5

الهندسة الاجتماعية: النشأة والتطور في العصر الرقمي

Social Engineering: Emergence and Evolution in the Digital Age

الكلمات المفتاحية: الهندسة الاجتماعية، الهجمات الإلكترونية، الأمن السيبراني، الاحتيال الإلكتروني، التصيد الاحتيالي.

Keywords: Social engineering, cyberattacks, cybersecurity, online fraud, phishing.

البـاحث: اسراء فاضل عباس

Researcher: Israa Fadel Abbas

أ.م.د.زينب محمد صالح

Asst. Prof. Dr. Zainab Mohammed Saleh

جامعة بغداد / كلية التربية للبنات/ قسم علم الاجتماع

Department of Sociology College of Education for Women, University of Baghdad

Israa.abbas2309d@coeduw.uobaghdad.edu.iq

zainab_mohammedsalih@coeduw.uobaghdad.edu.iq

المستخلص:

تُعد الهندسة الاجتماعية من أخطر الأساليب التي يستخدمها المهاجمون لتحقيق أهداف غير قانونية، خاصة في العصر الرقمي، حيث تستهدف الأفراد والمؤسسات عبر استغلال نقاط الضعف البشرية بدلًا من الاختراقات التقنية. تشمل هذه الأساليب التصيد الاحتيالي (Phishing)، المكالمات الهاتفية المضللة (Vishing)، والرسائل النصية الاحتيالية (Smishing)، وتزداد خطورتها مع توسع استخدام وسائل التواصل الاجتماعي، يستعرض هذا البحث نشأة الهندسة الاجتماعية وتطورها من الخداع التقليدي إلى الهجمات الإلكترونية المتقدمة، ويحلل تأثيرها السلبي على الأفراد والمؤسسات، بما في ذلك سرقة البيانات وتهديد الأنظمة الحساسة. كما يناقش سبل التحصين الأمني، مثل سياسات الأمان، التدريب المستمر، وتعزيز الوعي الأمني، للحد من مخاطر هذه الهجمات في العصر الرقمي.

Abstract:

Social engineering is one of the most dangerous techniques used by attackers to achieve illegal objectives, especially in the digital age. It targets individuals and institutions by exploiting human vulnerabilities rather than technical breaches. These techniques include phishing, vishing (voice phishing), and smishing (SMS phishing), and their risks increase with the widespread use of social media.

This research examines the origins and evolution of social engineering, from traditional deception to advanced cyberattacks, analyzing its negative impact on individuals and institutions, including data theft and threats to critical systems. It also discusses security measures, such as security policies, continuous training, and awareness enhancement, to mitigate the risks of these attacks in the digital age.

مقدمة:

تعتبر الهندسة الاجتماعية واحدة من أخطر التهديدات التي تواجه الأفراد والمؤسسات في العصر الرقمي، حيث تعتمد على استغلال نقاط الضعف البشرية لتحقيق أهداف غير قانونية، مثل سرقة المعلومات الشخصية أو التسلل إلى الأنظمة الإلكترونية. وقد شهدت الهجمات الهندسية الاجتماعية نمواً سريعاً بفضل التقدم التكنولوجي وانتشار وسائل التواصل الاجتماعي، مما جعلها تشكل تهديداً حقيقياً لأمن المعلومات وحمايتها.بدأت الهندسة الاجتماعية كوسيلة للخداع التقليدي، حيث كانت

تعتمد على أساليب نفسية وتقنيات متنوعة لإقناع الأفراد بالكشف عن معلومات حساسة. مع تطور التكنولوجيا، تطورت هذه الأساليب لتشمل هجمات إلكترونية متقدمة تتجاوز قدرة الأنظمة الأمنية التقليدية. يتناول هذا البحث نشأة الهندسة الاجتماعية، وتطورها عبر الزمن، بالإضافة إلى تأثيراتها في العصر الرقمي، وسبل الحماية منها، مع تسليط الضوء على التحديات التي تطرأ في هذا المجال.

مشكلة البحث: تتمثل مشكلة هذا البحث في دراسة تأثير الهندسة الاجتماعية في العصر الرقمي على الأفراد والمؤسسات، وكيفية مواجهة هذا النوع من الهجمات التي تعتمد على الخداع البشري بدلاً من الاختراقات التقنية المباشرة. بالإضافة إلى ذلك، يتمثل التحدي في عدم القدرة الكافية على اكتشاف هذه الهجمات في الوقت المناسب، ما يجعل الأفراد والمؤسسات عرضة لهجمات تسعى إلى سرقة المعلومات الحساسة أو التلاعب بالبيانات.

أهمية البحث:

تتمثل أهمية البحث في إبراز دور الهندسة الاجتماعية كأحد أخطر تهديدات العصر الرقمي، واستكشاف تداعياتها على أمن المعلومات وحماية الأنظمة الإلكترونية. كما يهدف البحث إلى تقديم سبل التحصين والحماية اللازمة للأفراد والمؤسسات من الوقوع ضحايا لهذه الهجمات. هذا البحث يساهم في توعية الأفراد والمنظمات بكيفية التعرف على أساليب الهندسة الاجتماعية، وتطبيق أساليب الوقاية المناسبة لتفاديها.

هدف البحث :دراسة الهندسة الاجتماعية من حيث نشأتها وتطورها، وتحليل أساليبها في استهداف الأفراد والمؤسسات لاختراق الأنظمة وسرقة المعلومات. كما يستعرض تأثيرها على الأمن السيبراني، وأنماط الهجمات القائمة على التلاعب النفسي، مع التركيز على المخاطر في العصر الرقمي. بالإضافة إلى ذلك، يناقش البحث وسائل الحماية والتوعية الأمنية للحد من هذه التهديدات.

تساؤلات البحث:

1. ما هي أساليب الهندسة الاجتماعية التي يستخدمها المهاجمون في العصر الرقمي؟
2. كيف تطورت أساليب الهندسة الاجتماعية من الخداع التقليدي إلى الهجمات الإلكترونية المتقدمة؟
3. ما تأثير الهندسة الاجتماعية على الأمن السيبراني للأفراد والمؤسسات؟
4. ما هي التحديات الرئيسية التي تواجه الأفراد والمؤسسات في مواجهة الهندسة الاجتماعية؟
5. ما هي وسائل التحصين التي يمكن أن تستخدمها المؤسسات لحماية نفسها من الهجمات الهندسية الاجتماعية؟
6. كيف يمكن تعزيز الوعي الأمني لمواجهة تهديدات الهندسة الاجتماعية؟

المبحث الاول: نشأة وتطور الهندسة الاجتماعية

المطلب الاول: نشأة الهندسة الاجتماعية

الهندسة الاجتماعية تعد أحد فروع علم النفس البشري وتركز على جمع المعلومات للكشف عن بعض الخفايا المجتمعية وتغييرها. ظهر مصطلح "المهندسين الاجتماعيين" لأول مرة في مقال كتبه الصناعي الهولندي جي سي فان ماركن عام 1894م، حيث كانت الفكرة أن أرباب العمل في العصر الحديث يحتاجون إلى دعم من متخصصين في التعامل مع مشكلات البشر، تمامًا كما يحتاجون إلى مهندسين تقنيين لحل المشكلات المادية المتعلقة بالمواد والمعدات والعمليات. انتقل هذا المفهوم إلى أمريكا عام 1899م، حيث تم استخدام مصطلح "الهندسة الاجتماعية" للإشارة إلى وظيفة المهندس الاجتماعي. في عام 1899، كان هذا المصطلح عنوانًا لمجلة صغيرة، وسُميت لاحقًا في عام 1922 بـ "الخدمة الاجتماعية". يمكن القول أيضًا أن إدارة عملية التحول الاجتماعي تتم تدريجيًا من خلال التعليم، الثقافة، الفن، والرياضة.[1]

لاحقًا، تطورت الهندسة الاجتماعية من مجرد نهج لتحليل المجتمعات وإدارتها إلى أداة تُستخدم لاختراق الأنظمة وجمع المعلومات بطرق غير تقليدية، وهو ما أظهره بوضوح كيفين ميتنيك، أحد أشهر المخترقين في التاريخ الحديث. في التسعينيات، استخدم ميتنيك تقنيات الهندسة الاجتماعية لاختراق العديد من الشركات الكبرى، معتمدًا على التلاعب النفسي واستغلال ثقة أو جهل الأشخاص للوصول إلى معلومات حساسة مثل كلمات المرور والأسرار التجارية، بل وحتى الحصول على إمكانية الدخول إلى أنظمة محظورة.[2]

كان ميتنيك بارعًا في انتحال الشخصيات، حيث اعتاد الاتصال بالشركات متظاهرًا بأنه موظف دعم تقني أو مسؤول رفيع، ويطلب من الموظفين تزويده بمعلومات سرية تحت ذريعة وجود مشكلة تقنية أو حالة طارئة. بهذه البساطة، كان يحصل على المفاتيح الرقمية التي تفتح له أبواب الشبكات والأنظمة. اعتمد في أساليبه على إتقان فنون الإقناع وبناء سيناريوهات مقنعة تجعل الضحية تقدم له المعلومات دون شك.

آمن ميتنيك بأن البشر، مهما تم تدريبهم، يظلون عرضة للخداع إذا استُخدمت الأساليب الصحيحة في الوقت المناسب، وهو ما جعله يصرّح مرارًا بأن "الناس هم الحلقة الأضعف في أي نظام أمني". تجربته مع الهندسة الاجتماعية أثبتت للعالم أن التقنية وحدها ليست كافية لحماية الأنظمة، وأن البشر سيظلون دائمًا نقطة الضعف الأخطر إذا لم يتم تدريبهم بشكل صحيح على اكتشاف أساليب التلاعب ومقاومتها.[3]

المطلب الثاني : مراحل تطورها عبر الزمن

البدايات التاريخية: الهندسة الاجتماعية ليست وليدة العصر الرقمي الحديث، بل تمتد جذورها إلى العصور القديمة، حيث كان المحتالون يعتمدون على الخداع النفسي لاستغلال الآخرين، سواء للحصول على أموال أو معلومات. ومن أشهر الأمثلة التاريخية على ذلك قصة حصان طروادة، التي تجسد أحد أقدم أشكال الهندسة الاجتماعية في التاريخ.[4]

تروي الأسطورة أن الإغريق، بعد حصار دام عشر سنوات لمدينة طروادة، لجأوا إلى حيلة ماكرة لكسر هذا الجمود. فصنعوا حصانًا خشبيًا ضخمًا مجوفًا تحت إشراف إبيوس، وأخفوا داخله مجموعة من المحاربين بقيادة أوديسيوس، بينما تظاهر الجيش الإغريقي بالانسحاب. ظن الطرواديون أن الحصان هدية سلام، فقبلوه وأدخلوه إلى مدينتهم.بعد الاحتفالات برفع الحصار، وفي ليلة طغت عليها مشاعر الفرح، خرج المحاربون الإغريق من الحصان الخشبي وفتحوا بوابات المدينة للجيش المتخفي. انتهت الخدعة بانهيار طروادة، حيث تم نهب المدينة بوحشية، وقتل جميع الرجال، وأُخذ النساء والأطفال كأسرى. هذه القصة تمثل مثالًا مبكرًا على كيفية استغلال الثقة البشرية لتحقيق أهداف خفية، وهو جوهر الهندسة الاجتماعية.[5]

العصر الحديث:

في أواخر القرن الـ19 وأوائل القرن الـ20، بدأ مصطلح "الهندسة الاجتماعية" يستخدم للإشارة إلى محاولات تشكيل السلوك الاجتماعي أو إدارة المجتمعات من قبل الحكومات أو النخب الاجتماعية.[6]

تطور المصطلح في عالم التقنية:

مع ظهور الحواسيب وشبكات الإنترنت، اكتسبت الهندسة الاجتماعية بُعدًا جديدًا. في الثمانينيات والتسعينيات، بدأت تُستخدم للإشارة إلى الهجمات الإلكترونية التي تستهدف العنصر البشري في الأنظمة الأمنية أول استخدام لمصطلح "الهندسة الاجتماعية" يعود إلى هولندا عام 1894، حيث أشار رجل الصناعة جي سي فان ماركين في مقال له إلى ضرورة وجود متخصصين للتعامل مع المشكلات المتعلقة بالعاملين، بقدر ما يحتاجون إلى متخصصين فنيين للتعامل مع المواد والمعدات والعمليات. بعد ذلك، انتشر المصطلح في الولايات المتحدة عام 1898 من خلال مجلة عامة نشرت تحت إشراف ويليام تولمان، الذي ألّف لاحقًا كتابًا بعنوان "الهندسة الاجتماعية" في عام 1909.

لكن التحول الكبير جاء مع عالم الاجتماع إدوين إل. إيوليت، الذي أصدر كتابًا بعنوان "المهندس الاجتماعي" في عام 1911، حيث وضع الأساس النظري لمفهوم الهندسة الاجتماعية، مشيرًا إلى إمكانية معالجة العلاقات الاجتماعية كما لو كانت أجهزة تقنية، بطريقة منظمة وقابلة للتحليل العلمي.

مع تقدم التكنولوجيا، تطورت أساليب وتقنيات الهندسة الاجتماعية لتصبح واحدة من أهم وسائل الاختراق الإلكتروني اليوم، حيث تشكل الحلقة الأضعف في دفاعات الأمن السيبراني. وتشير الإحصاءات إلى أن حوالي 90% من عمليات الاختراق تعتمد على فهم العقل البشري وآلياته ونقاط ضعفه، بينما تشكل تقنيات وبرامج القرصنة حوالي 10% فقط من تلك الهجمات.[7]

العصر الرقمي الحالي:

في العصر الرقمي الحالي، ومع الانتشار الواسع لوسائل التواصل الاجتماعي وتطبيقات المراسلة، أصبحت الهندسة الاجتماعية أكثر تعقيداً وتنوعاً. يعتمد المهاجمون اليوم على البريد الإلكتروني، المكالمات الهاتفية، والتواصل عبر وسائل التواصل الاجتماعي لخداع الضحايا وكسب ثقتهم بسهولة.

تتزايد الهندسة الاجتماعية بوتيرة سريعة في شبكات اليوم، مما يؤدي إلى إضعاف أمن الإنترنت، حيث تهدف هذه الأساليب إلى التلاعب بالأفراد والمؤسسات للحصول على بيانات حساسة لصالح مجرمي الإنترنت. ورغم قوة جدران الحماية، وتقنيات التشفير، وأنظمة كشف التسلل ومكافحة الفيروسات، تظل الهندسة الاجتماعية تحدياً كبيراً لأمن الشبكات.[8]يُعد الإنسان الحلقة الأضعف أمنيًا لثقته بالآخرين أكثر من الأنظمة، مما يجعله هدفًا سهلاً للهندسة الاجتماعية التي تستغل التفاعل البشري لكشف المعلومات. لذا، لا تكفي الحلول التقنية وحدها، بل يتطلب التصدي لها تدريبًا مناسبًا للأفراد.[9]

المبحث الثاني

الهندسة الاجتماعية في العصر الرقمي: مع تطور الهندسة الاجتماعية، أصبح مجرمو الإنترنت يعتمدون على أساليب مخصصة تعتمد على الذكاء الاصطناعي، وتقنيات التزييف العميق، ووسائل انتحال الهوية المتطورة. تستغل هذه الأساليب ثقة الأفراد، مما يجعل اكتشافها ومنعها أكثر صعوبة. يعتمد المهاجمون في الهندسة الاجتماعية على خداع المستخدمين للكشف عن معلومات حساسة أو تقديمها بهدف الوصول غير المصرح به إلى أنظمة الكمبيوتر.[10]

تشمل هذه الأساليب استغلال مشاعر الطيبة أو الطمع أو الفضول لاختراق أنظمة معلومات محمية أو الوصول إلى مستويات سرية غير مسموح بها. إضافةً إلى ذلك، قد يتم خداع الضحايا لتثبيت برامج ضارة تتيح للمهاجمين الوصول إلى الأنظمة عبر الثغرات الخلفية. وفي هذه الحالات، يقوم المهاجمون بالتخطيط بدقة لجمع المعلومات اللازمة، بدءًا من البيانات الشخصية للضحية، وذلك لتحقيق أهدافهم في اختراق النظام المعلوماتي.[11]

هذا التطور في اساليب الهندسة الاجتماعية يُظهر كيف أصبحت هذه الهجمات أكثر تعقيدًا، حيث تجمع بين التلاعب النفسي والتقنيات المتقدمة، مما يجعلها من أكبر التهديدات لأمن المعلومات في العصر الرقمي.

المطلب الاول : أبرز أساليب الخداع والتلاعب :[12]

1. أساليب بشرية: تُعد الأكثر شيوعًا في مجال الهندسة الاجتماعية، حيث يعتمد المهندسون الاجتماعيون على تقنيات نفسية لإقناع الضحايا. تشمل هذه الأساليب بناء علاقات مع الضحية، التصيد المباشر، الطُعم، والهندسة الاجتماعية العكسية. وتُعتبر الهجمات مثل التصيد الاحتيالي، الرسائل النصية القصيرة، والتصيد عبر البريد الإلكتروني والمكالمات الهاتفية من أكثر الأساليب استخدامًا في الهجمات الإلكترونية.

2. أساليب تقنية: تتم هذه الأساليب عادةً عبر الإنترنت، حيث تُستخدم وسائل مثل مواقع التواصل الاجتماعي لجمع المعلومات المتعلقة بالضحايا. غالبًا ما يلجأ المهاجمون إلى محركات البحث للوصول إلى بيانات مهمة، أو يحاولون اختراق كلمات المرور. بالإضافة إلى ذلك، يستخدم مجرمو الإنترنت أدوات آلية مثل Maltego و(SET Social Engineer Toolkit) لتحقيق هجمات إلكترونية ناجحة.

3. أساليب بشرية–تقنية: تُعتبر هذه الأساليب الأقوى في الهندسة الاجتماعية لأنها تجمع بين العنصرين البشري والتقني. يأخذ المهندس الاجتماعي في الاعتبار العوامل الاجتماعية والثقافية للضحية، والسلوك البشري، بالإضافة إلى التقنيات المستخدمة والبنية التحتية. يُساهم هذا المزج بين الأساليب الاجتماعية والتقنية في زيادة فرص نجاح الهجمات الإلكترونية.

المطلب الثاني : المخاطر على الافراد والمؤسسات

تُعد الهندسة الاجتماعية من أخطر الأساليب الاحتيالية التي تستهدف الأفراد والمؤسسات، حيث تعتمد على خداع الضحايا للوصول إلى معلوماتهم السرية. وينقسم هذا الأسلوب إلى نوعين رئيسيين: الهندسة الاجتماعية المعتمدة على التكنولوجيا، وتلك التي تستغل العنصر البشري مباشرة.

1. الهندسة الاجتماعية المعتمدة على التكنولوجيا

يشير هذا النوع إلى الأساليب التي يستخدمها المخترقون عبر الإنترنت، مستفيدين من البرامج والتقنيات المختلفة للوصول إلى المعلومات والبيانات السرية. وتتركز هذه الهندسة في البيئة الرقمية والواقع الافتراضي. ومن أبرز الأمثلة على ذلك:

1. الاحتيال الإلكتروني (Phishing):

يتجسد هذا الأسلوب في الرسائل الإلكترونية الاحتيالية التي تصل إلى الضحية، حيث تظهر وكأنها مرسلة من جهة موثوقة، مثل بنك أو شركة ائتمان أو مؤسسة حكومية. تطلب هذه الرسائل من المستلم التحقق من معلوماته الشخصية، وقد تتضمن رابطًا يؤدي إلى موقع إلكتروني مزيف مصمم ليبدو مطابقًا للموقع الرسمي. عند إدخال المستخدم بياناته السرية، يتم سرقتها قبل إعادة توجيهه إلى الموقع الحقيقي دون أن يدرك ما حدث.[13]

2. رسائل الاحتيال النيجيري (Nigerian Scam)

تُعد هذه الطريقة من أكثر أساليب الاحتيال انتشارًا عبر الإنترنت. تعتمد الفكرة على إرسال رسالة إلكترونية من شخص يدّعي أنه مواطن من دولة معينة، يزعم أن أمواله قد تمت مصادرتها، لكنه يمتلك رصيدًا في أحد البنوك ويحتاج إلى مساعدة مالية لاستعادته. في المقابل، يعد الضحية بمبلغ ضخم لقاء تقديم مساعدة مالية أولية. ومن أمثلة ذلك، الرسائل المنتشرة على وسائل التواصل الاجتماعي التي يدّعي فيها شخص ذو مكانة مرموقة، مثل شيخ أو أمير، تقديم مساعدات مالية، لكن بعد التواصل معه يُطلب دفع مبلغ كرسوم أو عمولة، ثم يختفي المحتال بعد حصوله على الأموال.[14]

3.الاحتيال الصوتي (Vishing)

يعتمد هذا الأسلوب على برامج آلية تتصل بأعداد كبيرة من الأرقام الهاتفية، وعند استجابة الضحية، يتم تشغيل رسالة مسجلة تدّعي أن بطاقته الائتمانية تتعرض لمحاولة سرقة أو احتيال. يُطلب منه إدخال رقم بطاقته ومعلوماته السرية، مما يؤدي إلى سرقة بياناته المالية دون أن يدرك الخدعة.[15]

4. الرسائل الاقتحامية المزعجة (Spam)

تتمثل هذه الطريقة في إرسال رسائل إلكترونية تحمل عناوين جذابة، مثل تهانٍ من صديق، تأكيد عملية شراء، أو عروض وخصومات مغرية لمنتجات عالمية. عند فتح الرسالة أو تحميل المرفقات، قد تحتوي على فيروسات أو برمجيات خبيثة تؤدي إلى سرقة البيانات الشخصية أو الإضرار بالجهاز.[16]

5. البرامج الوهمية

تتضمن هذه الطريقة خداع الضحايا عبر توفير برامج تبدو مفيدة أو ضرورية، فيقوم المستخدم بتحميلها دون أن يدرك أنها تحتوي على فيروسات أو برمجيات خبيثة تمنح المحتالين القدرة على اختراق أجهزتهم وسرقة بياناتهم.

الخصائص المميزة لهذه الأساليب عند تحليل هذه الأمثلة من الهندسة الاجتماعية المعتمدة على التكنولوجيا، نجد أنها لا تتطلب جهدًا بدنيًا كبيرًا من المحتالين، بل تعتمد على الذكاء والاحترافية

في استغلال الضحايا من خلال خبرتهم في التعامل مع الإنترنت. كما أن هذه الأساليب غالبًا لا تترك أثرًا ماديًا واضحًا، مما يجعل تتبع المحتالين أمرًا صعبًا.[17]

ب. الهندسة الاجتماعية المعتمدة على العنصر البشري

يرتكز هذا النوع من الهندسة الاجتماعية على التلاعب المباشر بالأفراد في الواقع الفعلي، دون الحاجة إلى استخدام التكنولوجيا، حيث يعتمد المحتال على الخداع والحيل المختلفة لخداع الضحية. ومن أبرز أساليبه ما يلي:

1. الانتحال: يتمثل في انتحال هوية شخص آخر أو اختلاق مواقف وهمية بهدف إقناع الضحية بالإفصاح عن معلومات شخصية، مثل الاسم أو تاريخ الميلاد، والتي يمكن استخدامها لاحقًا لأغراض احتيالية.
2. استغلال المهملات: يحدث ذلك عندما يتخلص الضحايا من أوراق أو مستندات تحتوي على معلومات شخصية دون إتلافها، مثل الفواتير التي تحمل بياناتهم أو صناديق الشحن التي لا تزال تحمل ملصقات بمعلوماتهم، مما يمنح المحتالين فرصة للحصول على هذه البيانات واستغلالها.
3. التجسس والتنصت: يعتمد هذا الأسلوب على مراقبة الضحية أثناء إدخال كلمات المرور أو البيانات الحساسة، أو التنصت على مكالماته الهاتفية بهدف جمع معلومات يمكن استخدامها في عمليات الاحتيال أو السرقة.[18]

المبحث الثالث: استراتيجيات التصدي للهندسة الاجتماعية/ المطلب الاول :الحماية من هجمات الهندسة الاجتماعية

إن الوقاية والحماية من الهجمات الهندسية الاجتماعية في هذا العصر تحتاج جهودًا مشتركة ما بين الأفراد والشركات والدولة على المستوى المحلي والعالمي، ومنها ما هو موضح في الآتي:

1. التعاون الدولي من خلال الاستفادة من خبرات الدول المتقدمة في كيفية مواجهة هجمات الهندسة الاجتماعية، والعمل على سن القوانين الدولية التي تعين على تسليم المجرمين المحتالين دوليًا.
2. يجب على الدولة أن تقوم بالدور التوعوي والتثقيفي للأفراد، لتعليمهم كيفية التصدي لهجمات الهندسة الاجتماعية، وتنويرهم بمخاطر وسائل الاحتيال المعاصرة.
3. يجب على المؤسسات تثقيف موظفيها بمجال الأمن المعلوماتي وكيفية التصدي للاختراقات، وتدريبهم على الحفاظ على سرية المعلومات، إلا بعد التأكد من هوية الشخص ووفقًا للحد المسموح به.[19]
4. يجب على المؤسسات أن تضع حماية أمنية تمنع الأشخاص غير العاملين في المؤسسة من الدخول إليها، كما يجب تنبيه الموظفين بعدم استخدام الأجهزة الإلكترونية الخاصة بالشركة إلا في حدود العمل المطلوب، وعدم الدخول إلى مواقع إلكترونية غير موثوقة، منعًا للفيروسات التي قد تؤدي إلى اختراق نظام الشركة والاستيلاء على معلوماتها وبياناتها السرية.

5. يجب وضع برامج الحماية التي تعين على سد الثغرات التي قد يستغلها المخترق لاختراق جهاز الضحية والاستيلاء على معلوماته وبياناته.
6. عدم الرد على الأرقام غير المعروفة لدى الشخص، وبالأخص المكالمات الدولية، إلا للضرورة، مع استحضار فكرة عدم الكشف عن المعلومات والبيانات في الهاتف حتى لا يستغلها المتصل لتنفيذ احتياله.[20]

مراحل هجمات الهندسة الاجتماعية :

عادةً ما يعتمد المهاجم في تنفيذ الهجمات الاجتماعية على مجموعة من المراحل المتسلسلة والمتكررة على النحو التالي:[21]

1.جمع المعلومات وتحديد الهدف: في هذه المرحلة، يقوم المهاجم بجمع أكبر قدر ممكن من المعلومات حول الضحية من مصادر متنوعة مثل مواقع التواصل الاجتماعي، المدونات، والموقع الإلكتروني الخاص بالمؤسسة. قد يلجأ المهاجم أيضًا إلى البحث في سلة المهملات للحصول على معلومات إضافية. تُعد هذه المرحلة الأساس لنجاح الهجوم الاجتماعي، حيث يعتمد عليها تحديد الضحية المستهدفة بعد اكتمال جمع المعلومات، تمهيداً لبناء وتطوير العلاقة في المرحلة التالية.[22]

2.تطوير العلاقة: بعد اختيار الضحية، يبدأ المهاجم في بناء علاقة معها واستغلال نقاط ضعفها، مثل العاطفة أو الثقة، لتطوير هذه العلاقة. الهدف من هذه المرحلة هو استخراج المعلومات الحساسة التي يحتاجها المهاجم، مثل بيانات الحسابات المصرفية، أرقام البطاقات الائتمانية، أو معلومات الدخول إلى الحسابات.

3.استغلال العلاقة: بمجرد أن يتمكن المهاجم من بناء وتطوير العلاقة مع الضحية، يبدأ في استغلال هذه العلاقة لصالحه للوصول إلى المعلومات أو البيانات التي يحتاجها.

4.التنفيذ والوصول إلى الهدف: في هذه المرحلة، يقوم المهاجم بتنفيذ خطته للوصول إلى الهدف النهائي. إذا لم يحقق النتائج المرجوة، قد يلجأ إلى تكرار المراحل السابقة لتحسين فرص النجاح.

5. مرحلة الهروب: بعد تحقيق أهدافه، يعمل المهاجم على إخفاء أي دليل قد يكشف هويته. قد يشمل ذلك إزالة البرامج الضارة التي تم تثبيتها أو حذف سجلات التواصل مع الضحية، وذلك لتجنب التتبع أو التعرف عليه لاحقًا. يوضح الشكل التالي المراحل الأساسية لدورة حياة الهجوم الاجتماعي.[23]

لذلك، أُطلق على الهندسة الاجتماعية مصطلح "علم أو فن اختراق العقول"، وقد ازدادت خطورتها في السنوات الأخيرة نتيجة النمو الهائل والمتسارع لشبكات التواصل الاجتماعي والبريد الإلكتروني ووسائل الاتصال الإلكترونية الأخرى. أصبح هذا المصطلح يستخدم على نطاق واسع للإشارة إلى

مجموعة من الأساليب التي يعتمد عليها المجرمون للحصول على معلومات حساسة أو لإقناع الضحايا المستهدفين باتخاذ إجراءات تسهّل اختراق أنظمتهم وإلحاق الضرر بها.[24]

انماط الهندسة الاجتماعية:

توجد أربعة أنماط رئيسية لتهديدات الهندسة الاجتماعية وهي كالتالي:[25]

1. هجمات الحرمان من الخدمة: تعتمد على إرسال عدد هائل من الطلبات إلى خوادم الضحية، بحيث تتجاوز قدرة الخادم أو الجهاز على التعامل معها، مما يؤدي إلى تعطيله جزئيًا أو كليًا أو إلى تباطؤ أدائه. هذا الهجوم يضر المستخدم النهائي ويستخدم غالبًا ضد مواقع الإنترنت أو البنوك أو المؤسسات بهدف التأثير عليها أو ابتزازها ماليًا.[26]
2. إتلاف أو تعديل المعلومات: يتمثل في اختراق معلومات الضحية عبر الإنترنت أو الشبكات الخاصة، وتعديل البيانات المهمة دون أن يلاحظ الضحية ذلك. رغم بقاء البيانات، تصبح مضللة وقد تؤدي إلى عواقب خطيرة لصاحبها.[27]
3. التجسس على الشبكات: يشير إلى الوصول غير المصرح به إلى شبكات الضحية بهدف التجسس والحصول على معلومات هامة، دون إلحاق أي ضرر بالبيانات أو تعديلها.[28]
4. تدمير المعلومات: في هذه الحالة، يتم حذف أو تدمير كامل للبيانات والمعلومات المخزنة على الشبكة، ويُعرف هذا النوع من الهجمات بـ"تهديد سلامة المحتوى"، حيث يتم تغيير البيانات أو حذفها بالكامل.[29]

المطلب الثاني : تعزيز الوعي الامني والتدريب

وسائل التحصين الأمني من أساليب الهندسة الاجتماعية للأفراد والمؤسسات تلعب دورًا هامًا في حماية المعلومات ونظمها من الوصول غير المصرح به، أو الاستخدام غير المشروع، أو التعطيل، أو التدمير، سواء أثناء التخزين أو المعالجة أو النقل. كما تحمي هذه الوسائل من حرمان المستخدمين المرخص لهم من الخدمة. يشمل أمن المعلومات مجموعة من التدابير اللازمة لاكتشاف التهديدات وتوثيقها ومواجهتها، إضافة إلى إجراءات أمان مادية واسعة النطاق، مثل حماية أصول المؤسسة المعلوماتية من الكوارث الطبيعية، والسرقة، وهجمات الهندسة الاجتماعية.[30]

ويوصي خبراء أمن المعلومات بمجموعة من الإرشادات التي ينبغي اتباعها لتفادي الوقوع ضحية لأساليب الهندسة الاجتماعية.[31]

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

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

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

4- التأكيد على ضرورة إتلاف الأوراق والمستندات المهمة بواسطة أجهزة مخصصة لهذا الغرض.

5- تجنب كل الرسائل الإلكترونية التي تحتوي على روابط مشبوهة في البريد الإلكتروني أو رسائل الجوال أو على المواقع الاجتماعية.

تنمية المهارات الرقمية كوسيلة لتعزيز الوعي الأمني

يُعد تطوير المهارات الرقمية بمستوياتها المختلفة (الأساسية، المتوسطة، والمتقدمة) عاملاً رئيسياً في تعزيز الوعي الأمني والتصدي لهجمات الهندسة الاجتماعية. فكلما زادت قدرة الأفراد على التعامل مع التقنيات وفهم مخاطرها، أصبحوا أكثر وعياً بتهديدات الأمن السيبراني. يساعد التدريب المستمر على المهارات الرقمية في تمكين الأفراد من حماية بياناتهم والتعامل بحذر مع محاولات الاحتيال والتصيد، مما يسهم في بناء بيئة رقمية أكثر أماناً.

1. المهارات الأساسية

تشمل المهارات الرقمية الأساسية القدرة على استخدام الأجهزة والبرمجيات، مثل إدارة الملفات، إعدادات الخصوصية، والتعامل مع البريد الإلكتروني. يساعد إتقان هذه المهارات في تقليل مخاطر الهجمات التي تستغل نقص الوعي الرقمي، مثل التصيد الاحتيالي.[32]

2. المهارات المتوسطة

تمكن الأفراد من استخدام التكنولوجيا بفعالية، مثل التصميم الرقمي والتسويق الإلكتروني، مع القدرة على تحليل البيانات وإنتاج المحتوى الرقمي. هذه المهارات ضرورية في سوق العمل وتساعد في التكيف مع التطورات التكنولوجية المتسارعة.[33]

3. المهارات المتقدمة

تتطلبها التخصصات التقنية مثل البرمجة، الأمن السيبراني، وتحليل البيانات الضخمة. مع تزايد الطلب على هذه المهارات عالميًا، توفر وظائف ذات رواتب مرتفعة، لكنها تتطلب تعليماً متخصصاً وتدريباً مستمراً لمواكبة التطورات.[34]

من أهم وسائل التحصين الأمني ضد أساليب الهندسة الاجتماعية هي :

1. السياسة الأمنية: هي وثيقة مكتوبة بعناية تهدف إلى تحديد نهج شامل يجمع بين الجوانب التقنية وغير التقنية. يجب أن تكون هذه السياسة مدمجة في الأهداف التشغيلية للمنظمة لضمان تحقيق الأمن الشامل.[35]

2. التعليم والتدريب: من الضروري أن يلتزم الموظفون بحضور التدريبات المطلوبة لتعزيز وعيهم الأمني. كما ينبغي على المنظمات تنظيم دورات تدريبية تنشيطية بشكل دوري لضمان استمرارية التعلم وتحسين الكفاءة الأمنية.
3. توجيه شبكة الاتصال: يجب أن تضع المنظمة خطة شاملة لحماية شبكة الاتصال، تتضمن تحديد المواقع الموثوقة وتعطيل التطبيقات والمنافذ غير المستخدمة. كما ينبغي على مستخدمي الشبكة الالتزام باستخدام كلمات مرور معقدة يتم تغييرها بشكل دوري كل 90 يومًا.[36]
4. مراجعة الحسابات: يجب على المنظمات ذات الأنشطة الفاعلة التحقق بشكل دوري من الالتزام بسياسة الأمن، مع التركيز على الجوانب الحيوية المتعلقة بأمن الأفراد والمنظمة.[37]

النتائج:

1. تزايد استخدام أساليب الهندسة الاجتماعية: يتزايد استخدام المهاجمين لأساليب الهندسة الاجتماعية في العصر الرقمي نتيجة للاعتماد على تقنيات متقدمة للاحتيال والتلاعب بالأفراد والمؤسسات عبر الإنترنت، مما يشكل تهديدًا حقيقيًا للأمن السيبراني.
2. التأثير السلبي على الأفراد والمؤسسات: تتراوح تأثيرات الهجمات الهندسية الاجتماعية بين سرقة البيانات الشخصية، تهديد الأنظمة الإلكترونية الحساسة، والتلاعب بالمعلومات التي قد تؤدي إلى خسائر مالية وسمعة مؤسساتية.
3. الاختلافات بين الأساليب التقليدية والرقمية: تطورت أساليب الهندسة الاجتماعية من الخداع التقليدي إلى الهجمات الإلكترونية المعقدة، مما يعكس التقدم التكنولوجي واستخدام وسائل التواصل الاجتماعي في جمع المعلومات الحساسة.
4. الوعي الأمني: يشير البحث إلى أن ضعف الوعي الأمني لدى الأفراد والموظفين في المؤسسات يعد من أكبر العوامل المساعدة في نجاح هذه الهجمات.

التوصيات:

1. تعزيز الوعي الأمني: ينبغي على المؤسسات والأفراد تعزيز الوعي الأمني من خلال تنظيم دورات تدريبية وورش عمل مستمرة لرفع مستوى الفهم حول أساليب الهندسة الاجتماعية وتوعية الجميع بأساليب الحماية الفعالة.
2. تطوير سياسات الأمان: يجب على المؤسسات وضع سياسات أمنية شاملة لضمان استخدام تقنيات وتدابير أمان موثوقة لحماية البيانات الحساسة.
3. استخدام أدوات أمنية متقدمة: يُوصى بتطبيق أنظمة مكافحة التصيد الاحتيالي (Phishing) وبرمجيات كشف الاحتيال على الشبكات والأنظمة الرقمية بشكل مستمر.
4. التعاون بين المؤسسات: يجب أن يتعاون القطاع الخاص والعام لمشاركة المعلومات حول تهديدات الأمن السيبراني وتطوير استراتيجيات مشتركة للتصدي للهجمات الهندسية الاجتماعية.

المصادر العربية :

1. أيمن عبدالله فكري، الجرائم المعلوماتية، مكتبة القانون الاقتصادي، ط1، السعودية، الرياض، 2014، ص351.
2. اكرم المشهداني، الجرائم الالكترونية التحديات وسبل المعالجة، مجلة الدراسات المالية والمصرفية، المجلد 23، العدد 1، 2015، ص25.
3. أسامة سمير حسين، الاحتيال الالكتروني، ط1، الجنادرية للنشر والتوزيع، 2011، ص148.
4. الحبابي مبارك الحبابي، دور إدارة المعرفة في مواجهة الهندسة الاجتماعية، المجلة العربية للنشر العلمي، العدد 68، جامعة الملك عبد العزيز، السعودية، 2024، ص455.
5. ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي، المركز العربي للنشر والتوزيع، ط1، مصر، القاهرة، 2017، ص38.
6. ضرغام جابر عطوش آل مواش، مصدر سابق، ص53.
7. سعد عبد القادر ماهر، الظل الرقمي، الطبعة الأولى، 2024، ص145.
8. سامي مرزوق نجاد المطيري، المسؤولية الجنائية عن الابتزاز الالكتروني في النظام السعودي: دراسة مقارنة، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، الرياض، 2015، ص38.
9. ساري محمد الخالد، اتجاهات في أمن المعلومات وأمانها، نشر وتوزيع العبيكان، ط1، السعودية، الرياض، 2018، ص169.
10. سهام حسن علي الشمري، تمظهرات الأمن السيبراني والممارسة الإعلامية وعلاقتهما بصناعة الحرب النفسية الافتراضية، مجلة دراسات دولية، العدد 83، جامعة بغداد، العراق، 2020.
11. شايب كمال، قيدة عبد الرؤوف، أخطار الهندسة الاجتماعية على المستهلك الإلكتروني، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي، المركز الجامعي عبد الحفيظ بو الصوف، الجزائر، 23 – 24 نيسان، 2018.
12. صالح خليل، الجرائم المستحدثة بطرق غير مشروعة لشبكة الإنترنت، ط1، دار النهضة العربية، القاهرة، 2009، ص100.
13. عبد الحكيم، اكمل، الهندسة الاجتماعية لأغراض التوعية، صحيفة الاتحاد الإماراتية، 2013.
14. عبد الحي، حسام فايز، مشاركة الجمهور في تقنيات الهندسة الاجتماعية عبر موقع فيس بوك وعلاقتها بالخصوصية والتعويض النفسي لديهم، مجلة البحوث الإعلامية، العدد 55، جامعة الأزهر، مصر، 2020.
15. عبد القادر بن عبدالله الفنتوخ، الجريمة في الإنترنت وطرق الحماية منها، العبيكان للنشر والتوزيع، الرياض، 2012، ص93-98.
16. قريقر فتيحة، مخاطر التعامل الإلكتروني وآليات التعامل معها، مجلة الحقوق والعلوم الإنسانية، المجلد 11، العدد 1، 2018، ص249.
17. الكندي، سالم سعيد، والبلوشي، حليمة سليمان، الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان، مجلة العلوم والآداب الاجتماعية، جامعة السلطان قابوس، 2020، المجلد 11، العدد 2.
18. كريستوفر هادناجي، الهندسة الاجتماعية فن اختراق العقل البشري، ملخصات لكتب عالمية تصدر عن مؤسسة محمد بن راشد آل مكتوم للمعرفة، 2017، ص25.
19. ماجد رجب العبد سكر، التواصل الاجتماعي: أنواعه وآثاره ومعوقاته، الجامعة الإسلامية، غزة، 2011، ص103.

20. محمد أحمد، الهندسة الاجتماعية، مجلة المال والاقتصاد، العدد 75، 2014، ص23.
21. محمد جولزار، مراجعة أدبية متعددة الأصوات حول زيادة الهجمات/التهديدات الإلكترونية القائمة على الهندسة الاجتماعية خلال جائحة كوفيد-19: التحديات والحلول المستقبلية، مجلة IEEE Access، المجلد 9، 2021.
22. مها أحمد إبراهيم، الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي، المجلة الدولية لعلوم المكتبات والمعلومات، جامعة بني سويف، 2018، ص119.
23. ميشيل مافيزولي، نظام الأشياء: التفكير في ما بعد الحداثة، المركز العربي للأبحاث ودراسة السياسات، ط1، قطر، 2020، ص109.
24. يمنى طريف الخولي، ركائز في فلسفة السياسة، مؤسسة هنداوي سي أي سي، 2017، ص56.

المصادر الانكليزية:

1. Barbara R. Jones & Suzanne L. Flannigan, *Connecting the Digital Dots: Literacy of the 80st Century*, 2022.
2. C. Girón-García & I. Navarro i Ferrando, *Literacy and Metaphorical Models*, *Multidisciplinary Journal for Education*, 2021.
3. Conteh, Nabie & Schmick, Paul J., *Cyber security risks vulnerabilities and countermeasures to prevent social engineering attacks*, International Journal of Advanced Computer Research, Vol 6(23), USA, 2016.
4. Michael Alexander, *Methods for Understanding and Reducing Social Engineering Attacks*, SANS Institute, April 30, 2016, p.11.
5. MITNICK, KEVIN D. & Simon, William L., *THE ART OF DECEPTION: Controlling the Human Element of Security*, Foreword by Steve Wozniak, 2015.
6. Oxford University Press, *A Social Engineering Article*, *Mind*, England, 2020.
7. S. Gastellier-Prevost, G. Gonzalez Granadillo, & M. Laurent, *A dual approach to detect attacks at the client-side*, New Technologies, Mobility and Security (NTMS), 4th IFIP International Conference, IEEE, 2011, p.2.
8. Salahdine, Fatima & Kaabouch, Naima, *Social Engineering Attacks: A Survey*, Future Internet Journal, Vol. 11, No. 89, 2019.
9. Salahdine, F., & Kaabouch, N., *Social engineering attacks: A survey*, Future Internet, Vol (11), Iss (4), University of North Dakota, USA, 2019.

[1] ماجد رجب العبد سكر ، التواصل الاجتماعي أنواعو وآثاره ومعوقاته، الجامعة الإسلامية، غزة ، 2011، ص 103.

[2] أسامة سمير حسين، الاحتيال الالكتروني ،ط1، الجنادرية للنشر والتوزيع ،2011، ص148.

[3] عبد القادر بن عبدالله الفنتوخ ،الجريمة في لانترنت وطرق الحماية منها ، العبيكان للنشر والتوزيع ، الرياض ،2012، ص93-98.

[4] ميشيل مافيزولي، نظام الاشياء التفكير في ما بعد الحداثة ، المركز العربي للابحاث ودراسة السياسات ،ط1، قطر ، 2020، ص 109.

[5]مطبعة جامعة اكسفورد,مقال عن الهندسة الاجتماعية, مجلة,Mind، انجلترا ، Mind © 1947 Oxford 2020 . University Press

[6]يمنى طريف الخولي ، ركائز في فلسفة السياسة ، مؤسسة هنداوي سي أي سي ،2017،ص 56.

[7]مها أحمد ابراهيم محمد, الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي, دراسة تطبيقية, كلية الآداب, جامعة بني سويف, مصر , 2018،ص62.

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

[9] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future internet, Vol (11), Iss (4), University of North Dakota, USA.

[10] سامي مرزوق نجاد المطيري، المسؤولية الجنائية عن الابتزاز الالكتروني في النظام السعودي، دراسة مقارنة، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، كلية العدالة الجنائية، الرياض، 2015، ص38.

[11] صالح خليل، الجرائم المستحدثة بطرق غير مشروعة لشبكة الانترنيت،ط1، دار النهضة العربية، القاهرة، 2009، ص100.

[12] محمد ، جولزار. مراجعة أدبية متعددة الأصوات حول زيادة الهجمات/التهديدات الإلكترونية القائمة على الهندسة الاجتماعية خلال جائحة كوفيد-19: التحديات والحلول المستقبلية." مجلة IEEE Access، المجلد 9، 2021.

[13] اكرم المشهداني ،الجرائم الالكترونية التحديات وسبل المعالجة ،مجلة الدراسات المالية والمصرفية ،المجلد 23 العدد 1 ،2015 ،ص25.

[14] قريقر فتيحة ،مخاطر التعامل الالكتروني وآليات التعامل معها ، مجلة الحقوق والعلوم الانسانية ، المجلد11 ،العدد 1 ،2018،ص249.

[15] كريستوفر هادناجي ، الهندسة الاجتماعية فن اختراق العقل البشري ، ملخصات لكتب عالمية تصدر عن مؤسسة محمد بن راشد آل مكتوم للمعرفة،2017،ص25.

[16] مها محمد ، الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها في المجتمع العربي ، المؤتمر الثامن العشرون ، شبكات التواصل الاجتماعي وتأثيرها في مؤسسات المعلومات في الوطن العربي ، الاتحاد العربي للمكتبات والمعلومات ، القاهرة ، 2017،ص8.

[17] S. Gastellier-Prevost, G. Gonzalez Granadillo, and M. Laurent, "A dual approach to detect attacks at the client-side," New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference, IEEE, 2011, p. 2.

[18] محمد احمد ،الهندسة الاجتماعية ،مجلة المال والاقتصاد ،العدد 75، 2014،ص23.

[19] مها محمد ، الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها في المجتمع العربي ، مصدر سبق ذكره ،ص 9.

[20] محمد احمد ،الهندسة الاجتماعية ،مصدر سبق ذكره ص22.

[21] شايب كمال ، قيدة عبد الرؤوف ، أخطار الهندسة الاجتماعية على المستهلك الالكتروني، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي المركز الجامعي عبد الحفيظ بو الصوف ،الجزائر، 23 – 24 نيسان، 2018 .

[22] Michael Alexander, "Methods for Understanding and Reducing Social Engineering Attacks", SANS Institute, April 30, 2016, page11.

[23] الحبابي مبارك الحبابي ، دور ادارة المعرفة في مواجهة الهندسة الاجتماعية ، المجلة العربية للنشر العلمي ،العدد 68، جامعة الملك عبد العزيز ، السعودية ،2024،ص455.

[24] عبد الحي،حسام فايز،مشاركة الجمهور في تقنيات الهندسة الاجتماعية عبر موقع فيس بوك وعلاقتها بالخصوصية والتعويض النفسي لديهم، مجلة البحوث الإعلامية، العدد 55 ،جامعة الأزهر،مصر ، 2020.

[25] سهام حسن علي الشمري، تمظهرات الامن السيبراني والممارسة الإعلامية وعلاقتهما بصناعة الحرب النفسية الافتراضية، مجلة دراسات دولية، العدد 83،جامعة بغداد ،العراق ،2020.

[26] ساري محمد الخالد، اتجاهات في أمن المعلومات وأمانها ، نشر وتوزيع العبيكان ، ط1 ، السعودية ، الرياض ، 2018 ، ص 169.

[27] أيمن عبدالله فكري ، الجرائم المعلوماتية ،مكتبة القانون الاقتصادي ، ط1، السعودية ،الرياض ،2014، ص351.

[28] ضرغام جابر عطوش آل مواش ، جريمة التجسس المعلوماتي ، المركز العربي للنشروالتوزيع ، ط1،مصر ، القاهرة ،2017، ص 38.

[29] ضرغام جابر عطوش آل مواش ، مصدر سابق ، ص 53.

[30] الكندي، سالم سعيد والبلوشي، حليمه سليمان ، الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان،مجلة العلوم والاداب الاجتماعية، جامعة السلطان قابوس ، 2020، المجلد 11 ، العدد ٢.

[31] مها احمد إبراهيم، الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي، المجلة الدولية لعلوم المكتبات والمعلومات، جامعة بني سويف.،2018، ص 119.

[32] سعد عبد القادر ماهر ، الظل الرقمي ، الطبعة الاولى ، 2024، ص 145.

[33] Barbara R. Jones Suzanne L. Flannigan (2022): Connecting the Digital Dots: Literacy of the 80st Century

[34] C. Gir6n-Garcia , I. Navarro i Ferrando (2021): Literacy and Metaphorical Models .nell Models "Multidisciplinary Journal for Education.

[35] Conteh,Nabie & Schmick, Paul J. Cyber security risks vulnerabilities and countermeasures to prevent social engineering attacks, International Journal of Advanced.Computer Research,2016, Vol 6(23) USA.

[36] عبد الحكيم، اكمل ، الهندسة الاجتماعية لاغراض التوعية ،صحيفة الاتحاد الاماراتية ،2013.

[37] MITNICK, KEVIN D, & Simon, William L, (2015), THE ART OF DECEPTION Controlling the Human Element of Security, Foreword by Steve Wozniak.