جامعة غرداية

كلية العلوم الاقتصادية و التجارية وعلوم التسيير

قسم علوم التسيير

بالتعاون مع مخبر الدراسات التطبيقية في العلوم المالية والمحاسبة

ينظمون ملتقى وطني (حضوري/ عن بعد) بعنوان:

" مخاطر الهندسة الاجتماعية ومتطلبات تحقيق الأمن المجتمعي

للمؤسسات الاقتصادية"، يوم 04 ماي 2025.

مداخلة بعنوان:

مخاطر الهندسة الاجتماعية وضرورة الوعي الرقمي

من إعداد الباحث :

- عبد الرحمان بن سانية، أستاذ التعليم العالي، جامعة غرداية، bensania.abderrahmane@univ-ghardaia.edu.dz

من خلال المحور رقم: 01 .

الملخص: (لا يتجاوز 150 كلمة)

اهتمت هذه المداخلة ببيان المخاطر المرتبطة بالهندسة الاجتماعية باعتبارها من أكبر التهديدات المتجددة التي تواجهها الشركات والأفراد والمجتمعات حاليا في ظل تطور الوسائط الرقمية وأدوات الذكاء الاصطناعي، وهو ما يطرح ضرورة الوعي الرقمي كضمانة تركز على تنمية حس الأمن السيبراني لدى البشر الذين يشكلون الحلقة الأضعف المستهدفة بهجمات الهندسة الاجتماعية، وضرورة تطرح أهمية التدريب المستمر للأفراد لضمان تحقيق المرونة السيبرانية التي تحقق استمرارية الأعمال رغم تبدّل الأشكال التي تظهر فيها الهجمات السيبرانية وتتجدد باستمرار.

الكلمات المفتاحية: تهديدات الهندسة الاجتماعية، الوعي الرقمي، الأمن السيبراني، المرونة السيبرانية .

Abstract:

This paper explored the risks associated with social engineering, one of the most significant emerging threats facing businesses, individuals, and societies today, given the development of digital media and artificial intelligence tools. This raises the need for digital awareness as a safeguard focused on developing a sense of cybersecurity among humans, who constitute the weakest link targeted by social engineering attacks. It also highlights the importance of ongoing training for individuals to ensure cyber resilience, which enables business continuity despite the ever-changing forms in which cyber attacks occur and are constantly recurring.

Keywords: Social engineering threats, digital awareness, cybersecurity, cyber resilience

مخاطر الهندسة الاجتماعية وضرورة الوعي الرقمي

أ/ عبد الرحمان بن سانية [1]

مقدمة

المجتمعات الحالية هي مجتمعات الرقمنة! حيث يعرف العالم انتشارا واسعا –وبسرعة متزايدة– لاستخدام الأنترنت في شتى مناحي الأفراد، وبذلك تبدلت المفاهيم التقليدية وصارت مصطبغة بلاحقة "الرقمنة" لزاما، فأصبح الكلام عن "المواطن الرقمي" و عن "محو الأمية الرقميّة" وصار رهان العيش في هذه المجتمعات هو الصراع من أجل البقاء على قيد الحياة في العصر الرقمي !

ولقد رافق ذلك الارتفاع الكبير في معدلات استخدام الأنترنت ارتفاع مواز في مخاطر الهجمات السيبرانية، هذه الهجمات التي ما فتئت تطور من تكتيكاتها باستمرار للبقاء –هي الأخرى– حاضرة في المشهد الرقمي الراهن.

وفي هذا الأفق، تعد هجمات الهندسة الاجتماعية من أخطر التهديدات الأمنية للأفراد والشركات والمجتمعات بالتبعية، وذلك بسبب الأساليب الجديدة التي تعتمدها والقائمة على استغلال نقاط الضعف البشري بدلا من الاستغلال التقليدي لنقاط الضعف التقنية، فبدلا من خرق الأنظمة وكسر برامج الحماية، صارت هذه الهجمات تعمل على استهداف الحلقة الأضعف في سلسلة الأمان وهم البشر المفتقرون إلى الوعي السيبراني، بخداعهم والتلاعب بهم نفسيا بأساليب مختلفة ككسب ثقتهم، وتقديم الرغبة في مساعدتهم، أو بالعكس تخويفهم وإرباكهم، كل ذلك من أجل الحصول على معلومات حساسة واختراق أنظمة الشركات التي يعملون بها، وغير ذلك كثير.

إن هذا الوضع أضحت معه حتى الشركات التي تعتمد إجراءات أمن سيبراني قوية كعمليات المصادقة المختلفة، وجدران الحماية والشبكات الافتراضية الخاصة وبرامج مراقبة الشبكات ..الخ ليست بمنأى عن الهجمات السيبرانية.

لذلك، وتأسيسا على ما سبق فقد بات من الضروري جدا فهم الأخطار المرافقة لهجمات الهندسة الاجتماعية وتهديداتها، وفهم الممارسات الضرورية للتقليل من مخاطرها والحد منها، ودور تنمية الوعي الرقمي لدى التعاملين بالوسائط الرقمية في تحقيق ذلك، وهو ما تسعى هذه المداخلة إلى بحثه وبيانه.

---

[1] أستاذ التعليم العالي بجامعة غرداية، ورئيس فرقة بمخبر التنمية الإدارية للارتقاء بالمؤسسات الاقتصادية.

1. الأمن السيبراني: واقع خطير ومستقبل مخيف

أوضحت شركة CrowdStrike الأمريكية المتخصصة في الأمن السيبراني في تقرير لها لسنة 2024 حول "رصد التهديدات السيبرانية" للفترة من 1 يوليو 2023 إلى 30 يونيو 2024، إلى أنه:[1]

- ازدادت عمليات الاختراق التفاعلية بنسبة 55% مقارنة بالسابق،
- 86% من عمليات الاختراق التفاعلية ترجع إلى أنشطة الجرائم الإلكترونية.
- ازدادت عمليات الاختراق التفاعلية المرتبطة بالجرائم الإلكترونية ضد قطاع الرعاية الصحية بـ75%.
- ازدادت عمليات الاختراق التفاعلية التي تؤثر على قطاع التكنولوجيا بنسبة 60%، مما يجعل التكنولوجيا القطاع الأكثر استهدافًا للعام السابع على التوالي.
- زاد استخدام أدوات إدارة المخاطر (RMM) من قِبل المنافسين بنسبة 70%، و27% من جميع التفاعلات.

وحسب "تقرير توقعات الأمن السيبراني العالمي 2025" الصادر في جانفي 2025، فإن المستقبل يحتاج اهتماما أكبر بما يسمى "المرونة السيبرانية Cyber résilience" ، وهذا المصطلح مكمل لمصطلح "الأمن السيبراني" ، وتقوم فكرته على أن المؤسسة لا تعمل فقط على مواجهة التهديدات السيبرانية القائمة ومعالجة نقاط الضعف، بل فوق ذلك التحضير للهجمات غير المتوقعة وبناء استراتيجية استباقية لتقييم المخاطر باستمرار وتكييف الدفاعات السيبرانية مع كل تطور جديد محتمل للهجمات الإلكترونية، وهو ما يجعل المؤسسة قادرة على تحديد حوادث الأمن السيبراني ومواجهتها والتعافي منها في أي مرحلة تتلقى فيها هجوما سيبرانيا، وبالتالي مواصلة نشاطها وتحقيق الأهداف، بغض النظر عن الحوادث السيبرانية التي قد تحدث مستقبلا. وفي هذا الصدد أشار التقرير إلى أن: [2]

- التهديدات السيبرانية المُستمرة في التطور لا تُهدّد وظائف الأنظمة فحسب، بل تُعرّض سلامة الإنسان للخطر أيضًا
- حوالي 35% من المنظمات الصغيرة تعتقد أن مرونتها السيبرانية غير كافية، وهي نسبة زادت سبعة أضعاف منذ عام 2022.
- يعتقد 71% من قادة الأمن السيبراني في الاجتماع السنوي للأمن السيبراني 2024 أن المؤسسات الصغيرة قد وصلت بالفعل إلى نقطة تحول حرجة حيث لم تعد قادرة على تأمين نفسها بشكل كافٍ ضد التعقيد المتزايد للمخاطر السيبرانية.

- يتجلى التفاوت في المرونة السيبرانية بشكل أكبر من خلال الاختلافات الإقليمية في الاستعداد: فبينما يفتقر 15% فقط من المشاركين في أوروبا وأمريكا الشمالية إلى الثقة في قدرة بلادهم على الاستجابة للحوادث السيبرانية الكبرى التي تستهدف البنية التحتية الحيوية ، ترتفع هذه النسبة إلى 36% في أفريقيا و42% في أمريكا اللاتينية.
- أيضا يتفاوت الأمر في ذلك بين القطاعين العام والخاص، حيث أفاد 38% من المشاركين بعدم كفاية المرونة السيبرانية في القطاع العام، مقارنة بـ 10% فقط من مؤسسات القطاع الخاص المتوسطة والكبيرة. ويمتد هذا التفاوت إلى القوى العاملة السيبرانية، حيث أشارت 49% من مؤسسات القطاع العام إلى أنها تفتقر إلى المواهب اللازمة لتحقيق أهداف الأمن السيبراني الخاصة بها – بزيادة قدرها 33% عن عام 2024.
- اتسعت فجوة المهارات السيبرانية منذ عام 2024، حيث أفادت منظمتان من كل ثلاث منظمات بوجود فجوات في المهارات تتراوح بين المتوسطة والحرجة. ولا تثق سوى 14٪ من المنظمات بامتلاكها الكفاءات والمهارات اللازمة.

ويخلص التقرير إلى أن التعقيد المتزايد للرقمنة يشكل تحديًا كبيرًا أمام تحقيق المرونة السيبرانية، مما يُفاقم أوجه عدم المساواة التي تُعرّض المؤسسات ذات الموارد المحدودة للخطر. وأن التطور المُتزايد لمجرمي الإنترنت لا يزال يُشكّل تحديًا مُستمرًا، حيث أضحت وسائل الحماية التقليدية متجاوزة بالتكتيكات المُعزّزة بالذكاء الاصطناعي، وبرامج الفدية، وأساليب الهندسة الاجتماعية المُتقدّمة. ولا تتطلب مُعالجة هذه التهديدات المُتطوّرة حلولًا تكنولوجية مُتقدّمة فحسب، بل تتطلب أيضًا تعاونًا بين القطاعات وتبادلًا للمعارف. من جهة أخرى فن التوترات الجيوسياسية تدفع المؤسسات إلى إعادة تقييم استراتيجياتها، وتحقيق التوازن بين المخاوف الأمنية والعمليات العالمية بسبب ما ينجم عن تلك التوترات من هجمات سيبرانية.[3]

2. الهندسة الاجتماعية: مفهومها ومخاطرها على الاقتصاد والأمن المجتمعي

2-1 مفهوم الهندسة الاجتماعية: مفهوم عام في فضاء خاص، الدلالة والتطور

حسب موسوعة ويكيبيديا: "الهندسة الاجتماعية هي نوع من الهجمات الإلكترونية التي تستغل السلوك البشري للتلاعب بهم، والكشف عن معلومات حساسة أو القيام بأي إجراء قد يعرض أمان النظام للخطر. وينطوي على استخدام التكتيكات النفسية لخداع الأشخاص لإفشاء معلومات سرية أو القيام بعمل

قد يضر بأمن الشركة أو المؤسسة مثلا. اجتماعياً، يمكن أن تأتي الهجمات الهندسية بأشكال عديدة ومختلفة، بما في ذلك التصيّد الاحتيالي (Phishing) والتذرُّع (Pretexting) واصطياد إغرائي (Baiting)، وغيره". [4]

يلاحظ أن مصطلح "الهندسة الاجتماعية" ارتبط تعريفه –بشكل كبير– في البحوث بالهجمات السيبرانية التي تستغل نقاط الضعف البشرية بدلا من نقاط الضعف التقنية، مستخدمة طرق الاحتيال وعلم النفس البشري للوصول إلى الهدف الإجرامي المنشود، وهي تعتبر في العصر الحالي واحدة من أكبر مخاطر الأمن السيبراني ذات الآثار الخطيرة على المجتمعات والأفراد.[5]

ويعتبر هذا التعريف الشائع للهندسة الاجتماعية هو التعريف الضيق لهذا المصطلح إذ أنه في مفهومه الواسع – كما يذكر *Christopher Hadnagy* في كتابه " الهندسة الاجتماعية: فن اختراق البشر *Social Engineering: The Art of Human Hacking* يشير إلى "فن أو بالأحرى علم المناورة بمهارة مع البشر لاتخاذ إجراءات في بعض جوانب حياتهم" [6]. والهندسة الاجتماعية بهذا الإطلاق تستخدم في الحياة اليومية بشكل مطرد، فهي قد تطلق على الطريقة التي يجبر بها الأطفال والديهم على الاستجابة لمطالبهم، وعلى الطريقة التي يتعامل بها المعلمون مع طلابهم، أو على الطريقة التي يسلكها الأطباء أو علماء النفس للحصول على معلومات من مرضاهم ...الخ

واعتبارا لذلك، يمكن اعتبار الهندسة الاجتماعية " فعل التلاعب بشكل ما لاتخاذ إجراء قد يكون في مصلحة "الهدف" أو قد لا يكون، ويشمل ذلك الحصول على معلومات أو الوصول إليها أو دفع الهدف للقيام بعمل معين"

وبذلك فإن أصل مصطلح "الهندسة الاجتماعية" لا يتعلق فقط بخداع الناس أو الكذب عليهم، ولكن هو يصف الطريقة التي تعتمد الحيلة في الوصول إلى الغرض، كما يحتال الطبيب النفسي –مثلا– إلى علاج المريض من خلال استدراجه بأسئلة متدرجة للإفصاح عن معلومات يكتمها، وذلك بالطبع في صالح المريض وإن تم بطريقة غير معلنة أو صريحة.[7]

وفي ذات المنحى، نجد أن قاموس *merriam-webster* يعرف الهندسة الاجتماعية بمنظورين:

- ✓ إدارة البشر وفقًا لمكانتهم ووظيفتهم في المجتمع
- ✓ الأساليب الاجتماعية (مثل التصيد الاحتيالي) المستخدمة للحصول على معلومات شخصية أو سرية يمكن استخدامها بشكل غير مشروع."[8]

وناقش Zuoguang Wang وآخرون التطور المفاهيمي للهندسة الاجتماعية في مجال الأمن السيبراني، منذ عام 1974 تقريبًا حتى تاريخ المقال (2020)، استنادًا إلى مراجعة متعمقة للأدبيات. وقد خلصوا بنوع من التحليل المفصل إلى أن مفهوم الهندسة الاجتماعية تطور خلال خمس مراحل هي:[9]

- ✓ **المرحلة الأولى: مرحلة الاختراق Phreak phase (1974-1983):**

حيث يرجح الباحثون –استنادا إلى مسح الأدبيات وتحليلها، أن يكون وقت نشأة مفهوم الهندسة الاجتماعية سابقًا لعام 1984 تاريخ انتشار المصطلح. ويعود إلى سنة 1974 تقريبًا. وقد كان يعني في هذه المرحلة " نهج للحصول على معلومات أو مساعدة من المشغلين في مراكز التحويل لشركات الهاتف بوسائل مثل الذريعة وانتحال الشخصية والإقناع."

- ✓ **المرحلة الثانية: Phrack Phase (1984-1995):**

ارتبط مفهوم الهندسة الاجتماعية في هذه المرحلة بجانبين: بالاختراق الهاتفي وذلك من خلال استغلال موظفي شركات الهاتف بوسائل مثل الذريعة وانتحال الشخصية والإقناع والخداع للحصول على معلومات مهمة مستهدفة؛ ومن جانب آخر، امتدت إلى اختراق أنظمة الحاسوب باستخدام الحيل التي توصل إلى المعلومات الهامة. لذلك يشير الباحثون المذكورون إلى تلك الازدواجية في مفهوم الهندسة الاجتماعية من خلال دلالة الكلمتين Phreak المنصرفة إلى الاستغلال الاحتيالي لموظفي شركات الهاتف و Hack المنصرفة إلى التفاعلات الاجتماعية للحصول على معلومات حول نظام حاسوب المستهدفين بوسائل مثل الخداع والتلاعب بالحوارات وغيرها.

- ✓ **المرحلة الثالثة: مرحلة الاختراق الاحترافي Professional hack phase (1996-2001)،**

شهدت هذه الفترة هائلاً في مجال أمن المعلومات وتجلى تطور الهندسة الاجتماعية بشكل رئيسي في ثلاثة جوانب:

1. تنوعت أساليب تطبيق الهندسة الاجتماعية بشكل أكبر من الناحية المادية.
2. مع تطور تكنولوجيا معلومات الشبكات، تطورت أساليب الهجوم التقني مثل التصيد الاحتيالي عبر البريد الإلكتروني وأحصنة طروادة، تدريجيًا إلى مفهوم الهندسة الاجتماعية.

3. بدأت مناقشة الخصائص المميزة في جانب علم نفس الهندسة الاجتماعية، مثل التأثير الاجتماعي والإقناع والتلاعب بالثقة، وأُدرك تدريجيًا أن البشر هم الحلقة الأضعف في سلسلة الأمن.

فيلاحظ أن الهندسة الاجتماعية صارت بذلك تمس جانبين:

- الجانب المادي: ويشمل أساليب الهجوم التقني كالتصيد الاحتيالي وأحصنة طروادة
- الجانب النفسي: وذلك باستخدام أساليب نفسية للتفاعل مع الضحية والتلاعب بها للحصول على المعلومات المطلوبة

لذلك في هذه المرحلة يمكن القول أن الهندسة الاجتماعية صارت تشير إلى ممارسة الحصول على المعلومات من خلال وسائل تقنية وغير تقنية، أو أنها العملية التي يخدع بها المخترق الآخرين ليكشفوا عن بيانات قيّمة من شأنها أن تفيده بطريقة ما، أو كما يرى غرانجر الهندسة الاجتماعية هي عمومًا التلاعب بالميل البشري الطبيعي للثقة.

- ✓ **المرحلة الرابعة: مرحلة التطور متعدد الاتجاهات Multidirectional evolution phase (2002-2011):**

مقارنةً بالمرحلة السابقة، شهدت هذه المرحلة زيادةً ملحوظةً في عدد الأعمال المتعلقة بالهندسة الاجتماعية، و دخل مفهوم الهندسة الاجتماعية مرحلة تطور متعددة الاتجاهات، ظهرت خلالها أنواع مختلفة من الأوصاف المفاهيمية، والتي تصل إلى حد التناقض أحيانا، وقد نجم عن ذلك العديد من المشاكل: كغموض الحدود المفاهيمية، وإساءة استخدام المصطلحات، والتمايز والتفكك المفاهيمي الناجم عن تطور المفاهيم في اتجاهات مختلفة.

- ✓ **المرحلة الخامسة: مرحلة هجمات الهندسة الاجتماعية المتقدمة Advanced social engineering attack phase (منذ عام 2012):**

منذ عام 2012 تقريبًا، وتبعا لتطورات التقنيات الجديدة والانتشار الواسع لمواقع التواصل الاجتماعي، وإنترنت الأشياء، والإنترنت الصناعي، والأجهزة القابلة للارتداء، والأجهزة المحمولة، تعززت هجمات الهندسة الاجتماعية وتنوعت أشكالها وزاد حجم ضحاياها وصارت تنفذ بطرق أكثر ذكاء وأعلى كفاءة وتشكل تهديدات أمنية متعددة المستويات، شاملة، وخطيرة على الفضاءات البشرية، والسيبرانية، والمادية.

2-2 مخاطر الهندسة الاجتماعية

تتعدد الأساليب المستخدمة في الهندسة الاجتماعية وتأخذ أشكالا متنوعة منها:[10]

1. **الهجمات القائمة على استغلال البشر:** وتشمل أساليب التلاعب بالضحايا للحصول على معلومات سرية تتعلق بالعمليات أو الأنظمة باستخدام طرق عديدة مثل: انتحال الشخصية، انتحال شخصية موظف جديد، التطفل على الآخرين، البحث في حاويات النفايات، تهديد الضحية بتقديم معلومات سرية، التذرع، الهاتفية، التظاهر بصفة شريك أو عميل أو جهة إنفاذ قانون للضحية.
2. **الهجمات القائمة على التكنولوجيا:** وهي نوع شائع من هجمات الهندسة الاجتماعية، تُستخدم فيها أجهزة الكمبيوتر وتتضمن رسائل التصيد الاحتيالي المستهدفة للأفراد للحصول على تفاصيل شخصية، مثل معلومات تسجيل الدخول إلى الحسابات المصرفية، ورسائل الإعلان عن منتجات أو منافسين مختلفين، وبرامج التخويف، ورسائل البريد الإلكتروني الاحتيالية، والفيروسات عبر مرفقات البريد الإلكتروني، ...الخ

وفقًا لوزارة العدل الأمريكية، تعتبر هجمات الهندسة الاجتماعية من أخطر التهديدات وأكثرها خطورة في جميع أنحاء العالم، وهي تؤثر بشكل كبير على الاقتصاد العالمي.[11]

ووفقًا لمسح عالمي شمل 853 متخصصًا في تكنولوجيا المعلومات، أُجري في الولايات المتحدة الأمريكية، والمملكة المتحدة، وكندا، وأستراليا، ونيوزيلندا، وألمانيا عام 2011، تعرضت 48% من الشركات الكبيرة و32% من الشركات من جميع الأحجام لـ 25 هجومًا أو أكثر من هجمات الهندسة الاجتماعية خلال العامين الماضيين. وتُشير 30% من الشركات الكبيرة إلى أن تكلفة الحادث الواحد تتجاوز 100,000 دولار أمريكي. ووفقًا لتقارير صادرة عن تقرير حالة الأمن السيبراني الصادر عن جمعية أمن المعلومات الأمريكية (ISACA)، تُعد الهندسة الاجتماعية أكبر تهديد سيبراني للمؤسسات من عام 2016 إلى عام 2018. وقد تعرضت 85% من المؤسسات لهجمات الهندسة الاجتماعية في عام 2018، بزيادة قدرها 16% خلال عام واحد، و تجاوز متوسط التكلفة السنوية لهجمات الهندسة الاجتماعية على المؤسسات في عام 2018 مبلغ 1.4 مليون دولار، بزيادة قدرها 8% مقارنة بالعام السابق.[12]

3. الوعي الرقمي: ضمانة أمنية وضرورة ملحة

مصطلح الوعي – كما في معجم المعاني– ينصرف في دلالته إلى الفهم وسلامة الإدراك، وفي علم النفس هو شعور الكائن الحي بما نفسه وما حوله، ويقال: وعي الشخص الأمر إذا أدركه على حقيقته،[13] ومتى غاب الإنسان عن إدراك ما حوله سمي فاقدا للوعي !

فالوعي الرقمي – تبعا للظل اللغوي للكلمة – ينصرف إلى تمكن الأفراد من امتلاك المعارف التقنية الأساسية والمهارات التي تمكنهم من مسايرة التطور الرقمي الحاصل.

إلا أن مصطلح "الوعي الرقمي" في بعده المفاهيمي لا ينحصر فقط في جانب امتلاك مهارات التعامل مع التقنية، بل له أبعاد أخرى تجعل من الصعب تحديد مفهوم دقيق له، كضرورة الوعي بالمخاطر المصاحبة للتعامل مع الوسائط الرقمية وكيفية التعامل معها بما يحقق الأمن السيبراني ويجنب الأفراد والشركات والاقتصاد الأضرار المصاحبة للهجمات الإلكترونية التي يتم تنفيذها في إطار الهندسة الاجتماعية، على سبيل المثال.

وفي هذا الإطار، قام *Leonie Brummer* بدراسة اهتمت باستكناه تعريف للوعي الرقمي من خلال مراجعة شاملة لمحو الأمية الرقمية وأدب المواطنة للفترة من نوفمبر 2015 إلى يونيو 2024، وكان مما توصل إليه من نتائج:[14]

- ✓ عدم وجود تعريف كامل للوعي الرقمي في عينة المقالات المدروسة،
- ✓ يرتبط مفهوم الوعي الرقمي بمفهومي "محو الأمية الرقمية"[15]، و"المواطنة الرقمية"[16] بسبب طبيعتهما الديناميكية، وزيادة وساطة التقنيات الرقمية في المجتمع الحالي، وحتمية التعلم مدى الحياة، ولا يوجد إجماع حول تعريفات واضحة لمحو الأمية الرقمية وبدرجة أقل المواطنة الرقمية.
- ✓ الوعي الرقمي مفهوم ذو طبيعة ديناميكية تتماشى مع ديناميكية عمليات محو الأمية الرقمية وتحقيق المواطنة الرقمية، فكون الفرد متعلمًا رقميًا أو مواطنا رقميا لا يعني بالضرورة وصوله للمستوى النهائي للمشاركة الفعالة في المجتمع، لأن التطور المستمر والسريع في الرقمنة يفرض بالتبعية تطويرا مستمرا ومرونة لتحقيق ما يطلبه المجتمع أو يحتاجه تبعا لما أفرزه التطور الرقمي من تحديات. لذلك فإن الوعي الرقمي يتطور باستمرار طوال حياة الفرد.

- ✓ الوعي الرقمي لابد أن لا ينحصر في وعي الجوانب السلبية للتقنيات الرقمية (وهذا جانب حاسم لحماية المواطن الرقمي في المجتمعات الحالية)، بل يجب أن ينسحب أيضا إلى وعي الجوانب الإيجابية التي تزيد من تطوير الفرد وتخلق إمكانيات من حيث اكتساب المعرفة والمهارات والكفاءات.
- ✓ الوعي الرقمي يمكن من الفرد من التعرف بشكل نقدي على المعرفة وتحديد الضروريات والفرص والمخاطر والعواقب المترتبة على استخدام التقنيات الرقمية، وهو أكثر من مجرد إدراك وتمكن من الجوانب التقنيات الرقمية، إذ يربط الجوانب الاقتصادية والثقافية والشخصية والسياسية والاجتماعية للسلوكيات والأنشطة والمواقف والقيم والمعتقدات التي تنطوي عليها التقنيات الرقمية.

وتأسيسا على ذلك، فإن الوعي الرقمي المقصود كضمانة أساسية للحماية من مخاطر الهندسة الاجتماعية هو ذلك الوعي الذي يتجاوز مجرد امتلاك الأفراد والعاملين في المؤسسات لمهارات التعامل مع الوسائط الرقمية، إلى امتلاك حس بخطورة الهجمات السيبرانية وأضرارها البالغة على أمن الأفراد والشركات والمجتمع ككل. "الوعي بالهندسة الاجتماعية هو معرفة وفهم أساليب التلاعب النفسي لمجرمي الإنترنت لاستغلال نقاط الضعف البشرية والوصول غير المصرح به إلى البيانات والأنظمة والمناطق المادية الحساسة"[17]

إن امتلاك مثل هذا الوعي يجعل الأفراد يمتلكون اليقظة الرقمية اللازمة لتحقيق الأمن السيبراني، سواء من خلال تدابير الحماية الوقائية أو من خلال التعامل الحذر مع الآخرين على الفضاءات السيبرانية والناجم عن إدراك واسع للحيل التي يستخدمها المهاجمون في إطار الهندسة الاجتماعية مثل التصيد الاحتيالي والخداع والتخويف وخلق الارتباك ولغة الاستعجال والمرسلين غير المألوفين والمرفقات غير المرغوب فيها وطلبات الحصول على المعلومات ...الخ، وذلك يستدعي تدريبا مستمرا لتحقيق التوعية الأمنية ومكافحة هذه المخاطر.

إذن، العنصر البشري هو حاجز الصد الأول في تقليل أضرار الهندسة الاجتماعية، بسبب أن هذا النوع من تهديدات الأمن السيبراني يعتمد بصفة أساسية على الخطأ البشري بدلاً من الدراية التقنية، مما يجعل يقظة الأفراد وتدريبهم على فهم حيل المهاجمين السيبرانيين واجتناب الوقوع كضحايا لها أمرا بالغ الأهمية.

الخاتمة

اهتمت هذه المداخلة بالتعرض لتهديدات الهندسة الاجتماعية كإحدى أبرز المخاطر السيبرانية التي تواجهها المجتمعات في ظل التطور السريع للرقمنة وأدواتها وانسحابها على شتى مناحي حياة الأفراد، وما تفرضه تلك التهديدات من ضرورة التحلي بالوعي الرقمي كحاجز أمان أول للتصدي لها وضمان استمرار الشركات في أداء أعمالها رغم تطور أشكال تلك الهجمات وتبدّل الأوجه التي تظهر فيها في كل مرة.

ولقد كان من أبرز نتائج هذا البحث ما نلخصه في النقاط التالية:

- ✓ هجمات الهندسة الاجتماعية من أخطر التهديدات الأمنية للأفراد والشركات والمجتمعات بالتبعية، وذلك بسبب الأساليب الجديدة التي تعتمدها والقائمة على استغلال نقاط الضعف البشري بالاحتيال والمخادعة والتأثير النفسي بدلا من الاستغلال التقليدي لنقاط الضعف التقنية،
- ✓ عرفت الهجمات المنفذة في إطار الهندسة الاجتماعية ارتفاعا متزايدا وتنوعا في أشكالها تبعا لتطور أدوات الذكاء الاصطناعي، والانتشار الواسع لمواقع التواصل الاجتماعي، وإنترنت الأشياء،، وأصبح كل تطور في أدوات الأمن السيبراني يترافق بتطور مواز وجديد في أساليب تلك الهجمات مما يطرح ضرورة التطوير المستمر، وضرورة تكميل "الأمن السيبراني" بـ"المرونة السيبرانية" التي لا تعمل فقط على مواجهة التهديدات السيبرانية القائمة بل تستهدف بناء استراتيجية مستقبلية استباقية للأخطار المحتملة وكيفية التصدي لها والتعافي منها، وضمان استمرار نشاط المؤسسة دون انقطاع ترجع أسبابه إلى الهجمات السيبرانية بالخصوص،
- ✓ الهندسة الاجتماعية في أصلها مفهوم واسع يشير إلى فن المناورة لدفع الشخص لتنفيذ أمر ما لا يكون بالضرورة سلبيا، ثم انصرف مفهومها إلى مجال ضيق يتصل بالهجمات السيبرانية التي تستغل نقاط الضعف البشرية بدلاً من نقاط الضعف التقنية ، مستخدمة طرق الاحتيال وعلم النفس البشري للوصول إلى الهدف الإجرامي المنشود ، وقد عرف هذا المفهوم تطورا وفق مراحل مختلفة تم شرحها وبيانها.
- ✓ الهندسة الاجتماعية ذات تكلفة اقتصادية باهظة على الشركات، وقد تؤدي إلى توقف الأعمال أو خسائر كبيرة جدا.

- ✓ يعتبر الوعي الرقمي ضمانة أساسية وضرورة ملحة لتقوية الحلقة الأضعف في سلسلة الأمان وهم البشر الذين يستغلهم المهاجمون السيبرانيون في إطار الهندسة الاجتماعية.
- ✓ "الوعي الرقمي" لا ينحصر فقط في جانب امتلاك مهارات التعامل مع التقنية، بل يتعدى ذلك إلى امتلاك حس ويقظة رقمية بخطورة الهجمات السيبرانية وأضرارها البالغة على أمن الأفراد والشركات والمجتمع ككل.
- ✓ العنصر البشري هو حاجز الصد الأول في تقليل أضرار الهندسة الاجتماعية، ويفرض تحقيق الوعي الرقمي ضرورة التدريب المستمر للموظفين على فهم أساليب الهندسة الاجتماعية ومخاطرها والكفاءة في التعامل مع معلومات الشركة الحساسة للتصدي للهجمات السيبرانية بكفاءة وفعالية.

هوامش البحث ومراجعه.

[1] *CROWDSTRIKE THREAT HUNTING REPORT 2024, p.5*
[2] *World Economic Forum, Global Cybersecurity Outlook 2025, January 2025 pp. 4-5.*
[3] *World Economic Forum, Global Cybersecurity Outlook 2025, January 2025 p.42*
[4] *https://fr.wikipedia.org/wiki/Ing%C3%A9nierie_sociale_(s%C3%A9curit%C3%A9_de_l%27information) (22/04/2025)*
[5] *ALOTAYAN, Turki, et al. Awareness of Social Engineering Attacks and their Relation to the Ability to Persuade among users of Social Networking Sites. Journal of Ecohumanism, 2024, vol. 3, no 7, p. 2581*
[6] *Hadnagy, C. (2010). Social engineering: The art of human hacking. John Wiley & Sons.p. 10*
[7] *Ibid. p.10.*
[8] *https://www.merriam-webster.com/dictionary/social%20engineering (22/04/2025)*
[9] *WANG, Zuoguang, SUN, Limin, et ZHU, Hongsong. Defining social engineering in cybersecurity. IEEe Access, 2020, vol. 8,*
[10] لمزيد من التفصل انظر:
MANOCHA, Tanu et SHARMA, Vinita. Essential awareness of social engineering attacks for digital security. Journal of Applied Management-Jidnyasa, 2021, p.p. 27-29.
[11] *MANOCHA, Tanu et SHARMA, Vinita.op. cit. p.26.*
[12] *Wang, Z., Sun, L., & Zhu, H. Defining social engineering in cybersecurity ; EEE Access ·VOLUME 8, , May 2020*
[13] *https://www.almaany.com/ar/dict/ar-ar/%D8%A7%D9%84%D9%88%D8%B9%D9%8A/? (23/04/2025)*
[14] *BRUMMER, Leonie. Conceptualizing Digital Awareness: Introducing a Definition of Digital Awareness via a Scoping Review of Digital Literacy and Citizenship Literature. 2025. file:///C:/Users/soft/Downloads/preprints202504.0069.v1.pdf*
[15] "**محو الأمية الرقمية Digital Literacy**" يعني تعليم المفتقرين للمهارات الرقمية الأساسية لتمكينهم من استخدام التكنولوجيا الحديثة (حواسيب وأجهزة ذكية وأنترنت ووسائط رقمية ...الخ) بطريقة فعالة. ومن أحسن ما عرف به محو الأمية الرقمية وصف إيشيت ألكالاي بأنه "مهارة البقاء على قيد الحياة في العصر الرقمي"، انظر:
Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. Journal of Educational Multimedia and Hypermedia, 13(1), 102
وهذا المفهوم يتعقد باستمرار لأن الفضاءات الرقمية وأدواتها تتغير باستمرار وتصبح أكثر تعقيدا، لذلك فإن ما يلزم الشخص حتى يكون "متعلما رقميا" يصبح أكثر تعقيدا. انظر:
PANGRAZIO, Luci et SEFTON-GREEN, Julian. Digital rights, digital citizenship and digital literacy: What's the difference?. Journal of new approaches in educational research, 2021, vol. 10, no 1, p. 15-27.

[16] يمكن تعريف **المواطنة الرقمية Digital Citizenship** على أنها "خلق الذات وتأكيد الذات للمواطنين كمشاركين نشطين في المجتمع من خلال الأعمال الرقمية"
[17] *ALOTAYAN, Turki, et al. Awareness of Social Engineering Attacks and their Relation to the Ability to Persuade among users of Social Networking Sites. Journal of Ecohumanism, 2024, vol. 3, no 7, p. 2581*