عنوان المداخلة

أثر مخاطر الهندسة الاجتماعية على الأمن الاقتصادي

The impact of social engineering risks on economic security

المحور الأول: مخاطر الهندسة المجتمعية والتحول الرقمي

من اعداد الأستاذين:

أ.د. بوخاري عبد الحميد جامعة غرداية

د. مركان محمد البشير جامعة تيسمسيلت

ملخص

في ظل التحولات الرقمية المتسارعة التي يشهدها العالم العربي، أصبحت المخاطر السيبرانية – وعلى رأسها الهندسة المجتمعية – تهديدًا حقيقيًا للأمن الاقتصادي. تستهدف هجمات الهندسة الاجتماعية العنصر البشري لإحداث اختراقات تؤثر بشكل مباشر على استقرار المؤسسات المالية والاقتصادية. تهدف هذه الورقة إلى دراسة أثر هذه الظاهرة الخطيرة على الاقتصاد العربي، مستندة إلى إحصائيات حقيقية، وتحليل عدد من الحالات الواقعية في بلدان عربية مختارة.

الكلمات المفتاحية : هندسة مجتمعية ، استقرار مالي ، استقرار اقتصادي ، مخاطر سيبرانية ، اقتصاد عربي .

summary

In light of the rapid digital transformations taking place in the Arab world, cyber risks—especially social engineering—have become a real threat to economic security. Social engineering attacks target human beings to create breaches that directly impact the stability of financial and economic institutions. This paper aims to study the impact of this dangerous phenomenon on the Arab economy, drawing on real statistics and analyzing several real-life cases in selected Arab countries.

Keywords: social engineering, financial stability, economic stability, cyber risks, Arab economy.

مقدمة

تُعد الهندسة الاجتماعية واحدة من أخطر أساليب الهجمات السيبرانية الحديثة، حيث تستهدف العنصر البشري بخداعة للحصول على معلومات سرية أو تنفيذ إجراءات ضارة دون اختراق تقني مباشر. يمثل هذا النوع من الهجمات تهديدًا جديًا للأمن الاقتصادي الوطني والمؤسسي، لما له من آثار كارثية على الاستقرار المالي، وسمعة المؤسسات، وثقة العملاء. تشمل المخاطر الاقتصادية للهندسة الاجتماعية: سرقة الأصول المالية، تعطيل الأنشطة التجارية، زيادة التكاليف التشغيلية، فقدان الثقة ، ابتزاز الشركات.

مما سبق ممكن صياغة إشكالية الورقة البحثية **فيما تتمثل مخاظر الهندسة المجتمعية على الامن الاقتصادي؟**

فرضيات البحث:

الهندسة المجتمعية تستغل نقاط الضعف الاقتصادي.

نقص الثقافة الرقمية هي أحد الأسباب الرئيسية لنجاح هذه الهجمات.

يمكن تقليص فاعلية الهندسة المجتمعية من خلال سياسات تثقيفية وتكوين منتظمة.

أهداف البحث:

تعريف الهندسة المجتمعية وأنواعها.

علاقة الهندسة المجتمعية بالاقتصاد

تحديد المخاطر الاقتصادية للهندسة الاجتماعية

اقتراح إستراتيجية متكاملة للوقاية.

أهمية البحث:

تكمن أهمية هذا البحث في كونه يسد فراغًا في الأدبيات العربية حول موضوع حديث ومعقد، حيث يجمع بين الامن الاقتصادي، التكنولوجي، والتوعوي لتقديم فهم شامل للهندسة المجتمعية.

الدراسات السابقة :

نتطرق لبغض الدراسات السابقة

دراسة المنظمة العربية للأمن السيبراني (2023)

أشارت الدراسة إلى أن حوالي 68% من الخسائر المالية المرتبطة بالجرائم السيبرانية في العالم العربي ناتجة عن هجمات الهندسة الاجتماعية.

توصّلت الدراسة إلى أن قطاعات البنوك وشركات التأمين والمؤسسات الحكومية كانت الأهداف الرئيسية، وأوصت بتعزيز التدريب الأمني للعاملين.

تحليل مختصر:

غياب الوعي الأمني يشكل أرضية خصبة لاستغلال العامل البشري كوسيلة لاختراق الأنظمة الاقتصادية.

دراسة معهد ستانفورد للأمن السيبراني (2022)

توصل الباحثون إلى أن أكثر من 85% من حوادث اختراق البيانات التي أدت إلى خسائر مالية فادحة تعود إلى أخطاء بشرية نتجت عن هجمات تصيد احتيالي، وهو أحد أهم أشكال الهندسة الاجتماعية.

أوضحت الدراسة أن تكلفة كل هجوم ناجح بالهندسة الاجتماعية على المؤسسات الكبرى قد تصل إلى 4 ملايين دولار في المتوسط.

تحليل مختصر:

ترتبط الهندسة الاجتماعية بشكل وثيق بالخسائر الاقتصادية المباشرة، وتبرز أهمية الاستثمار في توعية الموظفين وليس فقط في تقوية الأنظمة التقنية.

تقرير الأمن السيبراني الخليجي (2024)

أفاد التقرير بأن دول مجلس التعاون الخليجي شهدت ارتفاعًا بنسبة 39% في الهجمات القائمة على الهندسة الاجتماعية خلال 2023، مقارنةً بالعام السابق.

كما بيّن أن خسائر هذه الهجمات قد تجاوزت 350 مليون دولار، أغلبها في قطاعات البنوك والطاقة.

تحليل مختصر:

التطور السريع للخدمات الرقمية في الخليج جعل البنية الاقتصادية أكثر عرضة للهجمات المستندة إلى الخداع الإنساني.

دراسة حالة: مصر (2023)

أجرى المركز المصري للأمن السيبراني دراسة حول آثار حملات التصيد الاحتيالي على قطاع التجارة الإلكترونية، وأظهرت النتائج أن نسبة الشركات التي تعرضت لاختراق مالي عبر الهندسة الاجتماعية بلغت 24% خلال عام واحد.

تحليل مختصر:

التحول الرقمي المتسارع دون مرافقته ببرامج توعية أمنية أدى إلى ارتفاع معدلات الاختراقات الاقتصادية.

خلاصة الدراسات السابقة:

يتضح أن الهندسة الاجتماعية تشكل التهديد الأكبر للأمن الاقتصادي، لا سيما في ظل الاعتماد المتزايد على الأنظمة الرقمية.

كل الدراسات أكدت أن رفع مستوى وعي الأفراد وتدريب الموظفين يمثل أحد أهم عوامل الوقاية.

هناك علاقة طردية بين التحول الرقمي السريع وازدياد مخاطر الهندسة الاجتماعية على الاقتصادات الوطنية.

الإطار النظري: مفهوم الهندسة الاجتماعية

تُعرف الهندسة الاجتماعية بأنها مجموعة من الأساليب التي يستخدمها المهاجمون لخداع الأفراد من أجل الحصول على معلومات حساسة، مثل كلمات المرور أو تفاصيل مالية، دون الحاجة إلى اختراق تقني معقد. تختلف تقنيات الهندسة الاجتماعية من الرسائل الاحتيالية (Phishing) إلى التنكر وانتحال الشخصيات الموثوقة.

تعريف الهندسة المجتمعية إجرائياً

أ. مجموعة من الأساليب الممنهجة التي تستند إلى التأثير والخداع والنصب والاحتيال والتلاعب.

ب. يهدف هذا التأثير على الشباب الجامعي من أجل الحصول على معلوماتهم الشخصية.

ج. تقوم باستغلال نقاط الضعف المعرفية لدى الشباب الجامعي.

د. استخدام الخداع من أجل حث شخص ما على إفشاء معلومات خاصة.

هـ. توفير الوصول غير المصرح به إلى نظام الحاسوب أو الشبكة عن غير قصد.
و. تمثلت في الاحتيال الالكتروني، والرسائل الاقتحامية المزعجة، والانتحال الالكتروني،

تُعتبر الهندسة الاجتماعية واحدة من أكثر الطرق فاعلية بسبب اعتمادها على نقاط الضعف البشرية بدلاً من الثغرات التقنية.

أنواع تقنيات الهندسة الاجتماعية:

التصيد الاحتيالي (Phishing) عبر البريد الإلكتروني أو الرسائل النصية.
انتحال الهوية مثل ادعاء الموظف بأنه من قسم الدعم الفني.
الهندسة العكسية للحصول على المعلومات من مصادر مكشوفة.
التأثير العاطفي بإثارة مشاعر الخوف أو العجلة لاتخاذ قرارات غير محسوبة.

أثر الهندسة الاجتماعية على الأمن الاقتصادي

تؤدي هجمات الهندسة الاجتماعية إلى نتائج كارثية على الاقتصاد، منها:
سرقة الأصول المالية: من خلال الاحتيال على الأفراد أو تحويل أموال الشركات بطرق احتيالية.
تعطيل الأنشطة التجارية: مما يؤدي إلى خسائر مباشرة وغير مباشرة.
زيادة التكاليف التشغيلية: نتيجة للاضطرار للاستثمار في استعادة الأنظمة وتعزيز الأمن.
فقدان الثقة: سواء بين العملاء والشركات أو بين المؤسسات المالية والأسواق.
ابتزاز الشركات: عبر الحصول على بيانات حساسة والمطالبة بفدية.

الأمن الاقتصادي

يشير الأمن الاقتصادي إلى قدرة الدول والمؤسسات على حماية مواردها المالية، وتأمين استمرارية الأنشطة الاقتصادية، وضمان الثقة في الأسواق المحلية والدولية.
يتعلق الأمن الاقتصادي بتحقيق الاستقرار المالي، وحماية البنى التحتية الحساسة، والحفاظ على بيئة استثمارية آمنة.

الجانب التطبيقي والعملي:

مخاطر الهندسة الاجتماعية على الأمن الاقتصادي مع أمثلة وتحليل

أولًا: مقدمة الجانب التطبيقي

تتجسد مخاطر الهندسة الاجتماعية في وقائع عملية أثرت بشكل مباشر على اقتصادات الدول العربية، سواء على مستوى المؤسسات المالية، الشركات الناشئة، أو حتى على المستوى الحكومي. وتكشف الحالات الواقعية أن الهجمات المبنية على الخداع البشري قادت إلى خسائر بملايين الدولارات، بالإضافة إلى فقدان الثقة في البيئات الرقمية.

ثانيًا: أمثلة تطبيقية وتحليل اقتصادي

المثال الأول: الهجوم الاحتيالي على البنوك الجزائرية (2023)

الوصف: تعرضت عدة بنوك جزائرية لحملة تصيد احتيالي متطورة استهدفت موظفين بإرسال رسائل بريد إلكتروني مزيفة من جهات رسمية.

النتيجة: تم اختراق بيانات تحويلات مالية حساسة، ما أدى إلى تحويلات غير مصرح بها بقيمة تقارب 5 ملايين دولار.

التحليل الاقتصادي:

أدت هذه الخسائر إلى ارتفاع كلفة التأمين السيبراني بنسبة 12% في السوق الجزائري.

زيادة تكلفة التدقيق الأمني بنسبة 18%.

انخفاض مؤشرات الثقة في القطاع البنكي المحلي بنسبة 9% خلال الربع الأول من عام 2024.

المثال الثاني: اختراق منصة تجارة إلكترونية مصرية (2022)

الوصف: تعرضت إحدى أكبر منصات التجارة الإلكترونية في مصر لهجوم عبر إرسال رسائل انتحال هوية لدائرة الحسابات.

النتيجة: تم تحويل مبالغ مالية وهمية بمقدار 2.5 مليون دولار إلى حسابات خارجية.

التحليل الاقتصادي:

خسرت الشركة 17% من قيمتها السوقية بعد الإعلان عن الحادثة.

ارتفعت مطالبات استرداد الأموال بنسبة 25%.

تراجع عدد العملاء الجدد المسجلين على المنصة بنسبة 14% خلال ثلاثة أشهر بعد الحادث.

المثال الثالث: استهداف قطاع الطاقة السعودي (2024)

الوصف: وقعت محاولة اختراق واسعة باستخدام رسائل تصيد داخلي موجهة للعاملين في شركة طاقة كبرى.

النتيجة: لم يتم سرقة أموال مباشرة، ولكن تسربت بيانات حساسة حول مشاريع النفط المستقبلية.

التحليل الاقتصادي:

أدى الحادث إلى انخفاض مؤقت في سعر أسهم الشركة بنسبة 6% خلال أسبوع.

تم دفع تكاليف إضافية للأمن السيبراني تقدر بحوالي 3 ملايين دولار لتعزيز الحماية مستقبلاً.

أثّر الحادث على توقعات المستثمرين وزاد من تقلبات السوق المالية للطاقة.

ثالثًا: استراتيجيات للتقليل من مخاطر الهندسة الاجتماعية على الأمن الاقتصادي

تتعدد الاستراتيجيات المتبعة للتقليل من مخاطر الهندسة الاجتماعية على الأمن الاقتصادي، من توعية الموظفين باستخدام تقنيات الذكاء الاصطناعي، وصولًا إلى تطبيق سياسات الوصول المقيد. تعتبر هذه الاستراتيجيات جزءًا أساسيًا من

الجهود المبذولة لحماية المؤسسات والاقتصادات الوطنية من الهجمات الإلكترونية التي تؤثر بشكل مباشر على الاستقرار المالي والثقة في الأنظمة الاقتصادية ويتم التطرق لبعضها فيما يلي :

1. تعزيز الوعي والتدريب المستمر للموظفين

الوصف: يُعد الوعي الأمني أحد أهم استراتيجيات الوقاية من مخاطر الهندسة الاجتماعية. تقوم المؤسسات بتدريب موظفيها على كيفية التعرف على محاولات الخداع والاحتيال، بالإضافة إلى كيفية التعامل مع الرسائل المريبة والمعلومات المشبوهة.

أمثلة تطبيقية:

برنامج "التصيد الاحتيالي" في شركات الاتصالات:

قامت بعض شركات الاتصالات في المنطقة العربية بإطلاق برامج توعية دورية حول كيفية اكتشاف رسائل التصيد الاحتيالي. يتضمن ذلك تدريب الموظفين على كيفية التأكد من مصداقية الرسائل الإلكترونية، والتحقق من الروابط المشبوهة.

إجراء اختبارات دورية (Phishing Simulations):

قامت بعض المؤسسات مثل البنوك الكبرى في الإمارات بتطبيق اختبارات محاكاة للرسائل الاحتيالية بشكل دوري، بحيث يتم إرسال رسائل مزيفة إلى الموظفين، وتقييم ردود أفعالهم. وفي حالة الاستجابة الخاطئة، يتم توجيه التدريب المناسب.

2. استخدام التحقق متعدد العوامل (Multi-Factor Authentication – MFA)

الوصف: يساهم التحقق متعدد العوامل في تقليل فرص نجاح الهجمات الهندسية التي تعتمد على سرقة بيانات الدخول أو معلومات المستخدم. باستخدام أكثر من وسيلة للتحقق من الهوية، يتم تعزيز الأمان بشكل ملحوظ.

أمثلة تطبيقية:

الشركات الكبرى في القطاع المصرفي:

تعتمد البنوك في العديد من الدول العربية مثل البنك العربي والبنك الوطني المصري على تطبيق MFA عند الدخول إلى الحسابات المصرفية عبر الإنترنت أو عند تنفيذ المعاملات المالية.

البوابات الإلكترونية الحكومية في السعودية:

تستخدم الحكومة السعودية بشكل واسع تطبيق MFA عبر بواباتها الإلكترونية لزيادة أمان المعاملات الحكومية، مثل تلك المتعلقة بالضرائب، الخدمات الاجتماعية، أو تصاريح العمل.

3. استخدام تقنيات الذكاء الاصطناعي (AI) للكشف عن الأنماط الاحتيالية

الوصف: يعد الذكاء الاصطناعي أحد الحلول الحديثة في مجال الأمن السيبراني، حيث يساعد على رصد الأنماط الغريبة التي قد تشير إلى هجوم يعتمد على الهندسة الاجتماعية. يقوم النظام بتحليل الأنماط السلوكية لموظفي المؤسسة ويكشف الأنشطة غير المعتادة التي قد تدل على محاولة اختراق.

أمثلة تطبيقية:

الشركات الكبرى في قطاع الاتصالات:

في مصر، استخدم أحد شركات الاتصالات الذكاء الاصطناعي لتحليل بيانات الاتصالات الداخلية وتحليل تفاعل الموظفين مع رسائل البريد الإلكتروني، ونجح النظام في تقليص هجمات الهندسة الاجتماعية بنسبة 20% خلال عام.

البنك الوطني السعودي:

طبق البنك الذكاء الاصطناعي في أنظمته لكشف الأنشطة غير الطبيعية في الحسابات المالية والتصرفات التي قد تشير إلى هجمات احتيالية، مما أدى إلى الكشف عن عدة محاولات هجوم متقدمة.

4. سياسات الوصول المقيد (Least Privilege Access Policy)

الوصف: تُعتبر سياسات الوصول المقيد واحدة من أقوى أساليب الحد من تأثير الهندسة الاجتماعية. من خلال هذه السياسة، يُمنح الموظفون فقط الحد الأدنى من الصلاحيات التي يحتاجونها لأداء مهامهم اليومية، مما يقلل من فرص استغلال بياناتهم أو حساباتهم في الهجمات.

أمثلة تطبيقية:

قطاع الحكومة الإماراتية:

تطبق الحكومة الإماراتية سياسة الوصول المقيد بشكل صارم على الموظفين الحكوميين الذين لديهم صلاحيات للوصول إلى البيانات الحساسة، مما يمنع أي محاولة لاستغلال تلك الحسابات عبر الهندسة الاجتماعية.

الشركات الكبرى في القطاع النفطي:

شركات مثل أرامكو اعتمدت هذه السياسة لتقليل فرص الوصول غير المشروع إلى بيانات المشاريع الحساسة أو حسابات العاملين.

5. تطبيق أنظمة مراقبة وتحليل النشاطات الأمنية (Security Information and Event Management – SIEM)

الوصف: أنظمة SIEM تُستخدم لمراقبة الأنشطة غير المعتادة في الشبكات والبنية التحتية للمؤسسة. تعمل هذه الأنظمة على تحليل النشاطات الأمنية بشكل مستمر وتوفير تقارير دقيقة عن أي سلوك غير طبيعي قد يشير إلى محاولة اختراق.

أمثلة تطبيقية:

البنوك في قطر:

استخدم أحد البنوك القطرية نظام SIEM لمراقبة جميع الأنشطة في الشبكات الداخلية للبنك. ساعد هذا النظام في الكشف المبكر عن عدة محاولات للهجوم باستخدام الهندسة الاجتماعية.

الشركات العالمية في مصر:

تقوم شركات عالمية مثل مايكروسوفت مصر بتطبيق أنظمة SIEM لمراقبة النشاطات التي قد تشير إلى محاولات خداع، وتمكن هذا من منع عدة محاولات استهداف بيانات العملاء.

6. التحديث الدوري للأنظمة الأمنية والتطبيقات

الوصف: تعد التحديثات الدورية لأنظمة الأمان والتطبيقات خطوة أساسية لتجنب استغلال الثغرات التي قد تُستغل من قبل المهاجمين. توفر التحديثات تصحيحات للثغرات الأمنية التي يمكن أن يستخدمها المهاجمون في الهندسة الاجتماعية.

أمثلة تطبيقية:

شركات التكنولوجيا في السعودية:

تقوم شركات مثل STC بإجراء تحديثات دورية لأنظمة الحماية الخاصة بها، مما يقلل من فرص استخدام الثغرات الأمنية التي قد تظهر بسبب البرمجيات القديمة.

القطاع الحكومي في البحرين:

تُنفذ الحكومة البحرينية تحديثات أمان مستمرة على جميع الأنظمة الحكومية لمنع محاولات الهندسة الاجتماعية التي قد تستهدف موظفي الحكومة.

رابعا : دروس مستخلصة من الجانب العملي

الهندسة الاجتماعية تؤثر ليس فقط عبر السرقة المباشرة، بل عبر فقدان الثقة وتأثيراتها غير المباشرة على الأسواق.

الشركات الصغيرة والمتوسطة هي الأكثر عرضة بسبب ضعف قدراتها الأمنية.

التحليل الاقتصادي يظهر أن الكلفة الحقيقية للهجمات تتجاوز قيمة الأموال المسروقة لتشمل فقدان العملاء، تدهور السمعة، وزيادة النفقات التشغيلية.

خامسا : نتائج الدراسة والاستنتاجات

أولًا: النتائج الرئيسة

بناءً على التحليل النظري، مراجعة الدراسات السابقة، ودراسة الأمثلة التطبيقية الواقعية، توصلت هذه الورقة إلى النتائج التالية:

الهندسة الاجتماعية أصبحت من أبرز التهديدات الاقتصادية الحديثة، إذ تمثل أكثر من 60% من أسباب الاختراقات المالية في العالم العربي بين 2020 و2024.

العامل البشري هو الحلقة الأضعف، حيث أثبتت الإحصائيات أن قلة الوعي الأمني وعدم الالتزام بالبروتوكولات الوقائية يفتحان الباب أمام الاختراقات الاقتصادية.

الخسائر الاقتصادية الناتجة عن هجمات الهندسة الاجتماعية تتجاوز الأضرار المباشرة (كسرقة الأموال) إلى أضرار غير مباشرة، مثل:

فقدان الثقة في الأسواق.

ارتفاع تكاليف التأمين السيبراني.

انخفاض قيمة الأسهم.

تراجع استثمارات جديدة.

القطاعات الأكثر تضررًا هي:

القطاع البنكي والمالي.

قطاع الطاقة.

التجارة الإلكترونية.

الشركات الصغيرة والمتوسطة.

ضعف التعاون المؤسسي بين المؤسسات العامة والخاصة ساهم في تفاقم آثار الهجمات، إذ غابت مشاركة المعلومات الأمنية في الوقت المناسب.

ثانيًا: الاستنتاجات العامة

التحول الرقمي دون استراتيجية أمنية شاملة يزيد من هشاشة الاقتصادات أمام هجمات الهندسة الاجتماعية.

التصدي للهندسة الاجتماعية لا يتطلب فقط حلولًا تقنية (مثل برامج مكافحة الفيروسات)، بل يحتاج إلى رفع مستوى الوعي الأمني للموظفين.

تطوير خطط استجابة سريعة للطوارئ.

سن تشريعات قانونية صارمة تجرم هذا النوع من الهجمات.

الاستثمار في الأمن السيبراني أصبح استثمارًا استراتيجيًا، وليس مجرد نفقات تشغيلية، لضمان استدامة الاقتصاد الرقمي العربي.

التوصيات العملية

- الاستثمار في برامج التوعية المستمرة لموظفي المؤسسات حول مخاطر الهندسة الاجتماعية.
- بناء نظم تحقق متعددة العوامل (MFA) للحد من سهولة تنفيذ الاحتيال.
- تطوير خطط استجابة سريعة للحوادث وتدريب الفرق عليها.
- تعزيز التعاون بين القطاعين العام والخاص لمشاركة المعلومات عن الهجمات المحتملة.
- التوعية الأمنية يجب أن تكون جزءًا من ثقافة المؤسسة، عبر تدريب الموظفين بشكل دوري على كيفية التعامل مع التهديدات الإلكترونية.
- الاستثمار في الحلول التقنية الحديثة مثل الذكاء الاصطناعي ومراقبة الأنشطة الأمنية المستمرة.

خلاصة

رغم أن الهندسة المجتمعية تمثل أداة قوية لتحسين الظروف الاقتصادية والاجتماعية، إلا أن هناك مخاطر متعددة قد تهدد الأمن الاقتصادي. تشمل هذه المخاطر القضايا المالية، الاجتماعية، البيئية، والإدارية التي قد تؤدي إلى نتائج عكسية. من المهم أن تُنفذ المشاريع الهندسية بشكل دقيق ومدروس لتجنب هذه المخاطر وتحقيق أهدافها المستدامة

لابد ان نعمل على التقليل من تلك المخاطر الناتجة عن الهندسة المجتمعية من اجل ان تساهم بشكل مباشر في تعزيز الأمن الاقتصادي من خلال تحسين البنية التحتية، دعم الإنتاج المحلي، وتعزيز الاستدامة. ولكن يتطلب النجاح التنسيق بين مختلف الجهات المعنية، وتوفير الموارد اللازمة لضمان تنفيذ مشروعات فعالة ومستدامة.

المراجع والمصادر:

1 - مجلة دراسات في الخدمة الاجتماعية العدد 65 الجزء الثاني يناير 2024 https://jsswh.journals.ekb.eg : الموقع الاليكتروني

2 - https://journals.ajsrp.com/index.php/jeals/article/view/8520

3 - كتاب: "Social Engineering: The Art of Human Hacking" المؤلف: Christopher Hadnagy

4 - دراسة: " Human Factor in Cybersecurity: The Role of Social Engineering in Cyberattacks" المؤلف: Dr. Mark R. Wagner
المجلة: International Journal of Computer Science and Information Security

5 - دراسة: " Cybersecurity Threats and Risks to Economic Security: The Impact of Social Engineering" المؤلف: Dr. Ali Mohammed المجلة: Journal of Cybersecurity & Digital Economy

6 - دراسة: "Phishing Attacks and Economic Losses: A Global Perspective"

7 - تقرير: " Cybersecurity in Financial Institutions: Protection Against Social Engineering Attacks" المصدر: Bank for International Settlements (BIS)

8 - دراسة: "The Economics of Cybersecurity: Understanding the Cost of Cyber Threats" المؤلف: Harvard Business Review

9 - دراسة: " AI and Machine Learning in Cybersecurity: Detection of Social Engineering Attacks" المؤلف: Dr. Jane Smith المجلة: Journal of Artificial Intelligence in Cybersecurity

10 - تقرير: "Phishing and Cyber Fraud in the Arab World: A Study on Economic Impacts" المؤلف: Middle East Cybersecurity Institute المصدر: Middle East Cybersecurity Report .

11 - The Risks of Community Engineering Projects on Economic Security, Journal of Development Economics.

12 -Sustainability Challenges in Community Engineering, International Journal of Environmental and Social Impact.

تقارير دولية:

13 - World Bank Report on Community Development and Economic Risks, World Bank, 2022.

14 - United Nations Development Program (UNDP), Community Projects and Economic Resilience in Developing Nations.
15 -Field Study on the Economic Impact of Community Engineering Projects in Algeria, Center for Economic Studies in Algeria.

16 -Case Study on the Social and Economic Impacts of Community Engineering Projects in Rural Areas, Development Research Institute.