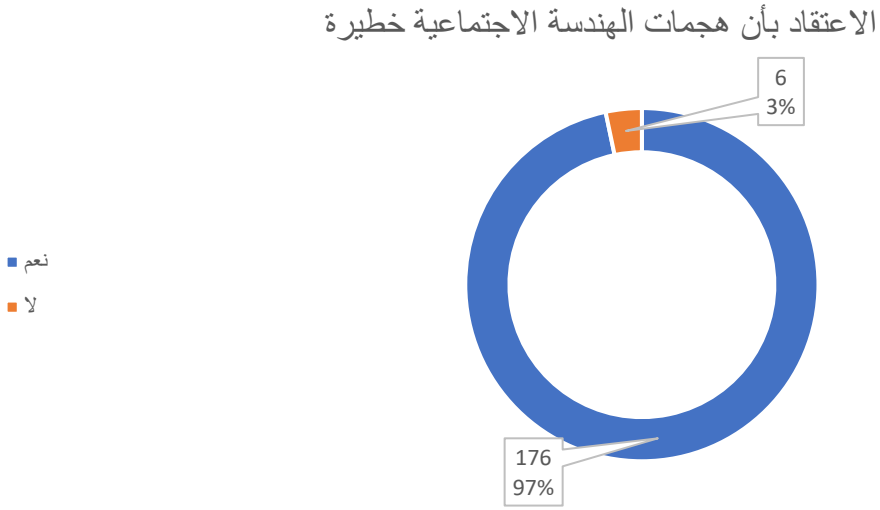


شكل (1): التعرض لهجمات الهندسة الاجتماعية

مخاطر الهندسة الاجتماعية من وجهة نظر العينة

من الجدير بالذكر أن الأفراد الذين يعتقدون أنهم على دراية بتكتيكات الهندسة الاجتماعية قد يكونون أقل يقظة، معتقدين أنهم قادرون على تحديد وتجنب هذه الهجمات بسهولة، مما يجعلهم في الواقع أكثر عرضة للخداع. لذا، يُعتبر الوعي والتدريب المستمر حول الهندسة الاجتماعية ضروريين للجميع، بغض النظر عن مستوى الخبرة أو الثقة في فهم هذه القضايا.

تشير نتائج الرسم البياني 2 إلى أن غالبية المشاركين يرون أن هجمات الهندسة الاجتماعية تمثل خطورة بالغة، حيث أن 97% أجابوا بـ"نعم"، بينما أجاب نسبة ضئيلة جدًا بلغت 3% فقط بـ"لا". وتعكس هذه النتائج تصور الغالبية العظمى من العينة بأن الهندسة الاجتماعية تشكل تهديدًا حقيقيًا، نظرًا لمخاطرها المحتملة على الخصوصية والأمن الرقمي والمعلوماتي. لذا، فمن المنطقي أن ينظر المشاركون إلى هذه الهجمات على أنها خطيرة وتستدعي اليقظة واتخاذ التدابير المناسبة للتصدي لها.



شكل (2): الاعتقاد بأن هجمات الهندسة الاجتماعية خطيرة

تحليل محاور الدراسة

المحور الأول: وعي أفراد العينة بمفهوم الهندسة الاجتماعية

تشير نتائج الجدول رقم (3) إلى أن المتوسط العام لمدى وعي أفراد عينة الدراسة حول الهندسة الاجتماعية هو وعي متوسط. إذ حصلت الفقرتان: "لدي معرفة بمفهوم الاختراق الرقمي"، و"لدي معرفة بمفهوم انتحال الهوية الرقمية "على أعلى متوسط حسابي، إذ جاءتا (3.48) و (3.41) على التوالي، وقد يعزى ذلك إلى الوضوح اللغوي في المصطلحات المستخدمة للتعبير عن الهندسة الاجتماعية وشيوع مصطلحي: "الاختراق الرقمي" و"انتحال الهوية الرقمية". بينما حصلت الفقرات المتبقية على متوسطات حسابية منخفضة حين تم استخدام مصطلحات أخرى للتعبير عن الهندسة الاجتماعية مثل التصيد الاحتيالي (phishing) والفدية الرقمية والهندسة الاجتماعية. وتتوافق نتائج الدراسة مع النتائج التي حصل عليها كلٌّ من الكندي والبلوشي (2020)، والكلباني والعزرية (2022)، حيث خرجت نتائج الدراستين بوعي منخفض في مبادئ ومصطلحات الهندسة الاجتماعية. بينما اختلفت مع نتائج الجنيبية (2023)، التي أظهرت وعيا مرتفعًا لدى عينة الدراسة بالمفاهيم المتعلقة بالهندسة الاجتماعية.

جدول (3): المتوسطات الحسابية والانحرافات المعيارية للمحور الأول

الفقرات	المتوسط	الانحراف	مدى الوعي
لدي معرفة بمفهوم الاختراق الرقمي	3.48	1.01	مرتفع
لدي معرفة بمفهوم انتحال الهوية الرقمية	3.41	1.10	مرتفع
لدي معرفة بمفهوم التصيد الاحتيالي (phishing)	3.17	1.19	متوسط
أمتلك معرفة بالهندسة الاجتماعية Social engineering	2.96	1.15	متوسط
لدي معرفة بمفهوم الفدية الرقمية	2.94	1.29	متوسط
لدي معرفة بتقنيات الهندسة الاجتماعية في مواقع الشبكات الاجتماعية	2.67	1.25	متوسط
المتوسط العام	**3.10**	**.989**	**متوسط**

المحور الثاني: الهندسة الاجتماعية وآثارها النفسية والاجتماعية

توضح نتائج الجدول رقم (4) وعيا مرتفعا بمهارات التصدي لهجمات الهندسة الاجتماعية لدى أفراد عينة الدراسة. إذ أشارت النتائج إلى متوسط حسابي مرتفع جداً يصل إلى (4.38)، حيث يحرص أفراد عينة الدراسة على حماية بياناتهم الشخصية كجزء من مهارات التصدي لهجمات الهندسة الاجتماعية. واتفقت هذه النتيجة مع دراسة روميصاء ولويزة (2021) التي أفضت إلى أن 78% من أفراد عينة الدراسة يتجنبون إعطاء معلومات سرية وبيانات شخصية لأشخاص غير معروفين. واختلفت هذه النتيجة مع دراسة .Harrison et al (2016) التي وجد فيها أن 47% من أفراد عينة الدراسة قاموا بالإفصاح عن بياناتهم في نموذج تصيّد مزيف.

كما أوضحت النتائج إلى أن ما متوسطه (4.34) من الأفراد يقومون بصد هجمات الهندسة الاجتماعية عن طريق وضع كلمة مرور قوية تحتوي على رموز وأرقام، إذ تعتبر كلمة المرور الجدار الأول الذي يستخدمه الأفراد لحماية بياناتهم الشخصية من الاختراق. كما وأشارت النتائج أيضاً، أنه وبمتوسط حسابي يساوي (4.0) يحرص الأفراد على تحميل البرامج الموثوقة من المصادر الموثوقة حتى يتجنبوا تحميل أي برامج قد تحتوي على ميليشيات خبيثة قد تؤدي إلى تسرب بياناتهم ووقوعهم في فخ الهندسة الاجتماعية لاحقاً. وبمتوسط حسابي مرتفع بلغ (3.96). يتجنب أفراد العينة فتح الروابط المرسلة من البريد الإلكتروني. وتتوافق هذه النتيجة مع نتائج .Alsulami et al (2021)، حيث أوضحت الدراسة مدى حذر أفرادها من فتح البريد الإلكتروني ومرفقاته.

وعلى الجانب الآخر، كان حضور الورش والمحاضرات التوعوية المتعلقة بالجوانب الأمنية، واستخدام برامج إدارة كلمات المرور هي أقل الممارسات المستخدمة للتصدي لهجمات الهندسة الاجتماعية، حيث حصلت على أدنى متوسطات حسابية هي (2.67) (2.57) على التوالي. واختلفت هذه النتيجة مع دراسة الكلباني والعزرية (2022) حيث أوضحت أن من أهم تقنيات التصدي لهجمات الهندسة الاجتماعية هو التوعية والتثقيف من خلال الورش والمحاضرات.

جدول (1): المتوسطات الحسابية والانحرافات المعيارية للمحور الثاني

الفقرات	المتوسط	الانحراف	مدى الاهتمام
أحرص دائما على حماية بياناتي الشخصية كجزء من الأمن الرقمي	4.38	.693	مرتفعة جدا
استخدم كلمة مرور قوية تحتوي على رموز وأرقام	4.34	.790	مرتفعة جدا
أحمل البرامج من المواقع الموثوقة فقط	4.00	.934	مرتفعة
أتجنب فتح المواقع من خلال الروابط المرسلة من البريد الإلكتروني	3.96	1.00	مرتفعة
أتأكد من رابط الموقع قبل أن أسجل بياناتي فيه	3.86	1.09	مرتفعة
أقوم بتغيير كلمات المرور الخاصة بين كل فترة	3.61	1.10	مرتفعة
استخدم برامج الحماية وكشف الفيروسات المشهورة مثل - NORTON Kaspersky وغيرها	3.35	1.31	متوسطة
أستخدم كلمة مرور مختلفة لكل موقع أسجل فيه	3.28	1.15	متوسطة
أستخدم التوثيق الثنائي للتسجيل في المواقع - Two-factor authentication	3.23	1.39	متوسطة
أحرص على حضور الورش والمحاضرات التوعية المتعلقة بالجوانب الأمنية	2.67	1.18	متوسطة
أستخدم برامج إدارة كلمات المرور	2.57	1.37	متوسطة
المتوسط العام	**3.57**	**.656**	**مرتفع**

المحور الثالث: آليات مكافحة الهندسة الاجتماعية

سجلت نتائج الجدول رقم (6) وعيا مرتفعا لدى أفراد عينة الدراسة حول الآثار الاجتماعية والنفسية التي خلفتها الهندسة الاجتماعية. حيث حصلت فقرة "انتشار الابتزاز" على أعلى متوسط حسابي، بلغ (4.56)، تلتها فقرة "تشويه السمعة" بمتوسط حسابي يساوي (4.41). وقد يعود ذلك إلى أن الضحية تفضي بمعلومات شخصية وسرية للمهندسين الاجتماعيين، والذين يكون هدفهم منها في الغالب، الربح المادي، مما يؤدي إلى ابتزاز الضحية باستخدام معلوماتهم، وفي حالة عدم استجابة الضحية، يتم تشويه سمعته من خلال نشر معلوماته التي تم الحصول عليها مسبقاً. واتفقت هذه النتيجة مع دراسة روميصاء

ولويزة (2021) التي أشارت بأن 28.3% من أفراد عينة الدراسة ظهرت عليهم آثار اجتماعية نتيجة تعرضهم للابتزاز وتشويه السمعة الناتج عن الهندسة الاجتماعية. كما واتفقت مع دراسة .Fuertes et al (2022) التي كشفت أن هجمات الهندسة الاجتماعية ألحقت أضرارا في السمعة على مستوى الأفراد والشركات.

كما أظهرت النتائج حصول فقرتي "فقدان الثقة بالآخرين" و "تشتت العلاقات الأسرية" على متوسطات حسابية مرتفعة بلغت (4.29) و (4.21) على التوالي. وقد يرجع ذلك إلى التجربة السيئة التي مر بها الفرد، مما يؤدي إلى فقدان ثقته بالآخرين. ومن الناحية الأخرى فإن تشتت العلاقات الأسرية قد يعود إلى نشر أسرار الضحية من خلال الابتزاز وتشويه السمعة ثم يعقبها الانطواء والانعزال. بينما حصلت فقرتا: "انتشار العنف" و"القلق من استخدام الإنترنت" على أدنى متوسطات حسابية كانت (3.80)، (3.65) على التوالي.

جدول (5): المتوسطات الحسابية والانحرافات المعيارية للمحور الثالث

الفقرات	المتوسط	الانحراف	مدى الوعي
انتشار الابتزاز	4.56	.588	مرتفع جدا
تشويه السمعة	4.41	.649	مرتفع جدا
فقدان الثقة في الآخرين	4.29	.765	مرتفع جدا
تشتت العلاقات الأسرية	4.21	.774	مرتفع جدا
الخسائر المادية	4.20	.805	مرتفع
الخوف من استخدام الإنترنت في المعاملات الإلكترونية	4.01	.943	مرتفع
انتشار العنف	3.80	.942	مرتفع
القلق من استخدام الإنترنت	3.65	1.09	مرتفع
المتوسط العام	**4.14**	**.580**	**مرتفع**

المحور الرابع: أنواع هجمات الهندسة الاجتماعية

تشير نتائج الجدول رقم (6) إلى وجود وعي مرتفع لدى أفراد عينة الدراسة حول أشكال الهجمات المستخدمة في الهندسة الاجتماعية. وحصلت فقرتا "مكالمات تليفونية احتيالية للحصول على البيانات البنكية" و "سرقة الحسابات البنكية" على أعلى متوسطات حسابية، تساوي (4.44)، (4.28) على التوالي. وقد تعزى هذه النتيجة إلى أن الهدف الأول لدى المهندسين الاجتماعيين هو الحصول على الأموال. واختلفت هذه النتيجة مع دراسة محمد (2017) التي لخصت إلى أن القليل ممن

تعرضت حساباتهم البنكية للاختراق، حيث جاءت نتيجة الدراسة بأن 6.8% فقط ممن تعرضوا للاختراق عن طريق حساباتهم المصرفية.

كما وأوضحت النتائج أيضاً حصول الفقرات "استغلال واتساب لاختراق الهواتف" و "اختراق البريد الإلكتروني" و "اختراق الحاسوب" على متوسطات حسابية مرتفعة ومتقاربة، جاءت (4.26)، (4.24)، (4.23) على التوالي. وقد يرجع ذلك إلى شيوع استخدام الاختراق للحصول على معلومات الضحية لتحقيق الهدف المرجو من قبل المهندسين الاجتماعيين. وهو ما أكدت عليه دراسة Adam et al. (2011) حيث كشفت أن 38% من هجمات التصيّد كانت عن طريق اختراق البريد الإلكتروني. ودراسة محمد (2017) التي أفضت إلى أن أكثر الأساليب المستخدمة للهندسة الاجتماعية هو اختراق البريد الإلكتروني والتي حصلت على نسبة 53.2%.

جدول (6): أنواع هجمات الهندسة الاجتماعية

الفقرات	المتوسط	الانحراف	مدى الوعي
مكالمات تليفونية احتيالية للحصول على البيانات البنكية	4.44	.724	مرتفع جدا
سرقة الحسابات البنكية	4.28	.760	مرتفع جدا
استغلال واتساب لاختراق الهواتف	4.26	.793	مرتفع جدا
اختراق البريد الإلكتروني	4.24	.798	مرتفع جدا
اختراق الحاسوب	4.23	.794	مرتفع جدا
هجمات تصيّد بالرسائل القصيرة	4.20	.805	مرتفع
اختراق عبر مقاطع الفيديو	3.67	.898	مرتفع
المتوسط العام	**4.19**	**.569**	**مرتفع**

ملخص المحاور

يتضح من خلال الجدول رقم (7) مدى وعي أفراد عينة الدراسة بموضوع الهندسة الاجتماعية، حيث حققت جميع المحاور وعيا مرتفعا باستثناء محور (الوعي بالهندسة الاجتماعية) الذي حقق وعيا متوسطا.

جدول (7): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد الدراسة حول جميع المحاور

الفقرات	المتوسط الحسابي	الانحراف المعياري	الوعي
المحور الأول: الوعي بالهندسة الاجتماعية	3.10	.989	متوسط
المحور الثاني: التأثير الاجتماعي والنفسي	4.14	.580	مرتفع
المحور الثالث: مهارات مكافحة الهندسة الاجتماعية	3.57	.656	مرتفع
المحور الرابع: أنواع هجمات الهندسة الاجتماعية	4.19	.569	مرتفع
المتوسط العام	**3.75**	**.501**	**مرتفع**

تحليل فرضيات الدراسة

الفرضية الأولي: هناك اختلاف في اتجاهات المجتمع العماني حول الهندسة الاجتماعية بناءً على الجنس

تشير النتائج في الجدول (8) إلى وجود فروق دالة إحصائيا لصالح الذكور في المحور الأول "الوعي بمفهوم الهندسة الاجتماعية". وأتت هذه النتيجة منافية لدراسة الكندي والبلوشي (2020)، التي خلصت إلى عدم وجود فروق ذات دلالة إحصائية في الوعي بمعرفة المصطلح تعزى لمتغير النوع. كما أشارت النتيجة أيضاً إلى وجود فروق دالة إحصائيا لصالح الإناث في المحور الرابع "أشكال الهجمات باستخدام الهندسة الاجتماعية". ولا توجد فروق دالة إحصائيا بين الذكور والاناث في محور "مهارات التصدي لهجمات الهندسة الاجتماعية" ومحور "الآثار الاجتماعية والنفسية التي خلفتها الهندسة الاجتماعية".

جدول (2): اختبارات لدراسة الفروق المعنوية في اتجاهات المجتمع العماني حول الهندسة الاجتماعية طبقًا للجنس

المحور	الجنس	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة ت	درجة الحرية	مستوى الدلالة
الوعي بالهندسة الاجتماعية	ذكور	83	3.36	1.00	3.271	180	.001
	إناث	99	2.89	.929	3.249	169.180	
مهارات التصدي لهجمات الهندسة الاجتماعية	ذكور	83	3.64	.663	1.423	180	.156
	إناث	99	3.50	.648	1.420	173.073	
الآثار الاجتماعية والنفسية التي خلفتها الهندسة الاجتماعية	ذكور	83	4.09	.662	-1.095	180	.275
	إناث	99	4.18	.500	-1.069	150.463	
أشكال الهجمات باستخدام الهندسة الاجتماعية	ذكور	83	4.09	.604	-2.043	180	.043
	إناث	99	4.26	.529	-2.019	164.345	

الفرضية الثانية: هناك اختلاف في اتجاهات المجتمع العماني حول الهندسة الاجتماعية بناءً على الفئة العمرية

تشير نتائج الجدول رقم (9) إلى عدم وجود فروق دالة إحصائيا في جميع المحاور، ما عدا المحور الثالث "الآثار الاجتماعية والنفسية التي خلفتها الهندسة الاجتماعية" حيث وجدت فروق دالة إحصائيا.

وبالرجوع إلى اختبار "شيفية" تبين أن الفئة العمرية من 31 – 35 و36 – 40 هما الفئتان الأكثر اعتقادا بتأثير الهندسة الاجتماعية.

جدول (3): اختبار انوفا لدراسة الفروق المعنوية في اتجاهات المجتمع العماني حول الهندسة الاجتماعية طبقًا للفئة العمرية

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	مستوى الدلالة
الوعي بالهندسة الاجتماعية	بين المربعات	1.501	6	.250	.249	**.959**
	ضمن المربعات	175.667	175	1.004		
	الكلي	177.168	181			
مهارات التصدي لهجمات الهندسة الاجتماعية	بين المربعات	4.115	6	.686	1.622	**.144**
	ضمن المربعات	74.003	175	.423		
	الكلي	78.119	181			
الآثار الاجتماعية والنفسية التي خلفتها الهندسة الاجتماعية	بين المربعات	4.674	6	.779	2.424	**.028**
	ضمن المربعات	56.228	175	.321		
	الكلي	60.902	181			
أشكال الهجمات باستخدام الهندسة الاجتماعية	بين المربعات	2.985	6	.498	1.561	**.161**
	ضمن المربعات	55.767	175	.319		
	الكلي	58.753	181			

الفرضية الثالثة: هناك اختلاف في اتجاهات المجتمع العماني حول الهندسة الاجتماعية بناءً على مستوى التعليم

تشير نتائج الجدول رقم (10) إلى عدم وجود فروق دالة إحصائيا في جميع المحاور، باستثناء المحور الثالث (الآثار الاجتماعية والنفسية التي خلفتها الهندسة الاجتماعية)، وبالرجوع إلى اختبار "شيفية" تبين أن حملة الدبلوم والدكتوراه لديهم اعتقاد أكبر بتأثير الهندسة الاجتماعية. واختلفت هذه النتيجة مع دراسة Adam et al. (2011)، حيث كانت نتيجتها وجود فروق إحصائية في الوعي بالهندسة الاجتماعية لدى متغير التعليم لصالح طلبة الدراسات العليا.

جدول (4): اختبار انوفا لدراسة الفروق المعنوية في اتجاهات المجتمع العماني حول الهندسة الاجتماعية طبقًا لمستوي التعليم

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	مستوى الدلالة
الوعي بالهندسة الاجتماعية	بين المربعات	3.665	3	1.222	1.253	.292
	ضمن المربعات	173.504	178	.975		
	الكلي	177.168	181			
مهارات التصدي لهجمات الهندسة الاجتماعية	بين المربعات	1.414	3	.471	1.094	.353
	ضمن المربعات	76.704	178	.431		
	الكلي	78.119	181			
الآثار الاجتماعية والنفسية التي خلفتها الهندسة الاجتماعية	بين المربعات	2.696	3	.899	2.749	.044
	ضمن المربعات	58.205	178	.327		
	الكلي	60.902	181			
أشكال الهجمات باستخدام الهندسة الاجتماعية	بين المربعات	1.014	3	.338	1.042	.375
	ضمن المربعات	57.739	178	.324		
	الكلي	58.753	181			

الفرضية الرابعة: هناك اختلاف في اتجاهات المجتمع العماني حول الهندسة الاجتماعية بناءً على مستوى الفئة الوظيفية

تشير نتائج الجدول رقم (11) إلى عدم وجود فروق دالة إحصائيا في جميع المحاور، باستثناء المحور الثاني " مهارات التصدي لهجمات الهندسة الاجتماعية"، وبالرجوع إلى اختبار "شيفية" تبين أن فئتي الموظفين وأعضاء هيئة التدريس لديهم درجة مرتفعة بمهارات التصدي لهجمات الهندسة الاجتماعية، بينما فئة الطلاب لديهم درجة متوسطة. وقد يعزى ذلك إلى النضج الفكري والمعرفي الذي يتمتع به أعضاء هيئة التدريس والموظفين مقارنة بالطلاب.

جدول (11): اختبار انوفا لدراسة الفروق المعنوية في اتجاهات المجتمع العماني حول الهندسة الاجتماعية طبقًا لمستوى الفئة الوظيفية

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	مستوى الدلالة
الوعي بالهندسة الاجتماعية	بين المربعات	1.798	2	.899	.918	.401
	ضمن المربعات	175.370	179	.980		
	الكلي	177.168	181			
مهارات التصدي لهجمات الهندسة الاجتماعية	بين المربعات	4.428	2	2.214	5.379	.005
	ضمن المربعات	73.690	179	.412		
	الكلي	78.119	181			
الآثار الاجتماعية والنفسية التي خلفتها الهندسة الاجتماعية	بين المربعات	.249	2	.124	.367	.693
	ضمن المربعات	60.653	179	.339		
	الكلي	60.902	181			
أشكال الهجمات باستخدام الهندسة الاجتماعية	بين المربعات	.564	2	.282	.868	.422
	ضمن المربعات	58.189	179	.325		
	الكلي	58.753	181			

التوصيات

استنادًا إلى نتائج الدراسة، تتضمن التوصيات مقترحات لمواجهة تحديات الهندسة الاجتماعية على شبكات التواصل الاجتماعي وتأثيرها على الأمن العام في عمان وفق الآتي:

1. **تعزيز الوعي الرقمي**: هناك حاجة ماسة لزيادة الوعي الرقمي داخل المجتمع العماني وتطوير المهارات لمواجهة تكتيكات الهندسة الاجتماعية.
2. **تطوير استراتيجية وطنية للأمن الرقمي:** كشفت نتائج الدراسة عن الحاجة إلى تطوير استراتيجية وطنية شاملة لتعزيز تدابير الأمن الرقمي في جميع أنحاء البلاد.
3. **تعظيم الاستفادة من التكنولوجيا**: استكشاف طرق مستحدثة لاستخدام التكنولوجيا بفعالية لمكافحة تحديات الهندسة الاجتماعية وتعزيز الثقافة الرقمية بين السكان.
4. **تشجيع التعاون بين القطاعات الخدمية**: تبرز أهمية دمج الجهود في مختلف القطاعات لضمان بيئة رقمية آمنة في عمان، مع التأكيد على ضرورة التحسين المستمر واعتماد استراتيجيات شاملة لمكافحة الهندسة الاجتماعية.

هذه التوصيات الاستراتيجية تهدف إلى التخفيف من المخاطر التي تشكلها الهندسة الاجتماعية وضمان حماية المعلومات الحساسة والأمن الرقمي العام للأفراد والمؤسسات في عمان.

الخاتمة

تُعد هذه الدراسة دراسة استكشافية حول هندسة الاجتماع في شبكات التواصل الاجتماعي وتأثيرها على الأمان العام في سلطنة عمان. هدفت الدراسة إلى تحليل تأثير هندسة الاجتماع والتحديات التي تنشأ عنها على مستوى الأمان الرقمي والجوانب الاجتماعية والنفسية للمستخدمين.

وفرت النتائج النهائية للدراسة نظرة شاملة حول مدى تأثير هندسة الاجتماع، وتقديم محتوى فعّال لفهم: كيف يمكن للهجمات الاجتماعية التأثير على الأمان العام؟

أشارت الدراسة إلى تأثير هندسة الاجتماع على مستوى الأمان العام، حيث يتعامل الهاكرز بشكل مباشر مع الجوانب الاجتماعية والنفسية للمستخدمين لاختراق أنظمة الأمان. كما سلطت الدراسة الضوء على التحليل التباين في اتجاهات المجتمع العماني بناءً

على عدة متغيرات مثل الجنس، العمر، المستوى التعليمي، والفئة الوظيفية، مما وفر فهمًا عميقًا لتفاعل المجتمع مع هجمات الهندسة الاجتماعية.

اختتمت الدراسة بدعوة إلى تبني نهج شامل لتعزيز الأمان العام في سلطنة عمان، مع التأكيد على أهمية تكامل الجهود بين الحكومة والقطاع الخاص والمجتمع المدني لتحقيق بيئة رقمية آمنة ومحمية.

يُعزز الختام فهمًا أعمق لمفهوم هندسة الاجتماع وضرورة تبني استراتيجيات شاملة لمكافحة هذه التحديات في المستقبل.

وبناءً على النتائج، قدمت الدراسة توصيات تعكس التحديات والفرص المستقبلية. تشمل التوصيات دعم التوعية الرقمية، وتعزيز مهارات مكافحة الهندسة الاجتماعية، وتطوير إطار قوانيني فعّال للحماية الرقمية. وتوسيع الأبحاث لتشمل مجالات مثل استخدام التكنولوجيا الحديثة في مكافحة هندسة الاجتماع واستكشاف أساليب تحسين الوعي الرقمي بشكل أفضل.

المراجع العربية:

- أحمد، عبد الخالق محمد (2014). الهندسة الإجتماعية. *المال والاقتصاد*، (75)،22 - 23. 630305/Record/com.mandumah.search://http
- الجنيبية، فاطمة بنت علي (2023). *دور مؤسسات المعلومات في تعزيز الوعي بمخاطر الهندسة الاجتماعية: دراسة حالة للمكتبات الأكاديمية في سلطنة عمان* [رسالة ماجستير غير منشورة]. جامعة السلطان قابوس.
- روميصاء، ميلودي و لويزة، لصقع (2021). *أثر الهندسة الاجتماعية في مواقع التواصل الاجتماعي على الطالب الجامعي: فيس بوك أنموذجا* [رسالة ماجستير، جامعة قاصدي مرباح ورقلة].
- عبد الرحيم، حسام فايز عبد الحي (2020). مشاركة الجمهور في تقنيات الهندسة الاجتماعية عبر موقع فيس بوك وعلاقتها بالخصوصية والتعويض النفسي لديهم. *مجلة البحوث الإعلامية، 1* (55) ،589 - 640. 1092380/Record/com.mandumah.search:/ Algarni/h
- عبد المنعم، أحمد السيد. (2021). الهندسة الاجتماعية وبناء العقل. *مجلة الإرشاد النفسي*، (67)،1 - 7. 1179124/Record/com.mandumah.search://http
- الكلباني، وليد والعزرية، عائشة (2022). الوعي المجتمعي بتقنيات الهندسة الاجتماعية وتداعياتها الأمنية في ظل التحول الرقمي للخدمات الحكومية في سلطنة عمان: جامعة التقنية والعلوم التطبيقية أنموذجا. *الأمانة*، (39)، 163-183.
- الكندي، سالم سعيد، البلوشي، حليمة سليمان. (2020). الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان: دراسة حالة لطلبة الكلية التقنية بالمصنعة. *مجلة الآداب والعلوم الاجتماعية، 11* (2)، 71 – 84
- محمد، مها أحمد إبراهيم (2017، نوفمبر 27-29). *الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي*. المؤتمر الثامن والعشرون الاتحاد العربي للمكتبات والمعلومات (اعلم): شبكات التواصل الاجتماعي وتأثيراتها في مؤسسات المعلومات في الوطن العربي، القاهرة، مصر. 854072/Record/com.mandumah.search://h
- محمد، مها أحمد إبراهيم. (2019). الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي. *المجلة الدولية لعلوم المكتبات والمعلومات، 6*(4)، 195 – 218. /1039004Record/com.mandumah.search://http

المراجع الإنجليزية

- Adam, M., Yousif, O., Al-Amodi, Y., & Ibrahim, J. (2011) Awareness of Social Engineering Among IIUM Students. *World of Computer Science and Information Technology Journal (WCSIT), 1* (9), 409-413.
- Aldawood, H., Alashoor, T., & Skinner, G. (2020). Does Awareness of Social Engineering Make Employees More Secure?. *International Journal of Computer Applications, 177* (38), 45-49.
- Alexander, M., & Wanner, R. (2016). Methods for understanding and reducing social engineering attacks. SANS Inst, 1, 1-32.
- Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. *European Journal of Information Systems, 26*, 661-687.
- Almutairi, B., & Alghamdi, A. (2022). The Role of Social Engineering in Cybersecurity and Its Impact. *Journal of Information Security*, *13*, 363-379.
- Alsulami, M., Alharbi, F., Almutairi, H., Almutairi, B., Alotaibi, M., Alanzi, M., Alotaibi, K., & Alharthi, S. (2021). Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. *Information, 12* (5), 208.
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in human behavior*, *38*, 304-312.
- Brody,R.G., Brizzee, W.B., & Cano, L. (2012). Flying under the radar: social engineering, *International Journal of Accounting and Information Management, 20* (4), 335 – 347.
- Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In *Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15* (pp. 63-72). Springer Berlin Heidelberg.
- Chetioui, k., Bah, B., ALami, A., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. *Procedia Computer Science, 189*, 656-661.

- Chinta, M., Alaparthi, J., & Koda, E. (2016). A Study on Social Engineering Attacks and Defence Mechanisms. *Int. J. Comput. Sci. Inf. Secur. IJCSIS*, *14*, 225-231.
- Chuang, J. (2021). Romance Scams: Romantic Imagery and Transcranial Direct Current Stimulation. *Frontiers in Psychiatry*, *12*, 12.
- Cusack, B., & Adedokun, K. (2018). The impact of personality traits on user's susceptibility to social engineering attacks. In *Proceedings of the 16th Australian Information Security Management Conference* (p. 83).
- Fuertes, W., Arévalo, D., Castro, J., Ron, M., Estrada, C., Andrade, R., Peña, F., & Benavides, E. (2022). Impact of Social Engineering Attacks: A Literature Review. In Á. Rocha, C. H. Fajardo-Toro & J. M. R. Rodríguez (Eds.), *Developments and Advances in Defense and Security* (pp.25-35). https://doi.org/10.1007/978-981-16-4884-7_3
- Harrison, B., Svetieva, E., &Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review, 40*(2), 265-281. https://doi.org/10.1108/OIR-04-2015-0106
- Hasan, M., Prajapati, N., &Vohara, S. (2010). Case study on social engineering techniques for persuasion .*International journal on applications of graph theory in wireless ad hoc networks and sensor networks, 2(*2), 17-23.
- Hussain, M., Siddiqui, S., & Islam, N. (2023). Social Engineering and Data Privacy. In A. Naim, P. Malik, & F. Zaidi (Eds.), *Fraud Prevention, Confidentiality, and Data Security for Modern Businesses* (pp. 225-248). IGI Global. https://doi.org/10.4018/978-1-6684-6581-3.ch010
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.
- Mashtalyar, N., Ntaganzwa, U., Santos, T., Hakak, S., & Ray, S. (2021). Social Engineering Attacks: Recent Advances and Challenges. In A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust* (pp.417-431). http://doi.org/10.1007/978-3-030-77392-2_27
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186-209.
- Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 1-17.

- Sandouka, H., Cullen, A. J., & Mann, I. (2009, September). Social engineering detection using neural networks. In *2009 International Conference on CyberWorlds* (pp. 273-278). IEEE.
- Tulkarm, P. (2021). A Survey of Social Engineering Attacks: Detection and Prevention Tools. *Journal of Theoretical and Applied Information Technology*, *99*(18).
- Twitchell, D. P. (2006, September). Social engineering in information assurance curricula. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 191-193).