تاثيرات أساليب الهندسة الاجتماعية على اختراق معلومات الطلبة الجامعيين في مواقع التواصل الاجتماعي

ـ دراسة تطبيقية على عينة من الطلبة الجامعيين ـ

م.د.ميادة كاظم جعفر

وزارة التعليم العالي والبحث العلمي، بغداد \ العراق

The Effects of Social Engineering on the Penetration of University Student's Information on Social Media

Lect. Dr. Mayada Kadhum Ja'afar

Ministry of Higher Education and Scientific Research, Baghdad / Iraq

mayadakadhum1@gmail.com

المستخلص

هدف البحث الى التعرف على توضيح أساليب الهندسة الاجتماعية وخطورتها على المجتمع عموماً وعلى شريحة الطلبة الجامعيين خصوصاً، فضلا عن التعريف بثغرات امن المعلومات على وسائل التواصل الاجتماعي، وتسليط الضوء على قاعدة المعرفة لدى طلبة الجامعات باساليب الهندسة الاجتماعية، وقد تم اجراء تطبيق عملي للبحث من خلال اجراء دراسة ذو اسلوب منهجي كمي على عينة من طلبة كلية الاعلام في جامعة بغداد ضمن الدراسات الأولية (البكالوريوس) والدراسات العليا (الماجستير والدكتوراه) فتكونت عينة البحث من 50 طالب وطالبة, وزعت استبيان عليهم التي شملت محوري البحث وهما (امن المعلومات وأساليب الهندسة الاجتماعية) لغرض التحقق من تاثيرات أساليب الهندسة الاجتماعية في اختراق معلومات الطلبة الجامعيين في مواقع التواصل الاجتماعي، أشارت النتائج الى وجود تاثيرات واسعة لتلك الأساليب على اختراق معلومات الطلبة، بالرغم من وجود معرفة لدى شريحة واسعة منهم بضرورة تحصين امن معلوماتهم. واوصى البحث بعدد من التوصيات كان اهمها دعم برامج ومهارات الوعي المعلوماتي لدى الافراد والمؤسسات وذلك من خلال التنسيق مع الجهات المتخصصة كاقسام دراسات المعلومات في الجامعات للرقي بمستوى الوعي المعلوماتي وتعزيز ثقافة تكنلوجيا الاتصالات لديهم التي تعتبر من الأساليب التنظيمية التثقيفية للحد من تلك السلوكيات.

الكلمات المفتاحية: الهندسة الاجتماعية , امن المعلومات وسائل التواصل الاجتماعي.

Abstract

The aim of the research is to identify the clarification of social engineering methods and their danger to the society in general and to the university students section in particular, as well as introducing information security gaps on the social media, and shedding light on the knowledge base of university students in social engineering methods, and a practical application of the research was carried out through conducting a quantitative methodological study on a sample of students from the College of Media at the University of Baghdad including both undergraduate (bachelor's) and postgraduate (master and doctorate) students. The research sample consisted of 50 male and female students. A questionnaire was distributed to them that included the two parameters of the study, meanly, information security and methods of social engineering for the purpose of verifying the effects of social engineering methods in penetrating university students' information on social networking sites, as it was found that there are wide effects of these methods on the penetrating students' information, despite the knowledge of a wide section of them of the need to fortify the security of their information. The research recommended a number of recommendations, the most important of which was to support information awareness programs and skills for individuals and institutions through coordination with specialized agencies such as Information Studies Departments in Universities to raise the level of information awareness and enhance their communication technology culture, which is one of the organizational and educational methods to reduce these behaviors.

Keywords: Social engineering, Information security and Social media.

المقدمة

صاحب التطور في وسائل الاتصال الحديثة وتكنولوجيا المعلومات والاتصالات، وما رافقها من ظهور تقنيات حديثة في الأجهزة الذكية، حالة من التواصل ونقل وتبادل المعلومات والمعرفة على مستوى الأفراد والمؤسسات، وصاحب ذلك كثير من المخاطر، فالتقنية أداة يمكن أن تتشكل إما لتحقيق أهداف تطويرية وتنظيمية لخدمة مجتمع ما، أو تستخدم لأهداف خبيثة تضر بالمجتمع وافراده، وقد يتطور ذلك الى حدوث جرائم تضر بامن ذلك المجتمع، وهو ما عرف فعلاً بظهور كثير من الجرائم المعلوماتية على الشبكات الالكترونية بفعل افراد او منظمات، لاسيما بعد ان اصبح الاعتماد على الإنترنت يشكل حلقة رئيسية في مختلف مجالات الحياة المعاصرة.

وفي مثل هذه البيئة تصاعدت التهديدات الإلكترونية والمخاطر الأمنية المحيطة بها، وعرف ظهور مصطلح الهندسة الاجتماعية الذي اختلف مفهومه عن علوم أخرى تتداوله، فتمثل المصطلح في مجال امن المعلومات عن أساليب ملتوية تهدف للحصول على معلومات سرية بواسطة التلاعب أو خداع الناس، واصبح المهندس الاجتماعي في هذا المجال هو الشخص البارع في كشف معلومات سرية قد تقع ضمن نطاق الخصوصية، وبالتالي عُدت الهندسة الاجتماعية مجموعة من التقنيات المستخدمة لجعل الناس يفضون بمعلومات سرية بعلمهم او بدون علمهم تحت ظروف يقعون بها.

في هذا البحث سيتم التعرف على ما تعنيه الهندسة الاجتماعية ومدى فاعلية اساليبها الذي تحدثه في وسائل التواصل الاجتماعي، وبالتالي التاثير على امن المجتمع وذلك من خلال التطبيق على عينة من الطلبة الجامعيين. أجريت الدراسة على عينة من طلبة كلية الاعلام – جامعة بغداد التي تكونت من (50) طالبا وطالبة من طلبة الدراسات الأولية والعليا، وزعت عليهم استمارة استبيان ومن ثم احصيت البيانات وحللت النتائج وصولا الى بعض الاستنتاجات والتوصيات التي تخص هذا الموضوع.

مشكلة البحث

ان التطور الحاصل في مجال المعلوماتية والاتصالات قد كشف عن وجود ثغرات في امن المعلومات يستغلها البعض من ضعاف النفوس للوصول الى اهداف غير مشروعة تضر بامن الفرد والمجتمع، ولما كانت وسائل التواصل الاجتماعي اليوم هي احدى القنوات ذات الشعبية العالية على جميع مستويات المجتمع، فانه يُخشى من استفحال أساليب ما يعرف بالهندسة الاجتماعية في تلك الوسائل مع جهل الكثيرون باساليبها وغاياتها.

ويمكن مما تقدم صياغة مشكلة البحث في التساؤلات الاتية:

1. ما مدى ادراك المجتمع لخطورة ظاهرة الهندسة الاجتماعية ونتائجها خصوصاً في وسائل التواصل الاجتماعي ذات الشعبية الكبيرة في المجتمع؟
2. هل تمتلك شريحة الطلبة الجامعيين تحصيناً كافياً ضد أساليب الهندسة الاجتماعية؟
3. هل تهتم الحكومات بتشريع القوانين للحد من ظاهرة الهندسة الاجتماعية؟

أهمية البحث

يعد موضوع الهندسة الاجتماعية من المواضيع الحديثة في مجال امن المعلوماتية، ولكون الموضوع لم يتم التأكيد عليه في المجال البحثي لاسيما على مستوى العراق، بالإضافة الى انه قد يؤثر تاثيراً كبيراً على فئات اجتماعية كبيرة نظراً لما يحدثه من ضرر على مستخدمي وسائل التواصل الاجتماعي، التي باتت اليوم تستخدم من قبل فئات المجتمع، فان هذا البحث يمكن ان يكون مساهمة للانتباه الى تلك الظاهرة وحث المشرعين والتقنيين على إيجاد الوسائل الكفيلة بمكافحتها والحد من تاثيراتها السلبية.

اهداف البحث

1. يسعى البحث الى توضيح أساليب الهندسة الاجتماعية وخطورتها على المجتمع عموماً وعلى شريحة الطلبة الجامعيين خصوصاً.
2. التعريف بثغرات امن المعلومات على وسائل التواصل الاجتماعي.
3. تسليط الضوء على قاعدة المعرفة لدى طلبة الجامعات باساليب الهندسة الاجتماعية.

المبحث الأول \ الجانب النظري

أولا: الهندسة الاجتماعية

ينظر الكثيرون إلى مفهوم الهندسة الاجتماعية باعتباره مصطلح يتضمن مجموعة من الإجراءات التي من شأنها تنظيم الجوانب الاجتماعية في حياة البشر, إلا أنه عند البحث عن هذا المفهوم وُجد أنه يتضمن العديد من المعاني التي قد تضر بحياة البشر وتسيطر على عقولهم وتفكيرهم، بل تتعدى ذلك إلى استخدام طرق وتقنيات الخداع والتلاعب او للحيل الذكية لتغيير أفكارهم وما يتبنوه من معتقدات وتراث وقيم واتجاهات مترسخة منذ قديم الأزل (عبدالتواب، 2021: 492). لذلك اتجه تعريف الهندسة الاجتماعية ضمن سياق أمن المعلومات وهذا حسب ما أورده العديد من الباحثين عندما بينوا انها تشير إلى "مختلف الوسائل المستخدمة للحصول على المعلومات الحساسة وتجاوز الأنظمة الأمنية من خلال استغلال نقاط ضعف العنصر البشري (شايب وقيدة، 2018: 2).

لقد سميت هذه التهديدات بالتهديد السيبراني، أو تهديد الأمن السيبراني وهو عمل ضار يسعى إلى إتلاف البيانات أو سرقتها أو تعطيل الحياة الرقمية بشكل عام، ويتضمن ذلك أنواعًا مختلفة من التهديدات مثل فيروسات الكمبيوتر وخروقات البيانات وهجمات رفض الخدمة (DoS) ونواقل الهجوم الأخرى، كما يشير أيضًا إلى إمكانية حدوث هجوم إلكتروني يهدف إلى الوصول غير المصرح به أو إتلاف أو تعطيل أو سرقة أصول تكنولوجيا المعلومات أو شبكة الكمبيوتر أو الملكية الفكرية أو أي شكل آخر من أشكال البيانات السرية، ويمكن حصول التهديدات السيبرانية من داخل المؤسسة عن طريق مستخدمين موثوق بهم أو من مواقع مجهولة من قبل أشخاص مجهولين (Rajitha and Priya ,2022:13).

وقد عُدت تقنيات الهندسة الاجتماعية اليوم الطريقة الأكثر شيوعًا لارتكاب الجرائم السيبرانية من خلال اختراق وإصابة أنظمة الكمبيوتر والبنى التحتية لتكنولوجيا المعلومات، حيث يستخدم خبراء الأمن السيبراني مصطلح "الهندسة الاجتماعية" لتسليط الضوء على "العامل البشري" في الأنظمة الرقمية (Witjes and Wentland, 2021: 1317).

وتحاول الباحثة عرض ماذكره الباحثون حول مفهوم الهندسة الاجتماعية واساليبها واغراضها فيما ياتي.

1: مفهوم الهندسة الاجتماعية

اختلف مفهوم الهندسة الاجتماعية 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، وعرف في العلوم الاجتماعية بانه استخدام التخطيط المركزي في محاولة لإدارة التغيير الاجتماعي، اما عند الحديث عن الأمن أو أمن المعلومات، فتتمثل في خداع الناس أو التلاعب بهم للإفصاح عن معلومات تتمتع بالسرية أو الخصوصية (الكندي والبلوشي، 2020: 74).

فالهندسة الاجتماعية أسلوب من أساليب الاختراق التي تعتمد على العنصر البشري تماماً وليس لها أية أبعاد تقنية حيث يستخدم الهاكر مهاراته في الاتصال مع الآخرين ويستعمل الخداع والكذب ليحصل منهم على معلومات ذات طابع تقني يتمكن بواسطتها من القيام بعملية الاختراق (محمد، 2018: 110).

وعرفها اخصائيو التواصل الاجتماعي بأنها استخدام المهاجم لحيل نفسية كي يخدع مستخدمي شبكة الإنترنت ليمكنوه من الوصول إلى معلومات عنهم (عبدالحي، 2020: 601).

وبصورة اشمل تعرف الهندسة الاجتماعية في سياق أمن معلومات التواصل الاجتماعي بأنها: وسائل الخداع بهدف التأثير على الأفراد للإفشاء عن معلومات سرية بشكل إرادي بهدف استغلال هذه المعلومات لارتكاب احتيال (عبدالتواب، 2021: 495).

2: مخاطر الهندسة الاجتماعية

تزايدت هجمات الهندسة الاجتماعية بشكل سريع في شبكات التواصل الاجتماعي، وهي تهدف إلى التلاعب بالأفراد والمؤسسات لإفشاء بيانات قيمة وحساسة لصالح مجرمي الإنترنت، متحديةً أمان جميع الشبكات بغض النظر عن قوة جدران الحماية وطرق التشفير

وأنظمة كشف التسلل وأنظمة برامج مكافحة الفيروسات، اذ انها تؤثر من خلال التفاعلات البشرية على الشخص نفسياً لإفشاء معلومات سرية أو لكسر الإجراءات الأمنية، فهي تتصف بانها أقوى الهجمات على وسائل التواصل الاجتماعي لأنها تهدد جميع الأنظمة والشبكات الالكترونية (Salahdine and Kaabouch ,2019:2).

وغالباً ما يستخدم متسللو ومجرمو الإنترنت أساليب الهندسة الاجتماعية بشكل متكرر لبناء استراتيجيات لخداع الأشخاص ومنحهم وصول آمن إلى النظام عن طريق كسر أفضل الممارسات والمعايير الأمنية بشكل غير قانوني أو حتى بدون خرق القانون (Hijji and Alam ,2021: 7152).

ان ما يقوم به المهندس الاجتماعي يصوره العديد من خبراء الأمن السيبراني بأنها مسألة معرفة / ومحو الأمية التكنولوجية، ووفقًا لهذا المنظور، تحدث الحوادث الأمنية لأن الذي وقع ضحية الهجوم الاجتماعي لم يكتشف تقنيات التلاعب التي يستخدمها المتسللون، فالنقص المعرفي المزعوم هو ناقل الهجوم الرئيسي الذي يمكن للمتطفلين من خلاله تجاوز الإجراءات الأمنية والوصول إلى البنى التحتية الرقمية. ووفق ذلك فان من ليس لديهم الخبرة المناسبة لاكتشاف الأنشطة المشبوهة والرد فانهم يحتاجون إلى التوعية والتعليم والتدريب لتجنب أن يصبحوا مخاطر أمنية على مجتمعهم (Witjes and Wentland, 2021: 1318).

وغالباً ما تكون طرق المهاجم لتنفيذ الهجمات الاجتماعية على شكل مراحل متسلسلة ومتكررة وكما يأتي (شايب وقيدة، 2018: 2):

1. جمع المعلومات وتحديد الهدف: في هذه المرحلة يتم جمع أكبر قدر من المعلومات حول الضحية عن طريق المواقع الالكترونية المختلفة مثل: مواقع التواصل الاجتماعي، المدونات، موقع المؤسسة وما إلى ذلك. كما يتم أيضا البحث في سلة المهملات عن معلومات إضافية حول الضحية. وتمثل هذه المرحلة أساس نجاح الهندسة الاجتماعية. بعد إتمام مرحلة جمع المعلومات، يقوم المهاجم اختيار الضحية المستهدفة من أجل بناء وتطوير العلاقة كمرحلة ثانية
2. تطوير العلاقة: يحاول المهاجم خلال هذه المرحلة بناء علاقة مع الضحية المستهدفة والعمل على تطويرها عن طريق استغلال نقاط الضعف لديها

(العاطفة، الثقة...الخ) حتى يتمكن من استخراج وانتزاع المعلومات الحساسة التي يريدها مثل: معلومات الحساب، أرقام بطاقة الائتمانية، معلومات الدخول وما إلى ذلك.

3. استغلال العلاقة: بمجرد بناء العلاقة مع الضحية المستهدفة وتطوريها يقوم المهاجم باستغلالها لصالحه.
4. التنفيذ والوصول إلى الهدف: في هذه المرحلة يقوم المهاجم التنفيذ الفعلي لما تم التخطيط له ومحاولة الوصول إلى الهدف النهائي. وفي حالة عدم وصول المهاجم إلى النتائج المرغوبة، فإنه من الممكن أن يعمل على تكرار الخطوات السابقة.

لذلك أُطلَق على الهندسة الاجتماعية مصطلح "علم أو فن اختراق العقول"، وقد تشكلت خطورتها في السنوات الأخيرة؛ نظرًا للنمو الهائل والمتسارع لشبكات التواصل الاجتماعي والبريد الإلكتروني والأشكال الأخرى للاتصالات الإلكترونية، وأصبح هذا المصطلح مستخدمًا على نطاق واسع للإشارة إلى مجموعة من الأساليب التي يستخدمها المجرمون في الحصول على المعلومات الحساسة أو إقناع الضحايا المستهدفَة بتنفيذ بعض الإجراءات التي تساعد على اختراق أنظمتهم والإضرار بها(عبدالحي، 2020: 600).

وهناك أربعة أنماط رئيسية لتهديدٌات الهندسة الاجتماعية تحصل نتيجة لما تقدم وهي كما يأتي (الشمري، 2020: 149):

1. **هجمات الحرمان من الخدمة:** إذ يتم إطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على معالجتها والاستجابة لها، مما يؤدي إلى توقفه بصورة جزئية او كلية أو إبطاء عمله، وهذا ما يسبب ضرر للمستخدم النهائي وتستعمل كثيرا ضد مواقع الأنترنت أو البنوك أو المؤسسات من أجل التاثير عليها أو لدفع فدية مادية.
2. **إتلاف المعلومات أو تعديلها:** ويقصد به الوصول إلى معلومات الضحية عبر شبكة الأنترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون ان يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج خطيرة لصاحبها.

3. **التجسس على الشبكات:** ويقصد به الدخول غير المصرح والتجسس على شبكات الضحية، دون تدمير البيانات او تغيير في البيانات والهدف منه الحصول معلومات هامة.
4. **تدمير المعلومات:** ويتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة واصطلح على تسميتها "تهديد لسلامة المحتوى" ويعنى بها إحداث تغيير في البيانات سواء بالحذف او بالتغيير.

وقد زادت خطورة الهندسة الاجتماعية لامكانية اكتشاف هجماتها مع استحالة إيقافها، اذ يستغل المهندسون الاجتماعيون الضحايا للحصول على معلومات حساسة يمكن استخدامها لأغراض محددة أو بيعها في السوق السوداء او على صفحات الويب السوداء، اما على مستوى المؤسسات يستخدم المهاجمون البيانات الضخمة للاستفادة من البيانات القيمة لأغراض الأعمال، فهم يجمعون كميات هائلة من البيانات لبيعها بالجملة كبضائع للأسواق.(Salahdine and Kaabouch, 2019:3)

من كل ما تقدم فقد ارتبطت الهندسة الاجتماعية في مجال امن المعلومات بالجرائم الإلكترونية ؛ وهو نشاط غير مشروع يتم عبر الفضاء السيبراني وغالباً ما تقوم به مجموعات منظمة من خلال اختراق أجهزة الحاسوب والذي يؤدي الى إلى نسخ أو تغيير أو حذف أو الوصول إلى المعلومات المُخزنة داخل الحاسوب أو التي تُنقل عن طريقه وهي سلوك غير مشروع فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات (المشهدي، 2019: 242).

وفي هذا المجال يمكن ان تستخدم شبكات الحاسوب العالمية في تبادل معلومات المجرم ونشرها او عرض بضائع غير مشروعة او عروض كاذبة لغرض الحصول على ارباح مالية غير مشروعة فالانترنت هنا هو كأي اداة لارتكاب الجريمة، كما ودخل ضمن اطار الجرائم الحاسوبية ايضًا عروض بيع بأسعار وحصص خاصة بصورة غير قانونية او استثمار عقارات تعود للدولة او قروض مالية لقاء فوائد غير مشروعة او الحث بالدخول في مشاريع وهمية او تزييف الوثائق الرسمية او الحث على تشغيل الاطفال بصورة غير قانونية او الحث على التمييز العنصري وغيره(المختار، 2008: 47).

3: مهارات وخصائص المهندس الاجتماعي

تُمارس الهندسة الاجتماعية من خلال مهاراتها للحصول على معلومات سرية وهامة بأسلوب التلاعب العقلي، حيث تبحث عن أخطاء بشرية كـ(الثقة الزائدة – عدم التركيز – الفضول) ليتمكن المهندس الاجتماعي من الحصول على غايته وتبدأ اللعبة عند اكتشاف نقطة الضعف التي يتم الاستغلال من خلالها (محمد، 2018: 110).

لذلك فان هناك مهارات يتصف بها ممارسو الهندسة الاجتماعية للوصول الى غاياتهم وهي كالآتي (عبدالتواب، 2021: 495):

1. ممارسة أوجه الخداع/الاحتيال من قبل شخص ما تجاه الآخر.
2. يستند المهندس الاجتماعي على مجموعة من المهارات والقدرات الخاصة التي تمكنه من الهجوم على الآخرين.
3. يتم استخدام العديد من الأساليب التقنية أو البشرية من قبل المهندس الاجتماعي لتنفيذ الهجمات.
4. تنطوي الهندسة الاجتماعية على أغراض خبيثة تستهدف جمع المعلومات والبيانات عن هؤلاء الأشخاص.
5. تتمثل تلك الأغراض في جمع المال، السرقة، تغيير الأفكار التي يتبناها الأشخاص، توجيه الفرد للقيام بأفعال كان من المستحيل أن يقوم بها في وقت سابق, مما قد يؤدي في النهاية إلى تغيير نمط حياتهم بالكامل.

4: اساليب وطرق الهندسة الاجتماعية

يأتي دور الهندسة الاجتماعية في عملية اختراق الاجهزة والأنظمة عن طريق مهارات المهندس الاجتماعي االبشرية والتقنية العالية، وأيضاً المقدرة على التمثيل واقناع الضحية بشكل غير مباشر بشتى الوسائل للوصول إلى المعلومات المطلوبة، وتختلف الوسائل المستخدمة في الهندسة الاجتماعية منها على سبيل المثال لا الحصر أن المهندس الاجتماعي قد ينتحل شخصية موظف بنك ويقوم بالاتصال على أحد عملاء البنك وبطريقته الخاصة يحصل على جميع البيانات البنكية وهذه الطريقة منتشرة بكثرة وأغلب الضحايا هم من كبار السن، وقد ينتحل شخصية عامل صيانة اجهزة وشبكات حاسب آلي أو يعمل بشكل

مؤقت في احدى الشركات ويختلط بالموظفين الذين لديهم صلاحيات الدخول لأنظمة المنشأة (محمد، 2018: 117).

وتقسم وسائل الهندسة الاجتماعية في شبكات الويب العالمية إلى ثلاث أنواع (Hijji and Alam,2021: 7154) وكالآتي:

1. اساليب بشرية: هذا هو النوع الأكثر استخدامًا من الهندسة الاجتماعية، حيث يستخدم المهندسون الاجتماعيون تقنيات نفسية لإقناع المستخدم المستهدف بأساليب مثل بناء علاقة معه، والتصيد المباشر، والطعم، والهندسة الاجتماعية العكسية، والأساليب الاجتماعية الأكثر استخدامًا للهجمات الإلكترونية هي التصيد الاحتيالي، الرسائل القصيرة، والتصيد عبر رسائل البريد الإلكتروني والنصوص والمكالمات الهاتفية.
2. اساليب تقنية: عادة ما يتم تنفيذ النوع التقني عبر الإنترنت، حيث تعد مواقع التواصل الاجتماعي مصادر معلومات معتبرة. وكثيرًا ما يستخدم المهندسون الاجتماعيون محركات البحث لجمع المعلومات ذات الصلة بالضحايا. يخمن المتسللون أو يحاولون اختراق كلمات المرور لجمع معلومات مهمة حول المستخدم المستهدف. في المقابل، يستخدم المتسللون ومجرمو الإنترنت أدوات آلية أيضًا، مثل (Mate go و-Social SET) (Engineer Toolkit) للهجمات الإلكترونية الناجحة.
3. اساليب بشرية – تقنية: هي أقوى تقنيات الهندسة الاجتماعية، حيث تجمع بين النوعين البشري والتقني. اذ يأخذ المهندس الاجتماعي بعين الاعتبار عوامل معينة مثل الثقافة الاجتماعية للضحية، والسلوك البشري، والتقنيات المستخدمة، وبناء البنية التحتية، فضلاً عن الأهداف والقيم، فالجمع بين كل من الأساليب الاجتماعية والتقنية يزيد من فرص نجاح الهجمات الإلكترونية للهندسة الاجتماعية.

وتختلف الطرق التي يتبعها المهندسون الاجتماعيون في الوصول لمرادهم حيث يتم اتباع طرق الهندسة الاجتماعية واهمها:

1. **استخدام الهاتف في الخداع:** 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 (الكندي والبلوشي، 2020: 75).

2. **أسلوب التصيد الاحتيالي:** هو هجوم هندسة اجتماعية معروف له أساليب وتقنيات مختلفة يستخدمها المهاجمون لاستهداف الضحايا غير المرتابين وغير المدركين، وقد بدأت هجمات التصيد في الأصل على منصات البريد الإلكتروني ولكنها انتشرت منذ ذلك الحين إلى مواقع الشبكات الاجتماعية، والرسائل الصوتية، والرسائل النصية القصيرة، والألعاب متعددة اللاعبين، وحتى الرسائل الفورية. (Kalio,2022:1) ويتم عن طريق هجوم التصيد على عناوين الأفراد عن طريق خداعهم بمواقع ويب (URL) مزيفة يقع فيها الضحية فريسة لهؤلاء المتسللين، فيعطي معلوماته الحساسة مثل حساب البريد الإلكتروني وغير ذلك من المعلومات الحساسة المعلومات المتعلقة بتفاصيل بطاقة الائتمان والمعلومات السرية التي قد تؤثر على سمعة الفرد أو المؤسسة، وقد ساهمت قنوات الاتصال المختلفة مثل البريد الإلكتروني ووسائل التواصل الاجتماعي والمنتديات في تسريع توزيع عناوين URL للتصيد الاحتيالي، ومن امثلتها، البرامج الضارة / أحصنة طروادة، مع العلم ان أدوات الأمان غير قادرة على ردع مثل هذه الهجمات لأنها تستهدف المستخدمين النهائيين بدلاً من الأنظمة (Abutaha, *et al.*, 2021: 147).

كما يستخدم المهندس الاجتماعي عدة طرق ليتمكن من خلالها اختراق الحسابات الشخصية في وسائل التواصل الاجتماعي، ويمكن تحديدها فيما يأتي (محمد، 2018: 110):

1. صفحات تسجيل الدخول المزيفة (Phishing Attacks)
2. تطبيقات الطرف الثالث المستخدمة في حساباتنا (Third party Applications)
3. تخمين كلمة المرور (Brute force attacks)
4. تخمين اجابات لاستعادة كلمة المرور.
5. كلمات المرور المسجلة على المتصفح.

ثانياً: وسائل التواصل الاجتماعي

تعد مواقع التواصل الاجتماعي من أهم تطبيقات الإنترنت في السنوات الاخيرة, فقد خلقت مجتمعات إفتراضية تنطوي على أنماط من التفاعل والسلوك, واجتذبت ملايين المستخدمين من مختلف الأماكن والأعمار، حيث عبرت عن عملية نقل وتبادل المعلومات والأفكار والمهارات والقيم والميول من فرد إلى آخر, أو من فرد إلى مجموعة من الأفراد, أو من مجموعة من الأفراد إلى مجموعة أخرى, أو من آلة إلى أخرى عن طريق وسيلة أو أكثر من وسائل الاتصال وبهدف توجيه أو تعديل أو تغيير سلوك الآخرين نحو اتجاهات معينة (زين العابدين واخرون، 2018: 6).

وفيما يأتي تعريف بوسائل التواصل الاجتماعي واهميتها في المجتمعات.

1: ماهية مواقع التواصل الاجتماعي:

مواقع التواصل الاجتماعي هي مواقع إلكترونية اجتماعية على إلانترنت وتعتبر الركيزة الاساسية للإعلام الجديد أو البديل، التي تتيح للافراد والجماعات التواصل فيما بينهم عبر الفضاء الافتراضي (يونس، 2016: 11).

يمكن تعريف وسائل التواصل الاجتماعي على أنها استخدام وسائط المحادثة بالاعتماد على الويب (التطبيقات التي تتيح إنشاء المحتوى ونقله في شكل كلمات وصور ومقاطع فيديو وتسجيلات صوتية) بين مجتمعات الأشخاص الذين يجتمعون عبر الإنترنت لمشاركة المعلومات والمعرفة والآراء (Koch, *et al.*,2018:2).

تتركز خدمة مواقع التواصل الاجتماعي في بناء وتعزيز الشبكات الاجتماعية لتبادل الاتصال بين الناس الذين تجمعهم نفس الاهتمامات والانشطة، او من يهتمون باكتشاف ميول وانشطة الآخرين، هذه الخدمات تعتمد بالمقام الأول توفير مجموعة متنوعة من الطرق للتفاعل بين المستخدمين مثل: المحادثات، الرسائل، البريد الفيديو، تبادل الملفات المدونات المناقشات الجماعية (الدليمي، 2020: 139).

والميزة الهامة لمواقع التواصل الاجتماعي انها تعمل على ربط عدد كبير من المستخدمين من شتى أرجاء العالم ومشاركتهم وتشبيكهم في موقع إلكتروني معا مباشرة ويتبادلون الأفكار والمعلومات ويناقشون قضايا لها أهمية مشتركة بينهم (بوبعاية،2016: 56).

و يستدرك البعض بأن مواقع التواصل الاجتماعي هي خدمات عبر شبكة الأنترنيت تسمح للأفراد بـ (توتاوي، 2015:67):

- بناء شخصية عامة أو شبه عامة من خلال نظام محدد.
- توضيح لائحة خاصة بالمستخدمين الذين يشاركونهم الاتصال.
- عرض واجتياز قائمة الاتصالات الخاصة بهم والقوائم الخاصة بآخرين خلال نفس النظام.

وهناك عدة تسميات تطلق على مواقع التواصل الاجتماعي (الشبكات الرقمية الاجتماعية، الشبكات الاجتماعية، وسائل الاعلام الاجتماعية، مواقع الشبكات الاجتماعية) وتسمى ايضاً مواقع التشبيك الاجتماعي، وهي المواقع التي تقوم على انشاء شبكات اجتماعية من مترددين عليها من أنحاء العالم، ويطلق عليها (social networking sites)، وتعتمد تلك الواقع على الاستفادة من تفاعلية شبكة الانترنت كوسيلة اتصال، اذ تسمح لأعضائها ان يقدموا أنفسهم، ويعبروا عن آرائهم وافكارهم للآخرين (الدليمي، 2020: 131).

فالشبكة هي بنية اجتماعية ديناميكية مُشكَّلة من قمم وأطراف، فالقمم تشير إلى أشخاص أو منظمات، وهي مرتبطة ببعضها من خلال تفاعلات اجتماعية، وبعد تشكل الجماعة الإلكترونية عبر الإنترنت، تأخذ بالبحث عن بعضها البعض عبر فضاءات مستقلة خاصة بهم (ألعاب– تسلية – مجال مهني – فضاءات أخرى)، حيث يحس الفرد بأنه مركز اهتمام الجماعة، وهذا ما يسمى بالفردانية الرقمية في الشبكة، التي تولد شعورا بالألفة أو الأنسة الاجتماعية (قواسمية، 2016: 26).

2: تطور مواقع التواصل الاجتماعي

أدى ظهور (الويب) إلى تغيير عالم وسائل التواصل الاجتماعي من خلال الاستخدام عبر الإنترنت للاتصال ومشاركة المعلومات والآراء الشخصية للآخرين، وتعدى الامر حتى الأعمال التجارية تمكنت أيضًا من التواصل وتعريف وتحسين منتجاتها وخدماتها من خلال الاتصال عبر وسائل التواصل الاجتماعي (Drus and Khalid,2019: 708).

كانت بداية التسعينات الفترة التي شهدت اهم تطور في تاريخ الانترنت حيث بدأت خدمة البحث بواسطة WWW(World Wide Web) التي أخترعها "Tim 1990 Berners- Lee"

بأعتماده على النص الفائق Hypertext. مما أدى الى تطوير الشبكة العالمية. كما أن (تيم) مبتكر الويب هو أول من كتب مزوداً للويب، كما أنه وضع اسس اول برنامج مستقل لتصفح الانترنت، حيث اطلق على "الانترنت" هذا الاسم في منتصف عام 1991. ومن ثم توفرت امكانية نقل الصور عالية الجودة والصوت عام 1993 من خلال مسارات اتصال فائقة السرعة. وفي عام 1994 بدأ الاستخدام الشخصي للانترنت بشكل اوسع حيث وصل عدد المراكز المربطة بالشبكة الى ثلاثة ملايين مركز حيث اصبحت الصحافة جزءاً من تطور شبكة الانترنت. ويعتبر عام 1995 انفجار الشبكة العنكبوتية الدولية حيث فرض نفسها كأدات اعلام واتصال بخاصة مع ظهور الصحف الالكترونية، حيث أصبحت هذه الشبكة تعد من أدوات الاتصال الجماهيري (الرحباني، 2012: 136).

ويمكن ارجاع شبكات التواصل الاجتماعي إلى عمر الويب، فمنذ اختراع صفحات الويب الخاصة بشبكة المعلومات، بدأت الافكار تتجه نحو ربط الأفراد من خلال تجمعات افتراضية الكترونية، بدأت بمواقع ضعيفة وتجارب اولية لم يكتب لها النجاح، وقد يرجع ذلك إلى ضعف امكانيات شبكة الويب في حينها، وعدم تمتعها بميزات تفاعلية مثل الدردشة الفورية، المحادثات الصوتية والفيديوية، الا انه في عام 1995 ظهر اول موقع لطلاب المدارس الأمريكية عمل على رفع مستوى التفاعل بين زملاء الدراسة، وهو موقع (class mate.com) وهذا الموقع قسم المجتمع الأمريكي إلى ولايات وقسم كل ولاية إلى مناطق، وقسم كل منطقة إلى عدة مدارس، وجميعها تشترك في هذا الموقع، ويمكن للفرد البحث في هذا التقسيم حول المدرسة التي ينتسب اليها، ويجد زملائه ويتعرف على اصدقاء جدد، ويتعامل معهم عبر هذه الشبكة (الدليمي، 2020: 128).

وعلى الرغم من توفير تلك المواقع لخدمات مشابهة لما توجد في الشبكات الاجتماعية الحالية إلا أن تلك المواقع لم تستطع أن تدر ربحا لمالكيها وتم إغلاقها، وبعد ذلك ظهرت مجموعة من الشبكات الاجتماعية التي لم تستطع أن تحقق النجاح الكبير بين الاعوام 1999 و2001 وفي السنوات اللاحقة ظهرت بعض المحاولات الاخرى، لكن الميلاد الفعلي للشبكات الاجتماعية كما نعرفها اليوم كان سنة 2002.فمع بداية العام ظهرت friend-star، في كاليفورنيا وفي النصف الثاني من العام نفسه، ظهرت في فرنسا شبكة sky-rock كمنصة للتدوين (عوض، 2014: 20).

ومن خلال تقنيات نظم الاتصال, وهندسة التحكم التلقائي, ظهرت نظم جديدة مثل البريد الالكتروني وشبكات الفيديو والتعليم عن بعد وتعلم اللغة وغيرها, وهذه بدأت تؤثر على العالم, في مختلف المجالات إبتداءاً من قطاع المعلومات والثقافة واللغة والتعليم والترفيه, والابعاد الاجتماعية المختلفة, لذا فهذه التقنية تفرض على الناس مفاهيم وقيم وأساليب جديدة في أنظمة العمل والمعرفة والفلسفة والتعاملات السلوكية والانسانية, مع أن نظم الإحصاء لا زالت عاجزة عن توفير معطيات أساسية لمعرفة آثار هذه التقنية وبناء نماذج يمكن الاعتماد عليها في تحسين المتغيرات المستقبلية (العصيمي،2014: 90).

لقد كانت النقلة الكبرى في عالم شبكات التواصل الاجتماعي، بانطلاق موقع التواصل الاجتماعي الشهير فيس بوك Facebook.com، والذي انطلق رسمياً في 4/ شباط/ 2004، وقد بدأ هذا الموقع بالانتشار الموازي مع شبكات التواصل الاخرى على الساحة، فطور خدماته فيما بعد، اذ أتاح عام 2007 تكوين التطبيقات للمطورين مما ادى الى زيادة أعداد مستخدميه بشكل كبير حتى تربع على عرش مواقع التواصل الاجتماعي، بل ومواقع الانترنت بصفة عامة على مستوى العالم (الدليمي، 2020: 130).

وتسمح مواقع التواصل الاجتماعي لمستخدميها حالياً بانشاء صفحات ومساحات خاصة ضمن الموقع نفسه ومن ثم تتيح التواصل مع الأصدقاء ونشر المحتويات والاتصالات، وتتمثل اهم المواقع الاجتماعية في المدونات والمنتديات بجانب مواقع عديدة مثل Wiki، Facebook، Twitter، والتطبيقات التي قدمتها الشركات الكبرى لدعم الفكر الاجتماعي في التفكير والمشاركة مع مستخدمي مواقعها مثل جوجل وياهو التي اهتمت بالتحرير الجمعي والكتابة وتنفيذ العروض المشتركة، وكذلك مواقع Ajax في مجالات التطبيقات المكتبية التي تتم بشكل تعاوني وأيضا شبكات التفاعل الاجتماعي مثل My-space ومواقع خدمات وتخزين الصور وإعادة عرضها وارسالها للغير مثل Flicker، ونشر مقاطع الفديو مثل YouTube وغيرها من الخدمات والتقنيات التي تجد اهتماما فرديا مع تبادل المشاركة والنشر بين المستخدمين (صباح والشجيري، 2018: 246).

تشير مجموعة كبيرة من الأبحاث السابقة إلى أنه من بين منصات التواصل الاجتماعي المختلفة، يتم استخدام Facebook وLinkedIn وTwitter بشكل أساسي في عملية تحديد المصادر، ويمكن تصنيف Facebook كأدوات للتواصل الاجتماعي، بمعنى آخر،

أدوات تسمح للمستخدمين بمشاركة المعلومات عن أنفسهم، من خلال ملف تعريف عبر الإنترنت قاموا بإنشائه بأنفسهم،بينما يقع Twitter ضمن فئة فرعية من المدونات الصغيرة تتيح للمستخدمين توصيل رسالة في أقل من 140 حرفًا. وقد اظهرت مواقع التواصل الاجتماعي والمدونات الصغيرة نموًا هائلاً على مدار السنوات القليلة الماضية، حيث شهد Facebook ما معدله 1.32 مليار مستخدم نشط يوميًا في يونيو 2019 (Koch, *et al.*,2018:2).

أن تصميم الشبكات الاجتماعية وطبيعتها اللامنتهية، بالإضافة إلى ذلك تنوع استخداماتها سيجعل منها حتماً معيار مهم سيغير معالم الإنترنت وطريقة تعامل الناس معه. كما ان وجود ملايين المستخدمين يقومون بالتسجيل بأسمائهم الصريحة والعناوين، إضافة لمعلومات شخصية ومعلومات احترافية عن تخصصاتهم الدقيقة تجعل من الشبكات الاجتماعية المكان الأول المناسب للبحث عن الأشخاص والقدرة على بدء التواصل معهم (توتاوي، 2015: 88).

ويمكن تحديد أهم مواقع التواصل الاجتماعي كما يلي (فارس، 2016: 50):

أ- **الفيسبوك:** هو شبكة اجتماعية تأسست في 2004 على يد شاب عشريني أمريكي اسمه مارك زيك بيرج بالتعاون مع اثنين من رفقائه بالسكن الجامعي في جامعة هارفارد وقد كان الموقع في البداية مقصورا على طلبة الجامعة ثم امتد ليشمل طلبة الجامعات الامريكية ثم خرج بعد ذلك إلى أوروبا والعالم، والفيسبوك من أهم وأشهر مواقع التواصل الاجتماعي حيث تمكن للعضو في هذا الموقع أن يقوم بإعداد نبذة شخصية عن حياته تكون بمثابة بطاقة هوية وتعارف لمن يريد أن يتعرف عليه ويتواصل معه، ويستطيع كل عضو فيه أن يقف على آخر أخبار أصدقاءه عن طريق ما يعرضه حائط العضو من رسائل أو نبذ من الاخبار لابلاغ أصدقائه بإخباره واجتماعاته وأي صور آو مقاطع فيديو أو قطع موسيقية يرغب في اطلاعهم عليها.

ب- **تويتر:** ظهر موقع التويتر عام 2006 كمشروع بحثي قامت به شركة obvians الأمريكية ثم أطلق رسميا للمستخدمين في نفس العام.وهو موقع من مواقع التواصل الاجتماعي يقدم خدمة تدوين مصغر وهو تدوين يسمح بعدد محدود

من المدخلات بحد أقصى مائة وأربعين حرفا فقط للرسالة الواحدة ويمكن إرسالها مباشرة من التويتر على شكل رسائل SMS وهي رسائل نصية مختصة ترسل عن طريق الهاتف النقال، وبالتالي فهو موقع يسمح بنشر خبر او فكرة بسرعة وسهولة وتركيز على طريقة خير الكلام ما قل ودل.

ج- **يوتيوب:** تقوم فكرة الموقع الذي تأسس عام 2005 على إمكانية إتاحة خدمة التبادل لملفات الفيديو التي تسمح للمستخدمين لتحميل الملفات المتوفرة على الانترنت ويستطيع أي شخص في الوقت نفسه أن ينشر ما يريد، واضافة إلى خدمة النشر التي يتيحها هذا الموقع فانه يسمح للمستخدم بإعادة نشر ما نشره الاصدقاء ومن أكثر الجوانب التي كان للموقع اثر كبير وواضح فيها الاجتماعية والفنية حيث أصبح الكثير ممن يبحثون عن الشهرة يتجمعون لليوتيوب باعتباره الوسيلة العالمية الوحيدة التي تتيح الى اي كان الظهور وتمنحه الفرصة للوصول إلى الملايين.

د- **انستغرام:** هو برنامج يستخدم لمشاركة الصور عبر البرنامج ومواقع التواصل الاجتماعي)فيس بوك، تويتر، (..ومايميزه أنه يتيح خاصية الهاشتاق وتخصص لكل مناسبة هاشتاق لتنشر فيه الصور ليراها الأصدقاء أو المهتمين في نفس المجال، بالإضافة لإمكانية التعديل على الصور واضافة تأثيرات عليها.

4: اهمية مواقع التواصل الاجتماعي

مع إشارة التقديرات الى زيادة عدد مستخدمي وسائل التواصل الاجتماعي كل يوم وانه في عام 2019 هناك ما يصل إلى 2.77 مليار مستخدم لوسائل التواصل الاجتماعي في جميع أنحاء العالم (Drus and Khalid,2019: 708)، فان منصات وسائل التواصل الاجتماعي أصبحت وسيلة للتواصل ليس فقط بين الأفراد ولكن أيضًا للعديد من جوانب قطاعات الأعمال، وأنظمة دعم القرار القائمة على المعرفة، وتسويق العلامات التجارية، كما شاركت في نشر المنتجات. وقد استثمرت المؤسسات قوة وسائل التواصل الاجتماعي للوصول إلى الجماهير، كما فائدته كانت مهمة في مختلف مجالات الأعمال والإدارة بما في ذلك التجارة الاجتماعية والحوكمة الإلكترونية والتسويق السياسي والتسويق الرقمي (Arora, *et al.*,2019:2).

ويمكن تحديد اهمية مواقع التواصل الاجتماعي في النقاط الآتية (الدليمي، 2020: 137):

أ- تلعب مواقع التواصل الاجتماعي دورا لا يستهان به في احداث التأثير باتجاهات الشرائح المختلفة في أي مجتمع.

ب- تعد مواقع التواصل الاجتماعي وسيلة اعلامية تتسم بأهمية كبيرة، ويتوقع ان لها مستقبلاً لا يستهان به لإتصافها بصفات ومزايا عدة كالسرعة في نقل الخبر العاجل، اضافة الى الصورة المصاحبة، وفيلم الفيديو المرافق، وغياب مقص الرقيب.

ج- لها دور فعال في التأثير في توقيت صنع القرار، وذلك من خلال خلق الأزمات وافتعالها، وكذلك من خلال طرح الشبهات والأسئلة عن الأعمال ونهايتها المرتقبة وتداعياتها.

د- ان اغلب التغييرات الحاصلة تظهر مدى أهمية مواقع التواصل الاجتماعي، والدور المنوط بها، ونشر ثقافة التعاطي مع مواقع التواصل لمختلف الشرائح المجتمع.

هـ- وهناك أدواراً حيوية لمواقع التواصل الاجتماعي في حياة الشباب خاصة في المجالات الفكرية والثقافية والسياسية، اذ تمكنهم من الاسهام في الأنشطة الفكرية والسياسية والاجتماعية.

و- لغة العصر وجزء من التطور العقلي والنفسي والتقني للعصر الذي تعيش فيه، وبالتالي فإن التعالي بلغة العصر ضرورة لاستمرار الحياة.

ز- اصبحت حقيقة واقعة يزورها الجميع للاطلاع على ما تنشره من موضوعات واخبار تهم الجمهور، كما فتحت الآفاق أمام الفرد للكتابة بكل الموضوعات التي تجول بخاطره.

ح- تتيح العديد من المواقع امكانية البحث عن عمل لمن يرغب ضمن مجال اهتمامه وتخصصه، اذ تبحث الكثير من الشركات والمؤسسات عن موظفين مؤهلين عبر هذه الشبكات، اذ تتم هذه العملية بسرعة وجهد قليل وقد خصصت الشبكات مجملها لهذا الغرض كموقع لينكدان.

ط- وتشجع الافراد خاصة الشباب على المشاركة في الأعمال الخيرية والحملات التطوعية.

5: خصائص مواقع التواصل الاجتماعي

بالإضافة الى الأنواع المختلفة من المعلومات التي يتم تحميلها ومشاركتها على وسائل التواصل الاجتماعي في شكل نصوص ومقاطع فيديو وصور وصوت، فان وسائل التواصل الاجتماعي الغنية بالبيانات الأولية وغير المعالجة، ستسمح التحسينات في التكنولوجيا وخصوصاً في التعلم الآلي والذكاء الاصطناعي، بمعالجة تلك البيانات وتحويلها إلى بيانات مفيدة يمكن أن تفيد معظم مؤسسات الأعمال (Drus and Khalid,2019: 708).

وفضلاً عن ذلك فقد تميزت مواقع التواصل الاجتماعي بمجموعة من الخصائص والتي يمكنها في حال توافرها من تحقيق أهدافها المختلفة, ومن تلك الخصائص ما يلي (توتاوي، 2015:81):

أ- العالمية:حيث تلغى الحواجز الجغرافية والمكانية، وتتحطم فيها الحدود الدولية، ويستطيع الفرد في الشرق التواصل مع الفرد في الغرب، في بساطة وسهولة.

ب- التفاعلية: فالفرد فيها كما أنه مستقبل وقارئ، فهو مرسل وكاتب ومشارك، فهي تلغي السلبية المقيتة في الإعلام القديم – التلفاز والصحف الورقية – وتعطي حيز للمشاركة الفاعلة من المشاهد والقارئ..

ج- التنوع وتعدد الاستعمالات: فيستخدمها الطالب للتعلم، والعالم لبث علمه وتعلمي الناس، والكاتب للتواصل مع القراء.

د- سهولة الاستخدام: فالشبكات الاجتماعية تستخدم بالإضافة للحروف وبساطة اللغة، تستخدم الرموز والصور التي تسهل للمستخدم التفاعل.

هـ- التوفير والاقتصادية: اقتصادية في الجهد والوقت والمال، في ظل مجانية الاشتراك والتسجيل، فالفرد البسيط يستطيع امتلاك حيز على الشبكة للتواصل الاجتماعي.

المبحث الثالث: دور أساليب الهندسة الاجتماعية في وسائل التواصل الاجتماعي وتاثيرها على امن المعلومات

يعد الأمن الرقمي للمواطن أحد ركائز المواطنة الرقمية حيث نجد حماية المواطن الرقمي من أهم الأولويات للأمن الوطني للمواطن ويتجلى هذا من خلال الاجراءات الوقائية والحماية الالكترونية وقوانين مكافحة الجرائم المعلوماتية، وخاصة مع انتشار ظاهرة "الهندسة الاجتماعية" او ما يعرف بـاختراق العقول، من خلال اقتحام شبكة ما أو نظام تشغيلي ما نتيجة خطأ بشري (محمد، 2018: 110).

ويمكن عرض مخاطر أساليب الهندسة الاجتماعية على امن المعلومات في وسائل التواصل الاجتماعي ومقترحات للحد من تاثيراتها فيما يأتي:

1: مخاطر أساليب الهندسة الاجتماعية على امن المعلومات في وسائل التواصل الاجتماعي

ان كل ثانية من الوقت تمر بملايين الأشخاص الذين يتفاعلون على وسائل التواصل الاجتماعي، يخلق كميات هائلة من البيانات التي تحتوي على العديد من الأنماط غير المرئية مصحوبة بالاتجاهات السلوكية، وباتت البيانات التي يتم نشرها على الويب ووسائل التواصل الاجتماعي ومنتديات المناقشة موضوعًا هائلاً لاهتمام التحليلات وكذلك النقاد لأنها تعكس السلوك الاجتماعي والاختيارات والتصورات وتفكير الناس (Meel and Vishwakarma,2020: 1).

في ظل هذه البيئة تتمثل مخاطر الهندسة الاجتماعية في وسائل التواصل الاجتماعي من ضخامة حجم المعلومات المنشورة على وسائل التواصل الاجتماعي ونطاقها، مما يجعل هذه المنصّات مكاناً محفوفاً بالتحديّات ومثالياً على حدّ سواء لجمع المعلومات فعلى سبيل المثال، ينشر مُستَخدمو تويتر وحدهم500 مليون تغريدة كل يوم وينشر المُستَخدِمون الصور ومقاطع الفيديو وتحديثات بشأن الحالة على وسائل التواصل الاجتماعي وغالباً ما تشمل ملفاتهم الشخصية تفاصيل شخصية مثل عمرهم، وجنسهم، وأفراد عائلتهم ومكان

عملهم، وتوفّر هذه المنشورات رؤية حول حياة الأفراد اليوميّة، بالإضافة إلى المواقف والسلوكيّات المرتبطة بالشبكات الاجتماعية (مارسيلينو واخرون، 2017: 11).

وقد لفتت العديد من الحالات البارزة لهجمات الهندسة الاجتماعية انتباه خبراء أمن تكنولوجيا المعلومات والمعلقين السياسيين مؤخرًا، فعلى سبيل المثال، في عام 2020، استهدف المتسللون منصة التواصل الاجتماعي Twitter، بما في ذلك حسابات المشاهير مثل بيل جيتس وإيلون موسك وكاني ويست بالإضافة إلى الملفات الشخصية العامة للرئيس الأمريكي السابق باراك أوباما ثم المرشح الديمقراطي جو بايدن لانتخابات الرئاسة الامريكية في حينها، واستخدم المتسللون وصولهم المؤقت لطلب مدفوعات العملة المشفرة من متابعي الحسابات المخترقة، وأوضح مسؤولو تويتر أنه لم تكن الشبكة هي التي استهدفها المتسللون ولكنهم "ضللوا موظفين معينين" و"استغلوا نقاط الضعف البشرية"، وقد كشفت هذه الحادثة عن احتمال واسع لهجمات الهندسة الاجتماعية، حيث استخدم المتسللون دعم عملاء الشركة للوصول إلى تلك الحسابات – وليس بابًا خلفيًا تقنيًا في برنامج خدمة الويب (Witjesa and Wentland, 2021: 1318)

من ناحية أخرى؛ فقد تسمح المواقع غير المحمية باستغلال الإعلانات المزيفة في ظل ظروف تشغل الرأي العام (على سبيل المثال جائحة كورونا (COVID-19))، والتي تقود الضحية إلى موقع ويب للتصيد الاحتيالي، حيث يلعب قلة وعي الأفراد بأمن المعلومات دورًا رئيسيًا في زيادة عدد ضحايا هذه الجريمة والتي تبدأ عندما ينسخ المهاجم محتوى أو تصميم صفحة من مواقع شرعية ثم يعيد بناء صفحة ويب الاحتيال. بمجرد أن يصبح المخادع جاهزًا، يرسل عنوان URL إلى الضحية، ليغريه لملء صفحة الويب الاحتيالية بمعلومات سرية، ليسرق المخادع معلومات الضحية للوصول إلى الموقع الأصلي (Abutaha, *et al* ,2021: 147).

ان طبيعة خدمات الويب والإنترنت التي يستخدمها اليوم الملايين من الافراد في انحاء العالم تمهد الطريق للهجمات الهندسية الاجتماعية المتطورة، وخاصة في ظل توجه الموظفين لاستخدام أجهزتهم الخاصة بما فيها الهواتف الذكية في بيئة العمل، فضلاً عن استخدام أدوات الاتصال والتعاون عبر الإنترنت فاستخدام شبكات التواصل الاجتماعي قد يؤدي لإنشاء نواقل هجوم جديدة لهجمات الهندسة الاجتماعية، فقد أظهرت

الهجمات الأخيرة على شركات مثل New York Times and RSA أن هجمات التصيد الاحتيالي المستهدفة هي خطوة تطورية فعالة لهجمات الهندسة الاجتماعية (الكندي والبلوشي، 2020: 75).

ينقل التصيد الاحتيالي الرسائل بقصد جعل الضحايا المحتملين ينفذون إجراءات معينة (مثل النقر على الارتباطات التشعبية غير الفعالة، أو فتح أو تنزيل مرفقات البرامج الضارة المضمنة، أو إدخال تفاصيل تسجيل الدخول في نسخ مستنسخة على صفحات الويب، التي قد تؤدي بالضحية إلى إفشاء معلومات سرية قد يستخدمها المهاجم، وافترض الباحثون ان معظم هجمات التصيد الاحتيالي تستخدم تقنيات اجتماعية أكثر من كونها تقنية بطبيعتها ومن شأنها أن تنقل إحساسًا بالإلحاح لجذب انتباه الضحية المحتملة (Kalio,2022:2).

ان تقنيات الهندسة الاجتماعية التي تستخدم بالأساس أساليب وحيل متعددة ومقربة لطبيعة النفس البشرية تمكن مستخدموها الحصول على المعلومات من المشاركين فيها، وبالتالي فأن أفضل مكان لذلك هو الفيس بوك؛ بصفته موقع التواصل الاجتماعي الأكثر من حيث عدد المشاركين فيه ومن حيث التفاعل فأكثر من 2 مليار مستخدم نشط للفيس بوك هو عدد ضخم من البشر من الصعب أن يجتمع في مكان واحد في الواقع المعاش، وبالتالي فبيئة العمل الخاص بفيس بوك، وخصائصه الفنية والتقنية تسمح بشكل أو بآخر للمشاركين أن يقعوا فريسة لتقنيات الهندسة الاجتماعية، حيث إن كثيرًا من المستخدمين يمكنهم التعرف على تطبيقات واختبارات التنبؤ المهندسة، من خلال (فيس بوك)، وبالتالي فالسماح بنشر نتائج المشاركات التي يجريها الجمهور ويشارك فيها من خلال تقنيات الهندسة الاجتماعية سواء أكانت تطبيقات أم اختبارات، عبر الموقع بدون عوائق أو تحقق تساعد بشكل أكبر في انتشار مثل هذه التقنيات (عبدالحي، 2020: 603).

وقد 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 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 (الكندي والبلوشي، 2020: 73).

ولعل اخطر عمليات الهندسة الاجتماعية هي عمليات التنظيمات الإرهابية التي وجدت ضالتها المنشودة في شبكات التواصل الاجتماعي واعطت الأولوية لها، وجندت عناصرها للتركيز على هذه الساحة الجديدة للصراع، وقد وفرت شبكات التواصل الاجتماعي أدوات عدة وساعدت هذه التنظيمات على العمل بشكل ميسر، اذ انها من حيث المبدأ تسمح لاي شخص ان ينتحل أي مسمى او اي صفة، واتاحت الفرصة لانشاء ما يطلق عليه الصفحات بانواعها المختلفة، سواء كانت مجموعات عامة متحه للجميع او مجموعات مغلقة، او مجموعات سري، حيث استفادت التنظيمات الإرهابية من هذه التقنيات والصفحات للترويج لافكارها والتواصل مع مؤيديها او من تسعى لاجتذابهم، فضلا عن تقنية المجموعات السرية لخلق بيئة افتراضية امنة للتواصل مع اشخاص افتراضيين ربما يكونون في بلاد مختلفة والايقاع بهم (عبدالوهاب وخلف، 2020: 8).

كما يشكل المساس بخصوصيات حياة الافراد نتيجة عمليات الهندسة الاجتماعية تهديداً جسيماً لخصوصيات واسرار حياة الافراد الشخصية وتعتبر من القضايا الخطرة التي تهدد النسيج الاجتماعي ليس على مستوى الافراد فحسب وانما على مستوى المجتمع ككل لأنها اودت بحياة الكثير من النساء اما بقتلهن من قبل الاهالي او لجوئهن الى الانتحار نتيجة انتشار البيانات الخاصة بهن وكثرة حالات الطلاق بسبب ذلك وان العوائل تمتنع في الكثير من الاحيان من اللجوء الى الجهات المختصة خشية من الفضائح ومحاولة حل القضية بنفسها مما يؤدي تحقيق غايات المبتز(المهندس الاجتماعي) في الحصول على الاموال (عبدالرضا والمعموري، 2020: 172).

2: وسائل التحصين الامني من أساليب الهندسة الاجتماعية للافراد والمؤسسات

يمكن لوسائل التحصين الامني ضد أساليب الهندسة الاجتماعية ان تساهم 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. اذ 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 (الكندي والبلوشي، 2020: 73).

و ينصح مسؤولو امن المعلومات بعدد من النصائح التي يجب مراعاتها لتجنب الوقوع ضحية للهندسة الاجتماعية (محمد، 2018: 119):

أ- عدم الوثوق بأي مكالمات هاتفية أو بريد الكتروني من أي شخص يطلب معلومات شخصية أو بنكية ويجب التأكد من هوية هذا الشخص عن طريق الاتصال بالمصدر للتحقق من هوية طالب المعلومات.

ب- تجنب استخدام البطاقة الائتمانية إلا عند الضرورة القصوى واستخدام البطاقات مسبقة الدفع عوضاً عن ذلك.

ج- تجنب وضع المعلومات الشخصية على الإنترنت مثل الاسم واللقب ورقم الجوال أو أي معلومات بنكية.

د- التأكيد على ضرورة أتلاف الأوراق والمستندات المهمة بواسطة اجهزة مخصصة لهذا الغرض.

ه- تجنب كل الرسائل الالكترونية التي تحتوي على روابط مشبوهة في البريد الالكتروني أو رسائل الجوال أو على المواقع الاجتماعية.

كما يمكن التوصل لعدد من طرق الحماية من الهندسة الاجتماعية في المؤسسات وكما يأتي:

أ- **وضع قوانين للحماية الأمنية للمؤسسة:** تقوم المؤسسة بالتوضيح للعاملين فيها قوانين الحماية الأمنية المتبعة والتي على العاملين تطبيقها. وعلى سبيل المثال:

- يقدم الدعم الفني المساعدة ضمن أمور معرفة ومحددة مسبقاً.
- وضع حماية أمنية لاقسام ومبنى المؤسسة: حيث يمنع دخول الأشخاص غير العاملين في المؤسسة.
- تحدد الزيارات في حدود الأعمال بمعرفة سابقة لحراس الأمن في المؤسسة وتحت مراقبة منهم.

ب- **التحكم بالمكالمات الهاتفية:** وذلك بوضع نظام امني للمكالمات مع قدرة على التحكم في من يستطيع مكالمة من حيث يتم:

- منع المكالمات الخاصة وحضر المكالمات الدولية وبعيدة المدى إلا للضرورة وبإذن المسئول عن المكالمات.
- عدم إظهار مدخل للخط الهاتفي للمنظمة لتجنب استخدام الهاتف من قبل شخص خارج المنظمة.

ج- **التعليم والتدريب:** تثقيف الموظفين داخل المنظمة بمجال أمن المعلومات والاختراقات التي من الممكن حصولها.

- تدريب الموظفين في مركز الدعم الفني وتثقيفهم على مستوى جيد من الناحية الأمنية وتوضيح أساليب المهاجمين وتدريسها لهم.
- تدريبهم على عدم إعطاء معلومات ذات سرية عالية إلا بعد التأكد من هوية الشخص ووفقاً للحد المسموح به.
- تدريبهم على كيفية رفض إعطاء المعلومات عند عدم الإمكانية بأسلوب لبق.

د- **إستراتيجية التصرف في المواقف الحرجة:** بأن يكون هناك إستراتيجية محددة تضعها المؤسسة تمكن الموظف من التصرف إذا طلب منه معلومات سرية تحت ضغط ما، فمثلا:

- إتلاف المستندات والأجهزة غير المستخدمة: وضع أجهزة لإتلاف الورق داخل المؤسسة كي لا يمكن استخدام المعلومات التي تحويها سواء كانت معلومات حساسة أو كلمات سر للدخول للنظام ونحو ذلك.
- إتلاف أجهزة الكمبيوتر القديمة كي لا تستعمل باستخراج معلومات سرية منها.

اما على الصعيد الحكومي فتعتبر التشريعات القانونية من الضرورة بمكان لمواكبة التطور الحاصل في مجال الجرائم الالكترونية من خلال المواجهة التشريعية الكافية والتصدي اللازم للتعامل مع هذه الجرائم من خلال إيجاد قواعد قانونية غير تقليدية لازمة لمعالجة الجرائم المعلوماتية وكافية للتعامل معها.

المبحث الثاني: الجانب التطبيقي
(دراسة تطبيقية على عينة من الطلبة الجامعيين)

في هذا المبحث درست تاثيرات أساليب الهندسة الاجتماعية على امن المعلومات في وسائل التواصل الاجتماعي على عينة من الطلبة الجامعيين.

أولا: منهجية الدراسة وإجراءاتها

اعتمدت الدراسة الحالية استخدام المنهج الكمي لتحقيق أهدافها، اذ يعرف المنهج الكمي بأنه تقنية يحكمها ترقيم الظاهرة وحساب الوحدات وتعدد الأشياء الواجب دراستها او وصفها، وتسجيل تكرار حدوث الظاهرة المدروسة، كما يعتمد المنهج الكمي على القياس ومحاولة تحديد الظاهرة كمياً حيث يعتمد في العلوم الإنسانية والاجتماعية في القياس على ترتيب العناصر في نظام ما اعتماداً على معيار صاعد او هابط، اكثر او اقل تاثيرا زيادة في المشاركة او النقص، فيصبح الترقيم الرياضي لمختلف الظواهر عبارة عن وصف رقمي يوضح مقدار هذه الظاهرة او حجمها ودرجة ارتباطها مع الظواهر المختلفة (أزواو، 2021: 357). ويعد استخدام المنهج الكمي في الدراسة الحالية الأفضل كونه يتيح فهم الوضع الحالي كمياً ويشكل فهماً أعمق لمشكلة الدراسة فيما يتعلق بقياس الواقع. وقد تم تحقيق ذلك من خلال استخدام أداة الاستبانة لجمع البيانات واجراء التحليل الاحصائي بعد الحصول على اجابات العينة المبحوثة للتوصل الى النتائج العملية حيث تم توزيع 60 استمارة استبيان على مجتمع الدراسة التطبيقية والمتكون من جميع طلبة كلية الاعلام – جامعة بغداد والبالغ عددهم (1422) طالب وطالبة للعام الدراسي (2021-20-22)، وكانت عينة البحث عشوائية وتتكون من طلاب اقسام الكلية (قسم الصحافة، قسم الصحافة الاذاعية والتلفزيونية، قسم العلاقات العامة) ومن جميع الدرجات (الدكتوراه والماجستير والبكلوريوس)، حيث اقتصرت المرحلة الرابعة من درجة البكلوريوس باعتبارهم الأكثر وعياً بفقرات الاستبيان والاختصاصات وقد تم استرجاع 50 استبانة اعتبرت عينة البحث.

ثانيا: وصف خصائص عينة الدراسة.

أ – الجنس: تظهر النتائج المبينة في الجدول (1) ادناه ان 66% من العينة هم من الذكور و34% من العينة هم من الاناث.

جدول (1) نوع الجنس المشاركين في الاستبيان

نوع الجنس	العدد	النسبة المئوية
ذكور	33	66%
اناث	17	34%
المجموع	50	100

من خلال ملاحظة البيانات الواردة في الجدول(1) نجد ان عدد الذكور اكثر من الاناث اذ بلغ عددهم (33) في حين بلغ عدد الاناث (17).

ب – الدرجة العلمية: تظهر النتائج الموضحة في الجدول (2) الدرجات العلمية لعينة الدراسة.

جدول (2) الدرجات العلمية للمشاركين في الاستبيان

الدرجة العلمية	العدد	النسبة المئوية
بكالوريوس	36	72%
ماجستير	10	20%
دكتوراه	4	8%
المجموع	50	100

يبين الجدول اعلاه بان عدد الطلبة الدارسين في درجة البكالوريوس هم الاكثر في العينة بواقع (36) طالب وطالبة وبنسبة (72%) وهي الاعلى قياسا بالنسبتين الاخريتين حيث ان نسبتهم الأعلى في الكلية، تلتها فئة درجة الماجستيرالتي عددها (10) طلاب وبنسبة (20%) ثم فئة الدكتوراه فكانت بواقع (4) طلبة وبنسبة (8%) من مجموع المبحوثين، أي ان عينة البحث غطت كافة الدرجات العلمية للطلبة للإجابة الدقيقة على فقرات الاستبانة.

ثالثاً: وصف وتحليل إجابات العينة

وصف وتشخيص متغيرات البحث من خلال فقرات الاستبانة التي توزعت في محورين رئيسيين ؛ المحور الأول حول مدى اهتمام الطلبة بامن المعلومات ضمن وسائل التواصل الاجتماعي ليتم التحقق منها، اما المحور الثاني فهو أساليب الهندسة الاجتماعية ليتم التحقق من تاثيرها لدى الطلبة الجامعيين في امن المعلومات لديهم وكما يأتي:

المحور الأول: بُعد امن المعلومات

في هذا المحور يتم تحليل إجابات العينة حول مدى تقيدهم بامن معلوماتهم على وسائل التواصل الاجتماعي من خلال الفقرات المتعلقة بذلك والتي ضمها الجدول (3):

جدول (3) النسب المئوية لاجابات عينة البحث على فقرات بُعد امن المعلومات.

ت	الفقرة	نعم	كلا	الى حد ما
1	أقوم بتغيير إعدادات الخصوصية في ملفي الخاص على مواقع الشبكات الاجتماعية	68%	24%	8%
2	أتيح بياناتي الشخصية على مواقع الشبكات الاجتماعية	22%	64%	14%
3	أشارك الآخرين على مواقع التواصل الاجتماعي معلومات عن الأسرة والأصدقاء	23%	59%	18%
4	أقوم بحذف ملفات الكوكيز من المواقع التي أقوم بزيارتها	46%	34%	20%
5	أقوم بحجب الإعلانات والدعايا التي تأتيني في البريد العشوائي	60%	27%	14%
6	أقوم بالرد على رسائل البريد الإلكتروني لأفراد لا أعرفهم	26%	56%	18%
7	أقوم بالرد على رسائل البريد الإلكتروني التي تحتوي على تعليمات لتحسين خدمة البريد الكتروني مع طلب للرقم السري.	25%	59%	16%
8	أقوم بإعطاء رقمي السري في حالة طلب مني أحد ذلك لانجاز اعمال تخصني	21%	60%	19%
9	أقوم بتمكين وتثبيت جدران الحماية في جهاز الحاسب الآلي الخاص بي	61%	28%	11%
10	أقوم بتحديث برامج ذد الفايروسات على جهازي الخاص	60%	29%	11%

تبين إجابات عينة البحث عن فقرات امن المعلومات ان النسبة الأعلى للطلبة الجامعيين في كلية الاعلام في جامعة بغداد متيقنون لامن معلوماتهم وانهم يقومون بما يجب للمحافظة على امن معلوماتهم، ومع ذلك فان نسب ليست قليلة منهم لايعيرون اهتماماً لذلك وهم بذلك يعرضون انفسم لمشاكل التواصل الاجتماعي ومنها أساليب الهندسة الاجتماعية.

المحور الثاني: أساليب الهندسة الاجتماعية

تضمن هذا المحورثلاثة أساليب يستخدمها مهندسو الهندسة الاجتماعية وهي (أساليب بشرية، أساليب تقتية، أساليب تقنية بشرية) وقد تكونت استبانة الدراسة خمس فقرات لكل أسلوب وأحصيت اعداد الإجابات فيها وحللت بياناتها كما يلي:

أ: **اساليب بشرية:** يتضمن الإجابة على فقرات استمارة الاستبانة من قبل عينة البحث وتحليل بياناتها وهذه النتائج موضحة في الجداول (4-8) وكما يلي:

جدول (4) يبين عدم التردد في اعطاء الطالب بياناته الخاصة عند تلقيه عرض مغري

عندما اتلقى اتصال تلفوني لابلاغي بان شركة الاتصالات ادخلتني في قرعة للفوز بعرض مغري فاني لا اتردد باعطاء بيانات خاصة عني	العدد	النسبة المئوية
نعم	35	70%
كلا	5	10%
الى حد ما	10	20%
المجموع	50	100

قد يحصل المهندس الاجتماعي على الرقم الخاص من مواقع التواصل الاجتماعي بسبب نشره من المشارك في تلك المواقع، وينجح المهنسون الاجتماعيون من خلال طريقة كلام خاصة بموظفي شركة الاتصالات التي يشترك بها الطالب بالتاثير عليه، ويلاحظ من خلال البيانات الواردة في الجدول (4) ان هناك نسبة عالية من الطلبة من خلال الشعور بالراحة والثقة في حال تلقيهم هكذا اتصالات تلفونية فانهم يُسلمون فوراً ان الشخص على الطرف الآخر من شركة الاتصالات فعلًا فيعطونه بيانات خاصة عنهم قد يستخدمها

المهندس الاجتماعي في غايات خبيثة، فقد بلغ عدد هؤلاء الطلبة (35) طالب وطالبة وبنسبة (70%) وهذا يعني ان تاثير طريقة الكلام (وهو أسلوب مهم يتبعه المهندس الاجتماعي) على الطلبة الجامعيين كبيرة في خداعهم وتضليلهم وسرعة انقيادهم للمهندس الاجتماعي، اما عدد الذين اجابوا بـ (الى حد ما) فبلغ عددهم (10) طلاب وبنسبة (20%)، وهذا يوحي بان هذه النسبة تتردد في إعطاء البيانات لشعورهم باهميتها ولكن الضغط النفسي الذي يقعون به من قبل المهندس الاجتماعي قد يجعلهم الى حد ما ينقادون اليه ويعطونه بياناتهم مما يبين ان هذه النسبة تتاثر ايضاً باساليب المهندس الاجتماعي لكنهم يترددون في ذلك وهم نسبة قلقة، اما الذين اجابوا بـ (كلا) فبلغ عددهم (5) طلاب وبنسبة (10%) وهم فقط الذين يشعرون بخطورة القائم على الاتصال ويتجنبون اعطاءه بيانات خاصة مما يعكس عدم تاثرهم باساليب الهندسة الاجتماعية.

جدول (5) يبين مدى تحري الطالب عن هوية الشخص الذي يتواصل معه على مواقع التواصل الاجتماعي

لا ارغب بالتحري عن هوية الشخص الذي أتواصل معه على مواقع التواصل الاجتماعي	العدد	النسبة المئوية
نعم	38	76%
كلا	4	8%
الى حد ما	8	16%
المجموع	50	100

ان المهندس الاجتماعي قد يتواصل مع الضحية لفترة طويلة قبل ان يتم التوصل الى غاياته الخبيثة وخلال هذه الفترة يحرص المهندس الاجتماعي على بناء علاقة ثقة واحترام فلا يهتم الضحية بالتحري عن الطرف الآخر مما يوقعه في مصائد الاحتيال والخداع، ومن خلال ملاحظة البيانات الورادة في الجدول (5) يتبين مدى تحري الطالب عن هوية الشخص الذي يتواصل معه على مواقع التواصل الاجتماعي، فنجد ان الذين اجابوا بـ (نعم) بلغ عددهم (38) طالب وطالبة وبنسبة (76%) وهو يعني ان هؤلاء قد وقعو تحت تاثير ثقتهم واحترامهم الذي عمل على ترسيخه المهندس الاجتماعي وهم غير مهتمون بالتحري عنه نتيجة لهذا الأسلوب الاجتماعي، اما الذين اجابوا بـ (الى حد ما) فبلغ عددهم (8) طلاب

وبنسبة (16%)، فهم يبقون مترددون وحائرون بين الوقوع تحت تاثير المهندس الاجتماعي والخوف من مجهوليته، وقد يقعون ضحية له او يستطيعون مقاومة تاثيره، ويبقى أولئك الذين يشكلون بنسبة (8%) والذين اجابوا بـ (كلا) والذين بلغ عددهم (4) طلاب فهم واعين لاساليب المهندس الاجتماعي ويحرصون على التحري عنه، وهذا يدل على ان اغلبية كبيرة من الطلاب واقعة تحت تاثير أساليب المهندس الاجتماعي ولا ترغب بالتحري عن هويته.

جدول (6) يبين النسبة المئوية للذين يطلبون اجراء علاقة اجتماعية مع اشخاص مجهولين

يراسلوني اشخاص مجهولين ويطلبون مني إقامة علاقة اجتماعية من نوع ما، ولا اتردد في ذلك	العدد	النسبة المئوية
نعم	19	38%
كلا	13	26%
الى حد ما	18	36%
المجموع	50	100

يقوم المهندس الاجتماعي بمراسلة الشخص المستهدف ويطلب منه إقامة علاقة اجتماعية من أي نوع ويمارس اساليب اقتاعية مختلفة للوصول الى هدفه استناداً الى خبرته في الموضوع، ويتبين من خلال ملاحظة البيانات الواردة في الجدول(6) ان الذين اجابوا بـ (نعم) بلغ عددهم (19) طالب وطالبة وبنسبة (38%) وهم يمثلون من لايترددون في إقامة علاقة اجتماعية مع من يراسلهم من اشخاص مجهولين،وهي بالرغم من كونها ليست نسبة كبيرة حيث ان القيم والعادات تفرض وجودها في مثل هذه العلاقات الا انها تعتبر النسبة الأكبر بين العينة، مما يعني ان تاثير المهندس الاجتماعي واضح حتى في مثل هذه الأمور مما يعبر عن نجاح أساليب الهندسة الاجتماعية في هذه المجال ايضاً لاسيما وان الذين اجابوا بـ (الى حد ما) بلغ عددهم (18) طالب وطالبة وبنسبة (36%)، أي انهم يميلون الى التردد في ذلك مما يعني وجود تاثير محدود لوسائل الهندسة الاجتماعية لتحديد عامل القيم فيهم، اما الذين اجابوا بـ (كلا) فكان عددهم (13) طالب وطالبة وبنسبة (26%) وهذا يدل على ان النسبة الأقل هي التي تدرك أساليب الهندسة الاجتماعية وتعمل على مقاومتها في هذا الجانب.

جدول (7) يبين تاثير الشعور بالتقدير \ الاحترام على الثقة والمشاركة بالمعلومات عن الزملاء في الكلية

يُجبرني الأشخاص الذين يمنحوني التقدير/ الاحترام على الثقة بهم ويمكن ان اشاركهم معلومات عن زملائي في الكلية	العدد	النسبة المئوية
نعم	38	76%
كلا	3	6%
الى حد ما	9	18%
المجموع	50	100

يمارس مهندسو الهندسة الاجتماعية اساليبهم الملتوية والمخادعة من خلال تاثير الشعور بالتقدير/ الاحترام على بناء الثقة مع الضحية والحصول على المعلومات عن اشخاص مستهدفين يكونون زملاء للضحية في الكلية، ونلاحظ من البيانات الواردة في الجدول(7) ان الذين اجابوا بـ (نعم) كان عددهم (38) طالب وطالبة وبنسبة (76%) وهم يمثلون النسبة الأعلى مما يتضح تاثير هذا الاسلوب الاجتماعي على الطلبة الجامعيين فعندما يتعزز شعورهم بالتقدير والاحترام فانهم لا يمانعون بمشاركة اشخاص غرباء بمعلومات عن زملاء مستهدفين من قبل المهاجمين الاجتماعيين، اما الذين اجابوا بـ (الى حد ما) فعددهم (9) طلاب وبنسبة (18%) فهم برغم ترددهم فانهم قد يتاثرون ويميلون الى الوقوع ضحية للطرق الاجتماعية ليزيدو من نسبة المتاثرين بهذا الفخ الاجتماعي، ويبقى الذين اجابوا بـ (كلا) وكان عددهم (3) طلاب وبنسبة (6%) فهو يدل على قلة النسبة التي تستطيع صد أساليب منح شعور التقدير والاحترام وعدم التاثر بها.

جدول (8) يبين الاهتمام بالحوار مع الأشخاص ذوو الأسلوب الجذاب في التواصل الاجتماعي مع تبادل الملفات الشخصية

أهتم بالحوار مع الأشخاص ذوو الأسلوب الجذاب في التواصل الاجتماعي مع تبادل الملفات الشخصية بيننا	العدد	النسبة المئوية
نعم	38	76%
كلا	4	8%
الى حد ما	8	16%
المجموع	50	100

يفرض المهندسون الاجتماعيون اسلوبهم الجذاب على الضحية بعد تحليلهم لنقاط الجذب عندهم، فيكون الحوار معهم متسلسلاً ومشوقاً وقد يبادلوهم ملفات شخصية كالصور والتسجيلات المرئية والصوتية، والتي قد يبتزونهم من خلالها لاحقاً وتكون وبالاً على الضحية، وتوضح البيانات الواردة في الجدول (8) ان ظهور نسبة عالية من المبحوثين الذين ينجذبون الى اجراء حوارات من هذا القبيل اذ بلغ عدد الذين اجابوا بـ (نعم) (38) طالب وطالبة وبنسبة (76%)، اما الذين اجابوا بـ (الى حد ما) فكان عددهم (8) طلاب وبنسبة (16%) فهم قابلين للوقوع في هذه المصيدة الاجتماعية بالرغم من مقاومتهم لها، اما الذين اجابوا بـ (كلا) فكان عددهم (4) طلاب وبنسبة (8%) من مجموع عدد المبحوثين وهم يمثلون نسبة قليلة تستطيع صد أساليب الاغراء الجذاب للحوار.

ومما تقدم (الجداول 4-8) يتضح التأثير الشديد للاساليب الاجتماعية على طلبة كلية الاعلام في جامعة بغداد وبالتالي اختراق امن المعلومات لديهم من خلال تلك الاساليب.

ب- اساليب تقنية: يتضمن الإجابة على فقرات استمارة الاستبيان من قبل عينة البحث وتحليل بياناتها ونتائجها موضحة في الجداول (9-12) وكما يلي:

جدول (9) يبين حالة الفضول للمشاركة في تطبيق جديد على شبكة الانترنت والمشاركة فيه

ينتابني فضول شديد في حال تمت دعوتي للمشاركة في تطبيق جديد على شبكة الانترنت واشارك فيه بلا تردد	العدد	النسبة المئوية
نعم	45	90%
كلا	3	6%
الى حد ما	2	4%
المجموع		100

يمارس مهندسو الشبكة الاجتماعية أساليب تقنية لاستدراج الضحية وخداعه ومن بينها انتاج تطبيقات الكترونية تستدرجه للمشاركة فيها من خلال وسائل جذب واغراء فيشعر الضحية بالفضول ويبادر الى المشاركة في تلك التطبيقات والتي تحصل على معلومات شخصية او حتى مرئية او صوتية كما في التطبيقات التي تتنبأ بشكل المستخدم بعد عدة سنوات، ونلاحظ من خلال البيانات الورادة في الجدول (9) ان الذين اجابوا

بـــ(نعم) بلغ عددهم (45) طالب وطالبة وبنسبة (90%) وهي تدل دلالة واضحة على وقوع نسبة كبيرة من العينة في هذا الفخ الالكتروني حيث التطبيقات الجاذبة والتي يرسلها المهندسون الاجتماعيون في وسائل التواصل الاجتماعي من خلال نشر رسائلهم الالكترونية الى من يريدون الإيقاع بهم من خلال البحث عن جميع المستخدمين الذين ينتسبون الى جهة معينة او نشاط معين ويقوموا بجمع الكثير من المعلومات التفصيلية التي يمكن استخدامها في الهجوم، في حين ان الذين اجابوا بـــ (كلا) فكان عددهم (3) طلبة وبنسبة (6%) وهي نسبة ضئيلة جداً استطاعت مقاومة هذه الاغراءات او ربما بانها غير مهتمة اصلاً بها، اما الذين اجابوا بـــ (الى حد ما) فعددهم (2) طالب وطالبة وبواقع نسبة (4%) وهذا يدل على ان هذه النسبة البسيطة هي من تبقى مترددة في الاستجابة لتلك التطبيقات.

جدول (10) يبين الاستعداد لاعطاء كلمة المرور الخاصة بموقع التواصل الاجتماعي عند البحث على مصادر علمية

عندما ابحث عن مصادر علمية في المنصات الالكترونية، وطُلب مني كلمة المرور الخاصة بحسابي على موقع تواصل اجتماعي فلا اتردد في اعطائها	العدد	النسبة المئوية
نعم	24	48%
كلا	4	8%
الى حد ما	22	44%
المجموع	50	100

يبدو ان لهفة الحصول على مصادر علمية من قبل الطلبة لانجاز بحوثهم تجعلهم يثقون بالمنصات الالكترونية العلمية فنلاحظ من خلال البيانات الواردة في الجدول (10) ان الذين اجابوا بـــ (نعم) حصلت على اعلى نسبة من بين المراتب الاخرى اذ كان عددهم (24) طالب وطالبة وبنسبة (48%) في حين الذين اجابوا بـــ (الى حد ما) فكان عددهم (22) طالب وطالبة وبنسبة (44%) وهم كانو في حالة التردد وربما ميالون لاعطاء كلمة المرور الخاصة بهم، والذين اجابوا بـــ (كلا) فكان عددهم (4) طلاب وبنسبة (8%) من مجموع المبحوثين وهذا يدل على تاثر نسبة كبيرة من العينة بالأسلوب التقني هذا ويبدو ان الرغبة في الحصول على المصادر العلمية لانجاز البحوث تكلف الطلبة الكثير من بياناتهم المخزونة في مواقعهم الالكترونية.

جدول (11) يبين مدى الاهتمام بفتح النوافذ الالكترونية

أفتح النوافذ المنبثقة المتعلقة باهتماماتي أثناء البحث عن شيء ما على متصفحات الإنترنت كـ Internet Explorer Google Chrome, Mozilla, Opera	العدد	النسبة المئوية
نعم	38	76%
كلا	8	16%
الى حد ما	4	8%
المجموع	50	100

يستخدم المهندسون الاجتماعيون أسلوب تقني يوجّه المستخدمين إلى صفحات تتضمّن احد ألاساليب التقنية للهندسة الاجتماعية عبر النوافذ المنبثقة أو النوافذ المنبثقة الخلفية أو الأنواع الأخرى من عمليات إعادة التوجيه، وفي كلتا الحالتين، سيؤدي هذا النوع من محتوى الهندسة الاجتماعية المضمّن إلى انتهاك السياسة الخاصة بصفحة المضيف، والتي قد يبتزونهم من خلالها لاحقاً وتكون وبالاً على الضحية، وتوضح البيانات الواردة في الجدول (11) ان ظهور نسبة عالية من المبحوثين الذين ينجذبون الى فتح النوافذ الالكترونية اذ بلغ عدد الذين اجابوا بـ (نعم) (38) طالب وطالبة وبنسبة (76%)، اما الذين اجابوا بـ (الى حد ما) فكان عددهم (4) طلاب وبنسبة (8%) فهم قابلين للوقوع في هذه المصيدة التقنية بالرغم من مقاومتهم لها، اما الذين اجابوا بـ (كلا) فكان عددهم (8) طلاب وبنسبة (16%) من مجموع عدد المبحوثين وهم يمثلون نسبة قليلة تستطيع صد أساليب اغراء النوافذ المفتوحة.

جدول (12) يبين مدى اهتمام العينة بفتح الروابط المرسلة عبر وسائل التواصل

اهتم بفتح الروابط "اللينكات" المرسلة لي من قبل أصدقائي عبر وسائل التواصل/ التطبيقات المختلفة.	العدد	النسبة المئوية
نعم	41	82%
كلا	3	6%
الى حد ما	6	12%
المجموع	50	100

يمارس مهندسو الهندسة الاجتماعية اساليبهم التقنية الملتوية والمخادعة من خلال ارسال روابط "اللينكات" كما يحصل في الواتساب، وأحيانًا في البريد الإلكتروني، وهي طريقة «الرابط المختصر»، إذ قد يستخدمها المهاجم كواجهة لإخفاء الرابط الضار، والتي توفر للمخترقين أساليب متعددة لتصيد الضحايا، ونلاحظ من البيانات الواردة في الجدول(12) ان الذين اجابوا بـ (نعم) كان عددهم (41) طالب وطالبة وبنسبة (82%) وهم يمثلون النسبة الأعلى مما يتضح تاثير هذا الاسلوب التقني على الطلبة الجامعيين فيتسرعون وبلا تفكير في اثرها او مجهولية وصولها، اما الذين اجابوا بـ (الى حد ما) فعددهم (6) طلاب وبنسبة (12%) فهم برغم ترددهم فانهم قد يتاثرون ويميلون الى الوقوع ضحية هذا التصيد الاحتيالي، ويبقى الذين اجابوا بـ (كلا) وكان عددهم (3) طلاب وبنسبة (6%) فهو يدل على قلة النسبة التي تستطيع الوقوف بوجه الأسلوب الاحتيالي التقني هذا.

جدول (13) يبين مدى الوقوع في فخ الاختبارات الالكترونية

أشارك في برامج الاختبارات الالكترونية (اون لاين) بالرغم من طلبها معلومات تتعلق بالخصوصية واثق بنتائج هذه البرامج	العدد	النسبة المئوية
نعم	25	50%
كلا	20	40%
الى حد ما	5	10%
المجموع	50	100

تبين بيانات الجدول (13) بان نصف العينة المبحوثة لا تهتم بموضوع الخصوصية وتنساق خلف برامج تطرح أسئلة لاختبار الشخصية او السعادة او التنبؤ بالمستقبل وغيرها، وينجح المهنسون الاجتماعيون من خلال الأسلوب التقني هذا في الحصول على معلومات تتعلق بالخصوصية لدى الضحية، ويلاحظ ان عدد هؤلاء الطلبة بلغ (25) طالب وطالبة وبنسبة (50%)، اما عدد الذين اجابوا بـ (الى حد ما) فبلغ نسبة (5) طلاب وبواقع (10%)، وهو يوحي بان هذه النسبة تتردد في إعطاء معلومات الخصوصية لشعورهم باهميتها وقد يقعون به تحت تاثير الرغبة بالمشاركة في هذه التطبيقات، وأخيرا فان

الذين اجابوا بـ (كلا) بلغ عددهم (20) طالب وطالبة وبنسبة (40%) وهم فقط الذين يشعرون بخطورة موضوع الافشاء بمعلومات الخصوصية مما يعكس عدم تاثرهم بهذا الاسلوب.

ومما يتقدم في الجداول من (9-13) يتضح التاثير المرتفع للاساليب التقنية على طلبة كلية الاعلام في جامعة بغداد وهو يشير الى اختراق امن المعلومات لديهم من خلال تلك الاساليب.

ج-أساليب تقنية – بشرية

يتضمن الإجابة على فقرات استمارة الاستبيان من قبل عينة البحث وتحليل بياناتها ونتائجها مبينة في الجداول (14-18) وكما يلي:

جدول (14) يبين اختراق الوصول للمعلومات من خلال أسلوب الاتصال التلفوني وعرض المشاركة بعمل تطوعي اجتماعي

أُدلي ببعض معلوماتي)الاسم – العنوان-مكان العمل او الدراسة(عند الاقتناع بالمشاركة بعمل تطوعي اجتماعي بمكالمة تليفونية.	العدد	النسبة المئوية
نعم	27	54%
كلا	15	30%
الى حد ما	8	16%
المجموع	50	100

قد يستخدم المهندسون الاجتماعيون أساليب تقنية بشرية كما يحصل في اتصالات عشوائية تلفونية بهدف التعرف على معلومات عن الشخص المستهدف، وتبين بيانات الجدول (14) نجاح المهنسون الاجتماعيون من خلال الأسلوب التقني- الاجتماعي المذكور مع اكثر من نصف العينة المبحوثة التي افصحت بمعلوماتها العامة وانخدعت بذريعة العمل التطوعي، اذ يلاحظ ان عدد هؤلاء الطلبة بلغ (27) طالب وطالبة وبنسبة (54%)، فضلاً عن ان الذين اجابوا بـ (الى حد ما) فبلغ (8) طلاب وبواقع (16%)، والذين يمثلون حالة تردد في إعطاء هذه المعلومات لاهميتها لديهم، ولكن العمل التطوعي يبقى مؤثراً عندهم وقد ينساقون تحت تاثير الرغبة بالمشاركة فيها، اما الذين اجابوا بـ (كلا) بلغ عددهم (15) طالب وطالبة وبنسبة (30%) والذين انتبهوا او قد يكونون غير مهتمين اصلاً للمشاركة مما يعكس نجاح الأسلوب.

جدول (15) يبين استجابة العينة لرسائل الكترونية تعلن تقديم دورات / منح تدريبية

اسجل بياناتي الشخصية كاملة في استمارة الكترونية وصلتني في رسالة على البريد الالكتروني من صديق على موقع للتواصل الاجتماعي تعلن بدء التقديم لدورات / منح تدريبية.	العدد	النسبة المئوية
نعم	43	86%
كلا	3	6%
الى حد ما	4	8%
المجموع	50	100

يمارس مهندسو الهندسة الاجتماعية اساليب تقنية- بشرية الغرض منها الحصول على معلومات عن الضحية من خلال ارسال رسائل على البريد الإلكتروني توهمه ببدء دورات للطلبة، ونلاحظ من البيانات الواردة في الجدول(15) ان الذين اجابوا بـــ (نعم) كان عددهم (43) طالب وطالبة وبنسبة (86%) وهم يمثلون نسبة مرتفعة تدل على تاثير هذا الاسلوب التقني - الاجتماعي على الطلبة الجامعيين فيتسرعون في إعطاء معلوماتهم، اما الذين اجابوا بـــ (الى حد ما) فعددهم (4) طلاب وبنسبة (12%) فهم يترددون وتساورهم الرغبة في إعطاء معلوماتهم وقد يتاثرون ويميلون الى الوقوع ضحية هذا التصيد الاحتيالي، ويبقى الذين اجابوا بـــ (كلا) وكان عددهم (3) طلاب وبنسبة (6%) فهو يدل على قلة النسبة التي تستطيع الوقوف بوجه الأسلوب الاحتيالي التقني- الاجتماعي هذا.

جدول (16) يبين مدى الرغبة في المشاركة في استبيانات على مواقع التواصل الاجتماعي

في حال عرض علي مسؤول مجموعة (جروب) على موقع للتواصل الاجتماعي المشاركة في استبيان فانني أشارك رغبةً في التفاعل	العدد	النسبة المئوية
نعم	39	78%
كلا	8	16%
الى حد ما	3	6%
المجموع	50	100

يعرض المهندسون الاجتماعيون أسلوب تقني-اجتماعي بارسال استمارات استبيان الى الأشخاص المستهدفين للحصول على ارائهم حول موضوع معين لتوجيهها الى اغراضهم الخبيثة مستقبلاً عن طريق ابتزازهم او استدراجهم، وتوضح البيانات الواردة في الجدول (16) ان ظهور نسبة عالية من المبحوثين الذين يتفاعلون مع هذا الاسلوب وقد بلغ عددهم (38) طالب وطالبة اجابوا بـ (نعم) وبنسبة (78%)، اما الذين اجابوا بـ (الى حد ما) فكان عددهم (3) طلبة وبنسبة (6%) وهم قابلين للوقوع في هذه المصيدة التقنية - الاجتماعية بالرغم من مقاومتهم لها، اما الذين اجابوا بـ (كلا) فكان عددهم (8) طلاب وبنسبة (16%) من مجموع عدد المبحوثين وهم يمثلون نسبة قليلة لم يتفاعلوا معه.

جدول (17) يبين مدى الاستعداد للايجاب تجاه تحديث تطبيق الكتروني مفضّل

عندما يصلني ملف من منصة الكترونية اشترك بها ويبلغني مرسله انه النسخة المُحدثة لتطبيق الكتروني مفضل لديّ وينبغي مسح التطبيق القديم وتنصيب الملف المرسل فاني انفذ ما يطلب مني	العدد	النسبة المئوية
نعم	24	48%
كلا	22	44%
الى حد ما	4	8%
المجموع	50	100

يبدو ان تحديث ملفات التطبيقات الالكترونية المفضلة لدى الطلبة شجعت اقل من نصف العينة للاستجابة معها وتقاربت معها نسبة الرافضين لمسح التطبيق الأصلي الموجود في الجهاز فنلاحظ من خلال البيانات الواردة في الجدول (17) ان الذين اجابوا بـ (نعم) كان عددهم (24) طالب وطالبة وبنسبة (48%) في حين الذين اجابوا بـ (كلا) كان عددهم (22) طالب وطالبة وبنسبة (44%) من مجموع المبحوثين، اما الذين اجابوا بـ (الى حد ما) فكان عددهم (4) طلاب وبنسبة (8%) وكانوا في حالة التردد وربما ميالون لتنفيذ ما طُلب منهم، ومع ذلك فان هذا الأسلوب التقني- الاجتماعي نجح مع النسبة الأكثر من العينة.

جدول (18) يبين استجابة العينة لقبول طلبات الصداقة بدون المعرفة بهم

أقوم بقبول طلبات الصداقة على الشبكات الاجتماعية بعد مراسلتي من اشخاص اعجبت باسلوبهم وبدون معرفتي بهم	العدد	النسبة المئوية
نعم	3	6%
كلا	43	86%
الى حد ما	4	8%
المجموع	50	100

يعرض مهندسو الهندسة الاجتماعية طلبات الصداقة على الضحية بعد ان قاموا بالتاثير عليه في الحديث، وعند اضافته الى مجموعة أصدقاء المستهدف يقومون بالتجسس على صفحته وما ينشر فيها من تعليقات ليكونون فكرة كاملة عنه ليتم استغلال ذلك في مقاصد خبيثة، ويلاحظ ان طلبة الجامعة المبحوثة لم يتاثروا بهذا الأسلوب الاجتماعي التقني ولم ينقادو له، ونلاحظ من البيانات الواردة في الجدول(18) ان الذين اجابوا بـ (نعم) كان عددهم (3) طلاب فقط وبنسبة (6%) وهي نسبة منخفضة مقابل (43) طالب وطالبة اجابوا بـ (كلا) وبنسبة (86%) فقد شعروا بخطورة إضافة أصدقاء جدد ليست لهم علاقة سابقة بهم، اما عدد الذين اجابوا بـ (الى حد ما) فعددهم (4) طلاب وبنسبة (8%) فهم يترددون وتساورهم الرغبة في إضافة الأصدقاء ولربما يقعون ضحية هذا التصيد الاحتيالي، ويدل ذلك على ان النسبة التي تستطيع الوقوف بوجه الأسلوب الاحتيالي التقني – الاجتماعي هذا مرتفعة جداً وهو الأسلوب الوحيد الذي يعتبر تاثيره منخفض في الطلبة الجامعيين المبحوثين.

رابعاً: التحليل العام للنتائج

ان النتائج اعلاه بصورة العامة بينت ان هناك نسبة عالية من عينة الدراسة تدرك اهمية امن معلوماتهم وانهم حريصون على المحافظة عليها، وان نسب مهمة منهم لايعيرون اهتماماً لذلك وهم بالتالي سيكونون معرضون بالتأكيد لاساليب الهندسة الاجتماعية والذين شكلوا النسبة الأكبر للمتاثرين بها، ومع ذلك فقد أظهرت نتائج المحور الثاني ان نسب المتاثرين باساليب الهندسة الاجتماعية كانوا الأعلى اجمالاً وهو ما يشير الى ان جزء ممن أظهرت النتائج اهتمامهم بامن المعلومات لديهم قد تاثروا بتلك الأساليب ووقعوا في فخها

بالرغم من حرصهم على معلوماتهم، مما يؤكد تاثير أساليب الهندسة الاجتماعية عموماً على اختراق معلومات الطلبة في مواقع التواصل الاجتماعي.

الاستنتاجات والتوصيات

الاستنتاجات

1. اختلف مفهوم الهندسة الاجتماعية في مجال امن المعلومات عن غيره من العلوم فهو يتضمن استخدام طرق وتقنيات الخداع والتلاعب او للحيل الذكية لتغيير أفكار الافراد وما يتبنوه من معتقدات وتراث وقيم واتجاهات.
2. ان مخاطر الهندسة الاجتماعية (البشرية والتقنية)على امن الافراد والمؤسسات أصبحت ظاهرة مستفحلة في المجتمع وتتضح تاثيراتها في وسائل التواصل الاجتماعي التي ازدادت شعبيتها في السنوات الماضية.
3. ساهمت وسائل وتنوع تقنيات شبكات التواصل الاجتماعي في انتشار وتسهيل ظاهرة الهندسة الاجتماعية.
4. ان ضعف الوعي بمخاطر الهندسة الاجتماعية وتقنياتها المختلفة قد اسهم باستفحالها بالنظر للثقة التي يبديها مستخدموا وسائل التواصل الاجتماعي تجاه الاخرين مما أدى للتلاعب بهم والاحتيال عليهم.
5. يلاحظ خلو التشريعات العراقية من قانون يحد من الجرائم الالكترونية ويضع حداً لها بالرغم من اقتراح مسودة قانون الجرائم الالكترونية منذ عام 2012.

التوصيات

1. العمل على توعية المجتمع افراداً ومؤسسات بمفهوم الهندسة الاجتماعية وأساليبها من خلال مجموعة من الندوات 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.

2. العمل على دعم برامج ومهارات الوعي المعلوماتي لدى الافراد والمؤسسات وذلك من خلال التنسيق مع الجهات المتخصصة كاقسام دراسات المعلومات في الجامعات للرقي بمستوى الوعي المعلوماتي وتعزيز ثقافة تكنلوجيا االتصالات لديهم التي تعتبر من الأساليب التنظيمية التثقيفية للحد من تلك السلوكيات.
3. تدريس مجالات الأمن المعلوماتي، وأخلاقيات المعلومات لطلاب الجامعات 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.
4. تفعيل دور اختصاصيي المعلومات في المؤسسات من خلال تبني برنامج توعوي متكامل للاختصاصيين بالتنسيق مع قسم دراسات المعلومات في الجامعات، لرفع ثقافة ومهارات اختصاصي المعلومات وتفعيل التنسيق بين الاكاديمين والمؤسسات في مجال معلومات الاتصالات.
5. ضرورة اهتمام المشرع العراقي بموضوع الجرائم التكنلوجية وإصدار تشريع سريع يحد من اخطارها على امن المجتمع.

المصادر

1. بو بعاية، يمينة (2016)، مستوى الإدمان على مواقع التواصل الاجتماعي "الفيسبوك" أنموذجا وعلاقته بظهور بعض المشكلات النفسية لدى عينة من تلاميذ المرحلة الثانوية، رسالة ماجستير في علوم التربية – كلية العلوم الإنسانية والاجتماعية –جامعة محمد بو ضياف- الجزائر.
2. توتاوي، صليحة (2015)، استخدام الأبناء لشبكات التواصل الاجتماعي وانعكاساتها على العلاقات الاسرية، رسالة ماجستير – في علم النفس الاسري – كلية العلوم الاجتماعية –جامعة وهران – الجزائر.
3. الدليمي، عثمان محمد (2020)، مواقع التواصل الاجتماعي - نظرة عن قرب – دار غيداء للنشر والتوزيع– عمان-الأردن - ط1.
4. الرحباني، عبير (2012)، الاعلام الرقمي الإلكروني، دار أسامة للنشر والوزيع عمان-الأردن.
5. شايب، كمال وقيدة، عبد الرؤوف (2018)، أخطار الهندسة الاجتماعية على المستهلك الالكتروني، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي المركز الجامعي عبد الحفيظ بو الصوف – ميلة – الجزائر، 23-24 نيسان، 2018.
6. الشمري، سهام حسن علي (2020)، تمظهرات الامن السيبراني ووالممارسة الإعلامية وعلاقتهما بصناعة الحرب النفسية الافتراضية، مجلة دراسات دولية – جامعة بغداد – العدد 83.
7. صباح، عائش والشجيري،عمر خلف رشَيد (2018)، أثر إدمان مواقع التواصل الاجتماعي علي التطرف الفكرّي لدى طلبة الجامعات -دراسة مقارنة بين جامعتي سعَيذة والانبار، مجلة جامعة الانبار للعلوم الإنسانية- العدد 4 – مجلد 2.
8. العابدين، فاطمة عبد الهادي زين واخرون (2018)، أثر خصائص مواقع التواصل الاجتماعي في القيم المختلفة لدى الشباب في المجتمع الأردني",بحث منشور في مجلة journal of social sciences ,v7,n3 الأردن.
9. عبد التواب، حنان طنطاوي (2021)، اتجاهات الشباب الجامعي نحو الهندسة الاجتماعية وعلاقتها بالهوية الثقافية، مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية - جامعة الفيوم – العدد 22.
10. عبد الحي،حسام فايز(2020)، مشاركة الجمهور في تقنيات الهندسة الاجتماعية عبر موقع فيس بوك وعلاقتها بالخصوصية والتعويض النفسي لديهم، مجلة البحوث الإعلامية- جامعة الأزهر- العدد 55.
11. عبدالرضا، اسعد طارش والمعموري، علي إبراهيم (2020)، الامن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد عام 2003، مجلة دراسات دولية - مركز الدراسات الأستراتيجية والدولية، العدد 80.

12. عبدالوهاب، احمد عبدالكريم وخلف، محمود عبدالرحمن (2020)، إشكالية الامن السيبراني العراقي بين التهديدات السيبرانية والتقنين المقيد للحريات، مجلة العلوم السياسية – جامعة النهرين، العدد 60.

13. العصيمي، عبد المحسن أحمد براك (2004)، "الآثار الاجتماعية للإنترنت", قرطبة للنشر والتوزيع, الرياض.

14. عمر ازواو (2020)، إشكالية تطبيق المنهج الكمي في العلوم الإنسانية والاجتماعية، مجلة العلوم الإنسانية والاجتماعية – المجلد 10 – العدد 1.

15. عوض، رشا أديب محمد (2014)، آثار استخدام مواقع التواصل الاجتماعي على التحصيل الدراسي للابناء، رسالة ماجستير –تخصص خدمة اجتماعية – كلية التنمية الاجتماعية والاسرية –جامعة القدس – طولكرم.

16. فارس، كاتب (2016)، أثر استخدام مواقع التواصل الاجتماعي على سلوك الشباب، رسالة ماجستير في علوم الاعلام والاتصال –جامعة ام البواقي – الجزائر.

17. قواسمية، حنان (2016)، مواقع التواصل الاجتماعي ودورها في زيادة العزلة لدى الطلبة الجامعيين، رسالة ماجستير في الاعلام والاتصال - كلية العلوم الإنسانية والاجتماعية - جامعة العربي التبسي- الجزائر.

18. الكندي، سالم سعيد والبلوشي، حليمه سليمان (2020)، الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان،مجلة العلوم والاداب الاجتماعية – جامعة السلطان قابوس -المجلد 11 – العدد ٢.

19. مارسيلينو، ويليام واخرون (2017)، رصد وسائل التواصل الاجتماعيّ، مؤسسة RAND سانتا مونيكا، كاليفورنيا.

20. محمد، مها احمد إبراهيم،) 2018)، الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي، المجلة الدولية لعلوم المكتبات والمعلومات- جامعة بني سويف.

21. المختار، طيبة جواد حمد (2008)، صعوبة الملاحقات القضائية في الجرائم الحاسوبية، مجلة جامعة بابل، المجلد 15 –العدد 1.

22. المشهدي، تغريد معين حسن (2019)،الأثر العسكري للأمن السيبراني في الجغرافية السياسية للدولة، مجلة البحوث الجغرافية – العدد 30.

23. يونـــس بسمـــه حســني عيـــد (2016)، إدمان شبكات التواصل الاجتماعي وعلاقتها بالاضطرابات النفسية لدى طلبة الجامعة في محافظة غزة، رسالة ماجستير في علم النفس- كلية التربية –جامعة الازهر، غزة.

24. Abutaha, Mohammed, *et al*.,(2021) , URL Phishing Detection using Machine Learning Techniques based on URLs Lexical Analysis , International Conference on Information and Communication Systems, No.12.

25. Anuja Arora, *et al.*, (2019), Measuring Social Media Influencer Index- I Insights from Facebook, Twitter and Instegram, Journal of Retailing and Consumer Services, No 49.

26. Drus, Zulfadzli and Khalid Haliyana (2019) , Sentiment Analysis in Social Media and Its Application: Systematic Literature Review , scientific committee of The Fifth Information Systems International Conference, Procedia Computer Science 161.

27. Hijji, Mohammad and Alam Gulzar (2021) , A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions, IEEE Access Journal , Volume 9.

28. Kalio, Sotonye (2022), Phishing Attacks: Raising Awareness and Protection Techniques In Bournemouth Universit, Society for the Improvement of Psychological Science, 11, January, 2022.

29. Koch, T., *et al.*, (2018). The impact of social media on recruitment: Are you LinkedIn? SA Journal of Human Resource, No. 16.

30. M, Rajitha and R, Priya (2022) , A Review on Cyber Threats Analysis Using Data Mining Techniques – With Special Reference to Phishing Attacks , International Journal of Modern Developments in Engineering and Science Volume 1, Issue 5.

31. Meel, Priyanka and Vishwakarma Dinesh Kumar (2020) , Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities , Expert Systems With Applications Journal, No. 153.

32. Salahdine, Fatima and Kaabouch, Naima (2019) , Social Engineering Attacks: A Survey , Future Interne journal ,Vol. 11, no. 89.

33. Witjes, Nina Klimburg and Wentland, Alexander (2021) , Hacking Humans? Social Engineering and the Construction of the “Deficient User” in Cybersecurity Discourses, Science, Technology and Human Values, Vol. 46, No.6.