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:

تحليل تأثير التغيرات الرقمية على سلوك الأفراد في مواجهة الهندسة الاجتماعية

من إعداد الباحثة: من خلال المحور رقم: 01

- راضية بابا، طالبة دكتوراه، جامعة الجزائر2 ، baba.radia@univ-alger2.dz

الملخص: (لا يتجاوز 150 كلمة)

في العقود الأخيرة، شهدنا تحولًا مذهلاً في مجال التكنولوجيا الرقمية الذي غير الكثير من جوانب حياتنا اليومية، بما في ذلك طريقة تفاعل الأفراد مع المعلومات. كان لهذا التحول تأثير كبير على سلوكيات الأفراد في بيئات العمل المختلفة، حيث أصبحوا يعتمدون بشكل متزايد على الإنترنت ووسائل التواصل الاجتماعي. هذا الاعتماد أدى إلى زيادة تعرض الأفراد لأنواع متعددة من الهجمات المعرفية، مثل الهندسة الاجتماعية. تعتمد هذه الهجمات على استغلال الثغرات النفسية في الأفراد بهدف تحقيق أهداف معينة، مثل سرقة البيانات أو التأثير على قراراتهم. في هذا السياق، تبرز أهمية دراسة تأثير التغيرات الرقمية على سلوك الأفراد في مواجهة هذه التهديدات. تهدف هذه المداخلة إلى تحليل هذا التأثير بشكل مفصل ضمن إطار علم النفس التنظيمي وعلم النفس العمل، لتحديد كيفية تأثير البيئة الرقمية الحديثة على سلوك الأفراد في السياقات المهنية وكيفية تصديهم لهذه التهديدات.

الكلمات المفتاحية: سلوك الافراد، الهندسة الاجتماعية، التغيرات الرقمية، الأبعاد النفسية، الوعي الرقمي

Abstract:

In recent decades, we have witnessed a remarkable transformation in digital technology that has altered many aspects of our daily lives, including how individuals interact with information. This transformation has significantly impacted individual behaviors in various work environments, as they increasingly rely on the internet and social media. This reliance has led to an increased exposure of individuals to various types of cognitive attacks, such as social engineering. These attacks exploit psychological vulnerabilities in individuals to achieve specific objectives, such as data theft, or influence their decisions. In this context, the importance of studying the impact of digital changes on individual behavior in the face of these threats becomes evident. This intervention aims to analyze this impact in detail within the framework of organizational psychology and work psychology, to determine how the modern digital environment influences individual behavior in professional contexts and how they confront these threats.

Keywords: Individual behavior, social engineering, digital changes, psychological dimensions, digital awareness.

1. مقدمة:

في ظل التحولات الرقمية السريعة التي شهدها العالم في العقود الأخيرة، أصبح الاعتماد على الإنترنت ووسائل التواصل الاجتماعي جزءًا أساسيًا من حياة الأفراد. وقد أدى هذا الاعتماد إلى زيادة تعرض الأفراد للهجمات الرقمية، بما في ذلك الهندسة الاجتماعية، التي تستغل الثغرات النفسية والسلوكية لتحقيق أهداف غير أخلاقية، مثل سرقة البيانات أو التأثير على القرارات.(Cialdini. 2009)

أظهرت الدراسات الحديثة أن الأفراد الذين يفتقرون إلى الوعي الرقمي يصبحون أكثر عرضة لهذه التهديدات. حيث أكدت دراسة (Bélanger et al. 2020) أن الأفراد غير الواعين رقميًا هم أكثر عرضة للهجمات الرقمية، مما يعزز الحاجة إلى تحسين الوعي الرقمي. كما أشار (Mayer et al. 2020) إلى أن الأشخاص الذين يقللون من خطورة المخاطر الرقمية يميلون إلى اتخاذ قرارات متهورة أثناء تعرضهم للهجمات.

في السياق العربي، أظهرت دراسة العوضي (2021) غياب برامج التوعية الرقمية في بعض المناطق العربية، مما يزيد من ضعف الأفراد في مواجهة هذه التهديدات. كذلك، أشارت دراسة الطيب (2019) في تونس إلى أن الوعي الرقمي يعد عاملًا حاسمًا في قدرة الأفراد على التعامل مع التهديدات الرقمية، مما يستدعي تعزيز التدريب على الأمان السيبراني في جميع القطاعات.

أما في الجزائر، فقد أظهرت دراسة بن فاطمة (2022) وجود ضعف كبير في مستوى الوعي الرقمي لدى الأفراد، لا سيما في المناطق النائية، حيث يُلاحظ غياب برامج توعية شاملة. كما أظهرت دراسة أخرى أجراها بلحاج (2021) أن المؤسسات الجزائرية لا تقدم تدريبًا كافيًا لموظفيها حول كيفية التصدي للهجمات الإلكترونية، مما يجعلهم عرضة لمخاطر الهندسة الاجتماعية. وأكدت دراسة موسي (2020) أن الأفراد الذين يتلقون تدريبًا على الأمان الرقمي في الجزائر يتمتعون بقدرة أكبر على تمييز الرسائل المشبوهة والتفاعل مع الإنترنت بشكل أكثر أمانًا، مما يشير إلى أهمية تعزيز برامج التدريب على الأمان الرقمي في المؤسسات الحكومية والخاصة.

رغم التقدم في فهم هذه الظاهرة، توجد فجوة بحثية واضحة تتعلق بتأثير البيئة الثقافية والاجتماعية على مقاومة هذه التهديدات في البلدان العربية، خاصة في الجزائر. على الرغم من وجود العديد من الدراسات التي تركز على التكنولوجيا في السياق الغربي، إلا أن الدراسات العربية لا تزال قليلة نسبيًا ولا تقدم بيانات كافية حول كيفية تأثير هذه التغيرات على الأفراد في ظل التحديات الاجتماعية والاقتصادية الخاصة بالمنطقة. هذه الفجوة تتطلب إجراء المزيد من الأبحاث لفهم تأثير البيئة الثقافية والنفسية في مواجهة

التهديدات الرقمية، مما يعزز من قدرة الأفراد والمؤسسات على التصدي لهذه التحديات في المستقبل (Gupta & Shalender. 2014).

التساؤلات المطروحة:

1. **كيف تؤثر التغيرات الرقمية على سلوك الأفراد في مواجهة محاولات الهندسة الاجتماعية في البيئة الرقمية؟**
2. **هل تؤثر الخلفية الثقافية والاجتماعية للأفراد في قدرتهم على مقاومة الهندسة الاجتماعية؟**
3. **هل يمكن أن يكون الوعي الرقمي العامل الرئيسي في الوقاية من الهندسة الاجتماعية؟**
4. **ماهي الاستراتيجيات النفسية للحد من الهندسة الاجتماعية في ظل التغيرات الرقمية في المجتمع وبيئات العمل؟**

قبل التطرق الى الإجابة عن تساؤلات دراستنا لابد من الإشارة الى المفاهيم التالية:

2. مفاهيم أساسية:

1.2 الهندسة الاجتماعية :(Social Engineering)

- **التعريف :**هي مجموعة من الأساليب النفسية التي تهدف إلى التلاعب بالعقول البشرية لاستخراج معلومات حساسة أو تنفيذ تصرفات معينة عن طريق الخداع أو التضليل. تعتمد الهندسة الاجتماعية على استغلال الثغرات النفسية والسلوكية للأفراد.
- **الأهمية :**من خلال الهندسة الاجتماعية، يمكن للمهاجمين أن يتلاعبوا بالثقة الاجتماعية للأفراد أو يشجعوهم على اتخاذ قرارات غير واعية، مما يسبب ضررًا للأفراد والمؤسسات (Mitnick & Simon. 2002) .

2.2التغيرات الرقمية:(Digital Transformation)

- **التعريف :**تشير التغيرات الرقمية إلى التحولات الكبيرة في استخدام التكنولوجيا الرقمية في حياتنا اليومية، بدءًا من الإنترنت ووسائل التواصل الاجتماعي وصولاً إلى الأنظمة الرقمية المعقدة في المؤسسات. يشمل ذلك التحول في كيفية وصول الأفراد للمعلومات والتفاعل مع البيئة المحيطة بهم.
- **الأهمية :**هذه التغيرات أوجدت بيئة رقمية تتسم بالسرعة والاتصال الدائم، مما يعرض الأفراد لفرص أكبر للوقوع في فخ الهندسة الاجتماعية.(Westerman et al. 2011) .

3.2 التغيرات الوعي الرقمي:(Digital Literacy)

- **التعريف :**هو القدرة على استخدام الأدوات الرقمية، مثل الإنترنت ووسائل التواصل الاجتماعي، بشكل آمن وفعّال. يشمل أيضًا القدرة على فهم المخاطر الرقمية وكيفية التعامل مع المعلومات والبيانات بشكل آمن.
- **الأهمية :**يعد الوعي الرقمي أحد العوامل الحاسمة التي تؤثر في قدرة الأفراد على التعرف على محاولات الهندسة الاجتماعية والوقاية منها. الأشخاص الذين يفتقرون إلى الوعي الرقمي يصبحون أكثر عرضة للهجمات.(Jones-Kavalier & Flannigan. 2006) .

4.2 الهجمات السيبرانية :(Cyber Attacks)

- **التعريف :**هي محاولات لاختراق الأنظمة الرقمية بهدف سرقة المعلومات أو تعطيل الخدمات. يمكن أن تكون هذه الهجمات مباشرة على الأنظمة أو عبر استراتيجيات الهندسة الاجتماعية.
- **الأهمية :**الهجمات السيبرانية هي جزء من التهديدات الرقمية التي تستفيد من ضعف الأفراد في التعامل مع التكنولوجيا، كما أنها تشمل أساليب مختلفة مثل التصيد الإلكتروني أو الاحتيال عبر الإنترنت.(Symantec. 2019) .

5.2 التهديدات الرقمية :(Digital Threats)

- **التعريف :**تشير إلى الأخطار التي يواجهها الأفراد في البيئة الرقمية، بما في ذلك محاولات سرقة البيانات، الاحتيال الإلكتروني، وعمليات اختراق الأنظمة.
- **الأهمية :**تزايد التهديدات الرقمية في العالم الرقمي يتطلب فهمًا أعمق لهذه التهديدات وكيفية حماية الأفراد منها.(Hathaway et al. 2012) .

6.2 التثقيف الرقمي:(Digital Education)

- **التعريف :**هو عملية تعليم الأفراد كيفية استخدام التكنولوجيا بطريقة صحيحة وآمنة، بما في ذلك فهم المخاطر والتهديدات الرقمية وكيفية الوقاية منها.
- **الأهمية :**التثقيف الرقمي يساعد الأفراد على أن يكونوا أكثر وعيًا بالمخاطر الرقمية وكيفية التعامل معها بفعالية.(Ally. 2008)

7.2 الضغط الاجتماعي:(Social Pressure)

- **التعريف :**هو التأثير الذي يمارسه الأقران أو المجتمع على الأفراد لتغيير سلوكياتهم أو اتخاذ قرارات معينة بناءً على القيم الاجتماعية أو المعايير الثقافية.

- **الأهمية :**في السياقات الرقمية، يمكن للضغط الاجتماعي أن يسهم في جعل الأفراد يتفاعلون بشكل أسرع أو بدون تفكير مع الرسائل المزيفة التي يتم إرسالها إليهم عبر الإنترنت (Cialdini & Goldstein. 2004).

8.2 الثقة الرقمية:(Digital Trust)

- **التعريف :**هي الثقة التي يضعها الأفراد في الأنظمة الرقمية، مثل مواقع الإنترنت أو منصات التواصل الاجتماعي، والتي قد تؤدي إلى اتخاذ قرارات مبنية على هذه الثقة، حتى وإن كانت قد تكون خاطئة.
- **الأهمية :**الثقة المفرطة في الأنظمة الرقمية تجعل الأفراد عرضة للتلاعب والخداع عبر أساليب الهندسة الاجتماعية.(McKnight et al. 2002) .

9.2 التصيد الإلكتروني:(Phishing)

- **التعريف :**هو نوع من أنواع الهندسة الاجتماعية حيث يقوم المهاجمون بإرسال رسائل بريد إلكتروني مزيفة أو رسائل عبر الإنترنت لمحاكاة مؤسسات موثوقة، بهدف الحصول على معلومات شخصية من الضحية مثل كلمات المرور أو تفاصيل الحسابات المصرفية.
- **الأهمية :**يعد التصيد الإلكتروني من أكثر أساليب الهندسة الاجتماعية شيوعًا، ويشكل تهديدًا كبيرًا للأفراد في البيئة الرقمية.(Hong. 2012) .

10.2 المصادقة متعددة العوامل:(Multi-Factor Authentication - MFA)

- **التعريف :**هي طريقة أمان تستخدم أكثر من عامل واحد للتحقق من هوية المستخدم، مثل كلمة مرور، رسالة نصية، أو رمز التحقق عبر تطبيقات الهاتف المحمول.
- **الأهمية :**استخدام المصادقة متعددة العوامل يعد من الطرق الفعالة للحد من مخاطر التعرض للهجمات الهندسية الاجتماعية.(Bodo. 2017) .

3. تأثير التغيرات الرقمية على سلوك الأفراد في مواجهة محاولات الهندسة الاجتماعية في البيئة الرقمية.

1.3 دور علم النفس التنظيمي في تحليل سلوك الأفراد:

من منظور علم النفس التنظيمي، فإن التغيرات الرقمية تؤثر بشكل مباشر على ثقافة العمل وسلوك الموظفين داخل المؤسسات. يُعزى ذلك إلى زيادة الاعتماد على التواصل الرقمي، مما يغير الطريقة التي يتعامل بها الأفراد مع المعلومات والمخاطر. وفقًا لـ (Mayer et al. 2020)، فإن وجود بيئة عمل رقمية قد يعزز من استخدام الهندسة الاجتماعية إذا لم تكن هناك آليات فعالة للتدريب على الأمن الرقمي.

من جهة أخرى، تشير الدراسات إلى أن المؤسسات التي تستثمر في توعية موظفيها وتحفيزهم على اتخاذ إجراءات أمان رقمية، يكون لديها قدرة أكبر على تقليل التأثيرات السلبية للهندسة الاجتماعية. دراسة أجراها (Harris.2019)حول تأثير برامج التوعية الأمنية على سلوك الأفراد، أظهرت أن الموظفين الذين تلقوا تدريبًا مستمرًا على كيفية اكتشاف محاولات الهندسة الاجتماعية كانوا أقل عرضة للوقوع في تلك الفخاخ.

2.3 التحليل النفسي لتأثير التغيرات الرقمية على الأفراد

أ **التحفيز العاطفي والاحتيال الرقمي:** يعتبر التحفيز العاطفي أحد الأدوات الأساسية التي يعتمد عليها المهاجمون في تطبيقات الهندسة الاجتماعية، حيث يستخدمون العواطف بشكل مكثف للتأثير على الأفراد ودفعهم لاتخاذ قرارات غير مدروسة. تتراوح هذه العواطف بين الخوف، الذي يثير القلق والارتباك، والطمأنينة الزائفة التي تعطي الأفراد إحساسًا بالأمان المبالغ فيه، أو الإثارة التي تدفعهم إلى التصرف بسرعة دون تفكير. على سبيل المثال، قد يتلقى الشخص رسالة بريد إلكتروني تهدد بإغلاق حسابه البنكي في حال عدم النقر على رابط معين، مما يستحث خوفًا غير مبرر ويؤدي إلى اتخاذ قرارات سريعة قد تعرضه للاختراق أو الاحتيال.

وتدعم الدراسات النفسية هذا التحليل، حيث أظهرت الأبحاث أن الأفراد يندفعون في اتخاذ قراراتهم في حالات يكون فيها التأثير العاطفي قويًا، وهو ما يوضح كيف يمكن للمهاجمين استخدام هذا الاندفاع العاطفي لصالحهم. في هذا السياق، تشير نظرية التحفيز العاطفي التي وضعها (Loewenstein. 2000) إلى أن العواطف تلعب دورًا محوريًا في تحفيز الأفراد لاتخاذ قرارات متسرعة قد تفتقر إلى التأمل النقدي. حيث يؤدي الاندفاع العاطفي الناتج عن التعرض لمحتوى عاطفي قوي إلى تحفيز الأشخاص على اتخاذ قرارات قد تكون ضارة، مثل المشاركة في أنشطة احتيالية أو التصرف بشكل يتعارض مع مصلحتهم.

ب **الثقة المفرطة والانفتاح على المجهول** في البيئة الرقمية، تتزايد ظاهرة الثقة المفرطة بين الأفراد، خاصة في تفاعلاتهم عبر الإنترنت. هذه الثقة غالبًا ما تؤدي إلى تجاهل بعض المؤشرات التحذيرية التي قد تشير إلى محاولات احتيال أو تهديدات رقمية. حيث يعزز الشعور بالراحة مع الأدوات الرقمية الثقة في الأفراد، مما يقلل من يقظتهم تجاه المخاطر الرقمية المحتملة. هذا يفتح المجال أمام المهاجمين للاستفادة من هذه الثقة المفرطة في استراتيجيات الاحتيال الرقمي.

يمكن ربط هذا السلوك بنظرية الغرور(Overconfidence Theory) ، التي تفترض أن الأفراد يميلون إلى تقييم قدراتهم في اتخاذ القرارات بشكل مبالغ فيه، مما يؤدي إلى تقدير خاطئ للمخاطر. وفقًا لدراسة قام بها (Lichtenstein et al. 1978)، أظهر الأشخاص الذين يعتقدون أن لديهم القدرة على اتخاذ قرارات سليمة في معظم الأحيان، عرضة أكبر للاستغلال من قبل المهاجمين الرقميين. في هذا السياق، يكون الأفراد الذين

يشعرون بالثقة المفرطة في قدرتهم على التمييز بين المحتوى الحقيقي والمحتوى المزيف أكثر عرضة لخطر الوقوع في فخاخ الاحتيال الرقمي، حيث يقل اهتمامهم بالعوامل التحذيرية التي قد تشير إلى أن التفاعل قد يكون ضارًا.

ج **التكيف الاجتماعي وتأثير وسائل التواصل:** تسهم وسائل التواصل الاجتماعي بشكل كبير في تعزيز التفاعل الرقمي بين الأفراد، حيث تتيح لهم الوصول إلى محتوى متنوع والتفاعل مع الآخرين في بيئة غير مادية. تشير الدراسات النفسية إلى أن هذه التفاعلات على الإنترنت تلعب دورًا مهمًا في التكيف الاجتماعي للأفراد، مما يعزز من قدرتهم على بناء الثقة بالآخرين وتقييم مصداقية الرسائل التي يتلقونها. هذا التكيف الاجتماعي قد يؤدي إلى زيادة الثقة في الرسائل القادمة من مصادر غير مألوفة أو غير موثوقة، مما يفتح المجال أمام المهاجمين لاستغلال هذه الثقة.

تنظر نظرية التفاعل الاجتماعي (Social Interaction Theory) إلى هذا السلوك من خلال فرضية أن الأفراد يتكيفون اجتماعيًا مع بيئتهم ويستجيبون للمحفزات بناءً على معرفتهم وثقتهم في الآخرين. في السياق الرقمي، يسهل التفاعل الاجتماعي عملية بناء الثقة في رسائل قد تكون غير موثوقة، مما يجعل الأفراد أكثر عرضة للتلاعب. من خلال هذه الديناميكية، يصبح الأفراد أكثر عرضة للاستغلال من قبل المهاجمين الذين يستخدمون أساليب الخداع والتلاعب النفسي في محاولاتهم للاحتيال عليهم.

د **الإنهاك النفسي وضغوط الحياة الرقمية:** إن تزايد الحمل المعلوماتي والإفراط في التفاعل مع البيئة الرقمية قد يؤدي إلى حالة من الإنهاك النفسي، مما يُضعف قدرة الأفراد على التفكير النقدي واتخاذ القرارات السليمة. الأفراد الذين يواجهون ضغوطًا يومية من العمل أو الحياة الشخصية يصبحون أكثر عرضة للانخداع بمحاولات الهندسة الاجتماعية، حيث يفتقرون إلى الطاقة أو التركيز اللازم لتحليل المعلومات المرسلة إليهم بشكل دقيق.

وفقًا لنظرية الإرهاق المعرفي(Cognitive Load Theory) ، التي وضعها(Sweller. 1988) ، إذا كان الشخص مثقلًا بالمعلومات أو الضغوط الخارجية، فإن قدرته على معالجة هذه المعلومات بفعالية ستنخفض. في سياق الهندسة الاجتماعية، يعني هذا أن الأفراد الذين يعانون من إجهاد معرفي قد يتخذون قرارات متسرعة بناءً على معلومات غير موثوقة، مما يزيد من خطر الوقوع في فخاخ الاحتيال.

يمكن القول إن التغيرات الرقمية قد أضافت طبقة من التعقيد لسلوك الأفراد في مواجهة محاولات الهندسة الاجتماعية. من خلال التحليل النفسي، يمكننا ملاحظة أن العواطف، الثقة المفرطة، التكيف الاجتماعي، والإرهاق النفسي تلعب دورًا كبيرًا في اتخاذ القرارات غير السليمة التي تفتح المجال

للهجمات الرقمية. من المهم أن تدرك المؤسسات والأفراد هذه العوامل النفسية وتعمل على تعزيز الوعي الرقمي لتقليل تأثيرات الهندسة الاجتماعية.

4. استجابة الأفراد للهندسة الاجتماعية بناءً على خلفياتهم الثقافية والاجتماعية والمهنية:

تلعب الثقافة دورًا أساسيًا في تفاعل الأفراد مع محاولات الهندسة الاجتماعية، حيث تؤثر القيم الاجتماعية والثقافية على كيفية استجابتهم للهجمات الرقمية. في بعض الثقافات التي تعزز الثقة المتبادلة والاحترام، قد يواجه الأفراد صعوبة في الشك في الرسائل التي تبدو موثوقة، حتى وإن كانت مشبوهة. هذه الثقة المفرطة تجعلهم عرضة للانخداع في البيئة الرقمية.

وفقًا لنظرية التفاعل الاجتماعي(Social Interaction Theory) ، يتكيف الأفراد مع بيئتهم الاجتماعية والثقافية، مما يحدد سلوكياتهم في التفاعل مع الآخرين. في الثقافات التي تقدر الاحترام والموثوقية، مثل الثقافات العربية والآسيوية، يميل الأفراد إلى الثقة بسهولة في التفاعلات الرقمية، مما يزيد من خطر تعرضهم للهجمات الهندسية.(Hofstede. 2001)

كما أن القيم الأخلاقية الثقافية تؤثر في استجابة الأفراد للهندسة الاجتماعية. في الثقافات التي تقدر الضيافة والكرم، يكون الأفراد أكثر تسامحًا في الرد على طلبات المساعدة، مما يجعلهم أكثر عرضة للاستغلال. نظرية الثقافة السلوكية (Cultural Behavior Theory) تشير إلى أن الأفراد يتبنون سلوكيات اجتماعية تؤثر على استجابتهم للهجمات الرقمية بناءً على القيم التي نشؤوا عليها، مما يساهم في تسهيل استغلالهم في محاولات الاحتيال.

1.4 التأثيرات النفسية التي تعتمد على الخلفية الاجتماعية والمهنية

أ. الطبقات الاجتماعية وتأثيرها على الثقة بالرسائل الرقمية

تنظر نظرية الطبقات الاجتماعية**(Social Interaction Theory)** إلى تأثير الوضع الاجتماعي على اتخاذ القرارات، حيث يمتلك الأفراد في الطبقات العليا قدرة أكبر على تحليل المعلومات الرقمية بفضل الخبرة الأكاديمية والتدريب المهني. بالمقابل، الأفراد في الطبقات الأقل قد يكونون أكثر عرضة للهندسة الاجتماعية بسبب قلة الوعي الرقمي أو غياب التدريب المناسب، مما يزيد من خطر الوقوع في فخ الاحتيال الرقمي (Becker & Jacobsen. 2019).

ب. المهنة والخبرة المهنية

يعد المجال المهني أحد العوامل النفسية المهمة التي تؤثر في استجابة الأفراد للهندسة الاجتماعية. فالموظفون في القطاعات التكنولوجية أو تلك التي تعتمد بشكل كبير على أمن المعلومات غالبًا ما يكونون

أكثر قدرة على التعرف على محاولات الاحتيال الرقمي مقارنةً بالأفراد الذين يعملون في مجالات غير مرتبطة بالأمن الرقمي.

وفقًا لنظرية التدريب المهني(Professional Training Theory) ، يظهر أن الأشخاص الذين يتلقون تدريبًا متخصصًا في التعامل مع المعلومات الحساسة أو في مجالات الأمن السيبراني يكونون أكثر وعيًا بالمخاطر الرقمية. لذا، فإن الأفراد الذين يعملون في بيئات تتطلب أمانًا عاليًا، مثل شركات التكنولوجيا أو المؤسسات المالية، يميلون إلى أن يكونوا أكثر مقاومة لهجمات الهندسة الاجتماعية.(Harris. 2017)

كما أن نظرية التعلم الرقمي :(Digital Learning Theory) أظهرت أن الأفراد الذين لديهم وصول مستمر إلى التعليم الرقمي يتطور لديهم وعي أكبر بالمخاطر الرقمية. يمكن لهؤلاء الأفراد أن يكونوا أكثر استعدادًا للتعامل مع محاولات الاحتيال بطريقة أكثر فاعلية، سواء في بيئات العمل أو في حياتهم الشخصية (Bélanger et al. 2013).

2.4 دور الخلفية الثقافية والمهنية في تصنيف المخاطر الرقمية

تختلف قدرة الأفراد على تصنيف المخاطر الرقمية بناءً على خلفياتهم الثقافية والاجتماعية والمهنية. الأفراد الذين نشأوا في ثقافات تُركّز على التحليل النقدي وتحقيق الشكوك في جميع المعلومات المرسلة يكونون أكثر قدرة على تمييز محاولات الهندسة الاجتماعية. على العكس، في الثقافات التي تكون فيها القيم الاجتماعية مثل الثقة الزائدة أو الاحترام المطلق هي السائدة، قد يكون الأفراد أقل قدرة على التمييز بين الرسائل الموثوقة وغير الموثوقة، وهذا ما تؤكده نظريات تحديد المخاطر الاجتماعية.(Hofstede. 2001)

4.3العوامل النفسية التي تؤثر في قدرة الأفراد على التعرف على محاولات الهندسة الاجتماعية:

أ **الثقة المفرطة:(Overconfidence)**

تُعد الثقة المفرطة من العوامل النفسية التي تؤثر بشكل كبير في قدرة الأفراد على التعامل مع محاولات الهندسة الاجتماعية. حيث يميل الأفراد الذين يعانون من الثقة المفرطة إلى المبالغة في تقدير قدراتهم واتخاذ قرارات سريعة دون تحليل كامل للتهديدات المحتملة. هذا يعرضهم للخطر، خاصةً عندما يثقون بسهولة في الرسائل الإلكترونية المريبة أو المكالمات الهاتفية المشبوهة. وقد أظهرت دراسة .Lichtenstein et al) (1978أن الأشخاص الذين يثقون في قراراتهم بشكل مفرط يكونون أكثر عرضة للمخاطر في بيئات غير مؤكدة مثل البيئة الرقمية. وللتعامل مع هذه الظاهرة، يُنصح بتعزيز التفكير النقدي من خلال تدريب الأفراد على الشك في الرسائل الغريبة والتمييز بين المواقف المألوفة وغير المألوفة، مما يساعد على تقليل تأثير الثقة المفرطة على استجابتهم للهجمات الرقمية.

ب **الضغط العاطفي:(Emotional Stress)**

يؤثر الضغط العاطفي بشكل كبير على قدرة الأفراد على اتخاذ قرارات مدروسة، حيث يؤدي إلى انخفاض قدرتهم على التفكير العقلاني، مما يدفعهم إلى اتخاذ قرارات سريعة دون تحليل دقيق. وفقًا لنظرية الإرهاق المعرفي(Cognitive Load Theory) ، الأفراد في حالات الضغط النفسي يفقدون القدرة على معالجة المعلومات بشكل فعال. يستغل المهاجمون هذا الضغط العاطفي لإجبار الأفراد على اتخاذ قرارات سريعة قد تؤدي إلى وقوعهم في فخ الاحتيال. لمواجهة هذا التحدي، يُنصح بتدريب الأفراد على التعرف على الإشارات العاطفية التي قد تشير إلى محاولات الهندسة الاجتماعية، بالإضافة إلى استخدام تقنيات مثل التنفس العميق للحفاظ على الهدوء أثناء التفاعل مع المحتوى المشبوه.

ج **التحفيز العاطفي:(Emotional Manipulation)**

يستفيد المهاجمون في محاولات الهندسة الاجتماعية من العواطف البشرية عبر التهديدات أو الوعود بالثروات، مما يدفع الأفراد إلى اتخاذ قرارات غير مدروسة. وفقًا لنظرية التحفيز العاطفي .Loewenstein) (2000، الأفراد الذين يتعرضون لتحفيزات عاطفية قوية يكونون أكثر عرضة لاتخاذ قرارات غير مدروسة نتيجة للضغط العاطفي. التأثير الفوري للتحفيز العاطفي، مثل الخوف أو الإغراء المالي، يسرع استجابة الأفراد ويقلل من قدرتهم على التحقق من صحة الرسائل. لمواجهة هذا التأثير، يُنصح بتدريب الأفراد على التمييز بين المشاعر العاطفية والتفكير العقلاني وتعزيز التفكير النقدي قبل اتخاذ أي إجراء عند التعامل مع محتوى مشبوه.

د **التفاعل الاجتماعي وميل الأفراد إلى الانخداع:(Social Influence)**

يعتبر التفاعل الاجتماعي من العوامل المؤثرة في استجابة الأفراد للهندسة الاجتماعية، حيث يصبحون أكثر عرضة للاستجابة عندما يتعرضون لتأثيرات اجتماعية مثل الضغط الجماعي أو التوافق الاجتماعي. وفقًا لنظرية الامتثال الاجتماعي(Cialdini. 2006) ، فيميل الأفراد إلى تقليد سلوك الآخرين أو اتباع تعليمات مجموعة معينة دون التفكير النقدي. يستغل المهاجمون تأثير الجماعة في محاولات الهندسة الاجتماعية، مثل ادعاء أن "جميع أصدقائك استجابوا لهذا العرض"، لزيادة الضغط الاجتماعي على الأفراد. لمواجهة هذه المحاولات، من الضروري تعزيز الوعي بالتحفيزات الاجتماعية وتعليم الأفراد تمسكهم بالقيم الشخصية والشك في الانطباعات التي يتلقونها من الآخرين.

5. دور الوعي الرقمي في الوقاية من الهندسة الاجتماعية

يعتبر الوعي الرقمي عاملاً رئيسيًا في الوقاية من الهندسة الاجتماعية، حيث يمكن أن يسهم في تمكين الأفراد من اكتشاف محاولات الاحتيال وتجنبها قبل الوقوع فيها.

تشير الدراسات إلى أن الأفراد الذين يتمتعون بوعي رقمي عالي يكونون أكثر قدرة على التمييز بين الرسائل المشروعة والمحتالة .(Bridges et al. 2019) فعندما يكون الأفراد على دراية بأنواع الهجمات المختلفة مثل التصيد الإلكتروني (Phishing) أو المهاجمين الذين يتنكرون في صورة مصدر موثوق، يصبحون أكثر حذرًا في التعامل مع المواقف المشبوهة. علاوة على ذلك، يساهم الوعي الرقمي في تعزيز التفكير النقدي، وهو عنصر حاسم في مواجهة التهديدات الرقمية. وفقًا لـ(Bada, Sasse, & Nurse. 2019) ، فإن الأفراد الذين يتلقون تدريبات متخصصة في الوعي الرقمي أكثر قدرة على تطبيق استراتيجيات الأمان الرقمي على حياتهم اليومية، وبالتالي يصبحون أقل عرضة للخداع.

ويكون التدريب على الوعي الرقمي من خلال تدريب الأفراد على مفاهيم الوعي الرقمي، يمكن تقليل فرص نجاح محاولات الهندسة الاجتماعية. يمكن أن يشمل التدريب على الوعي الرقمي مجموعة من الأنشطة مثل ورش العمل التفاعلية التي تركز على تقنيات الحماية، وشرح أساليب الهندسة الاجتماعية التي قد يواجهها المستخدمون في بيئاتهم الرقمية. كما يجب أن يتضمن التدريب على كيفية التحقق من صحة الرسائل الواردة، ومراجعة المصادر قبل اتخاذ القرارات الرقمية، واستخدام أدوات الأمان مثل التحقق الثنائي-Two) (Factor Authentication لمنع الوصول غير المصرح به إلى الحسابات الرقمية.(Verizon. 2020)

على الرغم من أهمية الوعي الرقمي، إلا أن تطبيقه يواجه العديد من التحديات. من أبرز هذه التحديات هو التنوع في مستوى المعرفة الرقمية بين الأفراد. ففي حين يمتلك البعض معرفة متقدمة بالأمن الرقمي، يفتقر آخرون إلى هذه المهارات الأساسية، مما يجعلهم عرضة للهجمات .(Harrington. 2021) لذلك، فإن التعليم المستمر حول أمن المعلومات يعد أمرًا حيويًا لتقليل هذه الفجوات المعرفية.

6. الاستراتيجيات النفسية للحد من الهندسة الاجتماعية في ظل التغيرات الرقمية في المجتمع وبيئات العمل

إن التغيرات الرقمية المتسارعة في المجتمع وفي بيئات العمل قد خلقت تحديات جديدة تتعلق بالأمن السيبراني والهندسة الاجتماعية. الهندسة الاجتماعية، التي تعتمد على التلاعب النفسي بالأفراد للحصول على معلومات حساسة، أصبحت أحد أكثر الأساليب المستخدمة في الهجمات الرقمية. في هذا السياق، تُعد الاستراتيجيات النفسية من الأدوات الفعالة في الحد من هذه الهجمات، إذ تساهم في تقوية الوعي الرقمي وتعزيز التفكير النقدي في مواجهة المحاولات الاحتيالية.

1.6 تعزيز الوعي الرقمي والنقدي

الوعي الرقمي يعتبر أحد الأسس النفسية التي تساعد الأفراد على التعرف على محاولات الهندسة الاجتماعية. وفقًا لـ(Hadnagy. 2018) ، يشمل الوعي الرقمي التدريب على كيفية التعامل مع المعلومات في

البيئة الرقمية، والتأكد من صحة الرسائل الواردة، والتحقق من مصادر المعلومات قبل اتخاذ القرارات. في بيئات العمل، يمكن أن يساهم تدريب الموظفين على معرفة الأساليب المتبعة في الهجمات الإلكترونية والتعامل معها بشكل نقدي في تقليل المخاطر المرتبطة بالهندسة الاجتماعية.

2.6 استخدام تقنيات التنبيه النفسي(Cognitive Behavioral Techniques)

تعتبر تقنيات التنبيه النفسي جزءًا أساسيًا من الاستراتيجيات النفسية التي يمكن أن تساعد الأفراد في الحد من تأثير الهندسة الاجتماعية. هذه التقنيات، مثل التفكير النقدي وإعادة تقييم المواقف، تساهم في تحفيز الأفراد على تحليل المعلومات بشكل منطقي وواقعي بدلاً من الانسياق وراء الانفعالات أو التحفيزات العاطفية. تشير دراسات (Bada et al. 2019) إلى أن تدريب الأفراد على استخدام هذه التقنيات يمكن أن يساعدهم في مقاومة التحفيزات العاطفية التي يستخدمها المهاجمون في محاولاتهم.

3.6 التحفيز الذاتي وتقنيات الهدوء العقلي

التحفيز الذاتي وتنظيم المشاعر يمكن أن يكون لهما تأثير كبير في الحد من الاستجابة السريعة للهجمات. وفقًا لنظرية الإرهاق المعرفي(Sweller. 1988) ، فإن الأشخاص الذين يعانون من ضغط عاطفي أو نفسي يكونون أكثر عرضة لاتخاذ قرارات متسرعة. لتقليل تأثير هذه الضغوط، يمكن تعليم الأفراد تقنيات مثل التنفس العميق، والانعزال المؤقت عن الموقف، وتقييم الرسالة بعقلانية قبل اتخاذ أي قرار.

4.6 تعزيز ثقافة الشك النقدي في بيئات العمل

في بيئات العمل الحديثة، يعد التحفيز على الشك النقدي والثقافة الأمنية جزءًا من الاستراتيجيات النفسية الأساسية للحد من الهندسة الاجتماعية. يُعتبر تعزيز التفكير النقدي ثقافة مؤسسية مهمة بحيث يتم تدريب الموظفين على كيفية التعامل مع المحفزات الخارجية التي قد تكون مشبوهة. وفقًا لـ(Cialdini. 2006) ، يمكن أن تساعد ثقافة الامتثال الاجتماعي في المؤسسات على تعزيز وعي الموظفين بالمخاطر الرقمية ومنعهم من الوقوع في فخاخ الاحتيال.

5.6 تعزيز الوعي الاجتماعي والتأثير الجماعي

من الاستراتيجيات النفسية المهمة هي فهم التأثير الاجتماعي. وفقًا لنظرية الامتثال الاجتماعي .Cialdini) (2006، يتأثر الأفراد بالمجموعة التي ينتمون إليها، مما يجعلهم أكثر عرضة لتقليد سلوك الآخرين دون التفكير النقدي. لتعزيز مقاومة الأفراد للهندسة الاجتماعية، من المهم تدريبهم على اتخاذ القرارات بناءً على قيمهم الشخصية وتجنب التأثيرات الاجتماعية السلبية التي قد تقودهم إلى اتخاذ قرارات غير مدروسة.

6.6 تقديم برامج تدريبية ومراجعة مستمرة

أخيرًا، من الاستراتيجيات النفسية الهامة للحد من الهندسة الاجتماعية، هي تقديم برامج تدريبية مستمرة تركز على تحديث المعلومات حول أساليب الهجوم الرقمي الجديدة وكيفية التعامل معها. مثل هذه البرامج تساهم في تعزيز الوعي والمناعة النفسية ضد محاولات الهندسة الاجتماعية. يمكن أن تشتمل البرامج على محاكاة لهجمات الهندسة الاجتماعية بهدف تدريب الأفراد على التعرف على الأنماط التي قد تكون مشبوهة والتعامل معها بشكل فعّال.(Harris, 2017)

النقدي والشجاعة في اتخاذ القرارات في تعزيز قدرة الأفراد على مواجهة محاولات الهندسة الاجتماعية بشكل فعّال.

5. الخاتمة:

لقد أظهرت التحولات الرقمية السريعة تأثيرًا كبيرًا على سلوك الأفراد في مواجهة محاولات الهندسة الاجتماعية. مع تزايد الاعتماد على التكنولوجيا والبيئات الرقمية في حياتنا اليومية وبيئات العمل، أصبح الأفراد أكثر عرضة للهجمات الرقمية التي تعتمد على التلاعب النفسي. وقد تم تحديد العديد من العوامل النفسية التي تؤثر في قدرة الأفراد على التعرف على هذه المحاولات والوقاية منها، مثل الثقة المفرطة، الضغط العاطفي، التحفيز العاطفي، والتفاعل الاجتماعي. على الرغم من التطور التكنولوجي، فإن تعزيز الوعي الرقمي والتفكير النقدي يعتبران من أبرز الاستراتيجيات الوقائية ضد هذه الهجمات. إذ إن فهم تأثير هذه التغيرات وتوفير التدريب المستمر للأفراد يساهم بشكل كبير في تقليل المخاطر المرتبطة بالهندسة الاجتماعية.

التوصيات:

1. تعزيز برامج التدريب على الوعي الرقمي في المجتمع وبيئات العمل لمساعدة الأفراد على التعرف على أساليب الهندسة الاجتماعية، مثل التصيد الإلكتروني والاحتيال الرقمي.
2. تدريب الأفراد على تعزيز التفكير النقدي والقدرة على تحليل الرسائل المشبوهة بشكل منطقي، بعيدًا عن الانفعالات العاطفية أو التحفيزات اللحظية.
3. استمرار برامج التدريب حول الأمن السيبراني والهندسة الاجتماعية بشكل دوري لمواكبة التغيرات الرقمية وأساليب الهجوم الجديدة.
4. توفير تقنيات لإدارة الضغوط النفسية مثل التنفس العميق أو التوقف للتفكير، لمساعدة الأفراد في اتخاذ قرارات مدروسة في المواقف المشحونة عاطفيًا.

5. يجب تبني ثقافة أمنية تشجع على الشك في الرسائل والمحتويات الرقمية التي قد تكون مشبوهة، وتحفيز الأفراد على التحقق من صحتها قبل اتخاذ أي إجراء.
6. تعاون المؤسسات الحكومية والشركات الخاصة في تطوير سياسات أمنية تضمن حماية الأفراد من محاولات الهندسة الاجتماعية، من خلال نشر الوعي وتنظيم حملات توعية جماعية.

باتباع هذه التوصيات، يمكن تقليل تأثير الهندسة الاجتماعية وتحقيق بيئة رقمية أكثر أمانًا، مما يعزز من قدرة الأفراد على مواجهة تحديات الأمن الرقمي بكفاءة.

6. قائمة المراجع:

- العوضي، ع. (2021). تأثير التغيرات الرقمية على سلوك الأفراد في الوطن العربي .دراسات أمنية عربية، 8(2)، 97-110.
- الطيب، م. (2019). الوعي الرقمي وأثره في مكافحة التهديدات الرقمية في تونس .مجلة أمن المعلومات، 14(3)، 60-75.
- بن فاطمة، س. (2022). الوعي الرقمي في الجزائر: دراسة تحليلية لتأثير التغيرات الرقمية على سلوك الأفراد . مجلة الأمن السيبراني الجزائرية، 5(1)، 45-58.
- بلحاج، م. (2021). تأثير غياب برامج التوعية الرقمية على المؤسسات الجزائرية .دراسات سيبرانية، 7(3)، 120-134.
- موسى، ف. (2020). التدريب على الأمان الرقمي في الجزائر: أثره على مقاومة الهجمات الهندسية الاجتماعية . مجلة تكنولوجيا المعلومات والاتصالات، 9(2)، 85-99.
- Cialdini, R. B. (2009). *Influence : Science and practice* (5th ed.). Pearson.
- Bélanger, F., et al. (2020). "The role of digital awareness in combating social engineering attacks." *Journal of Digital Security*, 12(4), 23-38.
- Mayer, R., et al. (2020). "Digital awareness and its effects on social engineering vulnerability." *Cybersecurity & Digital Protection*, 25(1), 45-59.
- Gupta, S., & Shalender, P. (2014). Cyber security: *Protecting against social engineering threats*. IGI Global.
- Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Wiley.
- Jones-Kavalier, B., & Flannigan, S. L. (2006). Connecting the digital dots: Literacy of the 21st century. EDUCAUSE Review, 41(1), 60-67.
- Symantec. (2019). *Internet security threat report*. Symantec Corporation.
- Hathaway, R., Libicki, M. C., & Alexander, W. (2012). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
- Ally, M. (2008). *Foundations of educational theory for online learning*. Athabasca University Press.

- Cialdini, R. B., & Goldstein, N. J. (2004). Social influence : Compliance and conformity. Annual Review of Psychology, 55, 591-621.
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with e-commerce vendors. Journal of Strategic Information Systems, 11(3-4), 297-323.
- Hong, J. (2012). *Phishing: Causes, concerns, and countermeasures*. Computers & Security, 31(5), 1-9
- Bodo, S. (2017). *Multi-factor authentication: Secure identity management*. Springer.
- Loewenstein, G. F. (2000). Emotions in economic theory and research. The Economic Journal, 110(460), 426-453.
- Lichtenstein, S., Fischhoff, B., & Phillips, L. D. (1978). Calibration of probabilities: The state of the art to 1980. In Judgment under uncertainty: Heuristics and biases (pp. 305-334). Cambridge University Press.
- Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. Cognitive Science, 12(2), 257-285.
- Becker, M. R., & Jacobsen, J. (2019). Social class and cybersecurity awareness: A study of the digital divide. Journal of Technology and Society, 15(2), 49-66.
- Bélanger, F., Crossler, R. E., & Neuville, C. (2013). Digital security and privacy in the digital age: A conceptual framework. Journal of Business Research, 66(5), 642-650.
- Harris, S. (2017). Security awareness and training: The keys to mitigating social engineering attacks. Information Systems Security, 14(3), 37-45.
- Hofstede, G. (2001). Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations. Sage Publications.
- Cialdini, R. B. (2006). Influence: The psychology of persuasion. Harper Business.
- Lichtenstein, S., Fischhoff, B., & Phillips, L. D. (1978). Calibration of probabilities: The state of the art to 1980. In Judgment under uncertainty: Heuristics and biases (pp. 305-334). Cambridge University Press.
- Loewenstein, G. F. (2000). Emotions in economic theory and research. The Economic Journal, 110(460), 426-453.
- Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. Cognitive Science, 12(2), 257-285.

- Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*.
- Bridges, L., Nancarrow, C., & Binns, R. (2019). Enhancing digital literacy skills to prevent online security breaches. *Journal of Information Security*, 12(4), 123-135.
- Hadnagy, C. (2018). *Social engineering: The art of human hacking* (2nd ed.). Wiley.

- Harrington, S. (2021). Cyber security training for all: Overcoming barriers to effective digital literacy. *Cybersecurity Education and Awareness Review*, 7(1), 15-28.
- Jones, A. (2015). The importance of digital literacy in the modern age. *International Journal of Digital Literacy*, 23(1), 1-15.
- Verizon. (2020). *2020 Data Breach Investigations Report*.