

بحوث – النص الكامل

دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي: نموذج مقترح

حقوق النشر (c) 2024، عبد
الرشيد عبد العزيز حافظ،
الحبابي مبارك القحطاني



هذا العمل متاح وفقا لترخيص
المشاع الإبداعي 4.0 ترخيص
دولي

ا.د. عبد الرشيد عبد العزيز حافظ

أستاذ، قسم علم المعلومات،

جامعة الملك عبدالعزيز، جدة، السعودية

aahafez@kau.edu.sa

د. الحبابي مبارك القحطاني

مدير إدارة البحث الأكاديمي،

كلية الملك عبدالله للقيادة والأركان، الرياض، السعودية

hubabi@hotmail.com

المستخلص

كان من شأن التطورات الكبيرة في مجال إدارة المعرفة، و تقنية المعلومات وما نتج عنها من تسريع وتيرة الابتكار، وزيادة معدلات استخدام الأجهزة الذكية والتطبيقات المحوسبة، كان أن ظهرت في المقابل وسائل وأساليب اختراق البيانات فيما يعرف بالهندسة الاجتماعية، مما أصبح يشكل تهديدا حقيقيا لمنظمات الأعمال على اختلاف أنواعها ونشاطاتها، من هنا كان لا بد من وجود أنظمة فعالة للحماية من الاختراق والاستخدام غير المصرح به، ولأن ذلك يعد أحد الأدوار الأساسية التي يجب أن تضطلع بها إدارة المعرفة، تسعى الدراسة الحالية إلى التعرف على مرئيات المسؤولين والعاملين في القطاع المصرفي، والبنك المركزي في المملكة العربية السعودية لتشخيص المشكلات والتعرف على الثغرات، ومن ثم الخروج بنموذج مقترح يركز على مجموعة متكاملة من المدخلات والمعالجة والمخرجات، ويساعد على الوقاية من تهديدات الهندسة الاجتماعية، تمت

الاستعانة بمجموعة تركيز تتكون من خبراء ومختصين أخذت ملاحظاتهم للخروج بالشكل النهائي للتطبيق في القطاع المصرفي.

الكلمات المفتاحية

إدارة المعرفة، الهندسة الاجتماعية، الاحتيال المالي، القطاع المصرفي

المقدمة

تتصف بيئة الأعمال -اليوم- بديناميكية شديدة وخطى سريعة، كما توظف تقنيات متقدمة، إلا أنها ليست في مأمن من التهديدات؛ فالطريقة التي تستخدم بها المنظمات أصولها، مثل: العمليات الرقمية والمعلومات وأنظمة تكنولوجيا المعلومات تتعرض -بشكل متزايد- للتهديدات الأمنية خارجيًا وداخليًا، مثل: السرقة، والاحتيال، والتخريب، والاختلاس، والتجسس، تركز هذه التهديدات بشكل كبير على العنصر البشري كحلقة ضعيفة في نظام الأمن السيبراني، ويتم استغلال نقاط الضعف مثل: الخداع والإقناع والتلاعب، وفي هذا السياق، تأتي أهمية إدارة المعرفة كوسيلة لتحليل، وفهم كيفية استغلال الفجوات التقنية والاجتماعية، وكيف يمكن استخدام المعرفة لصنع طرق فعالة للوقاية والحماية؟ وبالتالي، يُعزز ذلك من القدرة على مواجهة الأساليب الاحتيالية التي تتم باقتناص نقاط القصور في الإجراءات الرقابية أو التقنية للبنوك والمصارف، أو استغلال ضعف الوعي لدى العملاء، من خلال نهج شامل يركز على تكنولوجيا المعلومات، والثقافة التنظيمية، وعمليات إدارة المعرفة المتكاملة، والخروج بحلول فعالة تحد من آثارها، ويأتي دور إدارة المعرفة في مواجهة الهندسة الاجتماعية من خلال تطوير نظام متكامل يشمل التكنولوجيا وثقافة المنظمة والعنصر البشري، ويتضمن بناء ثقافة معلوماتية قوية تعزز الوعي بأساليب الهندسة الاجتماعية، وتساعد في كشف المخترقين ومقاومتهم، باستخدام أساليبهم وأدواتهم نفسها عند الحاجة، وتسعى الدراسة الحالية إلى بناء نموذج متكامل وفعال يبدأ بتحسين وتطوير النماذج الحالية للوقاية، وإجراء دراسات تحليلية لسلوك الموظفين وممارساتهم، ومدى الامتثال للسياسات الأمنية، وتنفيذ حملات توعية بتهديدات الهندسة الاجتماعية، وتطبيق المعايير الدولية والوطنية ذات الصلة بتكنولوجيا المعلومات لضمان الوقاية الشاملة.

مشكلة الدراسة:

أحدث تطور الثورة التكنولوجية تحولًا كبيرًا في العالم، وأتاح ظهور وسائل متعددة ومبتكرة ساهمت في ربط الأمم وتسهيل وسائل التواصل، ومع ذلك، أسفر هذا التقدم عن فتح الأبواب أمام أنماط مختلفة من السلوك الإجرامي المخالف للقواعد والمعايير الاجتماعية والقوانين المختلفة، مما يشكل تهديدًا للأفراد والمجتمعات وأمن المعلومات، وفي هذا السياق، يبرز دور إدارة المعرفة في مواجهة الهندسة الاجتماعية، وبخاصة في قطاع المصارف، ويتم اتخاذ الإجراءات ووضع السياسات المتكاملة لتحقيق الأمن وحماية الخصوصية وسلامة المعلومات، وبالنظر إلى الإنتاج الفكري يمكن ملاحظة قلة الدراسات العربية التي تناولت هذا الموضوع، ويمكن تلخيص مشكلة الدراسة في السؤال التالي: ما دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي ؟

أهمية المشكلة:

بالرغم من كل ما ورد من أنظمة وأدلة وضوابط، والجهود التي يقوم بها البنك المركزي السعودي وغيرها من الجهات العامة والخاصة، ما زالت هناك حاجة ماسة لإدارة المعرفة المستهدفة والمتخصصة، وتشمل هذه الجهود إطلاق حملات توعية على مستوى الوطن، وإرسال رسائل تنبيهية بأنماط وأساليب الاحتيال المالي وسبل الوقاية منها، وتطبيق مفاهيم إدارة المعرفة لفهم الهندسة الاجتماعية والتصدي لها في القطاع المصرفي، وعلى الرغم من هذه الجهود، لا يكاد يمر يوم لا نسمع فيه عن حالة احتيال مالي، ومصرفي بأسلوب، ونمط جديد ومبتكر، مما يتطلب جمع وتحليل وتوزيع المعلومات الضرورية لفهم هذه التهديدات والتصدي لها، وتعزيز الأمان في القطاع المصرفي السعودي.

أهمية الدراسة :

تنبع أهمية الدراسة من حيوية الموضوع، وما تمثله الهندسة الاجتماعية من تهديدات خطيرة وضرورة الوقاية منها، وتعتبر أيضاً من الاتجاهات الحديثة في المجال من حيث ربط إدارة المعرفة بالهندسة الاجتماعية، وكتسب الدراسة كونها تتناول تطبيق إدارة المعرفة في القطاع المصرفي السعودي وعلاقتها في تفعيل الوقاية من الهندسة الاجتماعية - الأمن السيبراني.

تكمن أهمية الدراسة كذلك في سد الفجوة في الدراسات السابقة، والتي يندر وجودها في العالم العربي، ودراسة الواقع المرتبط بالاحتيال المالي في القطاع المصرفي السعودي، من المأمول أن يستفيد القطاع المصرفي السعودي من هذه الدراسة في تبني نموذج مقترح لإدارة المعرفة في مواجهة تهديدات الهندسة الاجتماعية.

أهداف الدراسة :

يتمثل الهدف الرئيسي لهذه الدراسة في اقتراح نموذج متكامل يستند إلى إدارة المعرفة لمواجهة تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي، ومن أجل تحقيق هذا الهدف، تتفرع الأهداف التالية:

1. التعرف على واقع تطبيق إدارة المعرفة بالقطاع المصرفي السعودي.
2. التعرف على مدى الوعي بأبرز تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي.
3. التعرف على الأدوار التي تقدمها إدارة المعرفة في مواجهة الهندسة الاجتماعية بالقطاع المصرفي السعودي.
4. الكشف عن التحديات التي تعيق دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي.
5. بناء نموذج مقترح لاستثمار دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي.

تساؤلات الدراسة :

يتمثل السؤال الرئيسي لهذه الدراسة في: ما دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي؟ وما النموذج المقترح لتفعيل هذا الدور؟ وتتفرع الأسئلة الفرعية التالية:

1. ما واقع تطبيق إدارة المعرفة بالقطاع المصرفي السعودي؟
2. ما مدى الوعي بأبرز تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي؟

3. ما الأدوار التي تقدمها إدارة المعرفة في مواجهة الهندسة الاجتماعية بالقطاع المصرفي السعودي؟
 4. ما التحديات التي تعيق دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي؟
 5. ما المقترحات التي تسهم في تفعيل دور إدارة المعرفة في مواجهة الهندسة الاجتماعية بالقطاع المصرفي السعودي؟
- حدود الدراسة :**

تنحصر الدراسة ضمن نطاق البنك المركزي السعودي والقطاع المصرفي السعودي في المنطقة الوسطى وتحديدًا مدينة الرياض، كما تقتصر الدراسة على مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى الذين لهم صلة مباشرة بالأمن السيبراني.

منهج الدراسة :

وظفت الدراسة منهج دراسة الحالة، والمنهج الوصفي المسحي للكشف عن دور إدارة المعرفة في مواجهة الهندسة الاجتماعية بالقطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي والقطاع المصرفي السعودي بالمنطقة الوسطى الذين لهم صلة مباشرة بالأمن السيبراني: كما تم تصميم استبانة موجهة إلى عينة قصدية من مسؤولي البنك المركزي السعودي والقطاع المصرفي بالمنطقة الوسطى الذين لهم صلة مباشرة بالأمن السيبراني، بهدف تحديد مدى وعيهم واستخدامهم لإدارة المعرفة في المواجهة، والوقاية من الهندسة الاجتماعية في القطاع المصرفي السعودي، كما استعانت بمجموعة التركيز لتقييم النموذج الذي تقترحه الدراسة الحالية الذي جاء نتيجة الاطلاع على الأدبيات والدراسات المتعلقة بإدارة المعرفة وتهديدات الهندسة الاجتماعية في القطاع المصرفي .

مصطلحات الدراسة:

فيما يلي تعريف لأهم مصطلحات الدراسة :

تهديدات (Threats):

أي: ظرف أو حدث من المحتمل أن يؤثر سلبيًا على أعمال الجهة المعنية بما في ذلك مهمتها، أو وظائفها، أو مصداقيتها، أو سمعتها، أو أصولها، أو منسوبيها، بواسطة أحد أنظمة المعلومات عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تغييرها أو حجب الخدمة، وأيضا قدرة مصدر التهديد على النجاح في استغلال أحد نقاط الضعف الخاصة بنظام معلومات معين" (الهيئة الوطنية للأمن السيبراني 2018).

التعريف الإجرائي للتهديدات: جميع ما يساعد في التعدي على خصوصية الأفراد، وأمن المعلومات، باستخدام الهندسة الاجتماعية.

الهندسة الاجتماعية (Social engineering):

هي فن استخراج معلومات سرية عن طريق التلاعب النفسي، وخداع الأفراد في إعطاء المعلومات الخاصة بهم مثل: كلمات المرور وغيرها من المعلومات" (الغنبر والقحطاني، 2009: 31).

التعريف الإجرائي: جميع الأساليب المتطورة والخدع المستخدمة بهدف التأثير على الضحية، والحصول على المعلومات المستهدفة بأساليب متعددة تستند على ذكاء المهاجم ومهاراته الفردية وخبراته التقنية.

إدارة المعرفة (knowledge management):

حظي مفهوم إدارة المعرفة في السنوات الأخيرة باهتمام متزايد من قبل الباحثين والمتخصصين، وذلك للدور الذي تلعبه هذه الإدارة في تحقيق إستراتيجيات وسياسات المنظمات بكفاءة وفعالية، وفي عالم اليوم أصبحت المعرفة الأساس الذي تستند عليه المنظمات في تحقيق الميزة التنافسية لها، ومن هنا يجب الاهتمام بها وإدارتها بالشكل السليم لجعلها جاهزة للتطبيق والانتشار داخل المنظمة.

تعرف إدارة المعرفة بأنها: "القيام بما يلزم للحصول على أكبر قدر ممكن من موارد المعرفة" (بيسرا وسايروال، 2014، 22).

التعريف الإجرائي: تنظيم وتنسيق عمليات الجمع، والتحليل، واستخدام المعلومات، والمعرفة، وذلك لتعزيز التفاهم واتخاذ القرارات المناسبة وزيادة الفعالية، بالإضافة إلى تحفيز المشاركة في المعرفة، وتسهيل الوصول إليها وحمايتها وتقدير قيمتها في سياق معين.

الإطار النظري للدراسة

تتناول الفقرة التالية أدبيات الدراسة، وما يتعلق بموضوعها من الدراسات السابقة، إضافة إلى استعراض النماذج التي تم طرحها:

أولاً: أدبيات الدراسة:

الهندسة الاجتماعية والأمن السيبراني:

يُعرف الأمن السيبراني بكونه عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني، والأمن السيبراني هو سلاح إستراتيجي بيد الحكومات والأفراد لاسيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول (الصحفي وعسكول، 2019، 498).

وحسب (محارب 2023) هو: "عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية؛ وتهدف هذه الهجمات السيبرانية عادةً إلى الوصول للمعلومات الحساسة أو تغييرها أو تدميرها؛ بغرض الاستيلاء على المال من المستخدمين أو مقاطعة عمليات الأعمال العادية" (محارب، 2023، 5)، وللأمن السيبراني أهمية كبيرة في حفظ المعلومات والبيانات الخاصة بالمؤسسات والأفراد، ولذلك يمكننا عرض أهميتها فيما يلي (الشهري، 2021):

1. السرية والأمان: يساعد الأمن السيبراني في التأكد من كون المعلومات لا يتم كشفها أو الاطلاع عليها من قبل أشخاص غير مخولين بذلك.
 2. التكاملية وسلامة المحتوى: وهو التأكد من محتوى المعلومات بأنه صحيح ولم يتم تعديله، وعلى نحو خاص لم يتم تدميره أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل، سواءً في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.
 3. استمرارية توفر المعلومات أو الخدمة: إذ يجب التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، والمستخدم لن يتعرض إلى منع الاستخدام أو الدخول إلى النظام.
 4. عدم إنكار التصرف المرتبط بالمعلومات ممن قام به: ويقصد به ضمان إنكار الشخص المتصل بالمعلومات أو مواقعها بقيامه بتصرف ما، بحيث تتوافر قدرة إثبات هذا التصرف و هناك شخص قد قام بذلك، كذلك عدم قدرة مستلم الرسالة على إنكار استلامه لها.
- مخاطر الهندسة الاجتماعية على الأمن السيبراني:**

هناك العديد من المخاطر التي تواجه المجتمعات نتيجة استخدام الهندسة الاجتماعية في الهجمات السيبرانية، ومن أبرز تلك المخاطر ما يلي:

- 1- تصاعد التهديدات للبنى التحتية الحيوية: تزايد التهديدات التي تمثلها الجرائم السيبرانية باستخدام العديد من الأساليب المعلوماتية ومنها الهندسة الاجتماعية، مثل: محطات الكهرباء وأنابيب النفط، وأيضًا الخطوط الجوية والسكك الحديدية، والبنوك.
 - 2- صعوبة تحديد هوية الطرف المهاجم: يعود ذلك إلى صعوبة ربط العمل العدائي في الفضاء السيبراني بدولة معينة أو شخص معين، إذ إن العمليات اللازمة لتحليل هوية المهاجم يمكن أن تأخذ شهورًا، وربما تفشل في النهاية للتوصل إلى هوية المهاجم (منصور، 2019).
 - 3- استحالة تحقيق الأمن الكامل: يعد التأمين الكامل للدولة من الهجمات السيبرانية أمرًا مستحيلًا، ولعل ما يؤكد هذا الواقع التصريحات السابقة لـ (جيمس كومي) مدير مكتب التحقيقات الفيدرالية الأمريكي السابق، الذي أكد أن هناك نوعين من الشركات الكبرى في الولايات المتحدة، وهما تلك التي تم اختراقهما من جانب الصينيين، وتلك التي لم تدرك بعد أنه تم اختراقها من جانبهم نتيجة استخدامهم أساليب مختلفة منها الهندسة الاجتماعية (منصور، 2019)، وتعد من أبرز الجرائم السيبرانية التي تؤكد على استحالة الأمن الكامل، اتهام روسيا للولايات المتحدة الأمريكية بشن هجوم سيبراني من خلال هكرز عسكريين، تمكنوا من التسلل إلى الأنظمة الإلكترونية الخاصة بشبكات الطاقة الكهربائية الروسية ونظم الاتصالات، بالإضافة إلى اختراق منظومة القيادة في الكرملين، واستطاعوا أن يجعلوها قابلة للتعرض للهجمات الإلكترونية من جانب الولايات المتحدة الأمريكية عن طريق استخدام سلاح إلكتروني سري (عبد الوهاب، 2017).
- جهود المملكة في تعزيز الأمن السيبراني:**

وصل حجم الإنفاق المتعلق بالأمن السيبراني في العالم إلى أكثر من 360 مليار دولار، وأعلنت شركة كاسير سكاي الأمنية في المملكة العربية السعودية بأن ما نسبته (60%) من المنشآت السعودية تعرضت لهجمات سيبرانية في الأعوام 2018-2022م، وأن هناك ما نسبته 40% مازالت بحاجة ماسة لتطوير أدواتها الدفاعية

ضد مثل هذه الهجمات، لذا وفي ضوء تعاظم دور الفضاء الإلكتروني في تحقيق رؤية المملكة 2030م، وبخاصةً مع تزايد التهديدات السيبرانية أضحت من الأهمية حماية أنظمة المعلومات والاتصالات ضد هجمات الفضاء السيبراني، وفي الوقت ذاته العمل للحفاظ على سرية وسلامة المعلومات، وإتاحة الوصول إلى ممتلكات البنى التحتية والجهات الحيوية الوطنية بطريقة سلسلة وآمنة (الذياني، 2022م).

وبالتالي، فقد استهدفت رؤية المملكة العربية السعودية التطوير الشامل للوطن وأمنه واقتصاده ورفاهية مواطنيه، وكان أحد أهدافها التحول نحو العالم الافتراضي الرقمي وتنمية البنية التحتية الرقمية بمواكبة التقدم العالمي المتسارع في الخدمات الرقمية وفي قدرات المعالجة الحاسوبية، وحتى يتم ضبط هذا التطور قامت الهيئة الوطنية للأمن السيبراني بتطوير الضوابط الأساسية للأمن السيبراني، والتي تكونت من مكونات أساسية وفرعية وضوابط أساسية للأمن السيبراني، وأخذت في الاعتبار المحاور الأساسية التي يركز عليها الأمن السيبراني (الصانع وآخرون، 2020).

وتم التأكيد على ذلك بتأسيس الهيئة الوطنية للأمن السيبراني، وتحديد اختصاصاتها التنظيمية والتشغيلية في مجال الأمن السيبراني من خلال العمل على تعزيز حماية الشبكات وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحويه من بيانات، مراعيةً في ذلك الأهمية الحيوية المتزايدة للأمن السيبراني في حياة المجتمعات، ومستهدفة التأسيس لصناعة وطنية في مجال الأمن السيبراني لتحقيق المملكة الريادة في هذا المجال، وعليه، قامت الهيئة ببناء الشركات مع الجهات العامة والخاصة، وتحفيز الابتكار والاستثمار في مجال الأمن السيبراني للإسهام في تحقيق نهضة تقنية تخدم مستقبل الاقتصاد الوطني للمملكة (القحطاني، 2019).

أدركت المملكة في ظل التحديات التي تواجهها لاستكمال بناء الدولة العصرية وفقاً لرؤية المملكة 2030 أنه من المهم أن تتكامل الجهود كافة، لتحقيق النهضة المستهدفة من خلال حماية نظمها وبنيتها المعلوماتية، ولذا فقد تكاتف الجميع في المملكة لضمان تحقيق الأمن السيبراني بدءاً من التعليم، واهتمت معظم الجامعات في المملكة بتدريس المواد الخاصة بالأمن السيبراني في كليات الحاسب لديها، مروراً بتأسيس المراكز والمؤسسات المعنية بقضية الأمن السيبراني، وذلك كله لمعاونة الهيئة الوطنية في مهامها وفي أهدافها، ومن أهم المراكز الخاصة بالأمن السيبراني في المملكة ما يلي (أبو ثنين، 2019):

1. الهيئة الوطنية للأمن السيبراني.
 2. المركز الوطني للعمليات الأمنية في وزارة الداخلية.
 3. المركز الوطني لتقنية أمن المعلومات بمدينة الملك عبدالعزيز للعلوم والتقنية.
 4. الاتحاد السعودي للأمن السيبراني والبرمجة.
 5. مركز التميز لأمن المعلومات بجامعة الملك سعود.
 6. وحدة الأمن السيبراني بجامعة الأمير سلطان بن عبدالعزيز.
- معوقات ممارسة إدارة المعرفة:**

تعرض إدارة المعرفة عدداً من المعوقات التي تحول دون التمكن من تنظيم وتخزين ونقل وتوليد المعرفة، ويشير (سعد ومعتوق 2020) عدداً من المعوقات فيما يلي:

1. **القيادة وأساليب الرقابة التقليدية:** تعتمد القيادة التقليدية على المركز الوظيفي ونقص الدعم والالتزام من جانب الإدارة العليا، والتركيز على الماضي والحاضر وليس المستقبل، قد يؤدي إلى عدم تطبيق المعرفة ونشرها أو تداولها بالشكل المطلوب.
 2. **عدم قبول الأفراد للتغيير:** ويمكن ذلك لأسباب تتعلق بالخلفيات الاجتماعية والثقافية والوظيفية، وذلك للحفاظ على الهوية الذاتية ومعارضتهم للأفكار الحديثة، وعدم السماح للأفراد بتولي المهام والمسؤوليات الإضافية.
 3. **غياب الثقافة التنظيمية:** ويؤدي ذلك إلى صعوبة التقدم في مجال المعرفة، وذلك نتيجة الافتقار إلى الإدراك الكافي لمفهوم إدارة المعرفة، وسيطرة الثقافة التقليدية وضعف الإدارة في الإرشاد والتطبيق وتبادل الخبرات، مما يكبح جماح الإبداع والابتكار داخل المنظمة.
 4. **قصور أنظمة الاتصال:** ويتم ذلك من خلال عزل المعرفة عن العاملين وحفظها في ملفات القيادات العليا، والاكتفاء بأنظمة الاتصال القائمة وعدم السعي لتطويرها، وعدم تطوير تعريف عملي لإدارة المعرفة عبر نظم المعلومات داخل المنظمة.
 5. **الافتقار إلى التكامل بين الأنشطة:** من أبرز الممارسات المعيقة في هذا المجال عدم وجود برامج تدريبية تتعلق بإدارة المعرفة، وعدم تنظيم أنظمة الاتصالات الداخلية والخارجية وتفعيلها، وإهمال التكامل بين الأنشطة المتعلقة بإدارة المعرفة.
 6. **عدم توفر البنية التحتية اللازمة** والتي تؤدي إلى انعكاسات سلبية على المنظمة.
 7. **عدم توفر الكادر البشري المؤهل للقيام بمهام إدارة المعرفة.**
- كما تضيف مدني وآخرون (2022) عددًا من المعوقات الأخرى تتمثل فيما يلي:
- الاعتماد على المعرفة المخزنة في القواعد المعرفية، وعدم الاهتمام بالتدفق المعرفي سيما المعرفة الجديدة.
 - التصور المطلق للمعرفة، بوصفها موجودة خارج العقول، في حين أغلب المعرفة تعد ضمنية وكامنة في العقول.
 - تجاهل الهدف الأساسي لإدارة المعرفة المتمثل في ابتكار السياقات المشتركة عبر الحوار.
 - التركيز على الماضي والحاضر، بدلاً من التفكير الإستراتيجي للتفكير في المستقبل.
 - ضعف التفكير والاستنتاج العقلاني باستخدام الافتراضات والمعتقدات للوصول إلى الحلول.
- ومن بين أهم المعوقات التي تواجه عمليات إدارة المعرفة، والتي ينبغي مواجهتها والوقوف على أسبابها وأساليبها (الهندسة الاجتماعية) التي تعتبر أحد أساليب الهجوم الذي يركز على الجانب البشري أكثر من الجوانب التقنية، وتهدف إلى التلاعب بالأفراد لتجاوز الإجراءات الأمنية المعتادة، وذلك لإقناع المستخدمين والتأثير عليهم لكشف المعلومات الخاصة أو الوصول إلى أماكن حساسة داخل المنظمة، ويقدم براين كريستيان وصفا موجزا للعملية التي يتبعها المهاجمون في الهندسة الاجتماعية في كتابه "الهندسة الاجتماعية: مقدمة" على الرغم من كل هجوم قد يتميز بتفاصيله الخاصة، إلا أن هناك دورة حياة عامة مكونة من أربعة مراحل رئيسية يمكن توضيحها كما يلي (كريستان، 2022):

1. مرحلة التخطيط:

في هذه المرحلة، يهتم المهاجم بجمع المعلومات حول الضحية المستهدفة، ويتم التقصي عن تفاصيل الضحية مثل: اسمه، ومكان عمله، ومعلومات شخصية وغيرها، كلما زادت كمية المعلومات التي يمكن جمعها عن الضحية، زادت فرص نجاح الهجوم، ويمكن استخدام مواقع التواصل الاجتماعي، والمواقع الرسمية، أو أية قاعدة بيانات عامة في هذه المرحلة.

2. مرحلة الاستهداف:

بمجرد جمع المعلومات الكافية، يبدأ المهاجم في التواصل مع الضحية مباشرة، وفي هذه المرحلة، يهدف المهاجم إلى بناء علاقة ثقة مع الضحية، مستغلاً المعلومات التي تم جمعها في المرحلة الأولى، ويحدد أفضل طريقة للتواصل معه، ويمكن أن يشمل ذلك إرسال بريد إلكتروني أو رسالة نصية احتيالية أو الاتصال بالضحية هاتفياً.

3. مرحلة الهجوم:

بعد بناء الثقة، يبدأ المهاجم الخطوة التالية من الهجوم، وقد يقوم بطلب معلومات حساسة، مثل: كلمات المرور أو أرقام بطاقات الائتمان، أو يقوم بتوجيه الضحية إلى روابط تحتوي على برامج ضارة.

4. مرحلة الاستفادة:

في هذه المرحلة، يستخدم المهاجم المعلومات أو النظام أو الشبكة المستهدفة لتحقيق أهدافه، ويمكن أن يشمل ذلك سرقة معلومات حساسة، أو نشر برامج ضارة أو تعطيل الأنظمة أو الشبكات.

5. مرحلة الهروب:

بعد تحقيق أهدافه، يسعى المهاجم لتغطية آثاره، وقد يقوم بحذف البرامج الضارة التي تم تثبيتها، أو حذف سجلات التواصل التي حدثت بينه وبين الضحية، بغرض تجنب الكشف والتعرف عليه في المستقبل، ويمثل الشكل رقم (1) كل مرحلة أساسية في دورة حياة الهجوم الاجتماعي.



الشكل رقم (1): دورة حياة الهندسة الاجتماعية

المصدر: كريستان، 2022

تأثير الهندسة الاجتماعية على القطاع المصرفي السعودي:

يمثل القطاع المصرفي في المملكة العربية السعودية نقطة محورية في الاقتصاد الوطني، ومع التطور السريع لتقنيات المعلومات والاتصالات، أصبحت البنوك تعتمد بشكل كبير على الأنظمة الإلكترونية لتقديم خدماتها للعملاء، من خلال التطبيقات البنكية والمعاملات الإلكترونية وغيرها.

التحديات التي يواجهها القطاع المصرفي السعودي، مثل: الهجمات السيبرانية ومحاولات الاحتيال، تحتاج إلى إستراتيجية مبنية على المعرفة لمواجهةها، فعندما يتم تبادل المعرفة بين الموظفين، وتعزيز الوعي حول التهديدات الأمنية، يصبح بإمكان البنك الاستجابة بشكل أسرع وأكثر فعالية لمثل هذه التحديات.

ووفقًا لتقرير هيئة الأمن السيبراني السعودي لعام 2023، بلغت نسبة الهجمات الهندسية الاجتماعية على القطاع المصرفي السعودي 70% من إجمالي الهجمات التي استهدفت القطاع في العام نفسه، كما وجد التقرير أن تكلفة الهجمات الهندسية الاجتماعية على القطاع المصرفي السعودي قد بلغت 10 مليارات ريال سعودي في عام 2023، ووفقًا لتقرير هيئة الأمن السيبراني السعودي لعام 2023، تمثل الهجمات الهندسية الاجتماعية 55% من جميع الهجمات التي استهدفت القطاع المصرفي العالمي في عام 2023، وعلى الرغم أن القطاع المصرفي السعودي أقل عرضة لهجمات الهندسة الاجتماعية من القطاع المصرفي العالمي، إلا أنه لا يزال يواجه تهديدًا خطيرًا، وتشير الإحصائيات الواردة في تقرير هيئة الأمن السيبراني السعودي إلى تهديدات الهندسة الاجتماعية التي تشكل تهديدًا خطيرًا للقطاع المصرفي السعودي، وتمثل هذه الهجمات نسبة كبيرة من إجمالي الهجمات التي استهدفت القطاع في عام 2023، كما تمثل تكلفة عالية، ووفقًا لتقرير هيئة الأمن السيبراني السعودي، فقد تنوعت أساليب الهندسة الاجتماعية التي استخدمت في الهجمات على القطاع المصرفي السعودي في عام 2022، ومن أبرزها: (الهيئة الوطنية للأمن السيبراني 2018)

1. رسائل البريد الإلكتروني الاحتيالية: وترسل هذه الرسائل إلى الموظفين أو العملاء بأنها من مصدر موثوق به، مثل: البنك أو شركة الخدمات المالية، وقد تحتوي هذه الرسائل على روابط ضارة أو مرفقات يمكن أن تؤدي إلى إصابة جهاز الضحية ببرامج ضارة.

2. مكالمات الهاتفية الاحتيالية: يتصل المحتالون بالموظفين أو العملاء عبر الهاتف ويتظاهرون بأنهم من البنك أو شركة الخدمات المالية، قد يسألون أسئلة حول بيانات اعتماد تسجيل الدخول أو تفاصيل الحساب المصرفي.

3. صفحات الويب الاحتيالية: يقوم المحتالون بإنشاء صفحات ويب تشبه مواقع الويب أو التطبيقات المصرفية الرسمية، عندما يدخل الضحية بياناته على هذه الصفحات، يتم سرقتها من قبل المحتالين.

ووفقًا لتقرير (OCED 2017) فإن متوسط مستوى معرفة الخدمات المصرفية عبر الإنترنت في المملكة العربية السعودية هو 12 نقطة من أصل 21 نقطة، هذا يعني أن حوالي 60% من البالغين في المملكة العربية السعودية ليس لديهم معرفة كافية بالمخاطر المرتبطة بالهندسة الاجتماعية، كما وجد التقرير أن 70% من البالغين في المملكة العربية السعودية لم يتلقوا أي تعليم رسمي حول الأمن السيبراني، وهذا يشير إلى العديد من الناس في المملكة العربية السعودية ليسوا على دراية بالمخاطر المرتبطة بالهندسة الاجتماعية، وكيفية حماية

أنفسهم منها، ويرجع السبب في ارتفاع نسبة الهجمات الهندسية الاجتماعية على القطاع المصرفي السعودي إلى عدة عوامل، منها:

1. زيادة استخدام الإنترنت والخدمات المصرفية عبر الإنترنت في المملكة العربية السعودية.
 2. انخفاض مستوى الوعي لدى العملاء والموظفين بالمخاطر المرتبطة بالهندسة الاجتماعية.
 3. ضعف أنظمة الحماية في بعض البنوك والشركات المالية.
- حسب تقرير البنك المركزي السعودي، بلغت قيمة الخسائر التي تكبدتها البنوك السعودية نتيجة الهجمات الهندسية الاجتماعية في عام 2022 حوالي 10 مليارات ريال سعودي، هذا يمثل زيادة بنسبة 20% عن عام 2021. كما وجد التقرير أن عدد الهجمات الهندسية الاجتماعية التي استهدفت القطاع المصرفي السعودي في عام 2022 بلغ حوالي 100 ألف هجوم، وهذا يمثل زيادة بنسبة 30% عن عام 2021.
- ووفقًا للتقرير المشار إليه أعلاه، تمثل الهجمات التالية أكبر نسبة من الهجمات الهندسية الاجتماعية التي استهدفت القطاع المصرفي السعودي في عام 2022: (تقرير البنك المركزي السعودي 2024)

1. الرسائل الإلكترونية الاحتيالية: بلغت نسبتها 70% من إجمالي الهجمات.
 2. الأسئلة الاحتيالية: بلغت نسبتها 20% من إجمالي الهجمات.
 3. التصيد الاجتماعي: بلغت نسبتها 10% من إجمالي الهجمات.
- وفي هذا السياق، يأتي دور إدارة المعرفة لتعزيز قدرة البنوك على حماية معلوماتها، وتقديم خدمات ذات جودة عالية، وإدارة المعرفة هي: عملية تجميع، وتنظيم، وتخزين، ومشاركة المعلومات بين الموظفين، لضمان تدفق المعلومات بسلاسة وتحقيق الأهداف الإستراتيجية للبنك، بما يساعد على مواجهة تهديدات أمن المعلومات عامةً، ومخاطر الهندسة الاجتماعية خاصةً، وذلك من خلال تطبيق عملياتها كسبيل لصنع توجهها المستقبلي الذي يتمثل في تحسين وتوسيع نطاق شبكات تبادل المعارف والخبرات المكتسبة، والاستفادة من التكنولوجيا في تحسين القدرة على تبادل المعلومات ومواجهة التهديدات، وبخاصةً أن المصارف منظمات تقع عليها مسؤولية خدمة شريحة كبيرة من المجتمع، وعليه، فإن ضرورة بقائها وصمودها في ظل تهديدات الهندسة الاجتماعية يدفعها بقوة إلى تبني تطبيق إدارة المعرفة (سعد ومعتوق، 2020).

من خلال البحث والاطلاع على الأدب المنشور في هذه الجزئية، تتبين ندرة الدراسات التي تطرقت لذلك وبالذات في الوطن العربي وبخاصة المملكة العربية السعودية، فالواقع المؤسسي يشير إلى عدم وجود تطبيق لإدارة المعرفة أو وجود وحدة تحمل مسمى إدارة المعرفة ككيان، ولكنها تطبق ضمنياً من قبل جهات متعددة، وتحقق جزئياً الميزات والأهداف التي تصبو إليها إدارة المعرفة، فهناك دراسات مثلاً بينت أثر تطبيق عمليات إدارة المعرفة في تطوير ثقافة التميز، وأثرها على جودة الخدمات المصرفية، وتعزيز الابتكار في المصارف.

ويمكن تحديد الملامح العامة لظاهرة عدم وجود تصور للمؤسسات المصرفية بتطبيق إدارة المعرفة في التالي:

1. ضعف الثقافة التنظيمية.
2. عدم ملائمة وحدانية الهيكل التنظيمي .
3. قصور آليات تكنولوجيا المعلومات .

وفي القطاع المصرفي -وكما ذكر سابقا- هو من المؤسسات التي تطبق أنشطة إدارة المعرفة بدون تنظيم رسمي لإدارة المعرفة وهذا ما ذكره (فيصل وآخرون، 2018) في دراسة تحليلية على قطاع البنك في المملكة الأردنية الهاشمية بعنوان: دور إدارة المعرفة في قطاع البنوك؛ بأن القطاع المصرفي قد نجح في ترسيخ مفهومه الخاص لإدارة المعرفة، وأظهرت النتائج أن أنشطة إدارة المعرفة التي تمارس كانت عالية في الغالب، وكانت هناك علاقة إحصائية إيجابية بين إستراتيجية إدارة المعرفة ودرجة ممارسة الأنشطة المعرفية.

إدارة المعرفة كذلك تلعب دورًا حيويًا في مساعدة المؤسسات المصرفية على التقيد بالتشريعات المحلية المتعلقة بالأمن السيبراني، من خلال توفير التوعية، والتدريب، وأدوات المراقبة والتقييم، تضمن إدارة المعرفة أن تكون المؤسسات المصرفية على استعداد جيد لمواجهة التحديات المرتبطة بالهندسة الاجتماعية وغيرها من التهديدات السيبرانية.

تشريعات إدارة المعرفة في القطاع المصرفي السعودي لمواجهة تهديدات الهندسة الاجتماعية:

يركز القطاع المصرفي السعودي عبر تشريعات إدارة المعرفة فيها على تطبيق إستراتيجيات متقدمة لمواجهة التهديدات السيبرانية، بما في ذلك الهندسة الاجتماعية، تم ذلك من خلال وضع أنظمة وإرشادات وضوابط تهدف بشكل أساسي إلى مواجهة التهديدات السيبرانية عمومًا، وتهديدات الهندسة الاجتماعية بخاصة، وذلك استنادًا على التوجيهات الإستراتيجية الوطنية للأمن السيبراني والضوابط والتشريعات الوطنية الصادرة للأمن السيبراني، التي تم البناء عليها باستخدام أفضل الممارسات والمعايير للحد من مخاطر الهندسة الاجتماعية وبخاصة في القطاع المصرفي.

وتأتي أهمية التشريعات والقوانين التي تضع الضوابط والمعايير لحماية البيانات وضمان سلامة العمليات المصرفية، وفي هذا السياق، تلعب إدارة المعرفة دورًا حيويًا في دمج وتنظيم هذه التشريعات وضمان تطبيقها بشكل فعال، كما يلي :

- **التشريعات والتوجيه المعرفي:** إدارة المعرفة تساعد في توثيق وتحديث القوانين والتشريعات المحلية المتعلقة بالأمن السيبراني في البنوك، وتحصر الهيئات الرسمية في المملكة العربية السعودية على تطوير التشريعات لمواكبة أحدث التقنيات وأساليب الهجمات الإلكترونية، وبذلك يمكن لإدارة المعرفة أن تساهم في رصد وتحليل أية تغييرات في التشريعات، وتوفير تدريب مستمر للموظفين حول كيفية التقيد بها.
- **تطبيق التشريعات على أرض الواقع:** ليس كافيًا الاعتماد على تطوير التشريعات فحسب، ولكن يجب ضمان تطبيقها بفعالية، ومن خلال إدارة المعرفة، يمكن للبنوك السعودية أن تقوم بتوفير نظم وأدوات تساعد في رصد أية مخالفات أو انحرافات قد تحدث، وذلك من خلال البيانات والمعلومات المخزنة والمعالجة.
- **تدريب الموظفين على التشريعات:** تقوم إدارة المعرفة بتطوير برامج تدريبية متخصصة بناءً على التشريعات الجديدة أو المحدثة، هذه البرامج تهدف إلى تعزيز فهم ووعي الموظفين حول القوانين، وكيفية الالتزام بها في أداء وظائفهم اليومية.
- **المراقبة والتقييم:** إلى جانب التدريب، تقوم إدارة المعرفة بتطوير أدوات ونظم لمراقبة وتقييم كيفية التزام الموظفين بالتشريعات، هذه الأدوات تساعد في التعرف على أية نقاط ضعف قد تكون موجودة، وتوجيه الجهود نحو تقوية هذه المناطق.
- **الإدراك وزيادة الوعي:** يعد مفتاح مواجهة الهندسة الاجتماعية هو الوعي، لأن المهندسين الاجتماعيين يستهدفون افتقار الأفراد للإدراك والجهل بالتكنولوجيا الحديثة، وزيادة الوعي يحتاج إلى تقديم حملات للتوعية

بمفهوم الهندسة الاجتماعية ومخاطرها على المجتمع ككل، وعلى القطاع المصرفي بشكل خاص، وذلك من خلال التركيز على تغيير السلوك المطلوب لمواجهة الهندسة الاجتماعية (عبدالمعظم، 2021).

دور البنك المركزي في مواجهة تهديدات الهندسة الاجتماعية:

وجّه البنك المركزي السعودي البنوك العاملة في المملكة إلى تطبيق عدد من الإجراءات الاحترازية لمواجهة تهديدات الهندسة الاجتماعية، وحماية المتعاملين مع البنوك، وذلك انطلاقاً من أهداف نظام البنك المركزي المتصلة بدعم استقرار القطاع المصرفي، وتعزيز الثقة به، واستناداً إلى المهام والصلاحيات الموكلة إلى البنك المركزي بموجب نظامه ونظام مراقبة البنوك، ومنها: وضع التعليمات والإجراءات الكفيلة بحماية عملاء البنوك، واتخاذ الإجراءات والتدابير المناسبة للحد من ارتكاب الجرائم المرتبطة بالعملاء، وقام البنك المركزي باتخاذ هذه الإجراءات الاحترازية الإضافية، بناءً على ما تم رصده من ازدياد المواقع الإلكترونية، وحسابات التواصل الاجتماعي الاحتيالية، بالإضافة إلى استمرار حالات الاحتيال المالي التي تستهدف عملاء البنوك بطرق ووسائل مختلفة مثل: الهندسة الاجتماعية، التي يقوم المحتال من خلالها بإيهام العميل بأنه يتعامل مع جهة رسمية أو خاصة أو أفراد موثوقين، والحصول على بياناتهم الخاصة، مما ينتج عنه تزويد عصابات الاحتيال المالي ببيانات الدخول على الحساب المصرفي ورمز التحقق، ثم إجراء عمليات الاحتيال المالي على حساب العملاء (ملتقى أسبار، 2023)،

وقد قدم ملتقى أسبار في ملتقى يناير لعام (2023م) عدداً من التوصيات حول كيفية مواجهة تهديدات الهندسة الاجتماعية في القطاع المصرفي، وتمثلت أبرزها فيما يلي (ملتقى أسبار، 2023):

1. التأكيد على البنك المركزي السعودي تطبيق الأنظمة والتعليمات التي أصدرها بشأن مكافحة الاحتيال المالي، ومتابعة البنوك في تطبيق ما يخصها منها، ومن ذلك: دليل مكافحة الاحتيال المالي وتعليمات البنك المركزي .
 2. تعزيز إدارات تلقي البلاغات والشكاوى في البنوك، بحيث تعطي شكاوى المتعاملين وبلاغاتهم أهمية ومعالجة، في سبيل تعزيز المصداقية والرضا.
 3. تعزيز الثقة في المنظومة المالية والمصرفية، تحقيقاً للأمن الاقتصادي والاجتماعي للجميع، مع التأكيد على خطورة جريمة الاحتيال المالي، لما تشكل من ممر للجريمة وغسل الأموال، وسلب الناس مدخراتهم.
 4. التأكيد على الموازنة والمواءمة بين تسهيل الإجراءات البنكية والرقمنة.
 5. تعزيز دور الهيئة الوطنية للأمن السيبراني، في التحقق من قوة وفعالية أنظمة الحماية التقنية للبنوك، وعملياتها، وتفعيل التكامل بين جميع الجهات في سبيل حماية المعلومات والعمليات والبرامج.
- إن التكامل بين القطاع المصرفي وإدارة المعرفة في المملكة العربية السعودية سيوفر طبقة حماية إضافية ضد التهديدات السيبرانية، من خلال توظيف إدارة المعرفة بفعالية، ويمكن للبنوك تحسين أمانها وحماية مواردها وعمالها من الهجمات المحتملة.

ثانياً : الدراسات السابقة :

فيما يلي مراجعة لبعض الدراسات ذات الصلة بموضوع إدارة المعرفة والهندسة الاجتماعية في القطاع المصرفي، سواء على المستوى السعودي أو العربي أو العالمي:

- من بين الدراسات التي طبقت في البيئة المحلية ، دراسة (Almutairi, Alghamdi, 2022): التي ركزت على مجموعة من المؤسسات في المملكة العربية السعودية، بغرض التعرف على أنواع الهندسة الاجتماعية، وللتأكد من مستوى الوعي بالهندسة الاجتماعية، وتقديم الحلول المناسبة للمشكلات للحد من تلك المخاطر الهندسية، وتجنب العقبات التي يمكن أن تمنع زيادة الوعي بمخاطرها، وتم تطوير استبيان ومسح 508 موظفين يعملون في مؤسسات مختلفة، وأظهرت الدراسة أن 63.4% من العينة البحث ليس لديهم فكرة عن الهندسة الاجتماعية، و67.3% من إجمالي العينات ليس لديهم فكرة عن تهديدات الهندسة الاجتماعية، و42.1% لديهم معرفة ضعيفة بالهندسة الاجتماعية، و7.5% فقط من العينة لديهم معرفة جيدة بالهندسة الاجتماعية، و64.7% من الذكور لا يعرفون ما الهندسة الاجتماعية، و68.0% من الإداريين لا يعرفون ما الهندسة الاجتماعية، وأظهر الموظفون الذين لم يأخذوا دورات فروق ذات دلالة إحصائية.
- أما دراسة (سعد ومعتوق، 2020)، فقد سعت إلى معرفة واقع ممارسة عمليات إدارة المعرفة بالمصارف الليبية، وكذلك التعرف على المعوقات التي تحول دون ممارسة عمليات إدارة المعرفة في مصرف الصحاري بطرابلس الليبية، ولتحقيق أهداف الدراسة تم استخدام المنهج الوصفي التحليلي، واستبانة كأداة لجمع البيانات تم توزيعها على عينة مكونة من (52) موظفاً من المدراء العاملين بالإدارات العامة، ومدراء الإدارات ورؤساء الأقسام، وتوصلت إلى متغيرات ممارسة عمليات إدارة المعرفة في المصرف كانت غير دالة معنويًا، وأن المعوقات التي تواجه المصرف في ممارسة عمليات إدارة المعرفة كانت ذات دلالة معنوية، وتوصلت إلى وجود العديد من المعوقات التي تحول دون ممارسة عمليات إدارة المعرفة في المصرف قيد الدراسة.
- من ناحية أخرى ، تناولت دراسة (عايض والعودي، 2020) أثر إدارة المعرفة في التطوير المنظمي في المصارف اليمنية، وتم تطبيق الدراسة على عدد 13 مصرفاً يمينياً، وتم اختيار عينة عشوائية نسبية بواقع (314) موظفاً من تلك المصارف، من خلال توزيع استبانة كأداة لجمع البيانات، وتوصلت النتائج أن المصارف اليمنية تولي التطوير المنظمي -بكافة أبعاده وممارسة إدارة المعرفة بكافة أبعادها- اهتماماً كبيراً، وأن أكثر أبعاد التطوير المنظمي تحققاً كان في البعد التكنولوجي، وأقلها في بُعد الموارد البشرية، وأكثر أبعاد إدارة المعرفة (ممارسة تطبيق المعرفة)، وأقلها (نقل المعرفة)، كما يوجد تفاوت في أثر أبعاد إدارة المعرفة في التطوير المنظمي، وكان أكثرها تأثيراً بُعد نقل المعرفة، وأقلها بُعد تطبيق المعرفة، وأوصت الدراسة بضرورة تعزيز مستوى تحقق التطوير المنظمي بجميع أبعاده، وكذلك الاهتمام بتعزيز ممارسة إدارة المعرفة لاسيما نقل المعرفة، وذلك لما له من أثر في تحقيق التطوير المنظمي.
- أما دراسة (العلي، 2021) فقد تناولت دور إدارة المعرفة في تعزيز الجاهزية المصرفية - دراسة تحليلية لآراء عينة من العاملين في المصارف العراقية في النجف الأشرف، من خلال المنهج الوصفي، وتم استخدام استبيان منظم لجمع البيانات عن طريق مجموعة من موظفي المصارف العراقية، وبلغ عدد

المصارف المستخدمة (3) المتمثلة في مصرف الرافدين والرشيد ومصرف TBI فرع النجف، وتوصلت النتائج أن الجاهزية المصرفية تتحقق بشكل سريع وأقوى بتوافر إدارة المعرفة، كما ظهر تقبل إيجابي لأفراد الدراسة في المصارف المبحوثة تجاه توفر فقرات متغيرات إدارة المعرفة، مما يؤكد على إدراكهم بأهميتها في تعزيز الجاهزية المصرفية، وفي ضوء ذلك أوصت الدراسة بضرورة الاهتمام بإيجاد إدارة معرفة فعالة، وتعمل بشكل فعال على زيادة إمكانيات الموظفين وتنفيذ توقعاتهم، واتخاذ ظروف عمل إنسانية التي بدورها تنعكس على تعزيز الجاهزية المصرفية وزيادة الخدمات المصرفية، وتطوير جودة الخدمة المصرفية من خلال تبني إدارة المعرفة.

- دراسة (سيف، 2023) التي تناولت أثر عمليات إدارة المعرفة في تطوير رأس المال الفكري في البنوك التجارية الأردنية، وتم استخدام المنهج الوصفي التحليلي، ولقياس متغيرات الدراسة تم تصميم استبانة كأداة لجمع البيانات من عينة الدراسة المكونة من عدد (13) بنكاً، وبلغ حجم العينة (275) مفردة، وتوصلت النتائج إلى وجود أثر ذي دلالة إحصائية لعمليات إدارة المعرفة بأبعادها: (تطبيق المعرفة، وتوزيع المعرفة، وتخزين المعرفة) مرتبة حسب الأهمية الإحصائية في تطوير رأس المال الفكري في البنوك التجارية الأردنية، في حين لم يكن هناك أثر ذو دلالة لبعدها (توليد المعرفة) في تطوير رأس المال الفكري في البنوك التجارية الأردنية، وبالاستناد إلى تلك النتائج أوصت الدراسة بأن تسعى البنوك التجارية الأردنية إلى توفير مصادر وبدائل خارجية للبيانات والمعرفة التي تحتاجها في عملياتها المختلفة، وأن تحسن من فهرسة المعرفة المخزنة لديها، لسهولة الوصول والتعديل عليها واستخدامها عند الحاجة.

- أما دراسة (علي، 2023)، فكان موضوعها: أثر إدارة المعرفة على جودة الخدمات المصرفية- دراسة حالة: بنك أم درمان الوطني-السودان، و تمثلت مشكلة البحث في مواجهة المصارف للعديد من التحديات في المحافظة على عملائها وجذب عملاء جدد، وذلك بسبب تغير حاجات ورغبات العملاء بصورة مستمرة، إلى جانب العمل على مواكبة الأساليب والوسائل الحديثة لتجويد وتطوير الخدمات المصرفية، وأصبح التحدي الحقيقي أمام المصارف ليس تقديم خدمات لهم فحسب؛ بل القدرة على الوفاء بمتطلباتهم بما يتطابق مع حاجاتهم ويشبع رغباتهم، وهذا لا يتأتى إلا من خلال تطبيق وتفعيل إدارة المعرفة بالشكل الذي يساهم في جودة الخدمات المصرفية المقدمة، وأوصت الدراسة بضرورة الالتزام بتطبيق المعرفة بشكل منتظم للمساهمة في تطوير الخدمات المصرفية، وكذلك الاستفادة من تجارب وخبرات المصارف العالمية في مجال تطبيق المعرفة، لمواكبة التطورات والمستجدات في عالم صناعة الخدمات المصرفية.

- ومن الدراسات المهمة (محمد، 2018) التي سعت إلى التعرف على مدى وعي المجتمع العربي بحماية حساباتهم الشخصية، والتعرف على سبل الاختراق وانتهاك الخصوصية بشكل عام مع التركيز على الهندسة الاجتماعية بشكل خاص وسبل التدريب المتاحة تجاه حماية المواطن الرقمي، من خلال التعرف بمفهوم الهندسة الاجتماعية، وأهمية شبكات التواصل الاجتماعي في الوطن العربي، وأهمية الخصوصية من وجهة نظر مستخدمي شبكات التواصل الاجتماعي في الوطن العربي، وكذلك التعرف عن طريق اختراق شبكات التواصل الاجتماعي وطرق الحماية من الهندسة الاجتماعية، ويعد وعي المجتمع العربي تجاه الهندسة الاجتماعية من أولويات المجتمع العربي لحماية حساباتهم في شبكات التواصل الاجتماعي، وتوافر مهارات التصدي لهجمات الهندسة الاجتماعية في شبكات التواصل

الاجتماعي، وتم تطبيق الدراسة على عينة قوامها (336) فرداً، ومن أبرز النتائج السلوك الإيجابي لمجتمع الدراسة تجاه حماية معلوماتهم الشخصية على شبكات التواصل الاجتماعي، واختيار أسماء مستعارة غير حقيقية يسجل بها ما يزيد عن نصف مجتمع الدراسة على شبكات التواصل الاجتماعي، وهذا ما وضحته نسبة (53.2%)، وعدم إتاحتهم للبيانات الشخصية تارة، وعدم صحة بياناتهم الشخصية المتاحة على حساباتهم تارة أخرى، بالإضافة إلى قلة من تعرض حساباتهم البنكية للاختراق، وتعرض نسبة 6.8% فقط لاختراق الحسابات المصرفية، ومن أكثر الطرق شيوعاً لهجمات الهندسة الاجتماعية للرسائل الاقترامية المزعجة (Spam) كتهنئة من صديق وهي 77.1%، تليها نسبة 53.2% يقعون ضحية إقناعهم بأهمية برامج من مواقع توهّمهم بضرورة تحميلها، وأوصت الدراسة بضرورة رفع درجة وعي المواطن العربي بالهندسة الاجتماعية، وحماية حساباتهم الشخصية عبر شبكات التواصل الاجتماعي والحرص على نشر الوعي التقني، ووضع إستراتيجية عربية واضحة وميثاق أخلاقي، تمكن المواطن العربي من التصرف بشكل نظامي مع الجهة المسؤولة في حالة الوقوع ضحية للهندسة الاجتماعية.

- أما دراسة (جيبات، 2018)، فقد هدفت إلى التوعية بمخاطر الهندسة الاجتماعية ومعرفة كيفية عمل الهندسة الاجتماعية، وطرق الوقاية منها والحفاظ على المعلومات الشخصية للفرد، واعتمدت الدراسة على جمع المعلومات من مصادر وجهات مختلفة ومختصة، وتوصلت الدراسة إلى عدد من النتائج أهمها: المجتمع الفلسطيني يعاني جهلاً وإهمالاً كبيراً في مجال الهندسة الاجتماعية ومفهومها، نظراً لقلة الدراسات والأبحاث وحملات التوعية بهذا الخصوص، والهندسة الاجتماعية وجهت بطريقة ذكية من قبل الشعب الفلسطيني، ويمكن استغلال الهندسة الاجتماعية لإيصال رسائل الشعب الفلسطيني للعالم الغربي ومطالبته بحقه، كما أوصت الدراسة بعقد الدورات والندوات وورش العمل لتعليم الجمهور بكيفية حماية أنفسهم وحساباتهم وتأمينهم من الوقوع ضحايا الهندسة الاجتماعية، وإيجاد المواقع الإخبارية الموثوقة التي تمكن الفرد الفلسطيني من استقصاء المعلومة الصحيحة من خلالها.

- بينما تناولت دراسة (الضب، 2023) دور الذكاء الاصطناعي وتعلم الآلة في تعزيز كشف الاحتيال على البطاقات الائتمانية، وهدفت الدراسة إلى إبراز أهم تطبيقات الذكاء الاصطناعي وتعلم الآلة في تعزيز كشف الاحتيال على البطاقات الائتمانية، والمقارنة بين نتائج خوارزميات تعلم الآلة الخاضع للإشراف، بالتطبيق على لغة بايثون للبرمجة، باستخدام بيانات اصطناعية تم إنشاؤها بطريقة عشوائية عن طريق المحاكاة للأرقام العشوائية لعينة تتكون من 200 ألف بطاقة ائتمانية، و20 متغيراً كخصائص لحامل البطاقة الائتمانية باستخدام أربع خوارزميات ممثلة في: خوارزمية الانحدار اللوجستي، وأقرب الجيران، والتحليل التمييزي الخطي، وشجرة القرار، وخلصت الدراسة أن خوارزميات تعلم الآلة تساهم في تعزيز كشف الاحتيال على البطاقات الائتمانية بقدرة تنبؤية فاقت (94%)، وخوارزمية التحليل التمييزي الخطي كانت أفضل أداءً من بقية الخوارزميات المستخدمة، مما يدعم التوجه نحو استخدام تقنيات تعلم الآلة الحديثة، وفرص الاستفادة من العديد من الخوارزميات، وأوصت الدراسة بضرورة استخدام الذكاء الاصطناعي وتعلم الآلة في تحليل عمليات الاحتيال على البطاقات الائتمانية في الدول العربية، مما يساعد المؤسسات المالية والهيئات الإشرافية والتنظيمية والرقابية على إدارة المخاطر وتقليل

التكاليف الناتجة عن هذه العمليات، وبخاصةً مع توجه العديد من المحتالين إلى استخدام التقنيات الحديثة ومنها: الهندسة الاجتماعية، مما يستدعي مواكبة التطورات العالمية الراهنة في هذا المجال.

- من الدراسات الأجنبية (Weerasinghe et al, 2023) التي ركزت على دور إدارة المعرفة في تعزيز الابتكار في المصارف، وهدفت الدراسة إلى استكشاف دور ممارسات إدارة المعرفة في تعزيز الإبداع والابتكار في قطاع الخدمات فيما يتعلق بالصناعة المصرفية، وتفترض الدراسة المعرفة كأصل داخلي غير ملموس والابتكار كوسيلة لتطوير قدرات إستراتيجية مستدامة يصعب تقليدها، واختبرت هذه الدراسة الكمية خمس فرضيات مقترحة على 437 عينة تم جمعها من موظفي البنوك من خلال طريقة PLS-SEM، وأشار الباحث إلى مشاركة المعرفة والتطبيق والحماية ساهمت بشكل مباشر في ابتكار البنك، وتجمع الدراسة بين وجهات نظر RBV و KM في تطوير القدرة الإستراتيجية طويلة المدى وتقوي النظرة التطورية للاقتصاديين، بما يتوافق مع تأثير حماية المعرفة وفق تقسيم قطاعات المعرفة، وقامت الدراسة بتطوير إطار عمل لإدارة المعرفة يتضمن حماية المعرفة العملية / التشغيلية كأحد الأبعاد الرئيسية لعملية إدارة المعرفة.

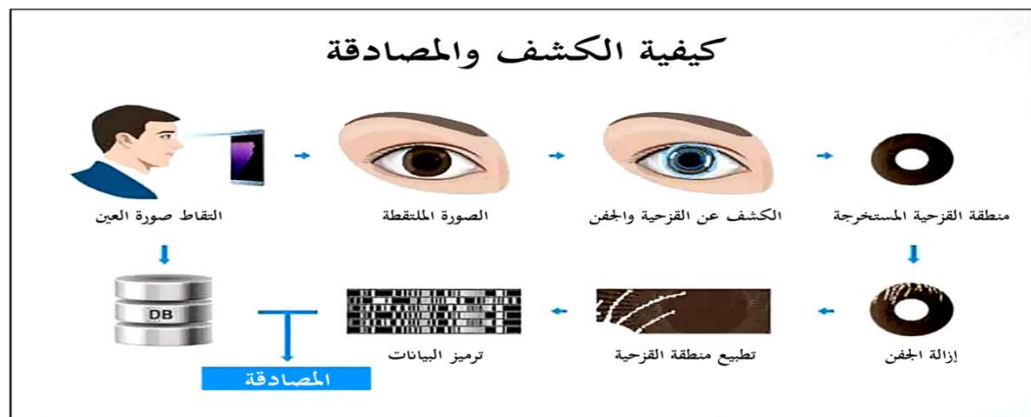
- بينما هدفت دراسة (Manyam, 2022) إلى استكشاف مفهوم هجمات الهندسة الاجتماعية وتأثير الذكاء الاصطناعي عليها، وقد تصاعدت التهديدات الأمنية التي تشكلها الهندسة الاجتماعية بشكل ملحوظ في السنوات الأخيرة، وعلى الرغم من توفر البرامج والأجهزة الأمنية المتقدمة، ولكن مع ذلك لا تزال هناك ثغرة أمنية موجودة في نظام الدفاع الخاص بالمنظمة أو الفرد، ولذلك سعت الدراسة إلى التعرف على أنواع هجمات الهندسة الاجتماعية والتقنيات الأساسية التي يستخدمها المهاجمون، كما تمثلت المجالات الأساسية للدراسة في كيفية تأثير الذكاء الاصطناعي على الهندسة الاجتماعية واستخدامها، واكتشاف ومنع هجمات الهندسة الاجتماعية، وتوصلت الدراسة بأنه يتم تطبيق الأنظمة الآلية بدأت تنمو بسرعة في كل أنماط الحياة، من خلال وسائل التواصل الاجتماعي، وتطبيقات البضائع، والسيارات ذاتية القيادة، وغيرها، وعلى الرغم أن الذكاء الاصطناعي قد أدى إلى تحسين الأمن السيبراني، إلا أنه يخدع مجرمي الإنترنت، وتوصلت النتائج أن الأكثرية لا تدرك إمكانية التحدث مع روبوت بدلاً عن شخص عادي، ولذلك ناقشت كذلك الدراسة أساليب ومفاهيم انتحال الصوت والتزييف العميق والهندسة الاجتماعية الآلية.

- أما دراسة (Zuoguang Wang, et al, 2021) فتناولت تطوير أنطولوجيا مجال الهندسة الاجتماعية في مجال الأمن السيبراني وتجري تقييم الأنطولوجيا من خلال تطبيق الرسم البياني المعرفي، وتحدد أنطولوجيا المجال 11 مفهوماً للكيانات الأساسية التي تشكل، وتؤثر بشكل كبير على مجال الهندسة الاجتماعية، إلى جانب 22 نوعاً من العلاقات التي تصف كيفية ارتباط هذه الكيانات ببعضها البعض، إنه يوفر مخططاً معرفياً رسمياً وصريحاً لفهم وتحليل، وإعادة استخدام مشاركة معرفة المجال بالهندسة الاجتماعية، علاوة على ذلك، تتبنى هذه الدراسة رسماً بيانياً معرفياً يستند إلى 15 حدثاً وسيناريوهات لهجوم الهندسة الاجتماعية، و7 أمثلة على تطبيق الرسم البياني المعرفي في 9 أنماط تحليل، توضح أن الأنطولوجيا جنباً إلى جنب مع الرسم البياني المعرفي، ومفيدة في فهم وتحليل سيناريو هجوم الهندسة الاجتماعية، والعثور على عناصر تهديد الهندسة الاجتماعية الأعلى تصنيفاً مثل: نقاط الضعف البشري الأكثر استغلالاً في الهندسة الاجتماعية.

ثالثا : النماذج المقترحة في الدراسات السابقة :

اقتُرحت العديد من الدراسات خططا ونماذج عمل بعضها لها علاقة مباشرة بإدارة المعرفة، بينما الأخرى ركزت على الهندسة الاجتماعية، وهناك نماذج تناولت ظاهرة المخاطر التي تتعرض لها المنظمات بصفة عامة، وقد تم تحليل تلك النماذج وتلخيصها في جدول رقم (1).

1- نموذج (راضي والشوري، 2019) تضمن تقديم برنامج مقترح بالقياسات الحيوية منتج بمعالجة الصورة الرقمية للتغلب على بعض التهديدات الأمنية في البنوك، ولإنتاج البرنامج حاولت الدراسة تحديد الوضع الأمني الحالي في البنوك المصرية، ومعرفة أهمية القياسات الحيوية في تأمين البيانات للعملاء في البنوك، ومعرفة أهم عناصر القياسات الحيوية التي تساعد على حماية بيانات العملاء، وتم استخدام المنهج الوصفي التحليلي في عرض البحث، والمنهج التجريبي في إنتاج البرنامج، وتم التوصل إلى النظام الحالي للحماية بالبنك الذي يحقق الغرض المطلوب، ولكنه ليس بالشكل الكافي الذي يحقق الطمأنينة للعملاء، وأن القياسات الحيوية أحد أهم أساليب التأمين المهمة التي يجب الاعتماد عليها في حماية وتأمين الحسابات الخاصة بهم في البنوك، وبصمة العين هي أهم وسيلة في القياسات الحيوية، كما يمكن زيادة أمان القياسات الحيوية باستخدام أكثر من نموذج للقياسات الحيوية وأكثر من طريقة وأكثر من صورة، بالإضافة إلى تشفير الصور المستخدمة في عمليات المضاهاة، وتفعيلها في مختلف المؤسسات للتحقق من الهوية وحماية نظم وأمن المعلومات، ويتمثل النموذج المقترح في الشكل رقم (2).

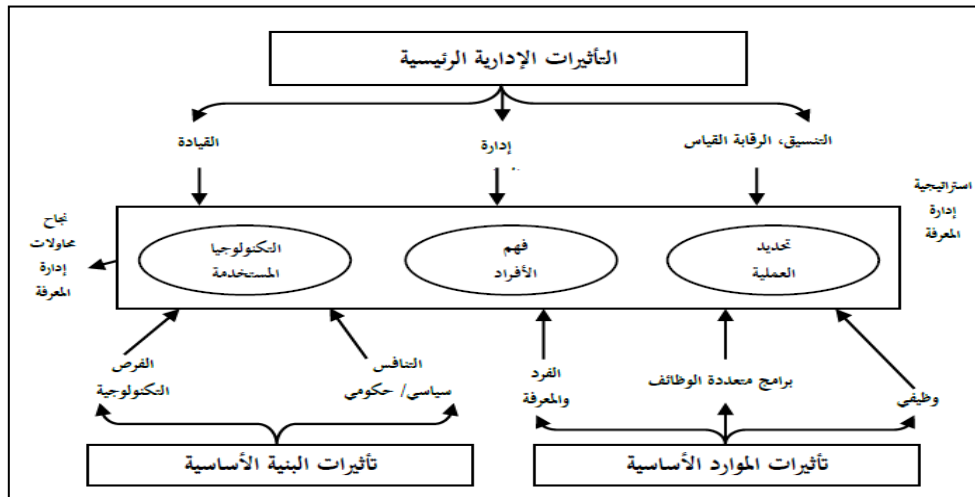


الشكل رقم (2) نموذج لاستخدام أنظمة القياسات الحيوية بمعالجة الصورة الرقمية للتغلب على التهديدات الأمنية في البنوك (راضي والشوري، 2019)

2- نموذج (Massey et al, 2008) ويقدم هذا النموذج الشكل رقم (3) باعتبار إدارة المعرفة هي أحد أهم عمليات التغيير الهيكلي التي لا يمكن فصل تميزها عن تميز عملية التغيير الذي ينعكس على الأداء التنظيمي للمنظمة ككل، ويتشكل هذا النموذج من العناصر التالية (اللهي، 2023):

- أ- إستراتيجية إدارة المعرفة: تحدد استخدام عناصر إدارة المعرفة، وأي معارف يتم اكتسابها والتعرف على مصدرها، والمستخدمين لها، وشكل تلك المعرفة.
- ب- التأثيرات الإدارية الرئيسية: تحدد العملية الإدارية في العمل المؤسسي من خلال الإدارة وموارد إدارة القسم، وكذلك عملية التنسيق والرقابة على الموارد.

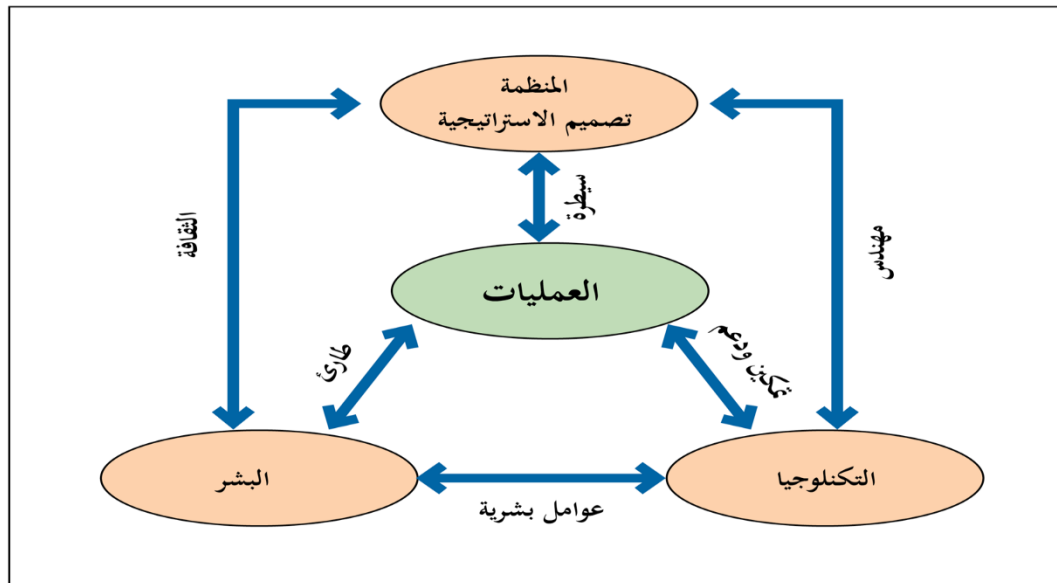
ت- 7 تأثيرات الموارد الرئيسية: تشمل الموارد المادية، وعناصر إدارة المعرفة التي يتطلب وجودها لبناء النظام.



الشكل رقم (3) نموذج Massey وآخرون لإدارة المعرفة

المصدر: (اللهيبي، 2023)

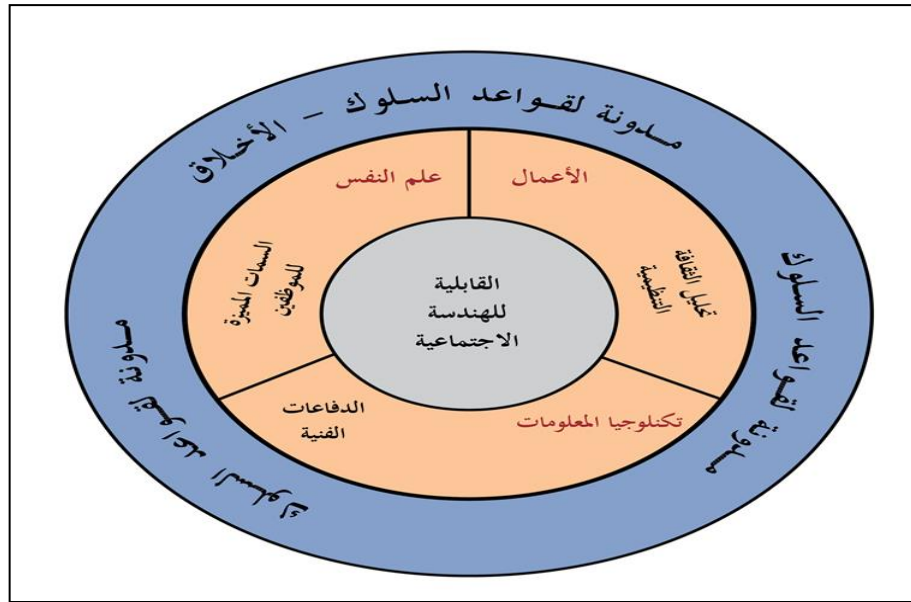
3- النموذج المتكامل لإدارة المعرفة لأمن تقنيات المعلومات، الشكل رقم (4) وفقاً لمعايير ISO/IEC 27000 ، الذي تم عرضه في دراسة (S. Dotsenko et al, 2019) التي قدمت تحليلاً لنماذج إدارة المعرفة الموجودة، وتبريراً لإدخال نموذج متكامل لإدارة المعرفة، ويُقترح بناء النموذج باستخدام معايير الأمان المعروفة في تكنولوجيا المعلومات ومنهجية تقييم الأمان لتكنولوجيا المعلومات، وتقوم الدراسة بتطوير نموذج إدارة المعرفة من خلال تحليل محتوى العناصر ذات الصلة بالمعايير المشهورة، وتحديد المحتوى المعرفي الذي يحدد أشكال العلاقات بينها، والباحثون في الدراسة يقترحون تطبيق نماذج لأربعة عوامل رئيسية لتكوين نماذج إدارة المعرفة لتنظيم نظام إدارة أمن المعلومات وفقاً لمعايير ISO / IEC 27000 ، والعوامل الأربعة هي: إستراتيجية المنظمة وتصميمها للسيطرة على العمليات التي هي العامل الثاني، وكذلك التكنولوجيا، وآخر العوامل العنصر البشري، وهذه العوامل هي عناصر إدارة المعرفة، وتفيد في تحويل المعلومات إلى معرفة تضمن الحصول على خدمات وفائدة تساهم في رفع مستوى كفاءة المنظمة والاستثمار في أهم موارد منظمة.



الشكل رقم (4) نموذج إدارة المعرفة لتنظيم نظام إدارة امن المعلومات

المصدر: (S. Dotsenko et al,2019)

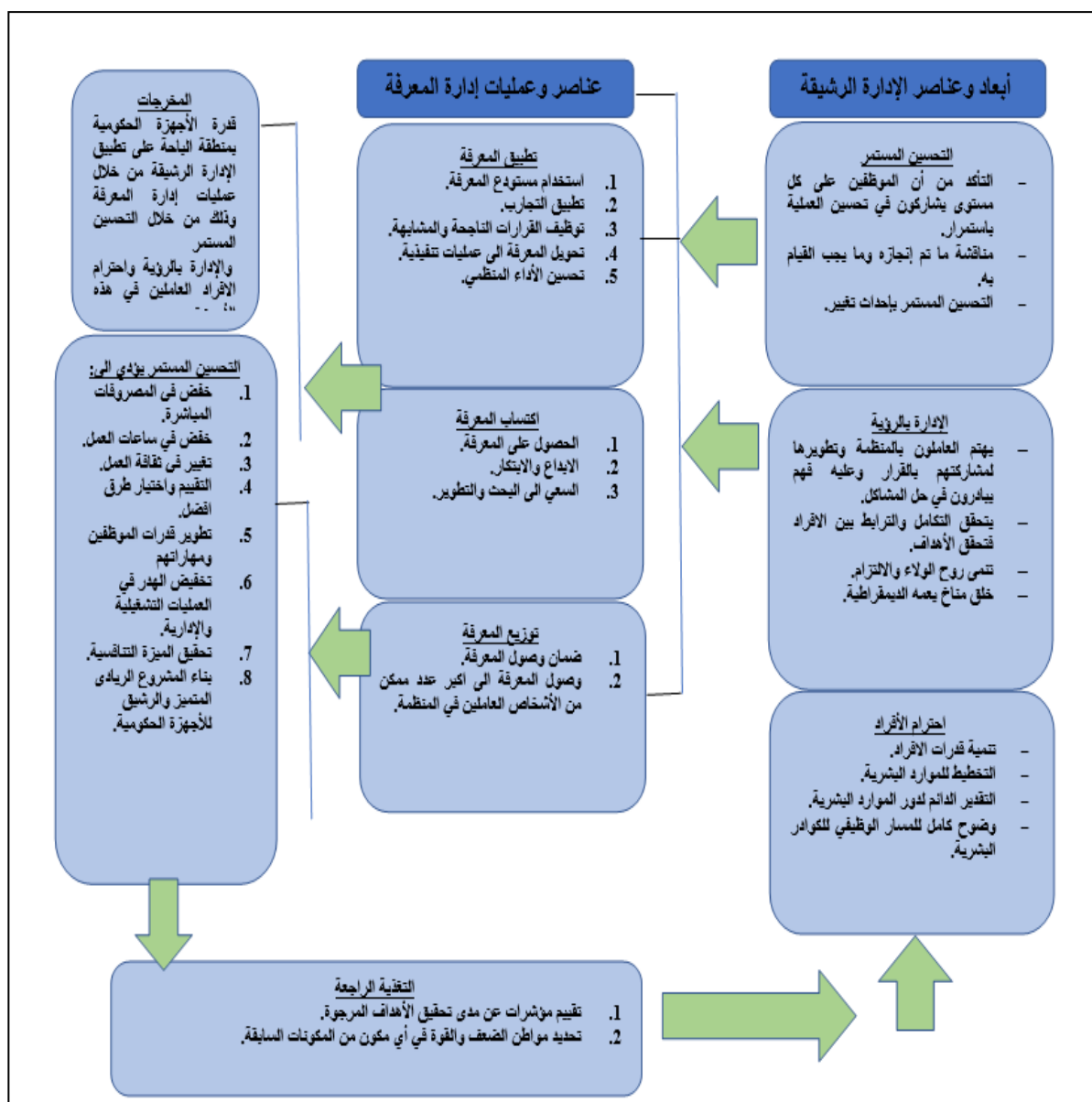
4- نموذج قابلية التعرض للهندسة الاجتماعية من منظور متعدد التخصصات الشكل رقم (5) الذي تم عرضه في دراسة (Amy Washo, 2021) بعنوان: نظرة متعددة التخصصات للهندسة الاجتماعية: دعوة للعمل من أجل البحث، والتي اعتبرت الهندسة الاجتماعية أحد التهديدات الرئيسية لأمن المعلومات اليوم، وأنها موضوع معقد ومتزايد الانتشار بين الأفراد والشركات، وأنها أكثر الجوانب إثارة للقلق، لأنه لا أحد محصن من آثارها، ومن الأفضل فهمها من منظور متعدد التخصصات وتحديد تخصصات تكنولوجيا المعلومات، وعلم النفس، والأعمال، وتم التطرق للهندسة الاجتماعية في هذه الدراسة من منظور متعدد التخصصات؛ وتمت مراجعة الأدبيات في تخصصات تكنولوجيا المعلومات وكيفية الدفاعات التقنية، وعلم النفس بالنظر في سمات الموظفين وسلوكياتهم، وفي الأعمال من حيث تحليل الثقافة التنظيمية وما يمكنه من مساحات للعمل؛ لتشجيع الثقة بين الموظفين، وثقافة التواصل ومشاركة المعرفة المناسبة، وما يشمل ذلك من منظور أخلاقي.



الشكل رقم (5) نموذج قابلية التعرض للهندسة الاجتماعية من منظور متعدد التخصصات

المصدر: (Amy Washo, 2021)

5- نموذج دعم الإدارة الرشيقة لمشاريع إدارة المعرفة ، الشكل رقم (6) ، الذي تم عرضه في دراسة (الشهري وعقيلي، 2024) بعنوان: دور الإدارة الرشيقة في دعم مشاريع إدارة مشاريع إدارة المعرفة في الأجهزة الحكومية بالمملكة العربية السعودية: نموذج مقترح، وتمثلت أبرز أهداف الدراسة في التعرف على دور الإدارة الرشيقة في دعم مشاريع إدارة المعرفة من خلال عمليات: (تحويل وتوزيع المعرفة - اكتساب المعرفة - تطبيق المعرفة) في الأجهزة الحكومية السعودية، والتعرف على تصور الموظفين حول الصعوبات التي تواجه تطبيقات الإدارة الرشيقة في دعم مشاريع إدارة المعرفة، وأظهرت نتائج هذه الدراسة وجود دور للإدارة الرشيقة في دعم مشاريع إدارة المعرفة، وكذلك أوضحت النتائج عدم وجود فروق بين دور الإدارة الرشيقة في دعم مشاريع إدارة المعرفة تعزى لمتغيرات المؤهل الدراسي، وسنوات الخبرة، وجهة العمل، ووجود علاقة ارتباطية دالة إحصائية بين دعم مشاريع إدارة المعرفة ومستوى الممارسات الحالية للإدارة الرشيقة، كما أوضحت النتائج وجود علاقة ارتباطية قوية ودالة إحصائية بين دعم مشاريع إدارة المعرفة وطرق وأساليب الإدارة الحديثة.

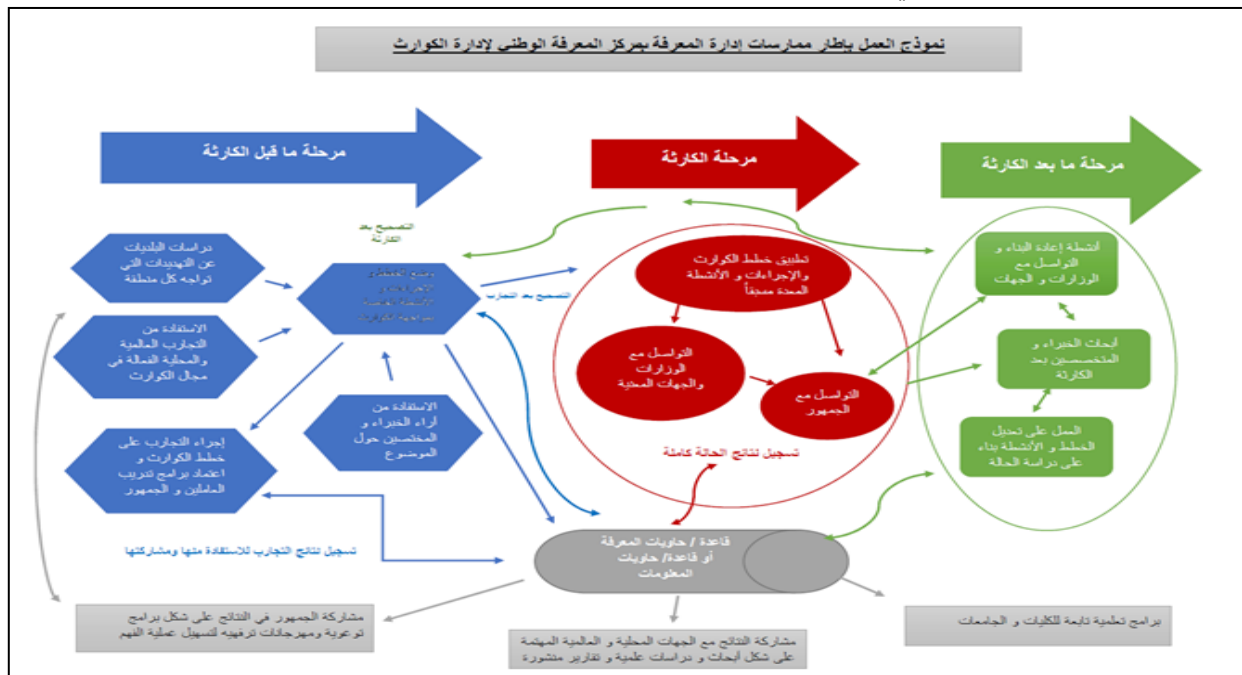


الشكل رقم (6) نموذج مقترح لدعم مشاريع إدارة المعرفة

المصدر: (الشهري وعقيلي، 2024).

6- نموذج استخدام إدارة المعرفة في إدارة الكوارث وتخفيف مخاطرها ، الشكل رقم (7) ، والذي تم عرضه في دراسة (مجلد، 2018) جاءت بعنوان: دور إدارة المعرفة في إدارة الكوارث وتخفيف مخاطرها: نموذج مقترح للبلديات بالمملكة العربية السعودية، والتي هدفت إلى التعرف على دور إدارة المعرفة في دعم عمليات وممارسات إدارة الكوارث ودورها في التخطيط الصحيح لمواجهتها والتعامل المبكر معها والتخفيف منها، ولتحقيق ذلك عمدت الدراسة إلى تحليل نماذج من الدراسات النظرية والتطبيقية والخطط التي ناقشت موضوع إدارة المعرفة، كما بنت الدراسة نموذج لمركز مقترح لإدارة الكوارث السعودية قائم على تطبيق ممارسات وأهداف إدارة المعرفة، وتوصلت نتائج الدراسة إلى توفر الجهود الدولية الرامية للحفاظ على حياة السكان، ويعد إطار سندي من هذه الجهود الرامية لتزويد الدول بمعايير تساهم في الحد من التهديدات من عام 2015 إلى 2030م، إلا أن ما يعيبه هو إغفال الدور

الحيوي لدور المعلومات والمعارف، كما اهتمت العديد من الدراسات بحجم التطبيق الفعلي لإدارة المعرفة وتسخيرها للتخفيف من الكوارث في البلديات في الإنتاج الفكري، أما فيما يتعلق بتحليل مواقع البلديات في المملكة، فقد احتلت محافظة مكة المكرمة الصدارة، وطورت محافظة مكة المكرمة وجدة صفحة ضمن موقعها الإلكتروني التابع للبلدية بهدف التعريف بموضوع الكوارث من أصل 4 مواقع بلدية إلكترونية سعودية، وبناءً على ما توصلت إليه الدراسة، فقد أوصت بزيادة الأنشطة البحثية للدول العربية حول إدارة المعرفة وتسخيرها للتخفيف من الكوارث في البلديات العربية، وضرورة تكامل الجهود بالمملكة المعنية بالكوارث في منظومة معلوماتية معرفية متكاملة تسهل الاستفادة من الخبرات والمعارف المكتسبة، والعمل على بناء قواعد معرفية تخص الكوارث وسن التشريعات الخاصة بتبادل المعلومات والمعارف في مجال إدارة الكوارث بالمملكة.



الشكل رقم (7) نموذج استخدام إدارة المعرفة في إدارة الكوارث وتخفيف مخاطرها

المصدر: (مجلد، 2018)

المستفاد من النماذج السابقة :

ولتحديد جوانب الاستفادة من النماذج السابقة تمت صياغة جدول رقم (1) من خلال إيضاح جوانب الضعف والقوة لكل نموذج والنقاط التي يمكن أن تفيد في بناء النموذج المقترح لهذه الدراسة :

جدول رقم (1) ملخص النماذج السابقة

م	النموذج	التقييم		ملاحظات
		جوانب القوة	جوانب الضعف	

1	نموذج راضي والشوري	<ul style="list-style-type: none"> • عدم تناول إدارة المعرفة بشكل خاص 	<ul style="list-style-type: none"> • تقديم برنامج للقياسات الرقمية للتغلب على التهديدات الأمنية 	<ul style="list-style-type: none"> • القياسات الحيوية أحد أهم أساليب حماية وتأمين الحسابات البنكية
2	نموذج Massey et al	<ul style="list-style-type: none"> • عدم التركيز على الهندسة الاجتماعية 	<ul style="list-style-type: none"> • تأثير إدارة المعرفة على الهيكل التنظيمي 	<ul style="list-style-type: none"> • أهمية التعديل في الهياكل التنظيمية لتشمل إدارة المعرفة • تحديد مهام ومسؤوليات غدارة المعرفة بشكل واضح
3	النموذج المتكامل لإدارة المعرفة لأمن تقنيات المعلومات	<ul style="list-style-type: none"> • عدم التركيز على الهندسة الاجتماعية • عدم وضع قاعدة معرفية 	<ul style="list-style-type: none"> • انشاء علاقة بين الهيكل والثقافة والأشخاص وتكنولوجيا المعلومات من خلال إدارة المعرفة والإبداع التنظيمي • وضع المعايير "ISO" التي تحدد متطلبات أنظمة امن المعلومات، 	<ul style="list-style-type: none"> • ان عوامل إدارة المعرفة هي الأساس في نظام أمن المعلومات • إن العنصر البشري هو العنصر الأهم في نظام أمن المعلومات
4	نموذج قابلية التعرض للهندسة الاجتماعية من منظور متعدد التخصصات	<ul style="list-style-type: none"> • عدم تحديد أساليب الهجمات • عدم توظيف إدارة المخاطر أو أساليب إدارة النظم 	<ul style="list-style-type: none"> • التركيز على دراسة السلوك و النفسية • فهم الهندسة الاجتماعية من عدة جوانب 	<ul style="list-style-type: none"> • أن الهندسة الاجتماعية هي أكبر تهديد في مجال أهمية أمن المعلومات للأفراد/المؤسسات مؤسسة
5	نموذج دعم الإدارة الرشيقة لمشاريع إدارة المعرفة	<ul style="list-style-type: none"> • عدم التطرق لإدارة امن المعلومات تحديداً 	<ul style="list-style-type: none"> • تحقيق الابداع والابتكار • تحسين الأداء التنظيمي والجودة 	<ul style="list-style-type: none"> • تحقيق التكامل والترابط بين افراد المنظمة • مشاركة الافراد في تحسين العملية والقرارات باستمرار

		• عدم تحديد العوامل الرئيسية لإدارة المعرفة	• خفض التكاليف، زيادة الإنتاجية ورضا العاملين والعملاء	
6	نموذج استخدام إدارة المعرفة في إدارة الكوارث	• النموذج عام لإجراءات مواجهة الكوارث • عدم تحديد العوامل الرئيسية لإدارة المعرفة	• الاعتماد على قاعدة معرفية مشتركة • الاستفادة من التجارب السابقة ومشاركتها مع الجهات المحلية والعالمية والعملاء والتوعية	• توظيف القرارات الناجحة مسبقا في اتخاذ قرارات مشابهة • العمل على مواجهة التحديات على مراحل قبل واثناء وبعد

تحليل نتائج الدراسة :

لتحقيق أهداف الدراسة وتحليل البيانات التي تم جمعها، فقد تم استخدام العديد من الأساليب الإحصائية المناسبة باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية Statistical Package For Social Sciences والتي يرمز لها اختصارًا بالرمز (SPSS)، وذلك بعد أن تم ترميز وإدخال البيانات إلى الحاسب الآلي، ولتحديد طول خلايا المقياس الخماسي (الحدود الدنيا والعليا) المستخدم في محاور الدراسة، تم حساب المدى (5-1=4)، ثم تقسيمه على عدد خلايا المقياس للحصول على طول الخلية الصحيح أي: (4/5=0.80)، بعد ذلك تمت إضافة هذه القيمة إلى أقل قيمة في المقياس (أو بداية المقياس وهي الواحد الصحيح) وذلك لتحديد الحد الأعلى لهذه الخلية، وهكذا أصبح طول الخلايا كما يتضح في جدول رقم (2) :

جدول رقم (2) توزيع مدى المتوسطات وفق التدرج المستخدم في أداة الدراسة

الفئة	مدى المتوسطات	درجة الموافقة
الأولى	من 1.00 إلى 1.80	غير موافق بشدة
الثانية	من 1.81 إلى 2.60	غير موافق
الثالثة	من 2.61 إلى 3.40	محايد
الرابعة	من 3.41 إلى 4.20	موافق
الخامسة	من 4.21 إلى 5.00	موافق بشدة

وتم حساب التكرارات والنسب المئوية للتعرف على الخصائص الشخصية والوظيفية لأفراد عينة الدراسة، وتحديد استجاباتهم للعبارات الرئيسية التي تتضمنها أداة الدراسة، وبعد ذلك تم حساب المقاييس الإحصائية التالية:

- المتوسط الحسابي (Mean): وذلك لمعرفة مدى ارتفاع أو انخفاض استجابات أفراد الدراسة عن أسئلة الدراسة (متوسط متوسطات العبارات) مع العلم بأنه يفيد في ترتيب عبارات الدراسة حسب أعلى متوسط حسابي موزون.

- تم استخدام الانحراف المعياري (Standard Deviation): وذلك للتعرف على مدى انحراف أو تشتت استجابات أفراد الدراسة لكل عبارة من عبارات متغيرات الدراسة، ولكل محور من المحاور الرئيسية عن متوسطها الحسابي، ويلاحظ أن الانحراف المعياري يوضح التشتت في استجابات أفراد عينة الدراسة لكل عبارة من عبارات متغيرات الدراسة للمحاور الرئيسية، فكلما اقتربت قيمته من الصفر تركزت الاستجابات وانخفض تشتتها بين المقياس.

- تم استخدام معامل الارتباط بيرسون "Person Correlation": لمعرفة درجة الارتباط بين كل سؤال من أسئلة الدراسة.

- استخدم معامل ألفا كرونباخ (Cronbach Alpha): لاختبار مدى ثبات أداة الدراسة.

النتائج المتعلقة بالبيانات الديموغرافية:

**المؤهل العلمي:

جدول رقم (3) يوضح توزيع أفراد الدراسة حسب متغير المؤهل العلمي

النسبة	التكرار	المؤهل العلمي
5.8	3	دكتوراه
48.1	25	ماجستير
5.8	3	دبلوم عالي
32.7	17	بكالوريوس
7.7	4	دبلوم أو أقل
100	52	المجموع

يبين الجدول أعلاه توزيع أفراد الدراسة حسب متغير المؤهل العلمي، و (48.1%) من أفراد الدراسة كان مؤهلهم العلمي ماجستير، وهم الفئة الأكبر في الدراسة، في حين (32.7%) من أفراد الدراسة كان مؤهلهم العلمي بكالوريوس، و (7.7%) من أفراد الدراسة كان مؤهلهم العلمي دبلوم أو أقل، في حين (5.8%) من أفراد الدراسة كان مؤهلهم العلمي دبلوم عالي، وأخيرًا تبين أن (5.8%) من أفراد الدراسة كان مؤهلهم العلمي دكتوراه، وهذا

ما يدل أن العينة على هذا المستوى التعليمي تكون قابلة لبرامج التدريب والتوعية والتي هي من أهم المستهدفات للوقاية من الهندسة الاجتماعية.
سنوات الخبرة:

جدول رقم (4) يوضح توزيع أفراد الدراسة حسب متغير سنوات الخبرة

النسبة	التكرار	سنوات الخبرة
21.2	11	أقل من 5 سنوات
21.2	11	من 5 سنوات إلى أقل من 10 سنوات
17.3	9	من 10 إلى أقل من 15 سنة
40.4	21	أكثر من 15 سنة
100	52	المجموع

يبين الجدول أعلاه توزيع أفراد الدراسة حسب متغير سنوات الخبرة، و (40.4%) من أفراد الدراسة كانت سنوات خبرتهم من 15 سنة فأكثر وهم الفئة الأكبر في الدراسة، في حين (21.2%) من أفراد الدراسة كانت سنوات خدمتهم أقل من 5 سنوات، في حين (21.2%) من أفراد الدراسة كانت سنوات خدمتهم من خمس إلى أقل من 10 سنوات، وأخيرًا تبين أن (17.3%) من أفراد الدراسة كانت سنوات خدمتهم من 10 إلى أقل من 15 سنوات، وهذا ما يدل أن هناك فرصة لتطوير النسبة الكبيرة من الأفراد ذوي سنوات الخدمة القليلة في المستقبل، والاستفادة من أصحاب سنوات الخبرة الأكثر فيما لديهم من تراكم معرفي ومعرفة ضمنية.
الدورات التأهيلية في مجال إدارة المعرفة:

جدول رقم (5) يوضح توزيع أفراد الدراسة حسب متغير الدورات التدريبية

النسبة	التكرار	الدورات التدريبية
38.5	20	لا يوجد
28.8	15	أقل من خمس دورات تدريبية
32.7	17	خمس دورات تدريبية وأكثر
100	52	المجموع

يبين الجدول أعلاه توزيع أفراد الدراسة حسب متغير البرامج التدريبية في مجال إدارة المعرفة، و(38.5%) من أفراد الدراسة لم يوجد لديهم دورات تدريبية في مجال إدارة المعرفة، وهم الفئة الأكبر في الدراسة، في حين (28.8%) من أفراد الدراسة كان لديهم أقل من خمس دورات تدريبية، في حين (32.7%) من أفراد الدراسة كان

الدورات التأهيلية في مجال الأمن السيبراني:

النسبة	التكرار	الدورات التدريبية
44.2	23	لا يوجد
38.5	20	أقل من خمس دورات تدريبية
17.3	9	خمس دورات تدريبية وأكثر
100	52	المجموع

و للتعرف على واقع تطبيق إدارة المعرفة بالقطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، تم حساب المتوسطات الحسابية، والانحرافات المعيارية، والرتب لاستجابات أفراد الدراسة على أبعاد واقع تطبيق إدارة المعرفة بالقطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، وجاءت النتائج كما يوضحها جدول رقم (7) :

جدول رقم (7) واقع تطبيق إدارة المعرفة بالقطاع المصرفي السعودي مرتبة تنازلياً حسب متوسطات الموافقة

الرتبة	الانحراف المعياري	المتوسط الحسابي	درجة الممارسة					التكرار	العبارات	م
			موافق غير	موافق غير	محايد	موافق	موافق بشدة	النسبة %		
1	0.94	4.12	0	6	2	24	20	ك	يوفر المصرف أنظمة أمن وحماية للمعرفة وسرية في الدخول	6
			0	11.5	3.8	46.2	38.5	%		

م	العبارات	درجة الممارسة						التكرار	
		النسبة %	موافق بشدّة	موافق	مجايد	موافق غير	موافق غير		
	إلى حسابات الموظفين مثل استخدام برنامج التصفح الآمن (SECURITY IP)								
2	تحقق استراتيجية المصرف تنمية مصادر المعرفة من خلال استقطاب الخبراء لتحقيق التميز والريادة	ك	15	31	2	3	1		
		%	28.8	59.6	3.8	5.8	1.9		
3	يتبنى المصرف استراتيجية أنظمة رقابية تتضمن دقة متابعة الأنشطة والعمليات والمحاسبة على التقصير والاهمال في حال حدوثه	ك	20	21	6	5	0		
		%	38.5	40.4	11.5	9.6	0		
1	تتضمن استراتيجية المصرف تعزيز البنية التحتية للتقنية والاتصالات من خلال زيادة بنود المصرف في	ك	14	28	4	6	0		
		%	26.9	53.8	7.7	11.5	0		
2	0.86	4.08							
3	0.94	4.08							
4	0.90	3.96							

الرتبة	الانحراف المعياري	المتوسط الحسابي	درجة الممارسة					التكرار	العبارات	م
			موافق	غير موافق	محايد	موافق	موافق بشدة	النسبة %		
									الميزانية لتحقيق إدارة المعرفة	
5	0.94	3.96	0	7	3	27	15	ك	يوفر المصرف برامج متطورة لتسهيل العمليات (إدارة الأداء، إدارة التعلم، إدارة التغيير وغيره)	7
			0	13.5	5.8	51.9	28.8	%		
6	1.01	3.85	0	8	7	22	15	ك	يتم استخلاص المعرفة داخل المصرف من خلال استخدام تقنية التنقيب في البيانات لمعرفة الاتجاهات الحديثة ورغبات العملاء	9
			0	15.4	13.5	42.3	28.8	%		
7	1.02	3.77	0	9	7	23	13	ك	يجري تدريب الموظفين بالمصرف لجعل إدارة المعرفة جزءا من ثقافة المنظمة بتحسين توجهاتهم نحو التعلم والمشاركة بالمعرفة على جميع المستويات	5
			0	17.3	13.5	44.2	25	%		
8	0.97	3.73	0	9	6	27	10	ك	يوجد تكامل بين الموظفين والعملاء من خلال تسهيل قنوات التواصل	8
			0	17.3	11.5	51.9	19.2	%		

من خلال الجدول أعلاه يتضح أن أفراد الدراسة، جاءت بدرجة موافق على واقع تطبيق إدارة المعرفة بالقطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى بمتوسط (3.90)، ويتبين من خلال ترتيب العبارات أن المصارف تتوفر فيها أنظمة أمن وحماية للمعرفة وسرية في الدخول إلى حسابات الموظفين مثل: استخدام برنامج التصفح الآمن (SECURITY IP) ولكن هناك تدني في التكامل بين الموظفين والعملاء من خلال تسهيل قنوات التواصل للسماح بمشاركة المعرفة بينهم، وكذلك عدم تحقيق المصارف لإستراتيجية الأمن الوظيفي لخبرائها ورأس المال الفكري من خلال تخفيض معدل تغيير الموظفين، إلا أن نتيجة هذا المحور تفسر أن لدى العاملين في القطاع المصرفي، إدراك محسوس بدور إدارة المعرفة في المساعدة في جمع وتنظيم وتحليل المعلومات التي تتعلق بأفضل الممارسات في مجال الأمان، ويمكن للمصارف استخدام هذه المعلومات لتدريب موظفيها بشأن كيفية التعرف على محاولات الهندسة الاجتماعية وكيفية الرد عليها، بالإضافة إلى ذلك، يمكن لإدارة المعرفة مساعدة المصارف في تطوير إستراتيجيات فعّالة لحماية البيانات والمعلومات الحساسة.

واتفقت هذه النتيجة مع دراسة (فيصل وآخرون، 2018): أجرى دراسة تحليلية على قطاع البنك في المملكة الأردنية الهاشمية بعنوان: دور إدارة المعرفة في قطاع البنوك، التي أظهرت النتائج أن أنشطة إدارة المعرفة التي تمارس كانت عالية في الغالب.

ومن خلال النتائج أعلاه، يتضح أن هناك تجانس في موافقة أفراد الدراسة على عبارات واقع تطبيق إدارة المعرفة بالقطاع المصرفي السعودي، وتراوح متوسطات موافقتهم على البُعد ما بين (4.12 إلى 3.62) وهي متوسطات تقع في الفئة الرابعة من فئات المقياس الخماسي، والتي تشير إلى (موافق) على أداة الدراسة، مما يوضح التجانس في موافقة أفراد الدراسة على واقع تطبيق إدارة المعرفة بالقطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، والتي تم ترتيبها تنازليًا حسب موافقة أفراد الدراسة عليها بدرجة موافق كالتالي:

1. جاءت العبارة رقم (6) وهي: " يوفر المصرف أنظمة أمن وحماية للمعرفة وسرية في الدخول إلى حسابات الموظفين مثل: استخدام برنامج التصفح الآمن (SECURITY IP)" بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (4.12)، وتفسر هذه النتيجة بأن قيادة القطاع المصرفي في المملكة تعمل على توفير أعلى وأفضل أنظمة أمن وحماية المعرفة.
2. جاءت العبارة رقم (2) وهي: " تحقق إستراتيجية المصرف تنمية مصادر المعرفة من خلال استقطاب الخبراء لتحقيق التميز والريادة " بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (4.08)، وتفسر هذه النتيجة وعي العاملين في القطاع المصرفي بدور الخبراء في تحقيق التميز والريادة للقطاع المصرفي، وتحقيق إستراتيجية تنمية مصادر المعرفة التي تسعى المصارف لتحقيقها في رؤيتها.
3. جاءت العبارة رقم (3) وهي: " يتبنى المصرف إستراتيجية أنظمة رقابية تتضمن دقة متابعة الأنشطة، والعمليات والمحاسبة على التقصير والإهمال في حال حدوثه " بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (4.08)، وتفسر هذه النتيجة بأن لدى المصارف إستراتيجية أنظمة للرقابة والمتابعة لمحاسبة التقصير والإهمال في حدوثه، ولكنها تحتاج إلى زيادة في دقة الأداء.
4. جاءت العبارة رقم (1) وهي: " تتضمن إستراتيجية المصرف تعزيز البنية التحتية للتقنية والاتصالات من خلال زيادة بنود الصرف في الميزانية لتحقيق إدارة المعرفة " بالمرتبة الرابعة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (3.96)، وتفيد هذه النتيجة بأن هناك إستراتيجية لتعزيز البنية التحتية للتقنية والاتصالات، ولكنها تحتاج إلى زيادة بنود الصرف في الميزانية لتحقيق إدارة المعرفة.
5. جاءت العبارة رقم (8) وهي: " يوجد تكامل بين الموظفين والعملاء من خلال تسهيل قنوات التواصل للسماح بمشاركة المعرفة بينهم لمعرفة رغباتهم واحتياجاتهم " بالمرتبة قبل الأخيرة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط (3.73)، وتشير النتيجة إلى تسهيل قنوات التواصل بين الموظفين والعملاء يساهم في تلافي الأزمات، وتساعد في التعرف على رغبات واحتياجات العملاء مما يؤدي إلى تحقيق رضا عملاء القطاع المصرفي

6. جاءت العبارة رقم (4) وهي: "يسعى المصرف نحو تحقيق إستراتيجية الأمن الوظيفي لخبرائها ورأس مالها الفكري من خلال تخفيض معدل تغيير الموظفين بالنقل والتقاعد وغيره للمحافظة على مصادرها الفكرية " بالمرتبة الأخيرة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط (3.62)، وتشير إلى ضرورة العمل من قبل إدارات المصارف بالعمل على تحقيق إستراتيجية الأمن الوظيفي لخبرائها ورأس مالها الفكري من خلال المحافظة على الموظفين الذين يعتبرون من المصادر الفكرية للمصرف أبرز تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي من وجهة نظر عينة الدراسة:

للتعرف على مدى الوعي بأبرز تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب، لاستجابات أفراد الدراسة لعبارات محور مدى الوعي بأبرز تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، وجاءت النتائج كما يوضحها جدول رقم (8) :

جدول رقم (8) مدى الوعي بأبرز تهديدات الهندسة الاجتماعية

م	العبارات	التكرار	درجة الموافقة					النسبة %	الرتبة
			غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة		
3	لدي الوعي بمخاطر إتاحة بياناتي الشخصية للعامة على المواقع الالكترونية	ك	0	4	2	18	28	%	1
			0	7.7	3.8	34.6	53.8		
5	أقوم باستخدام البرامج الأصلية والمواقع الموثوقة في تحميل الملفات	ك	1	6	3	18	24	%	2
			1.9	11.5	5.8	34.6	46.2		
2	أسعى دوما نحو الاطلاع على ضوابط الأمن السيبراني وما يصدر من وثائق تخص	ك	0	8	4	17	23	%	3
			0	15.4	7.7	32.7	44.2		

الرتبة	الانحراف المعياري	المتوسط الحسابي	درجة الموافقة					التكرار	العبارات	م
			غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	النسبة %		
									سياسات وإجراءات الأمن السيبراني	
4	1.16	3.98	1	9	2	18	22	ك	لدي وعي تام بالأساليب المستخدمة في اختراق الأنظمة من خلال انتحال الهوية، والتصيد الاحتيالي، والتتبع وخداع الضحية	6
			1.9	17.3	3.8	34.6	42.3	%		
5	1.01	3.90	0	7	8	20	17	ك	أسعى للاطلاع بشكل مستمر بشأن ما يستجد من قوانين تتعلق بمواجهة الهندسة الاجتماعية	1
			0	13.5	15.4	38.5	32.7	%		
6	1.19	3.90	2	8	3	19	20	ك	أستطيع تمييز رسائل الاحتيال، وروابط التصيد الواردة في المواقع الخاصة بالمصرف والبرامج المزيفة.	7
			3.8	15.4	5.8	36.5	38.5	%		
7	1.11	3.83	0	10	7	17	18	ك	أقوم بشكل دوري بتحديث كلمة المرور لحساباتي داخل المصرف	4
			0	19.2	13.5	32.7	34.6	%		
8	1.22	3.73	2	9	8	15	18	ك		8

م	العبارات	التكرار	درجة الموافقة					الانحراف المعياري	المتوسط الحسابي	الرتبة
		النسبة %	موافق بشدة	موافق	محايد	غير موافق بشدة	غير موافق			
		34.6 %	28.8	15.4	17.3	3.8				
. أقوم بالإبلاغ الفوري عن المواقع الالكترونية المشبوهة التي تريد التواصل مع المصرف										
المتوسط العام										
3.98										
0.91										

من خلال الجدول 8 يتبين أن أفراد الدراسة موافقون على محور مدى الوعي بأبرز تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي، والقطاع المصرفي في المنطقة الوسطى بمتوسط حسابي (3.98)، وترى الدراسة الحالية أن المنظمات والأفراد في القطاع المصرفي بحاجة لتعزيز أمن المعلومات وحماية المستخدمين من تهديدات الهندسة الاجتماعية، التي تؤثر سلبًا على الأداء وتسبب خسائر مادية ومعنوية، وتعمل هذه التهديدات على استغلال الحالة النفسية للأفراد والتأثير على المعرفة الضمنية والصريحة لديهم، مما يجعل من إدارة المعرفة أمراً ضرورياً في مواجهة هذا التحدي عبر تطوير نماذج وإستراتيجيات حماية متكاملة تشمل تحليل وتوظيف المعرفة الضمنية والصريحة للأفراد والمنظمات في القطاع المصرفي، وتحويلها إلى أدوات فعّالة للوقاية من تهديدات الهندسة الاجتماعية.

واتفقت هذه النتيجة مع دراسة (محمد، 2018): وسعت الدراسة إلى التعرف على مدى وعي المجتمع العربي بحماية حساباتهم الشخصية، التي من أبرز ما توصلت إليه الدراسة أن مجتمع الدراسة يتم حماية بياناتهم الشخصية بشكل تلقائي وبمعدل مرتفع.

واختلفت هذه النتيجة مع دراسة (جيبات، 2018): وهدفت الدراسة إلى التوعية بمخاطر الهندسة الاجتماعية ومعرفة كيفية عمل الهندسة الاجتماعية، وطرق الوقاية منها والحفاظ على المعلومات الشخصية للفرد، التي توصلت الدراسة إلى عدد من النتائج أهمها: المجتمع الفلسطيني يعاني جهلاً وإهمالاً كبيراً في مجال الهندسة الاجتماعية ومفهومها.

ومن خلال النتائج الموضحة أعلاه يتضح أن هناك تبايناً في موافقة أفراد الدراسة حول محور مدى الوعي بأبرز تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، وتراوحت متوسطات موافقتهم على العبارات ما بين (4.35 إلى 3.73) وهي متوسطات تقع في الفئة الخامسة والرابعة من فئات المقياس الخماسي واللذان تشير إلى (موافق بشدة - موافق) على أداة الدراسة، مما يوضح التباين في موافقة أفراد الدراسة حول محور

مدى الوعي بأبرز تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، والتي تم ترتيبها تنازلياً حسب متوسطات الموافقة عليها من قبل أفراد الدراسة كالتالي:

1. جاءت العبارة رقم (3) وهي: "لدي الوعي بمخاطر إتاحة بياناتي الشخصية للعامة على المواقع الإلكترونية بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بدرجة موافق بشدة بمتوسط حسابي (4.35) وتشير هذه النتيجة إلى وعي العاملين في القطاع المصرفي بمخاطر التي تواجههم عند إتاحة البيانات الشخصية على المواقع الإلكترونية.
 2. جاءت العبارة رقم (5) وهي: "أقوم باستخدام البرامج الأصلية والمواقع الموثوقة في تحميل الملفات" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (4.12) وتشير هذه النتيجة إلى أهمية اقتناء العاملين في القطاع المصرفي البرامج الأصلية التي توفر مزيداً من الحماية وتقليل أخطار تهديدات الهندسة الاجتماعية.
 3. جاءت العبارة رقم (2) وهي: "أسعى دوماً نحو الاطلاع على ضوابط الأمن السيبراني، وما يصدر من وثائق تخص سياسات وإجراءات الأمن السيبراني" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (4.06).
 4. جاءت العبارة رقم (6) وهي: "لدي وعي تام بالأساليب المستخدمة في اختراق الأنظمة من خلال انتحال الهوية، والتصيد الاحتيالي، والتتبع وخداع الضحية" بالمرتبة الرابعة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (3.98).
 5. جاءت العبارة (4) وهي: "أقوم بشكل دوري بتحديث كلمة المرور لحساباتي داخل المصرف" بالمرتبة قبل الأخيرة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (3.83)، ويمكن تفسير هذه النتيجة بأن التحديث الدوري لكلمات المرور للحسابات داخل المصرف، يساهم في الحماية وتقليل أخطار تهديدات الهندسة الاجتماعية.
 6. جاءت العبارة رقم (8) وهي: "أقوم بالإبلاغ الفوري عن المواقع الإلكترونية المشبوهة التي تريد التواصل مع المصرف" بالمرتبة الأخيرة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (3.73) وتشير إلى وعي العاملين في القطاع المصرفي بأن الإبلاغ الفوري عن المواقع الإلكترونية المشبوهة التي تريد التواصل مع المصرف يساهم في مواجهة تهديدات الهندسة الاجتماعية.
- دور إدارة المعرفة في مواجهة الهندسة الاجتماعية بالقطاع المصرفي السعودي حسب عينة الدراسة:**
- للتعرف على الأدوار التي تقدمها إدارة المعرفة في مواجهة الهندسة الاجتماعية بالقطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب، لاستجابات أفراد الدراسة لعبارات محاور الأدوار التي تقدمها إدارة المعرفة في مواجهة الهندسة الاجتماعية بالقطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، وجاءت النتائج كما يوضحها جدول رقم (9):

جدول رقم (9) الأدوار التي تقدمها إدارة المعرفة في مواجهة الهندسة الاجتماعية

م	العبارات	التكرار		درجة الموافقة					الرتبة
		النسبة %	شدة موافقة	موافقة	محايد	موافقة غير	غير موافقة	المتوسط الحسابي	
1	يقوم المصرف بحماية الأصول المعلوماتية والتقنية وذلك بالتركيز على سرية المعلومات وسلامتها وتوافرها	ك	22	22	3	5	0	4.17	1
		%	42.3	42.3	5.8	9.6	0		
3	يعمل المصرف على توثيق ونشر متطلبات الأمن السيبراني والالتزام بها	ك	22	21	2	7	0	4.12	2
		%	42.3	40.4	3.8	13.5	0		
10	يهتم المصرف بشكل حثيث بتوفير الأجهزة والمعدات عالية الجودة والتي تضمن أمن المعلومات	ك	20	23	3	5	1	4.08	3
		%	38.5	44.2	5.8	9.6	1.9		
2		ك	21	20	3	8	0	4.04	4

الرتبة	الانحراف المعياري	المتوسط الحسابي	درجة الموافقة					التكرار	العبارات	م
			موافق غير	موافق غير	مجايد	موافق	موافق بشدة	النسبة %		
			0	15.4	5.8	38.5	40.4	%	يقوم المصرف بالتحديث المستمر لأمن المعلومات بما يتناسب مع تطور أساليب الهندسة الاجتماعية	
5	1.02	3.96	0	8	4	22	18	ك	يتم تحديث المعرفة بشكل مستمر في المصرف من خلال تطويع التقنية في التعامل مع الكم الهائل من المعلومات	5
			0	15.4	7.7	42.3	34.6	%		
6	0.93	3.94	0	5	9	22	16	ك	يتم تصنيف المعرفة في المصرف وفهرستها إلكترونياً وتبويبها حسب النوع والتخصص ووضع كلمات مساعدة للبحث لتسهيل استرجاعها عند الحاجة	4
			0	9.6	17.3	42.3	30.8	%		
7	1.06	3.92	1	7	4	23	17	ك	يقوم المصرف بتحديد وتوثيق واعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين	9
			1.9	13.5	7.7	44.2	32.7	%		

م	العبارات	التكرار	درجة الموافقة					النسبة %
			موافق بشدة	موافق	محايد	موافق غير	غير موافق	
	قبل توظيفهم وإثناء عملهم وعند انتهاء عملهم في المصرف							
7	يوجد في المصرف فريق عمل لتوفير الحلول الفعالة لمواجهة أخطار الهندسة الاجتماعية	ك	16	20	5	10	1	3.77
		%	30.8	38.5	9.6	19.2	1.9	
8	يسعى المصرف نحو تطوير العنصر البشري بالمعرفة وتأهيله لمواجهة هجمات الهندسة الاجتماعية	ك	15	20	7	9	1	3.75
		%	28.8	38.5	13.5	17.3	1.9	
6	يستخدم المصرف البرمجيات والذكاء الاصطناعي في حل المشكلات التي تتعلق بالهندسة الاجتماعية	ك	13	15	14	9	1	3.58
		%	25	28.8	26.9	17.3	1.9	
0.88		3.93		المتوسط العام				

من خلال الجدول السابق يتضح أن استجابة أفراد الدراسة، جاءت بدرجة موافق على الأدوار التي تقدمها إدارة المعرفة في مواجهة الهندسة الاجتماعية بالقطاع المصرفي السعودي بدرجة موافق وبمتوسط حسابي (3.93)، وتظهر أهمية ودور إدارة المعرفة في مواجهة الهندسة الاجتماعية في قطاع المصارف، ويتم اتخاذ الإجراءات ووضع السياسات المتكاملة لتحقيق الأمن وحماية الخصوصية وسلامة المعلومات، ويمكن لإدارة المعرفة أن تكون عاملاً حاسماً في فهم ومنع هذه المخاطر، من خلال تحليل وتوجيه السلوك البشري، وتطوير الأدوات

والممارسات التي تسهم في تعزيز الوعي والحماية ضد محاولات الاختيال والتلاعب، مما يضمن بناء نظام أمني متكامل يراعي التحديات المعقدة للعصر الرقمي.

ومن خلال النتائج الموضحة أعلاه، يتضح أن هناك تجانس في موافقة أفراد الدراسة حول محور الأدوار التي تقدمها إدارة المعرفة في مواجهة الهندسة الاجتماعية بالقطاع المصرفي السعودي، وتراوحت متوسطات موافقتهم على العبارات ما بين (4.17 إلى 3.58)، وهي متوسطات تقع في الفئة الرابعة من فئات المقياس الخماسي والتي تشير إلى (موافق) على أداة الدراسة، مما يوضح التجانس في موافقة أفراد الدراسة حول محور الأدوار التي تقدمها إدارة المعرفة في مواجهة الهندسة الاجتماعية بالقطاع المصرفي السعودي، وتم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها بدرجة موافق كالتالي:

1. جاءت العبارة رقم (1) وهي: "يقوم المصرف بحماية الأصول المعلوماتية والتقنية، وذلك بالتركيز على سرية المعلومات وسلامتها وتوافرها" بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (4.17)، وتفسر هذه النتيجة أن جميع المصارف تعمل على توفير أقصى درجات الحماية للأصول المعلوماتية والتقنية من خلال الحفاظ على سرية وسلامة المعلومات.
 2. جاءت العبارة رقم (3) وهي: "يعمل المصرف على توثيق ونشر متطلبات الأمن السيبراني والالتزام بها" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (4.12)، وتفسر هذه النتيجة بأهمية رفع الوعي لدى العاملين في المصارف بدور التوثيق ونشر متطلبات الأمن السيبراني وضرورة الالتزام بها في مواجهة الهندسة الاجتماعية.
 3. جاءت العبارة رقم (10) وهي: "يهتم المصرف بشكل حثيث بتوفير الأجهزة والمعدات عالية الجودة والتي تضمن أمن المعلومات" بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (4.08)، ويمكن تفسير هذه النتيجة سعي المصارف في الممكنة بالعمل على توفير الأجهزة والمعدات عالية الجودة التي تعمل على توفير وضمان أمن المعلومات.
 4. جاءت العبارة رقم (2) وهي: "يقوم المصرف بالتحديث المستمر لأمن المعلومات بما يتناسب مع تطور أساليب الهندسة الاجتماعية" بالمرتبة الرابعة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (4.04).
 5. جاءت العبارة (8) وهي: "يسعى المصرف نحو تطوير العنصر البشري بالمعرفة وتأهيله لمواجهة هجمات الهندسة الاجتماعية" بالمرتبة قبل الأخيرة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (3.75)، وتشير هذه النتيجة إلى وعي قادة المصارف في المملكة بدور العنصر البشري وأهمية تطويره وتأهيله لمواجهة هجمات الهندسة الاجتماعية.
 6. جاءت العبارة رقم (6) وهي: "يستخدم المصرف البرمجيات والذكاء الاصطناعي في حل المشكلات التي تتعلق بالهندسة الاجتماعية" بالمرتبة الأخيرة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (3.58)، وتشير إلى ضرورة رفع الوعي لدى العاملين باستخدام البرمجيات والذكاء الاصطناعي في حل المشكلات التي تتعلق بالهندسة الاجتماعية.
- العوامل التي تعيق دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي:

للتعرف على التحديات التي تعيق دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، تم حساب التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، والرتب، لاستجابات أفراد الدراسة لعبارات محور التحديات التي تعيق دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، وجاءت النتائج كما يوضحها جدول رقم (10)

جدول رقم (10) محور التحديات التي تعيق دور إدارة المعرفة في مواجهة الهندسة الاجتماعية

م	العبارات	التكرار النسبة %	درجة الموافقة					الرتبة
			موافقة كبيرة	موافقة متوسطة	موافقة صغيرة	موافقة كبيرة	موافقة متوسطة	
3	ضعف الوعي لدى بعض الموظفين بمخاطر الهندسة الاجتماعية وكيفية مواجهتها	ك	14	22	10	5	1	1
		%	26.9	42.3	19.2	9.6	1.9	
4	يوجد ندرة في تقديم البرامج التدريبية التوعوية في المصرف لتثقيف الموظفين بمخاطر الهندسة الاجتماعية	ك	13	24	6	7	2	2
		%	25	46.2	11.5	13.5	3.8	
1	يوجد ضعف في البنية التحتية للإدارات داخل المصرف لتفعيل دور إدارة المعرفة في مواجهة الهندسة الاجتماعية	ك	12	19	10	8	3	3
		%	23.1	36.5	19.2	15.4	5.8	
2	هناك محدودية في التنسيق مع الجهات المختصة بالأمن السيبراني بهدف	ك	11	20	8	10	3	4
		%	21.2	38.5	15.4	19.2	5.8	

الرتبة	الانحراف المعياري	المتوسط الحسابي	درجة الموافقة					التكرار	العبارات	م
			موافقة	غير موافقة	محايد	موافقة	موافقة شديدة	النسبة %		
									مواجهة أخطار الهندسة الاجتماعية في المصرف	
5	1.25	3.40	5	9	8	20	10	ك	عدم اكتشاف حوادث وتهديدات الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعال والتعامل معها استباقيا من اجل منع او تقليل الآثار المترتبة	8
			9.6	17.3	15.4	38.5	19.2	%		
6	1.22	3.31	4	10	15	12	11	ك	الإهمال في تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول وصلاحيات الوصول المصرح به	5
			7.7	19.2	28.8	23.1	21.2	%		
7	1.23	3.27	5	10	12	16	9	ك	عدم توثيق واعتماد متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للمصرف	7
			9.6	19.2	23.1	30.8	17.3	%		
8	1.25	3.27	4	13	10	15	10	ك	هناك ندرة في تحديث الشبكة الداخلية وإدارة أمنها بشكل دقيق بهدف مواجهة أي اختراق	6
			7.7	25	19.2	28.8	19.2	%		

م	العبارات	التكرار	درجة الموافقة					النسبة %	المتوسط الحسابي	الانحراف المعياري	الرتبة
			ممتازة	جيدة	مقبولة	محايدة	مرفوضة				
			المتوسط العام						3.48	0.99	

من خلال الجدول 10 يتضح أن استجابة أفراد الدراسة جاءت بدرجة موافق على التحديات التي تعيق دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي بدرجة موافقة بشدة وبمتوسط حسابي (3.48)، ومن خلال النتائج الموضحة أعلاه يتضح أن هناك تباين في موافقة أفراد الدراسة حول محور التحديات التي تعيق دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي، حيث تراوحت متوسطات موافقتهم على العبارات ما بين (3.83 إلى 3.27) وهي متوسطات تقع في الفئة الرابعة والثالثة من فئات المقياس الخماسي والتي تشير إلى (موافق - محايد) على أداة الدراسة، مما يوضح التباين في موافقة أفراد الدراسة حول محور التحديات التي تعيق دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي، وتم ترتيبها تنازلياً حسب موافقة أفراد الدراسة عليها كالتالي:

1. جاءت العبارة رقم (3) وهي: "ضعف الوعي لدى بعض الموظفين بمخاطر الهندسة الاجتماعية وكيفية مواجهتها"، بالمرتبة الأولى من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (3.83)، وتفسر هذه النتيجة بضرورة رفع الوعي لدى بعض الموظفين بمخاطر الهندسة الاجتماعية وكيفية مواجهتها، وذلك من خلال وضع السياسات المتكاملة لتحقيق الأمن وحماية الخصوصية وسلامة المعلومات.
2. جاءت العبارة رقم (4) وهي: "توجد ندرة في تقديم البرامج التدريبية التوعوية في المصرف لتثقيف الموظفين بمخاطر الهندسة الاجتماعية" بالمرتبة الثانية من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (3.75)، وتفسر هذه النتيجة بأهمية العمل من قبل الإدارات المصرفية بتوفير البرامج التدريبية، وورش العمل في توعية العاملين في المصارف بمخاطر الهندسة الاجتماعية.
3. جاءت العبارة رقم (1) وهي: "يوجد ضعف في البنية التحتية للإدارات داخل المصرف لتفعيل دور إدارة المعرفة في مواجهة الهندسة الاجتماعية"، بالمرتبة الثالثة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (3.56)، ويمكن تفسير هذه النتيجة وعي عينة الدراسة بدور البنية التحتية للإدارات في المصارف في تفعيل دور إدارة الهندسة الاجتماعية في المصارف.
4. جاءت العبارة رقم (2) وهي: "هناك محدودية في التنسيق مع الجهات المختصة بالأمن السيبراني بهدف مواجهة أخطار الهندسة الاجتماعية في المصرف"، بالمرتبة الرابعة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (3.50).
5. جاءت العبارة رقم (7) وهي: "عدم توثيق واعتماد متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للمصرف"، بالمرتبة قبل الأخيرة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بشدة بمتوسط حسابي

(3.27)، وتشير هذه النتيجة بضرورة الاهتمام بمتطلبات الأمن السيبراني لمواجهة مثل هذه الهجمات ومخاطرها، من خلال توفير الجهود وتوحيدها لمواجهة هجمات الفضاء المعلوماتي وأثرها على المنشآت المختلفة ومن أبرزها القطاع المصرفي.

6. جاءت العبارة رقم (6) وهي: "هناك ندرة في تحديث الشبكة الداخلية وإدارة أمنها بشكل دقيق بهدف مواجهة أي اختراق" بالمرتبة الأخيرة من حيث موافقة أفراد الدراسة عليها بدرجة موافق بمتوسط حسابي (3.27)، وتشير إلى فاعلية تحديث الشبكة الداخلية وإدارة أمنها بشكل دقيق في مواجهة أي اختراق.

المقترحات التي تسهم في تفعيل دور إدارة المعرفة في مواجهة الهندسة الاجتماعية:

للتعرف على المقترحات التي تسهم في تفعيل دور إدارة المعرفة في مواجهة الهندسة الاجتماعية بالقطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى، كما يلي:

1. زيادة الوعي بالهندسة الاجتماعية بين الموظفين في القطاع المصرفي السعودي من خلال إقامة دورات تدريبية وورش عمل تركز على أهمية الأمن السيبراني، وكيفية التعامل مع هجمات الهندسة الاجتماعية.
2. تعزيز ثقافة الأمان في بيئة عمل المصارف.
3. تطوير أدوات وتقنيات لكشف ومنع هجمات الهندسة الاجتماعية.
4. تدريب وتطوير الموظفين في القطاع المصرفي السعودي حول كيفية حماية أنفسهم من الهندسة الاجتماعية.
5. التحديث المستمر لأن الهجمات تتطور باستمرار، فإن برامج التدريب والتوعية يجب أن تكون ديناميكية وتتجدد بشكل دوري، هذا يضمن أن الموظفين ليس فقط على دراية بأساليب الهجمات القديمة، ولكن أيضا بأساليب الهجوم الجديدة التي قد تستخدم في المستقبل.
6. العمل على إيجاد أفضل ممارسات إدارة المعرفة في القطاع المصرفي من خلال مجموعة متنوعة من المصادر مثل: المعايير والتقارير والدراسات البحثية.
7. العمل على احتياجات الأمن السيبراني في مجموعة متنوعة من المصادر مثل: تقارير المخاطر والتهديدات والتوصيات من الخبراء.
8. تطبيق التقنيات الحديثة المتقدمة التي يمكن استغلالها في إدارة المعرفة المناسبة لطبيعة القطاع المصرفي، ومواجهة الهندسة الاجتماعية مثل: تحليل البيانات، وتعلم الآلة، والذكاء الاصطناعي.
9. تطبيق أنظمة التحليل التنبؤي من خلال الجمع بين الذكاء الاصطناعي وأنظمة إدارة المعرفة، يمكن للبنوك الاستفادة من التحليل التنبؤي للكشف عن محاولات الهندسة الاجتماعية المحتملة والاستجابة لها بسرعة.
10. تطوير وتنفيذ محاكاة الهجمات باستخدام المعرفة المكتسبة، والتي يمكن للبنوك من تطوير محاكاة لهجمات الهندسة الاجتماعية لاختبار استعدادها وفعاليتها إجراءات الاستجابة، وهذه

المحاكاة تمكن الموظفين من التدريب على مواجهة هجمات الهندسة الاجتماعية في بيئة مراقبة، مما يزيد الوعي والاستعداد.

11. إنشاء قاعدة بيانات تحتوي على أمثلة حقيقية عن هجمات الهندسة الاجتماعية التي واجهت البنوك، يمكن من خلالها للموظفين التعلم من التجارب السابقة وتطوير إستراتيجيات فعالة للتصدي لهذه المحاولات في المستقبل.

12. التكامل مع منصات أمان الطرف النهائي، وذلك باستخدام الحلول التقنية المتقدمة لمراقبة نشاط الموظفين والتفاعلات على الأجهزة والشبكات، لضمان تحديد والتعامل مع أي محاولات هندسة اجتماعية بسرعة.

13. إنشاء تعاون بين البنوك في المملكة العربية السعودية لتبادل المعرفة والخبرات الأمنية المتخصصة حول التهديدات الأمنية بما فيها الهندسة الاجتماعية، ويشمل منصات التعاون الرقمية الآمنة وقواعد معرفة مشتركة، وكذلك ورش العمل والندوات المشتركة وتبادل الخبرات.

14. وضع التشريعات والقوانين والضوابط المحلية المتعلقة بالأمن السيبراني في البنوك لحماية البيانات، وضمان سلامة العمليات المصرفية.

15. التعاون الوثيق مع الهيئات الرسمية في المملكة للتأكد من مواكبة أحدث التشريعات والتوجيهات المتعلقة بالأمن السيبراني.

16. زيادة الاستثمار في التعليم والمعرفة المالية للمواطنين السعوديين والمستفيدين من البنوك بشكل عام.

17. إقامة مؤتمرات توعوية من قبل البنك المركزي السعودي تركز على أحدث تقنيات وأساليب الهندسة الاجتماعية وكيفية الحماية منها، كمؤتمرات التوعية التي أقامتها وزارة الصحة أثناء أزمة كورونا.

18. تعزيز التعاون بين البنوك والشركات المالية والجهات الحكومية الأخرى، مثل: هيئة الاتصالات وتقنية المعلومات والهيئة العامة للأمن السيبراني والبنك المركزي السعودي.

19. اعتماد معايير عالمية للحماية من تهديدات الهندسة الاجتماعية.

20. إنشاء نموذج خاص يدمج بين أفضل ممارسات إدارة المعرفة، بهدف تقديم حل شامل لمواجهة تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي.

دلالات نتائج الدراسة:

في ضوء تحليل بيانات الدراسة في الفصل الرابع، تمّ التوصل إلى العديد من النتائج، وذلك حسب أسئلة الدراسة على النحو التالي:

- فيما يخص واقع تطبيق إدارة المعرفة في القطاع المصرفي السعودي، اتضح من خلال النتائج أن هناك تقديرًا عاليًا لأهمية إدارة المعرفة في هذا القطاع، وبخاصة فيما يتعلق بتوفير أنظمة الأمان والحماية، واستقطاب الخبراء لتحقيق التميز والريادة، وتبني إستراتيجيات رقابية دقيقة، هذه النتائج تشير إلى الدور الحاسم الذي تلعبه إدارة المعرفة في تعزيز الأمان والكفاءة في القطاع المصرفي.

- يتضح أيضًا أن هناك اتفاقًا بين أفراد الدراسة على عبارات واقع تطبيق إدارة المعرفة بالقطاع المصرفي السعودي، وتراوح متوسطات موافقتهم على البُعد ما بين (4.12 إلى 3.62)، وهي متوسطات تقع في الفئة الرابعة من فئات المقياس الخماسي، والتي تشير إلى (موافق) على أداة الدراسة، هذه النتائج تشير إلى التجانس في موافقة أفراد الدراسة على واقع تطبيق إدارة المعرفة بالقطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى.
- يتضح من خلال النتائج أن هناك موافقة عالية لأهمية الوعي بتهديدات الهندسة الاجتماعية والأمن السيبراني في هذا القطاع، وبخاصة فيما يتعلق بمخاطر إتاحة البيانات الشخصية على المواقع الإلكترونية، واستخدام البرامج الأصلية والمواقع الموثوقة في تحميل الملفات.
- هذه النتائج تشير إلى الدور الحاسم الذي يلعبه الوعي بتهديدات الهندسة الاجتماعية في تعزيز الأمان والكفاءة في القطاع المصرفي، يتضح أيضًا أن هناك تباين في موافقة أفراد الدراسة على محور مدى الوعي بأبرز تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي.
- تراوحت متوسطات موافقتهم على محور مدى الوعي بأبرز تهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي ما بين (4.35 إلى 3.73)، وهي متوسطات تقع في الفئة الخامسة والرابعة من فئات المقياس الخماسي، والتي تشير إلى (موافق بشدة - موافق) على أداة الدراسة، هذه النتائج تشير إلى التباين في موافقة أفراد الدراسة على الوعي بالتهديدات الهندسة الاجتماعية في القطاع المصرفي السعودي من وجهة نظر مسؤولي البنك المركزي السعودي والقطاع المصرفي في المنطقة الوسطى.
- اتضح من النتائج أن الأفراد المشاركين في الدراسة يتفقون بشكل عام على الأدوار التي تقدمها إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي، يظهر التجانس في ردود الأفراد، وقد تراوحت متوسطات موافقتهم على العبارات ما بين (4.17 إلى 3.58)، وهذا يشير إلى موافقة عامة على أداة الدراسة.
- العبارات التي تم تقييمها تشمل مجموعة من الأدوار المهمة التي تقوم بها إدارة المعرفة، بدءًا من حماية الأصول المعلوماتية والتقنية، وصولًا إلى استخدام البرمجيات والذكاء الاصطناعي في حل المشكلات المتعلقة بالهندسة الاجتماعية، هذه النتائج تشير إلى المصارف في المملكة التي تعمل بجد لتحقيق أمن المعلومات ومواجهة التحديات المتعلقة بالهندسة الاجتماعية.
- اتضح من النتائج أن الأفراد المشاركين في الدراسة يتفقون بشكل عام على التحديات التي تعيق دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي، يظهر التباين في ردود الأفراد، وتراوح متوسطات موافقتهم على العبارات ما بين (3.83 إلى 3.27)، وهذا يشير إلى موافقة عامة على أداة الدراسة.
- كما أشارت النتائج أن العبارات التي تم تقييمها تشمل مجموعة من التحديات المهمة التي تعيق دور إدارة المعرفة، بدءًا من ضعف الوعي لدى بعض الموظفين بمخاطر الهندسة الاجتماعية وكيفية مواجهتها، وصولًا إلى ندرة في تحديث الشبكة الداخلية وإدارة أمنها بشكل دقيق بهدف مواجهة أي اختراق، هذه النتائج تشير إلى المصارف في المملكة تواجه تحديات معقدة في تحقيق أمن المعلومات ومواجهة التحديات المتعلقة بالهندسة الاجتماعية.

توصيات الدراسة :

- في ضوء النتائج التي تم التوصل إليها، تتقدم الدراسة بالتوصيات التالية :
- أهمية تعزيز الوعي والتدريب، بحيث يكون لدى الموظفين في القطاع المصرفي تدريب دوري حول كيفية التعامل مع هجمات الهندسة الاجتماعية، ويمكن أن يشمل ذلك التعرف على أنماط الاحتيال الشائعة وكيفية التعامل معها.
 - دراسة البحث عن أفضل الأساليب لتوعية الموظفين والعملاء في البنوك السعودية بمخاطر الهندسة الاجتماعية، وتدريبهم على كيفية التعامل معها.
 - ضرورة تطوير سياسات وإجراءات دقيقة، بحيث يكون هناك إطار قوي للسياسات والإجراءات المتعلقة بالأمان والهندسة الاجتماعية، يجب أن يتم توزيع هذه السياسات والإجراءات بشكل منتظم على جميع الموظفين.
 - العمل على تحديث التقنيات الأمنية المتمثلة في تحديث أنظمة الأمان والتقنيات المستخدمة في القطاع المصرفي بشكل دوري، يمكن أن يشمل ذلك تحديث أنظمة الكشف عن الاحتيال والتحقق من الهوية.
 - توجيه جهود التوعية للموظفين والعملاء على حد سواء، يجب أن يكون لديهم فهم جيد لأنماط الهندسة الاجتماعية وكيفية التعامل معها.
 - أن يكون هناك تعاون مستمر مع الجهات المختصة في مجال الأمان والهندسة الاجتماعية، يمكن أن يشمل ذلك تبادل المعلومات والتحديات حول التهديدات الجديدة.

الدراسات المستقبلية :

- في ضوء نتائج وتوصيات الدراسة، تقترح الدراسة إجراء الدراسات التالية:
- تحليل أثر إستراتيجيات إدارة المعرفة في مواجهة الهندسة الاجتماعية في البنوك السعودية.
 - دراسة استخدام التقنيات المتقدمة مثل: الذكاء الاصطناعي وتحليل البيانات للكشف عن أنماط الاحتيال الاجتماعي في القطاع المصرفي.
 - دراسة تبحث عن مراجعة السياسات والإجراءات الأمنية المعمول بها في البنوك السعودية في مواجهة الهندسة الاجتماعية.
 - دراسة أثر الثقافة التنظيمية في تعزيز الوعي بمخاطر الهندسة الاجتماعية وتطبيق إجراءات الأمان.

النموذج المقترح :

تم بناء النموذج شكل رقم (8) اعتماداً على ما توصلت إليه الدراسة من نتائج، ومراجعة الأدب النظري، وتحليل بيانات الاستبانة ونتائجها من وجهة نظر العينة، واستناداً على مجموعة من النماذج التي تم بناؤها فيما يتعلق بإدارة المعرفة والهندسة الاجتماعية، وذلك طمعا في الوصول إلى نموذج يخدم القطاع المصرفي في ظل ازدياد تهديدات الهندسة الاجتماعية، والاستفادة منه في هذا المجال.

حاولت الدراسة الاستفادة من النماذج التي لها علاقة بموضوع الدراسة، وكذلك نتيجة استطلاع آراء المبحوثين، والخروج بفكرة النموذج المقترح الذي تم عرضه على مجموعة التركيز لأخذ مرئياتهم، وتوصلت إلى ما يلي :

1. نطاق تطبيق النموذج المقترح:

إن واقع التطبيق الذي يستهدفه هذا النموذج هو القطاع المصرفي السعودي، والذي تقع مسؤولية تطبيقه على البنك المركزي السعودي والبنوك السعودية، وذلك للحصول على الفائدة المرجوة من التطبيق، وهي: استثمار دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي.

2. أهمية النموذج المقترح:

يمر العالم بتحديات في أساليب التهديدات السيبرانية التي تثير المخاوف بشأن أمن المعلومات وخصوصية المستخدمين، وتركز هذه التهديدات بشكل كبير على العنصر البشري كحلقة ضعيفة في نظام الأمن السيبراني، ويتم استغلال نقاط الضعف مثل: الخداع والإقناع والتلاعب، هنا يأتي دور إدارة المعرفة في مواجهة الهندسة الاجتماعية من خلال تطوير نظام متكامل يشمل التكنولوجيا وثقافة المنظمة والعنصر البشري، وتنبغي الإشارة إلى ضرورة دراسة عمليات الاحتيال المالي والهندسة الاجتماعية، وبخاصة في البيئات ذات الاستهداف العالي مثل القطاع المصرفي، ويتطلب هذا الأمر تطوير إستراتيجية شاملة للوقاية من الاحتيال المالي، تتضمن حملات توعية فعالة ضد الهندسة الاجتماعية، من أجل الوصول إلى حلول فعالة، يجب أن يتم البناء على نموذج يتضمن عناصر إدارة المعرفة في قطاع المصارف، مثل: تكنولوجيا المعلومات والدفاعات التقنية، والثقافة التنظيمية والأعمال، وسلوكيات الموظفين والمستفيدين، إضافة إلى عمليات إدارة المعرفة والإستراتيجية العامة للحماية.

3. أهداف النموذج المقترح:

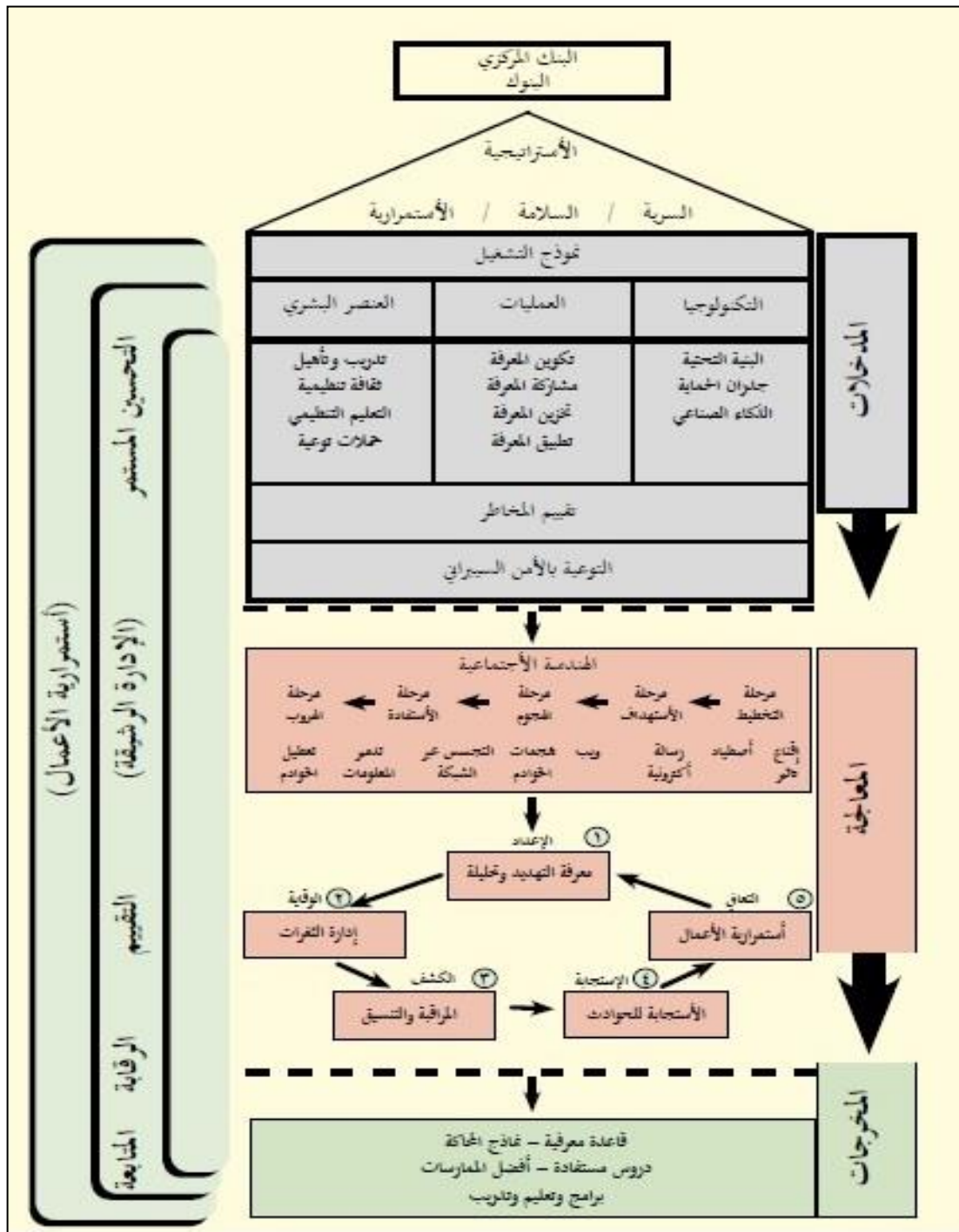
الهدف الرئيسي من النموذج المقترح هو استثمار دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي، ويكون ذلك من خلال تحقيق الأهداف الفرعية التالية:

1. اهتمام المسؤولين في القطاع المصرفي بأهمية تطبيق إدارة المعرفة لمواجهة تهديدات الهندسة الاجتماعية.
 2. تطبيق إدارة المعرفة في القطاع المصرفي بالشكل النموذجي العلمي.
 3. تبني البنك المركزي السعودي لإستراتيجيات التشريعات الوقائية من تهديدات الهندسة الاجتماعية، بما في ذلك حملات التوعية والإشراف والمتابعة لتطبيق هذه الإستراتيجيات.
 4. تعزيز الثقافة التنظيمية الداعمة لتطبيق إدارة المعرفة، بما يعزز الوعي الأمني داخل القطاع المصرفي.
 5. قياس العوامل المؤثرة على أمن المعلومات التي تساعد على التعرض لتهديدات الهندسة الاجتماعية.
 6. رصد التحديات التي تعيق أمن المعلومات في القطاع المصرفي.
 7. تعزيز البنية التحتية التقنية اللازمة لأمن المعلومات من تهديدات الهندسة الاجتماعية.
 8. زيادة الوعي لموظفي القطاع المصرفي بتهديدات الهندسة الاجتماعية وكيفية الوقاية منها.
 9. توفير البيئة المناسبة للحماية من تهديدات الهندسة الاجتماعية داخل القطاع المصرفي السعودي.
- يرتكز النموذج المقترح على مجموعة متكاملة توضح من خلالها الدراسة دور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي بشكل عام، بدء من البنك المركزي والبنوك الرئيسية والفروع التابعة لها، لتصبح كيانا واحدا يسهل من خلاله إدارة المعرفة في مواجهة الهندسة الاجتماعية، وذلك بآلية ثلاثة مراحل وهي كالتالي:

المرحلة الأولى- الإعداد الأولي: تم فيها إعداد الدراسة بتحليل الواقع الفعلي لدور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي، من خلال الأخذ بنتائج أدوات الدراسة (الاستبانة- مجموعة التركيز).

المرحلة الثانية- تحقيق المتطلبات: إدراك البنك المركزي والبنوك بأهمية دور إدارة المعرفة في مواجهة الهندسة الاجتماعية والوقاية من تهديداتها.

المرحلة الثالثة- أهم المخرجات: تحسين وتطوير الواقع الفعلي بتفعيل إستراتيجية الأمن السيبراني والدفاعات التقنية، والرفع من تأهيل العنصر البشري وتوعيتهم بخطر الهندسة الاجتماعية وتعزيز الثقافة التنظيمية، والاستفادة من الذكاء الاصطناعي، وبناء قاعدة معرفية تساند استمرارية الأعمال.



الشكل رقم (8) النموذج المقترح لدور إدارة المعرفة في مواجهة الهندسة الاجتماعية في القطاع المصرفي السعودي.

وقد ارتكز النموذج المقترح على أهم العمليات والعناصر التي بها تتم إدارة المعرفة الفاعلة لدى القطاع المصرفي والبنوك والفروع التابعة، لتصبح كيانا واحدا يسهل من خلاله أفضل الممارسات، والتي تندرج تحت ثلاثة مراحل وهي كالتالي:

مرحلة المدخلات: وهذه المرحلة تختص بتبني البنك المركزي والبنوك لإستراتيجية الأمن السيبراني المتمثلة في السرية والسلامة والاستمرارية، وذلك للوقاية من تهديدات الهندسة الاجتماعية والتي تستهدف العنصر البشري، وهو أحد أهم ركائز هذه المرحلة فتشمل الإستراتيجية تدريبهم وتأهيلهم وتوعيتهم بخطر الهندسة الاجتماعية، وتعزيز الثقافة التنظيمية والتعلم التنظيمي، وذلك عند ممارسة عمليات إدارة المعرفة في تشخيص المعرفة وتوليدها ومشاركتها وتخزينها وتوزيعها وإعادة استخدامها، والتي تتم باستخدام التكنولوجيا التي تحتاج إلى حماية الدفاعات التقنية وجدران الحماية، والاستفادة من تقنيات الذكاء الاصطناعي وتقييم المخاطر، ووضع التدابير الوقائية والتوعية بالأمن السيبراني.

مرحلة المعالجة: في هذه المرحلة تحدث تهديدات الهندسة ، ويبرز دور الإدارات المعنية بالأمن السيبراني، فعند بداية مراحل الهندسة الاجتماعية بدء بالتخطيط الذي يشمل الإقناع والتأثير والترصد، ومحاولة الاصطياد والذي قد يتطور إلى مرحلة الاستهداف باستخدام الوسائل مثل: الرسائل الإلكترونية واستخدام الويب التي تمكنهم من الانتقال إلى مرحلة الهجوم بالهجمات على الخوادم، والاستفادة من ذلك بالاقتراق والتجسس على الشبكة، وتدمير المعلومات وتعطيل الخوادم الذي يساعدهم في إخفاء آثار الاقتراق والهجوم، وهذا ما يسمى مرحلة الهروب، كل ذلك يتطلب من إدارة الأمن السيبراني الاستعداد الدائم، ومعرفة التهديد وتحليله منذ بداية مراحل، ثم إدارة الثغرات للوقاية من التهديد وكشفه ومراقبته للاستجابة ومواجهته ومنعه، وبعد ذلك التمكن من استمرارية الأعمال التي تسمى بالتعافي والتي بها تنتقل المرحلة إلى مرحلة المخرجات.

مرحلة المخرجات: وهي امتداد لاستمرارية الأعمال- التعافي والتي تكون أهم مخرجاتها الدروس المستفادة والتي يبني عليها محاكاة للهجمات والتقارير، وبحوث التطوير وبرامج التعليم والتدريب وأفضل الممارسات، وللإدارة الرشيقة دور في هذه المرحلة لتحسين المستمر والمتابعة والتقييم، ويكون هناك خطط لاستمرارية الأعمال كمرجع ودليل للبنوك لمساعدتها في بناء أهم الإجراءات والعمليات التي من شأنها زيادة مرونتها للاستجابة لتهديدات الهندسة الاجتماعية، واستعادة خدماتها بشكل مرن وسلس، للمساهمة في استمرارية تقديم الخدمات وتعزيزا للأمن السيبراني وإدارة المخاطر.

المراجع العربية:

- أبو ثنين، سعود عبيد، (2019)، *الأبعاد الاجتماعية والأمنية للجرائم المعلوماتية في المجتمع السعودي*، الرياض: كلية الملك فهد الأمنية، مركز الدراسات والبحوث.
- بيسرا، إرما؛ وسابيروال، فرنانديز، (2014)، *إدارة المعرفة والنظم والعمليات*، ترجمة: محمد شحاتة وهبي، وعبد المحسن فالح اللحيد، الرياض: مركز البحوث بمعهد الإدارة العامة.
- تقرير البنك المركزي السعودي <https://www.sama.gov.sa/ar-sa/Pages/default.aspx>

- جيبات، مزهر هاني، (2018)، *الهندسة الاجتماعية وآثارها على المجتمع الفلسطيني*، رسالة ماجستير غير منشورة، جامعة النجاح الوطنية، كلية الفنون، قسم الفنون التطبيقية.
- الذيابي، فلاح بن علي، (2022)، *فاعلية الولاء التنظيمي في مواجهة الهجمات السيبرانية*، بحث تكميلي مقدم للمعهد العالي للدراسات الأمنية، كلية الملك فهد الأمنية، دبلوم مكافحة الجرائم المعلوماتية.
- راضي، محمد سامي؛ والشوري، عمرو إبراهيم عوض، (2019)، برنامج مقترح بالقياسات الحيوية منتج بمعالجة الصورة الرقمية للتغلب على بعض التهديدات الأمنية في البنوك، *المجلة العلمية للدراسات المحاسبية*، جامعة قناة السويس، 21(2)، 56-123.
- سعد، عبدالرزاق عمران؛ ومعتوق، طارق أبو شعفة، (2020)، واقع ممارسة عمليات إدارة المعرفة في قطاع المصارف الليبية، *مجلة البحوث الأكاديمية*، ع15، 360-379.
- سيف، محمد عاطف جابر، (2023)، *أثر عمليات إدارة المعرفة في تطوير رأس المال الفكري في البنوك التجارية الأردنية*، رسالة ماجستير غير منشورة، جامعة آل البيت، كلية الأعمال، الأردن.
- الشهري، عبدالعزيز عبدالله، (2021)، *مستوى الوعي بأسياسات الأمن السيبراني في قوات الطوارئ الخاصة بمنطقة جازان*، بحث تكميلي مقدم للمعهد العالي للدراسات الأمنية، كلية الملك فهد الأمنية، دبلوم مكافحة الجرائم المعلوماتية.
- الشهري، عبدالمنعم ياسين؛ وعقيلي، عثمان موسى، (2024)، دور الإدارة الرشيقة في دعم مشاريع إدارة مشاريع إدارة المعرفة في الأجهزة الحكومية بالمملكة العربية السعودية: نموذج مقترح، *المجلة العربية الدولية لإدارة المعرفة*، المؤسسة العربية لإدارة المعرفة، 3(1)، 121-172.
- الصانع، نورة عمر؛ وآخرون، (2020)، وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم، *مجلة كلية التربية*، جامعة أسيوط، 36(6)، 41-90.
- الصحفي، مصباح أحمد حامد؛ وعسكول، سناء بنت صالح، (2019)، مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة، *مجلة البحث العلمي في التربية*، جامعة عين شمس، كلية البنات للآداب والعلوم والتربية، 10(20)، 493-534.
- الضب، علي، (2023)، دور الذكاء الاصطناعي وتعلم الآلة في تعزيز كشف الاحتيال على البطاقات الائتمانية، *مجلة دراسات تطوير القطاع المالي*، صندوق النقد العربي، 22(2)، 1-43.
- عايض، عبداللطيف مصلح؛ والعودي، نجاته عبده محمد، (2020)، أثر إدارة المعرفة في التطوير التنظيمي دراسة ميدانية في المصارف اليمنية، *مجلة الآداب*، الدراسات والبحوث الإنسانية، ع14، 432-476.
- عبدالمنعم، أحمد السيد، (2021)، *الهندسة الاجتماعية وبناء العقل*، *مجلة الإرشاد النفسي*، جامعة عين شمس، ع68، 1-7.
- عبدالوهاب، شادي، (2017)، *حروب الجيل الخامس: التحولات الرئيسية في المواجهات العنيفة غير التقليدية في العالم*، مجلة دراسات المستقبل، أبو ظبي، ع1.

- علي، أيمن ميرغني إبراهيم، (2023)، أثر إدارة المعرفة على جودة الخدمات المصرفية- دراسة حالة: بنك أم درمان الوطني-السودان، *المجلة العربية للعلوم الإنسانية والاجتماعية*، 18(1)، 2-4.
- العلي، علي حميد؛ والحسناوي، بنين زهير، (2021)، دور إدارة المعرفة في تعزيز الجاهزية المصرفية، *مجلة كلية التربية للبنات للعلوم الإنسانية*، جامعة الكوفة، 15(26)، 421-444.
- الغنبر، خالد سليمان؛ والقحطاني محمد عبدالله، (2009م)، *أمن المعلومات بلغة ميسرة*، ط1، الرياض: مكتبة الملك فهد الوطنية.
- القحطاني، نورة بنت ناصر، (2019)، مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي، *مجلة شؤون اجتماعية*، جمعية الاجتماعيين في الشارقة، 36(144)، 85-120.
- كريستيان، براين، (2022)، *الهندسة الاجتماعية: مقدمة*، وارنر بوكس، نيويورك.
- اللهبي، عيسى بن حامد بن ناصر، (2023)، *عناصر إدارة المعرفة في الأداء المؤسسي في هيئة تطوير منطقة المدينة المنورة ودورها لتفعيل الاستثمار المعرفي: نموذج مقترح*، رسالة دكتوراه غير منشورة، جامعة الملك عبدالعزيز، كلية الآداب والعلوم الإنسانية، قسم علم المعلومات / إدارة المعرفة.
- مجلد، رباب عبدالرحمن، (2018)، *دور إدارة المعرفة في إدارة الكوارث وتخفيف مخاطرها: نموذج مقترح للبلديات بالمملكة العربية السعودية*، رسالة دكتوراه غير منشورة، جامعة الملك عبدالعزيز بجدة، كلية الآداب والعلوم الإنسانية، قسم علم المعلومات.
- محارب، عبدالعزيز قاسم، (2023)، *الذكاء الاصطناعي والأمن السيبراني، مجلة المال والتجارة*، نادي التجارة، (653)، 4-23.
- محمد، مها أحمد إبراهيم، (2018)، *الهندسة الاجتماعية وشبكات التواصل الاجتماعي وتأثيرها على المجتمع العربي، المجلة الدولية لعلوم المكتبات والمعلومات، الجمعية المصرية للمكتبات والمعلومات والأرشيف*، 5(3)، 109-128.
- مدني، إلهام؛ ومرابط، رباب؛ وطاهري، شريفة؛ وقاسمي، فريال، (2022)، *دور إدارة المعرفة في تحسين جودة الخدمات في المؤسسات الاقتصادية*، رسالة ماجستير غير منشورة، جامعة الشهيد حمه لخضر بالوادي، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، الجزائر.
- ملتقى أسبار، (2023)، *الاحتيايل المالي، أثره على الثقة في المؤسسات المالية*، تقرير رقم (98)، لجنة الشؤون القانونية والاستشارية، الرياض.
- منصور، شادي عبدالوهاب، (2019)، *حروب الجيل الخامس: أساليب التفكير من الداخل على الساحة الدولية*، ط1، القاهرة: دار العربي للنشر والتوزيع.
- الهيئة الوطنية للأمن السيبراني، (2018)، *الضوابط الأساسية للأمن السيبراني*، الرياض: الهيئة الوطنية للأمن السيبراني.

المراجع الأجنبية:

- Almutairi, Bandar & Alghamdi, Abdurahman.(2022). The Role of Social Engineering in Cybersecurity and Its Impact, *Journal of Information Security*. Vol.13 No.4, October.
- Amy Hetro Washo. (2023). An interdisciplinary view of social engineering: A call to action for research. Available at: [https://www.sciencedirect.com/\(7/7/2023\)](https://www.sciencedirect.com/(7/7/2023)).
- Manyam, Sowjanya. (2022). *Artificial Intelligence's Impact on Social Engineering Attacks*. Submitted in partial fulfillment of the requirements. For the degree of master of science, Governors State University. .
- G20/OECD INFE report on adult financial literacy in G20 countries . <https://doi.org/10.1787/04fb6571-en>
- S. Dotsenko, O. Illiashenko, S. Kamenskyi & V. Kharchenko. (2019). Integrated Model of Knowledge Management for Security of Information Technologies: Standards ISO/IEC 15408 and ISO/IEC 18045. *Information Security* vol. 43, no. 3, 305–317.
- Weerasinghe, Salinda & Seder, Darshana. (2023). Role of Knowledge in Creativity and Innovation in the Service Sector: An Example from the Banking Sector in a Developing Nation. IGI Global Business Science Reference. book: Embracing Business Sustainability Through Innovation and Creativity in the Service Sector, pp.47–66.
- Zuoguang Wang, Hongsong Zhu, Peipei Liu, and Limin Sun. (2023). Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. Available at: [https://cybersecurity.springeropen.com/\(2/2/2023\)](https://cybersecurity.springeropen.com/(2/2/2023)).