الهندسة الاجتماعية بين استغلال الثغرات البشرية وبناء مجتمع واعٍ

Social Engineering : Between Human Vulnerability Exploitation and the Pursuit of Digital Awareness

رحيمة شخوم [*]، مخبر السياحة الإقليم والمؤسسات، جامعة غرداية (الجزائر)، chekhoum.rahima@univ-ghardaia.edu.dz

فاطمة زهرة عزوزة، مخبر السياحة الإقليم والمؤسسات، جامعة غرداية (الجزائر)، azzouza.fatima-zahra@univ-ghardaia.edu.dz

تاريخ الاستلام: 2025/08/17 تاريخ القبول: 2025/09/24 تاريخ النشر: 2025/09/30

ملخص:

تناولت هذه الدراسة ظاهرة الهندسة الاجتماعية بوصفها أحد أبرز التهديدات الأمنية التي تستغل الثغرات البشرية لاختراق الأنظمة والوصول إلى المعلومات الحساسة، عبر أساليب تعتمد على التلاعب النفسي والاجتماعي بدلًا من الاختراق التقني المباشر. وقد تم تحليل هذه الظاهرة باعتبارها سلاحًا ذو حدين، حيث تُستخدم في تنفيذ هجمات إلكترونية خادعة مثل التصيّد وانتحال الهوية، كما يمكن توظيفها لأغراض إيجابية في تعزيز التفاعل المجتمعي وبناء الثقة الرقمية

خلصت الدراسة أن التعامل مع تحديات الهندسة الاجتماعية يتطلب مقاربة شاملة تدمج بين التبعية المستمرة للأفراد والمؤسسات، وتطوير أدوات وتقنيات الحماية، إلى جانب ترسيخ ثقافة قائمة على التفكير النقدي. كما أبرزت الدراسة أن الجانب الإيجابي للهندسة الاجتماعية يمثل عنصرًا مهمًا في دعم جهود التنمية المستدامة، من خلال تصميم حملات توعية فعالة، وتعزيز القيم الأخلاقية، ونشر الوعي الرقمي.

كلمات مفتاحية: هندسة اجتماعية، مجتمع، انتحال هوية، ثغرات، مواقع الكترونية.

تصنيفات JEL : D83، D91، L86 ، K24 ، O33.

[*] **المؤلف المرسل.**

Abstract:

This study looks into social engineering as a significant security risk that takes advantage of human tendencies to get into systems without permission. Unlike hacking that targets technology, it uses psychology and social skills to influence people. The topic is seen as having two sides—it can be used for harmful actions like phishing and stealing identities, but it can also help build trust online and increase awareness about safety.

A good response, according to the study, requires constant learning, enhanced cybersecurity tools, and a willingness to think carefully. It also points out that social engineering can be helpful when used wisely, by promoting ethics, improving digital skills, and running well-planned campaigns to spread the message.

Keywords: Social Engineering, Society, Identity Theft, Vulnerabilities, Websites.

Jel Classification Codes : D83 ،D91 ،L86 ، K24 ، O33.

1. مقدمة:

في عصرنا الرقمي والاجتماعي الحديث، أصبحت المعلومات والبيانات من أثمن الموارد التي تحكم مصير الأفراد والمؤسسات والدول. ومع توسع الاعتماد على التكنولوجيا والاتصالات، برزت ظاهرة "الهندسة الاجتماعية" كأحد أخطر الأساليب التي تستهدف الإنسان نفسه، وليس فقط الأجهزة أو الأنظمة التقنية.

الهندسة الاجتماعية، بمعناها الواسع، هي فن وعلم التأثير على السلوك البشري، واستغلال نقاط الضعف النفسية والاجتماعية لتحقيق أهداف محددة. هذه الظاهرة تحمل في طياتها بعدين متناقضين: الأول هو الاستغلال الضار الذي يهدد الأمن الشخصي والمجتمعي، والثاني هو الاستخدام الإيجابي الذي يمكن أن يسهم في بناء مجتمع واع ومتماسك.

وفي هذه الورقة البحثية، سنقوم بتحليل معمق لكيفية استغلال الهندسة الاجتماعية للثغرات البشرية، ثم ننتقل إلى استعراض دورها في بناء مجتمع واعٍ، لنختم بتسليط الضوء على التحديات والفرص التي تواجه هذا التوازن الحيوي.

الإشكالية

كيف يمكن تحقيق التوازن بين مخاطر الهندسة الاجتماعية كأداة استغلال للثغرات البشرية، وإمكاناتها كأداة لبناء مجتمع واعٍ ومتماسك في العصر الرقمي؟

أهمية الدراسة:

تتمثل أهمية هذه الدراسة في إبراز الدور المتنامي للهندسة الاجتماعية في البيئة الرقمية المعاصرة، وذلك من خلال تسليط الضوء على قيمتها العلمية في توضيح الكيفية التي تستغل بها الثغرات النفسية والسلوكية لاختراق الأنظمة والمعلومات، وما يترتب على ذلك من تحديات أمام أمن الأفراد والمؤسسات. كما تكمن أهميتها العملية في قدرتها على المساهمة في تطوير استراتيجيات فعالة للتوعية والوقاية من الهجمات السيبرانية، إلى جانب إبراز الاستخدامات الإيجابية للهندسة الاجتماعية في تعزيز الثقافة الأمنية وبناء مجتمع أكثر وعيا بالمخاطر الرقمية. ومن ثم فإن الدراسة تسد فجوة معرفية بين الرؤى النظرية والتطبيقات العملية، بما يعزز من الجهود البحثية والممارسات الميدانية في مجال الأمن السيبراني.

أهداف الدراسة:

1. **التحليل العلمي** لظاهرة الهندسة الاجتماعية بوصفها سلاحًا ذو حدين.
2. **التوعية المجتمعية** بأساليب الحماية من الهجمات الخادعة.
3. **توظيف الأدوات النفسية والاجتماعية** لأغراض إيجابية مثل تعزيز القيم المجتمعية.
4. **رصد الأساليب الخبيثة** الشائعة (التصيد، انتحال الشخصية، الاصطياد الإغرائي).

المنهج المستخدم:

في إطار إعدادنا لهذه الورقة البحثية حول التوازن بين الأمن الاجتماعي والحرية الرقمية اعتمدنا على المنهج الوصفي إذ تطرقنا لظاهرة الهندسة الاجتماعية من حيث مفهومها أنواعها وأساليب استخدامها سواء الإيجابي أو السلبي، كما قمنا بتحليل ظاهرة الهندسة الاجتماعية مستخدمين المنهج التحليلي على أنها سلاح ذو حدين مع تقديم استراتيجيات للتعامل معها.

2. المحور الأول: الهندسة الاجتماعية كأداة استغلال للثغرات البشرية.

1.2 مفهوم الهندسة الاجتماعية في الاستغلال:

الهندسة الاجتماعية في هذا السياق هي مجموعة من التقنيات النفسية والاجتماعية التي يستخدمها المهاجمون لاستدراج الأفراد إلى تقديم معلومات حساسة أو اتخاذ إجراءات تضر بمصالحهم. (Bezuidenhout, F. Mouton, & H. S. Venter,, 2010, p. 1)

تتمحور عمليات الاحتيال القائمة على الهندسة الاجتماعية حول كيفية تفكير الناس وتصرفهم على هذا النحو، حيث تعد هجمات الهندسة الاجتماعية مفيدة بشكل خاص للتلاعب بسلوك المستخدم وهذا بمجرد أن يفهم المهاجم ما الذي يحفز تصرفات المستخدم، كما يمكنه من خداع المستخدم والتلاعب به بالإضافة إلى ذلك يحاول المتسللون استغلال افتقار المستخدم إلى المعرفة بفضل سرعة التكنولوجيا. (Administration, 2008, p. 1)

حيث لا يدرك العديد من المستهلكين والموظفين بعض التهديدات مثل تنزيل البرامج مجهولة المصدر، وقد لا يدرك المستخدمون أيضا القيمة الكاملة للبيانات الشخصية مثل أرقام هواتفهم ونتيجة لذلك فإن العديد من المستخدمين ليست لهم الدراية الكافية باختيار أفضل الطرق لحماية أنفسهم ومعلوماتهم. (معتصم، 2019)

بشكل عام يسعى مهاجمو الهندسة الاجتماعية إلى:

- تخريب وتعطيل البيانات أو إتلافها لإحداث ضرر أو إزعاج.
- سرقة المعلومات الشخصية للحصول على الأشياء الثمينة والأموال.

2.2 الثغرات النفسية والسلوكية المستهدفة:

تستهدف الهندسة الاجتماعية عدة ثغرات نفسية وسلوكية في الإنسان، من أهمها:

- الثقة في السلطة :يميل الإنسان بطبعه إلى احترام السلطة والامتثال لأوامرها، وهذا ما يستغله المحتالون بانتحال شخصيات رسمية أو موظفين في مؤسسات معروفة.
- التحفيز العاطفي :استثارة مشاعر الخوف، الطمع، التعاطف أو القلق تجعل الضحية أقل قدرة على التفكير النقدي، مما يسهل خداعه.
- التحيزات المعرفية :مثل تحيز التأكيد، حيث يبحث الإنسان عن المعلومات التي تدعم معتقداته، مما يجعله عرضة لتلقي معلومات مغلوطة دون تمحيص.
- الإلحاح والضغط الزمني :خلق شعور بالعجلة يدفع الضحية لاتخاذ قرارات متسرعة دون التأني، وهو أسلوب شائع في هجمات التصيد الاحتيالي. (مراد، 2017، صفحة 18)

هناك بعض الاستثناءات لهذه الثغرات، حيث في بعض الحالات يستخدم المهاجمون أساليب أكثر بساطة في الهندسة الاجتماعية للوصول إلى الشبكة أو الكمبيوتر، على سبيل المثال قد يتردد أحد المخترقين على قاعة الطعام العامة في مبنى إداري كبير به عدد معتبر من مستخدمي الولوج الجماعي للأنترنت (نشير هنا إلى وجود واي فاي مجاني) والذين يعملون على أجهزة الكمبيوتر اللوحية أو أجهزة الكمبيوتر المحمولة الخاصة بهم، ويمكن أن يؤدي القيام بذلك إلى تراكم عدد كبير من كلمات المرور وأسماء المستخدمين كل ذلك دون إرسال بريد إلكتروني أو كتابة سطر من رمز الفيروس.

3.2 أساليب الهندسة الاجتماعية الشائعة

تتعدد أساليب الهندسة الاجتماعية التي يستخدمها المهاجمون، ومن أبرزها: (سعيد، 2017، صفحة 78)

- **التصيد الاحتيالي** (Phishing): إرسال رسائل إلكترونية أو مكالمات هاتفية مزيفة تهدف إلى سرقة بيانات الدخول أو المعلومات الشخصية، وغالبًا ما تحتوي على روابط خبيثة أو مرفقات ضارة.

ومن أمثلته أن يقوم أحدهم بسرقة بعض بياناتك عبر معرفته بعنوان بريدك الإلكتروني وكلمة المرور الخاصة به. فقد تصلك رسالة بريد إلكتروني مزيفة تطلب منك تغيير كلمة المرور كإجراء احترازي لحمايتك من السرقة، وتُصاغ هذه الرسالة بطريقة مقنعة توهمك بأنها صادرة عن الشركة الرسمية. يتضمن البريد رابطًا يقودك إلى صفحة مزيفة مطابقة لتصميم صفحة تسجيل الدخول الحقيقية. وبمجرد إدخال معلوماتك، يتم حفظها لدى المحتال، ليستخدمها لاحقًا للحصول على بياناتك الشخصية وتنفيذ عمليات احتيال.

- **التذرع** (Pretexting): اختلاق قصة أو سيناريو للحصول على ثقة الضحية، مثل الادعاء بأنك من قسم الدعم الفني أو من جهة حكومية.
- **الاصطياد الإغرائي** (Baiting): تقديم عروض مغرية أو ملفات مجانية تحتوي على برمجيات خبيثة، تستغل فضول الضحية للوقوع في الفخ
- **المقايضة مقابل منفعة** (Quid Pro Quo): تقديم خدمة مزيفة مقابل معلومات أو وصول إلى النظام، كأن يعرض المهاجم مساعدة تقنية مقابل بيانات سرية.
- **التنصت**: الاستماع غير المصرح به للتواصل بين الأشخاص، سواء عبر الهاتف أو البريد الإلكتروني، للحصول على معلومات سرية.

ويُعد استغلال الهوية أحد الأساليب التي يُمكن للمحتالين من خلالها الوصول إلى المعلومات الشخصية، حيث يقوم بعض الأشخاص بإنشاء حساب مزيف على موقع فيسبوك مثلًا، ويتمكنون من الحصول على معلومات عنك من خلال أصدقائك. بعد ذلك، يُمكنهم استخدام هذه المعلومات لمحاولة الوصول إلى حسابك البنكي، إذ أن البيانات التي حصلوا عليها، مثل اسمك وتاريخ ومكان ميلادك ورقم هاتفك ومعلومات أخرى، قد تُستخدم للإجابة على بعض أسئلة الأمان التي تطرحها المواقع الإلكترونية، مثل:

- ✓ ما هو تاريخ ميلادك؟
- ✓ من هو أفضل صديق لديك؟
- ✓ ما نوع أول سيارة اشتريتها؟
- ✓ ما هو لونك المفضل؟

✓ ما اسم صديق ابنك؟

هناك العديد من حالات انتحال الهوية، مثل أن يقوم المحتال بإنشاء بريد إلكتروني يحمل اسم صديقك، ثم يرسل لك رسالة تحتوي على ملف خبيث يُستخدم لسرقة بيانات جهازك. كما يمكن إنشاء صفحات مزيفة تشبه تمامًا صفحات بعض مواقع التواصل الاجتماعي، بهدف خداع المستخدمين للحصول على بيانات تسجيل الدخول وكلمات المرور، ومن ثم استخدامها في تنفيذ عمليات احتيال. (سليماني و نقاز، 2020، صفحة 103)

4.2 مراحل هجوم الهندسة الاجتماعية

يمر هجوم الهندسة الاجتماعية بأربع مراحل رئيسية: (سامر، 2018، صفحة 55)

- **مرحلة البحث** :يجمع المهاجم أكبر كمية ممكنة من المعلومات عن الضحية من مصادر مختلفة (مواقع التواصل الاجتماعي، مواقع الويب، الوثائق المتاحة).
- **مرحلة الإيقاع في الشراك** :يبدأ المهاجم بالتواصل مع الضحية، يستخدم مهارات الإقناع والتمويه لاكتساب الثقة، ويختلق قصة مناسبة لخداع الضحية.
- **مرحلة اللعب** :يقوم المهاجم بتوسيع موطئ قدمه، ويبدأ في تنفيذ الهجوم للحصول على المعلومات أو تعطيل الأنظمة.
- **مرحلة الانسحاب** :بعد تحقيق الهدف، يحاول المهاجم إخفاء آثاره لتجنب الكشف والملاحقة.

5.2مخاطر الهندسة الاجتماعية

1- مخاطر تكنولوجية: أو رقمية أو نقول معلوماتية وتتمثل في اختراق الأنظمة المعلوماتية، وضرب البنية التحتية لارتكاب الجرائم الإلكترونية مثل نشر الشائعات، الأكاذيب، التجسس الإلكتروني، الإرهاب الإلكتروني، والحقائق المزيفة والمغلوطة.

2- مخاطر ثقافية: تتمثل في القضاء على الهوية الثقافية للمجتمع، وغرس سلوكيات غريبة ودخيلة على المجتمع، وتزييف الوعي واستعماره.

3- مخاطر اجتماعية: تتمثل في تهديد القيم والعادات الموجودة بالمجتمع مثل: التماسك الاجتماعي والانتماء والولاء، وحب الوطن والمحافظة على أراضيه.

4- مخاطر قومية: تتمثل في تهديد الأمن القومي للمجتمع، من خلال التشكيك في قدرات الشعب وقيادته، وتحريض الشعب ضد الجيش والشرطة والنظام الحاكم.

5- مخاطر سياسية: تتمثل في زعزعة استقرار الدولة، ونشر الفوضى وزيادة الاحتجاجات والاعتصامات، وتأجيج الصراعات الطائفية والعرقية والمذهبية في المجتمع.

6- مخاطر اقتصادية: تتمثل في زيادة مديونية الدولة، وضعف الاقتصاد القومي، وارتفاع معدل القروض الدولية، وتراجع الاستثمار المحلي والدولي، وضعف السياحة.

7-مخاطر نفسية: تتمثل في التوتر، والخجل، والإهمال، واللامبالاة، وفقدان الثقة بالنفس، والسلوك العدواني، وسهولة الاستثارة والحساسية الزائدة، بالإضافة إلى الغضب والصراع مع الآخرين، وصراع الفرد مع نفسه، وفقد العطف والحنان، وفقد السيطرة على النفس. (عنيشل و يحياوي، 2025، صفحة 06)

حيث وفي الآونة الأخيرة، بدأت الشركات تدرك بشكل متزايد المخاطر الناتجة عن الهندسة الاجتماعية، حتى أصبحت تُصنّف ضمن أعلى التهديدات الأمنية. على سبيل المثال، تعتبر شركة "**سادينتك** "من الشركات الرائدة في مجال أمن المعلومات، وتصدر سنويًا تقريرًا خاصًا بتهديدات أمن المعلومات.

وفي تقريرها الصادر في **أفريل 2017**، احتلت الهندسة الاجتماعية المرتبة الثانية ضمن الأسباب العشرة الرئيسية لاختراق البيانات خلال عام 2016، وذلك نتيجة سرقة الهوية .وهذا يُعد مؤشرًا واضحًا على أن المخاطر المرتبطة بالهندسة الاجتماعية في تزايد مستمر، لا سيما في ظل التطور التكنولوجي المتسارع. (سليماني و نقاز، 2020، صفحة 103)

6.2 دراسات حالة وأمثلة واقعية :

1/ إنشاء صفحة مزيفة Fake profiles وخداع الضحية المستهدفة

في جانفي 2017 تم استخدام حساب مزور تحت اسم Mia Ash على مواقع التواصل الاجتماعي Facebook LinkedIn DeviantArt Instagram على أساس أنها مصورة فوتوغرافية وقامت بنشر عدة صور وكتابات على صفحاتها لإضفاء نوع من الشرعية.

جاء ضمن التقرير الذي نشره باحثوا شركة Secure Works Counter Threat Unit في 2017 حول الهجمات التي تتعرض لها المؤسسات وجدوا أن العديد من الهجمات كانت تستهدف مؤسسات في الشرق الأوسط وشمال أفريقيا. وحسب الباحثين فإن المهاجم استخدم حساب LinkedIn المزور Min Ash» في شن هجمات الهندسة الاجتماعية وفق المراحل التالية:

1- إنشاء صفحة مزورة.

2- البحث عن الضحية في موقع LinkedIn للشركة المستهدفة.

3-إضافة الضحية والتواصل معه (لبناء العلاقة وكسب الثقة)؛ ثم تطوير العلاقة إلى مواقع أخرى Facebook واستخدام البريد الالكتروني وتطبيقات WhatsApp.

4- بعد مدة من استقرار العلاقة وكسب الثقة أرسل المهاجم ملف Microsoft Excel إلى الضحية عن طريق البريد الالكتروني للمؤسسة وطلب منه فتحه في مكان العمل وكانت النتيجة تسميم كل حواسيب المؤسسة ببرنامج خبيث «PupyRAT »واستطاع فيما بعد الولوج إلى بيانات المؤسسة.

(SecureWorks Counter , 2017).

2/حالة احتيال وتصيد عبر انتحال هوية DHL أستراليا، 2025

في يوليو 2025، تعرض العديد من المستخدمين في أستراليا إلى حملة تصيد إلكتروني واسعة استهدفتهم عبر رسائل بريد إلكتروني مزيفة تدعي أنها صادرة عن شركة الشحن العالمية DHL

Expressجاءت هذه الرسائل في سياق عمليات التسليم المتزايدة خلال مواسم الشراء عبر الإنترنت، حيث أبلغ المستلمون بضرورة "تأكيد عنوانهم البريدي" أو "دفع رسوم استيراد صغيرة" من أجل استلام طرودهم.

اعتمد المهاجمون على تقنيات الهندسة الاجتماعية لتضليل الضحايا، إذ استخدموا شعار DHL الرسمي وأسلوبا لغويا مشابها للخطاب المهني للشركة، كما أرسلت الرسائل من نطاقات بريدية مزيفة تحاكي العنوان الأصلي للشركة بمجرد النقر على الرابط المرفق يوجه المستخدمون إلى صفحات ويب مصممة بعناية لتشبه الموقع الرسمي لـDHL ، حيث يطلب منهم إدخال بيانات شخصية ومالية مثل أرقام البطاقات البنكية وتفاصيل الاعتماد.

رغم احترافية التصميم، كانت هناك مؤشرات مبكرة يمكن من خلالها كشف الاحتيال، من بينها: اختلاف طفيف في نطاق المرسل عن النطاق الرسمي للشركة، وجود روابط مختصرة أو مشبوهة، بالإضافة إلى الطلب غير المعتاد لإدخال بيانات مالية أو كلمات مرور لمجرد تتبع طرد. هذه العلامات تعد من مؤشرات التصيّد الشائعة التي غالبا ما تغفل عند التعامل تحت ضغط "العجلة" التي يتعمد المهاجمون خلقها.

أبرزت هذه الحادثة الحاجة إلى تعزيز أنظمة الحماية التقنية مثل تطبيق سياسات التحقق من البريد الإلكتروني (SPF/DKIM/DMARC) لمنع الانتحال، إلى جانب أهمية تدريب المستخدمين على التحقق من الروابط ومصداقية الرسائل المتعلقة بالشحن. كما أوصت جهات مختصة بضرورة تبني سياسات تحقق داخل المؤسسات التجارية، بحيث لا يتم إدخال أي بيانات بنكية أو اعتماد عبر روابط البريد الإلكتروني غير المؤكدة. (MailGuard، 2025)

3/حالة تصيد موجه ضد المديرين الماليين(2025)

كشفت تقارير أمنية عن حملة تصيّد موجه (Spear-Phishing) في مايو 2025 حيث استهدفت مديرين ماليين وتنفيذيين في مؤسسات مالية كبرى عبر العالم. اعتمد المهاجمون على رسائل بريد

إلكتروني مصممة بعناية تنتحل هوية شركة استشارات وتوظيف مرموقة، حيث عرضت على المستلمين "فرص مهنية قيادية" لجذب اهتمامهم. تضمنت الرسائل مرفقا بصيغة PDF يحيل إلى رابط مستضاف على منصة Firebase، والذي بدوره يقدّم ملفا مضغوطا (ZIP) يحتوي على سكريبت خبيث. عند تشغيله، يقوم السكريبت بتحميل أدوات وصول عن بعد مثل NetBird وOpenSSH، ما يمنح المهاجمين إمكانية التحكم في أنظمة الضحايا والوصول إلى بياناتهم الحساسة.

رغم أن الرسائل بدت مقنعة من حيث الشكل والأسلوب، إلا أن هناك مؤشرات مبكرة كان يمكن من خلالها كشف الاحتيال، مثل: استخدام روابط خارجية غير مرتبطة بالمجال الرسمي للشركات، الاعتماد على منصات طرف ثالث غير معتادة(Firebase) ، ووجود خطوات تقنية غير مبررة مثل طلب اجتياز CAPTCHAقبل الوصول إلى المحتوى. هذه العلامات، إلى جانب السياق غير المعتاد لعرض فرص عمل عبر ملفات مرفقة تبرز طبيعة الهندسة الاجتماعية في استغلال الثقة والتلاعب بتوقعات الضحايا. وكشفت هذه الحادثة عن مستوى التطور الذي بلغته هجمات التصيد الموجه، وعن خطورتها بشكل خاص على القيادات المالية التي تمتلك صلاحيات حساسة. وقد أوصى الخبراء بضرورة تعزيز آليات الحماية مثل المصادقة المتعددة العوامل، وإجراء دورات تدريبية متخصصة للتنفيذيين حول الهجمات المستهدفة. (Dive، 2025)

7.2 الآثار السلبية للهندسة الاجتماعية على الأفراد والمجتمع

- **خسائر مالية ضخمة** :يتعرض الأفراد والمؤسسات لخسائر مالية نتيجة الاحتيال أو سرقة البيانات.
- **تدمير الثقة** :يؤدي انتشار هذه الهجمات إلى تراجع الثقة بين أفراد المجتمع والمؤسسات، وهو ما يضر بالنسيج الاجتماعي.
- **تهديد الأمن القومي** :قد تؤدي تسريب المعلومات الحساسة إلى تهديد الأمن القومي، خاصة إذا استُخدمت في هجمات سيبرانية ضد البنى التحتية الحيوية.

- **التأثير النفسي** :يعاني الضحايا من آثار نفسية سلبية مثل القلق، فقدان الثقة بالنفس، والشعور بالعجز. (Dhull و Sumedha Singh، 2016، صفحة 67)

3. المحور الثاني: الهندسة الاجتماعية كأداة لبناء مجتمع واعٍ

1.3 إعادة تعريف الهندسة الاجتماعية في السياق الإيجابي:

الهندسة الاجتماعية ليست حكراً على الاستغلال، بل يمكن استخدامها كأداة فعالة لتشكيل السلوكيات الإيجابية، وتعزيز القيم المجتمعية، وبناء وعي جماعي قادر على مواجهة التحديات. وفي هذا السياق، تُعرف الهندسة الاجتماعية بأنها عملية مدروسة لتشكيل السلوك الجماعي للأفراد بهدف تحقيق أهداف اجتماعية إيجابية، مثل تعزيز التعاون والاحترام المتبادل. (عبد العزيز، 2017، صفحة 19)

2.3 الأهداف الاجتماعية الإيجابية للهندسة الاجتماعية:

- **تعزيز قيم التسامح والتعاون** :بناء مجتمع متماسك قادر على التعايش السلمي.
- **تنمية مهارات التفكير النقدي** :تمكين الأفراد من تحليل المعلومات واتخاذ قرارات واعية.
- **تشجيع المشاركة المجتمعية** :تحفيز العمل التطوعي والمبادرات المجتمعية.
- **الالتزام بالقوانين والنظم** :تسهم القواسم المشتركة للمجتمع في بقائه واستمراره ونموه والحفاظ على خصوصيته عند التعرض للتهديدات (العنبكي، 2025، صفحة 636)، وهي بدورها تساعد على تعزيز احترام القوانين للحفاظ على النظام والاستقرار.

3.3 دور التعليم في الهندسة الاجتماعية الإيجابية:

يعتبر الفضاء الرقمي بيئة تفاعلية تجمع بين الأفراد من مختلف الثقافات والخلفيات الاجتماعية، ومن خلال دراسة تأثيرات الهندسة الاجتماعية يتمكن الباحثين في مجال علم الاجتماع من فهم كيفية تأثير هذه العمليات على التفاعلات الاجتماعية وتشكيل العلاقات بين الأفراد في المجتمع (صالح محمد حسن و عبد الرحمان، 2024، صفحة 14)، حيث أن للتعليم في الهندسة الاجتماعية عدة إيجابيات نذكر منها:

- **إدماج مهارات الحياة والقيم الأخلاقية** :في المناهج الدراسية لتنشئة أجيال واعية.
- **تطوير برامج تعليمية تفاعلية** :تَبني الوعي الأمني والرقمي، وتعلّم مهارات الحماية من الاحتيال.
- **تدريب المعلمين** :على طرق التأثير الإيجابي في سلوك الطلاب، واستخدام الهندسة الاجتماعية في التوجيه والتربية.

4.3 دور الأسرة والمجتمع المدني:

- **الأسرة** :كنواة أساسية لبناء القيم والسلوكيات، وتعزيز الثقة بالنفس والوعي.
- **منظمات المجتمع المدني** :تلعب دورًا فعالًا في نشر الوعي والتثقيف وتعمل على تحديد توجهات ومسارات وسلوكيات أفراده (العنبكي، 2025، صفحة 630) ، وتنظيم حملات توعية.
- **المبادرات المجتمعية** :تعزز روح الانتماء والمسؤولية الاجتماعية، وتدعم بناء مجتمع متماسك.

5.3 الدعم النفسي والاجتماعي:

الطبيعة البشرية هي مجموعة من الخصائص النفسية على المستوى الكلي تصف السمات النفسية الأساسية التي يشترك فيها الكائن البشري بأكمله بشكل طبيعي، حيث توجد بعض السمات البشرية عبارة عن

ثغرات أمنية يمكن استغلالها في هجمات الهندسة الاجتماعية؛ كما وتساهم السمات الشخصية للأفراد بشكل كبير في قابليتهم لاستغلال الهندسة الاجتماعية مثل التأثير والتلاعب والخداع. ويتعامل المهندسون الاجتماعيون مع سمات الشخصية البشرية على أنها نقاط ضعف ويستخدمون اللغة كسلاح لخداع الضحايا وإقناعهم والتلاعب بهم في النهاية (HUSSEIN FALAH & MOHAMED Ferhat, 2024, p. 3).

مما سبق تظهر جليا أهمية الدعم النفسي والاجتماعي في حماية الأفراد وتعزيز الثقة بالنفس من خلال ما يلي:

- **برامج الدعم النفسي**: والتي تلعب دورا في تعزيز الثقة بالنفس والقدرة على مقاومة الاستغلال.
- **شبكات الدعم الاجتماعي** :تحمي الأفراد من العزلة والضعف، وتوفّر بيئة آمنة للتعلم والنمو.

3.6 التعاون بين الهندسة الاجتماعية والتقنيات الأمنية:

وبهدف تعزيز الأمن السيبراني لمواجهة مخاطر الهندسة الاجتماعية سعت الدول لتوفير إطار قانوني وتقنيات أمنية لحماية البيانات والأفراد نذكر مثالا على ذلك:

1. في إطار الجهود التشريعية لتعزيز الأمن السيبراني، أصدرت دولة الكويت القانون رقم (37) لسنة 2014 المتعلق بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات، حيث تضمّن هذا القانون أحكامًا خاصة بإنشاء مركز وطني معني بحماية البنية التحتية للمعلومات الحرجة،

وذلك من خلال المادة 70 التي شددت على ضرورة مكافحة إساءة استخدام وسائل الاتصال وحماية الأنظمة المعلوماتية الحيوية. (Kuwait, 2014, p. 52)

2. التنبيهات والتهديدات السيبرانية وإشعارات التدابير المضادة الصادرة عن .CERT-In (الفريق الوطني للاستجابة لحوادث أمن المعلومات في الهند، يصدر تنبيهات وتحذيرات وإشعارات تدابير مضادة). (Government of India, 2022, p. 01)

3. إصدار توجيهات بشأن الواجبات والمسؤوليات الأساسية لكبير مسؤولي أمن المعلومات (CISOs) في مجال حماية التطبيقات/البنية التحتية والامتثال.

4. إجراء عمليات تدقيق منتظمة قبل وبعد التدقيق في المواقع الإلكترونية والتطبيقات الحكومية.

5. إنشاء منظومة تدقيق أمني تدعم وتدقق في تنفيذ أفضل الممارسات في مجال أمن المعلومات.

6. تصميم خطة إدارة الأزمات للاعتداءات السيبرانية.

7. إجراء تدريبات منتظمة للأمن السيبراني ومحاكاة لاختبار الموقف الأمني للمؤسسات الحكومية ومؤسسات القطاع الحيوي واستعداداتها.

8. إجراء برامج تدريبية متكررة حول أمن البنية التحتية للمعلومات والتهديدات السيبرانية لمسؤولي الشبكات/النظم، والوكالات الحكومية ورؤساء الإدارات الرئيسية. (Aboalhab و Farhat، 2024، صفحة 8)

4. المحور الثالث: التوازن بين الاستغلال والبناء: تحديات وفرص

1.4 التحديات التي تواجه الهندسة الاجتماعية:

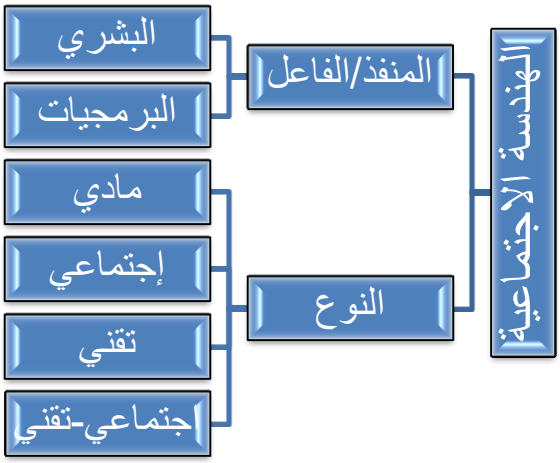
- **التطور المستمر في أساليب الهجوم** :مما يتطلب تحديث مستمر في استراتيجيات الحماية خاصة مع ظهور فئات من المجرمين أكثر تطورا كالعاملين مثلا على أجهزة الكمبيوتر قد يكونون مهندسين، محللي النظم، مبرمجين، أو حتى مشغلي البرامج الرقمية. (أحمد محمد عبد الرؤوف، 2021، صفحة 07).
- **ضعف الوعي الرقمي والأمني** :بين شرائح واسعة من المجتمع، مما يزيد من تعرضهم للهجمات. (Švehla, Sedinić , & Pauk, 2016, p. 1419)
- **نقص البرامج التوعوية والتعليمية:** المتخصصة في مجال الهندسة الاجتماعية.
- **صعوبة مراقبة وتنظيم المحتوى الرقمي**:خاصة مع انتشار وسائل التواصل الاجتماعي والمنصات.

4.2 الفرص المتاحة لتعزيز الهندسة الاجتماعية الإيجابية:

- **تطوير برامج تدريبية متخصصة** :للأفراد والمؤسسات لرفع مستوى الوعي الأمني.
- **تعزيز التعاون بين الجهات الحكومية والخاصة** :في مجال الأمن السيبراني والتوعية.
- **استثمار التكنولوجيا الحديثة** :لبناء منصات توعية ذكية وتفاعلية.
- **تشجيع البحث العلمي** :في مجال السلوكيات الاجتماعية والأمن الرقمي لتطوير حلول مبتكرة.

يعتمد تعزيز الهندسة الاجتماعية الإيجابية على تطوير البرامج وتشجيع البحث العلمي في هذا المجال، وفي بحثه حول تصنيفات الهندسة الاجتماعية قام **كرمبولز KREMBHOLZ** بتصنيفها إلى ما يلي:

الشكل رقم (01): يوضح التصنيفات المختلفة للهندسة الاجتماعية حسب كرمبولز KREMBHOLZ



Source : (KROMBHOLZ & AL, 2015),

لقد صنف كرومبولز الهندسة الاجتماعية حسب الفاعل والذي يمكن أن يكون مصدره إما عاملا بشريا أو من البرمجيات ، بينما صنف أنواعها إلى عنصر مادي أو اجتماعي أو تقني كما يمكن أن يجتمع العنصر الاجتماعي والتقني معا.

4.3 استراتيجيات مقترحة لتحقيق التوازن:

- **تبني منهجيات شاملة** :تجمع بين التوعية، الحماية، والتعليم المستمر.
- **بناء ثقافة مجتمعية** :قائمة على الشفافية والمسؤولية الاجتماعية.
- **دعم الابتكار** :في مجال الأمن السيبراني والتعليم الرقمي.
- **إشراك جميع فئات المجتمع** :في برامج التوعية لضمان وصول الرسائل للجميع.
- **تفعيل قوانين الجرائم الالكترونية وانتهاك الخصوصية بشكل فعال**: وذلك لتعزيز مواجهة وردع الاختراقات والانتهاكات (مها محمد، 2018، صفحة 126).

5. خاتمة:

في ختام هذه الورقة البحثية، يمكننا التأكيد على أن الهندسة الاجتماعية تمثل ظاهرة معقدة ذات وجوه متعددة، تجمع بين الخطر والفرصة في آن واحد. فمن ناحية، تظل أداة خطيرة في يد المخترقين والمحتالين الذين يستغلون الثغرات النفسية والاجتماعية لاختراق الأنظمة وسرقة البيانات. ومن ناحية أخرى، يمكن توظيف مبادئها لبناء مجتمع أكثر وعيا وتماسكا.

إن تحقيق التوازن المنشود بين مخاطر الهندسة الاجتماعية وإمكاناتها البناءة يتطلب تعاوناً وثيقاً بين جميع الأطراف: الأفراد، المؤسسات، الحكومات، والمجتمع المدني. فقط من خلال هذا التعاون يمكننا تحويل التحديات إلى فرص، والتهديدات إلى إنجازات، لبناء مستقبل رقمي آمن ومجتمع واعٍ قادر على مواكبة متغيرات العصر.

انطلاقا من الأهداف التي سعت إليها هذه الدراسة في تحليل ظاهرة الهندسة الاجتماعية من جوانبها المختلفة، تم التوصل إلى مجموعة من النتائج التي تبرز طبيعة هذه الظاهرة كتهديد أمني متنام، وفي الوقت نفسه كأداة يمكن توظيفها إيجابيا لبناء وعي رقمي مسؤول. وقد جاءت هذه النتائج لتسهم في سد فجوة معرفية تتعلق بالبعد الإنساني للأمن السيبراني، ولتدعم النقاش الأكاديمي والممارسات العملية في هذا المجال.

- أكدت الدراسة أن **الهندسة الاجتماعية تمثل سلاحا ذا حدّين**؛ فهي من جهة أداة خطيرة يستغلها المهاجمون لاختراق الأنظمة وسرقة البيانات عبر الثغرات البشرية، ومن جهة أخرى يمكن توظيفها في **تعزيز الثقة الرقمية وبناء مجتمع أكثر وعيًا**.
- وأظهرت النتائج أن **المخاطر المرتبطة بالهندسة الاجتماعية تتجاوز الجانب التقني** لتشمل أبعادًا ثقافية، اجتماعية، اقتصادية ونفسية، مما يضاعف من خطورتها على الأفراد والمجتمعات.
- بيّنت الدراسة أن نجاح الهجمات يعود بالأساس إلى **ضعف الوعي الرقمي، ونقص البرامج التوعوية**، إضافة إلى اعتماد الأفراد على الثقة العفوية والتأثر بالعوامل النفسية والعاطفية.
- أبرزت الدراسة أن الجانب الإيجابي للهندسة الاجتماعية يمكن أن يكون **رافعة تنموية** إذا استخدم في تصميم حملات توعية، وتنمية التفكير النقدي، وتعزيز القيم الأخلاقية.

- أظهرت حالات الدراسة والأمثلة الواقعية أنّ **الهجمات آخذة في التطور والاحترافية**، ما يستلزم مقاربات أكثر شمولية تجمع بين التكنولوجيا، التعليم، والمجتمع.

وبناءً على هذه النتائج، تم صياغة مجموعة من التوصيات التي تسعى إلى تعزيز الحماية الرقمية وتطوير استراتيجيات وقائية شاملة وتمثلت في:

- **اعتماد مقاربة شاملة** لمواجهة الهندسة الاجتماعية، تقوم على التوعية المستمرة، وتطوير أدوات الحماية التقنية، وبناء ثقافة قائمة على التفكير النقدي والمسؤولية.
- **تصميم برامج تدريبية متخصصة** للأفراد والمؤسسات، تشمل سيناريوهات عملية للهجمات وأساليب كشفها، مع التركيز على الفئات الأكثر استهدافًا مثل الموظفين التنفيذيين.
- **إشراك مؤسسات التعليم والأسرة والمجتمع المدني** في تعزيز الوعي الرقمي ونشر ثقافة أمنية قائمة على التعاون والمسؤولية المشتركة.

6.قائمة المراجع:

✓ **مراجع باللغة العربية:**

1. **إبراهيم محمد مها محمد، (جويلية–سبتمبر، 2018)**. الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي. المجلة الدولية لعلوم المكتبات والمعلومات، المجلد 5(العدد 3)، ص ص 128-109.
2. **معتصم محمد النور أحمد، (2019)**، الهندسة الاجتماعية، كتاب إلكتروني متوفر في موقع مكتبة النور الالكتروني على رابط التحميل التالي: الهندسة الإجتماعية /download/703441 /https://ketabpedia.com
3. **العمري صالح محمد حسن، العمري عبد الرحمان. (جانفي، 2024)**. الآثار الاجتماعية للهندسة الاجتماعية في الفضاء الرقمي على المجتمع السعودي. المجلة الدولية للتصاميم والبحوث التطبيقية، المجلد 3(العدد 8)، ص ص 1-32.
4. **المنيفي أحمد محمد عبد الرؤوف. (2021)**. الاحتيال الإلكتروني وحكمه في الاسلام والقوانين المعاصرة، دار الشبكة للنشر والتوزيع، بيروت – لبنان.
5. **حسين إبراهيم حمادي العنبكي. (فيفري، 2025)**. الهندسة الاجتماعية الرقمية وتأثيرها على المنظومة القيمية للمجتمع. مجلة الوسيط للعلوم الانسانية، المجلد 21(العدد 1)، ص ص 668-626.
6. **خديجة سليماني، وأحمد نقاز. (2020)**، الهندسة الاجتماعية لارتكاب الاحتيال ودور التدقيق الداخلي للحد من الظاهرة، مجلة ابحاث اقتصادية معاصرة، العدد الثاني، جامعة المسيلة، ص ص 112-100.
7. **زيوش سعيد. (2017)**. ظاهرة الابتزاز الالكتروني وأساليب الوقاية منها قراءة سوسيولوجية وآراء نظرية. مجلة العلوم الاجتماعية، المجلد 11، العدد 1، جامعة عمار ثليجي، ص ص 70-87.
8. **سلمان الجبوري سامر. (2018)**. جريمة الإحتيال الإلكتروني – دراسة مقارنة –. منشورات زين الحقوقية، لبنان.

9. **عبد الله عنيشل، و حسين يحياوي**. (**2025**). مخاطر الهندسة الاجتماعية ومتطلبات تحقيق الأمن المجتمعي للمؤسسات الاقتصادية. الملتقى الوطني الاول حول: مخاطر الهندسة الاجتماعية ومتطلبات تحقيق الأمن المجتمعي للمؤسسات الاقتصادية المنعقد بجامعة غرداية يوم 04 ماي 2025، ص ص 01-13.

10. **على عباس مراد**. (**2017**). الهندسة الاجتماعية -صناعة الإنسان والمواطن-. بيروت، لبنان: دار الروافد الثقافية.

11. **لطف جاد الله عبد العزيز**. (**2017**). أمن المجتمع الالكتروني. الاسكندرية، مصر: مكتبة الوفاء القانونية.

✓ **المراجع باللغة الأجنبية:**

12. *Cybersecurity Dive .(May, 2025) Pear-Phishing Campaign Targets CFOs with advanced remote access techniques, this citation is taken from the website below: https://www.cybersecuritydive.com/news/spearphishing-remote-access-campaign-cfos-finance-executives-trellix/749192/?*
13. *Hussein Falah Aboalhab & Mohamed Farhat .(2024) .Social Engineering and Its Role in Maintaining Information Security And Privacy .Scientific Research Journal of Engineering and Computer Sciences ،India, vol 5(12), p p 1-10.*
14. *K Administration .(2008) .https://usa.kaspersky. com/resource-center/definitions/what-is-social-engineering.*
15. *KROMBHOLZ, K. & HOBEL, H; HUBER, M & WEIPPLE (2015), Advanced Social Engineering Attacks. Journal of Information Security and Application, pp 113-122.*
16. *M. Bezuidenhout ،F. Mouton و ،H. S. Venter(2010), Social engineering attack detection model: SEADM in Information Security for South Africa.*
17. *MailGuard, (July, 2025) .DHL-branded phishing scam prompts confirm delivery address. MailGuard Blog, this citation is taken from*

the website below: https://www.mailguard.com.au/blog/dhl-branded-phishing-scam-prompts-confirm-delivery-address?utm_source=chatgpt.com

18. *Ministry of Electronics & Information Technology. Government of India.(April, 2022) .Ministry of Electronics & Information Technology Government of India, this citation is taken from the website below: https://www.cert-in.org.in/PDF /CERT-In_Directions_70B_28.04.2022.pdf?utm_source*
19. *R. Dhull و ،Hooda Sumedha Singh .(2016) . Contrast Study of Social Engineering Techniques .IOSR Journal of Computer Engineering (IOSR-JCE) .(4)18 ، p p 66-68.*
20. *SecureWorks Counter , T. (2017, July 27). The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets. Consulté le June 25, 2025, sur https://www.secureworks.com/research/the-curious-case-of-mia-ash*
21. *State of Kuwait .(2014) .Law No. 37 of 2014 on the Establishment of Communication and Information Technology Regulatory Authority (CITRA),this citation is taken from the website below: https://www.citra.gov.kw/sites/en/LawofCITRA/Law%20No.%2037-%202014.pdf?utm_source=chatgpt.com*
22. *Švehla, Z. L., Sedinić , I., & Pauk, L. (2016). Going White Hat: Security Check by Hacking Employees Using Social Engineering Techniques. Information and Communication Technology, Electronics and Microelectronics (MIPRO).*