Journal of Economic, Administrative and Legal Sciences (JEALS) • Vol 9, Issue 1(2025) • P: 25 - 1
https://journals.ajsrp.com/index.php/jeals
ISSN: 2522-3372 (Online) • ISSN: 2522-3372 (Print)

The impact of social engineering on cybersecurity risks in banks in the city of Riyadh in the Kingdom of Saudi Arabia

Mr. Abdullelah Saeed Al Mohayya*[1], Ms. Arwa Ahmed Makeen[2]

[1] Zakat, Tax and Customs Authority | KSA

[2] Ministry of Interior | KSA

Received: 20/06/2024

Revised: 29/06/2024

Accepted: 15/07/2024

Published: 30/01/2025

* Corresponding author: almohayya2020@gmail.com

Citation: Al Mohayya, A. S., & Makeen, A. A. (2025). The impact of social engineering on cybersecurity risks in banks in the city of Riyadh in the Kingdom of Saudi Arabia. *Journal of Economic, Administrative and Legal Sciences, 9*(1), 1 – 25 . https://doi.org/10.26389/AJSRP.A230624

Abstract: This study aims to assess the social engineering factors that significantly affect cybersecurity risks in the banking sector in Riyadh, Saudi Arabia. The study specifically addressed the impact of these factors on employees' awareness and behaviors that may make them more vulnerable to social engineering risks. Through the use of a quinquennial Lecter scale to evaluate responses, data has been collected and analyzed to extract results related to levels of awareness, personal and social factors, and the efficiency of preventive actions in place in banks. The results showed that average awareness of social engineering among bank employees was high, with computational averages ranging from 3.94 to 4.41, indicating a good level of awareness of cyber risks and threats. The study also showed that there is an urgent need to strengthen preventive measures and develop stricter security policies within banks to address social engineering threats more effectively.

The study also addressed the importance of ongoing training and improved regulatory culture in banks as necessary steps to reduce security gaps and improve response to cyberattacks. Results suggest that improving security training and strengthening security policies can play an important role in raising awareness and ability to effectively address social engineering. The study recommends the need to invest in intensive security awareness programmes and develop training methodologies that replicate realistic scenarios of cyberattacks to enable staff to identify and respond efficiently to social engineering attempts. By applying these strategies, banks can strengthen their cyber defenses and protect their sensitive information from growing security threats in the digital age.

Keywords: Social engineering, cybersecurity, Riyadh banks, organizational culture, employee training.

أثر الهندسة الاجتماعية على مخاطر الأمن السيبراني في البنوك في مدينة الرياض في المملكة العربية السعودية

أ. عبد الإله سعيد آل محيا*[1]، أ. أروى أحمد مكين[2]

[1] هيئة الزكاة والضريبة والجمارك | المملكة العربية السعودية

[2] وزارة الداخلية | المملكة العربية السعودية

المستخلص: تهدف هذه الدراسة إلى تقييم العوامل الهندسية الاجتماعية التي تؤثر بشكل كبير على أخطار الأمن السيبراني في قطاع البنوك بمدينة الرياض، المملكة العربية السعودية. تناولت الدراسة تحديدًا تأثير هذه العوامل على وعي الموظفين وسلوكياتهم التي قد تجعلهم أكثر عرضة لمخاطر الهندسة الاجتماعية. من خلال استخدام مقياس ليكرت الخماسي لتقييم الاستجابات، تم جمع بيانات وتحليلها لاستخراج النتائج المتعلقة بمستويات الوعي، العوامل الشخصية والاجتماعية، وكفاءة الإجراءات الوقائية المعمول بها في البنوك. وقد بينت النتائج أن متوسط الوعي بالهندسة الاجتماعية بين موظفي البنوك كان مرتفعًا، حيث تراوحت المتوسطات الحسابية بين 3.94 و4.41، ما يدل على وجود مستوى جيد من الوعي بالمخاطر والتهديدات السيبرانية. أظهرت الدراسة أيضًا أن هناك حاجة ماسة لتعزيز الإجراءات الوقائية وتطوير سياسات أمنية أكثر صرامة داخل البنوك لمواجهة تهديدات الهندسة الاجتماعية بفعالية أكبر. كما تناولت الدراسة أهمية التدريب المستمر وتحسين الثقافة التنظيمية في البنوك كخطوات ضرورية لتقليل الفجوات الأمنية وتحسين الاستجابة للهجمات السيبرانية. تشير النتائج إلى أن تحسين التدريب الأمني وتعزيز سياسات الأمن يمكن أن يلعب دورًا مهمًا في رفع مستوى الوعي والقدرة على التصدي للهندسة الاجتماعية بشكل فعال. توصي الدراسة بضرورة الاستثمار في برامج توعية أمنية مكثفة وتطوير منهجيات تدريب تحاكي السيناريوهات الواقعية للهجمات السيبرانية لتمكين الموظفين من التعرف على ومواجهة محاولات الهندسة الاجتماعية بكفاءة. من خلال تطبيق هذه الإستراتيجيات، يمكن للبنوك تعزيز دفاعاتها السيبرانية وحماية معلوماتها الحساسة من التهديدات الأمنية المتزايدة في العصر الرقمي.

الكلمات المفتاحية: هندسة اجتماعية، أمن سيبراني، بنوك الرياض، ثقافة تنظيمية، تدريب الموظفين.

1- المقدمة:

يشهد العصر الحديث تطورًا هائلاً في مجال التكنولوجيا والاتصالات، حيث أصبحت الشبكة العنكبوتية العالمية (الإنترنت) جزءًا لا يتجزأ من حياة البشر. ومع تزايد استخدام التكنولوجيا والتوسع السريع للشبكات الإلكترونية، تزايدت أيضًا التهديدات التي تواجهها البنوك والمؤسسات المالية في مجال الأمن السيبراني. واستجابةً لهذه التهديدات المتنامية، أصبح من الضروري بالغ الأهمية تحقيق أمن سيبراني قوي وفعال لحماية المعلومات والأصول المالية.

تحظى البنوك بأهمية استراتيجية في النظام المالي، حيث تعتبر الحوسبة المصرفية والخدمات المالية عبر الإنترنت جزءًا أساسيًا من عملياتها اليومية. ومع زيادة استخدام التكنولوجيا في هذا القطاع، تزداد المخاطر المرتبطة بالهجمات السيبرانية على البنوك. واختراق البنوك وسرقة المعلومات المالية أو الهوية للعملاء يمكن أن يتسبب في أضرار مالية هائلة وتأثيرات سلبية على الثقة العامة في النظام المصرفي والاقتصاد.

من بين العديد من الأساليب المستخدمة في الهجمات السيبرانية، تبرز الهندسة الاجتماعية كأداة فعالة يستخدمها المهاجمون للوصول إلى المعلومات الحساسة. تعتمد الهندسة الاجتماعية على استغلال العوامل النفسية والاجتماعية لدى البشر من أجل الحصول على معلومات سرية أو إقناعهم بتنفيذ أفعال تخدم أهداف المهاجم. يمكن أن تشمل تلك الأفعال الاحتيال الإلكتروني والتلاعب بالهوية والتصيد الاحتيالي عبر البريد الإلكتروني والتلاعب بالمشاعر وغيرها.

وفي هذا السياق، يهدف هذا البحث إلى استكشاف عوامل الهندسة الاجتماعية المؤثرة على مخاطر الأمن السيبراني في البنوك في مدينة الرياض في المملكة العربية السعودية. يركز البحث على دراسة كيفية استخدام الهندسة الاجتماعية في الاختراقات الإلكترونية وتحليل أهمية الأمن السيبراني للبنوك والمؤسسات المالية. سيتم تحديد نطاق البحث ليتمركز حول البنوك في مدينة الرياض في المملكة العربية السعودية، حيث تعد الرياض واحدة من أكبر المراكز المالية في المملكة وتضم عددًا كبيرًا من البنوك والمؤسسات المالية الرئيسية.

سيتم تحليل العوامل الاجتماعية التي تؤثر على مخاطر الأمن السيبراني في البنوك، بما في ذلك العوامل النفسية والثقافية والتكنولوجية. واستكشاف كيفية استغلال المهاجمين للعوامل الاجتماعية في الهندسة الاجتماعية وتأثيرها على مستوى الأمان السيبراني في البنوك. واستعراض السياسات والإجراءات الحالية المتبعة في البنوك في مدينة الرياض للتصدي لتهديدات الأمن السيبراني وتحديد النقاط التي يمكن تحسينها وتعزيزها.

من خلال هذا البحث، يأمل الباحثون في توفير رؤى قيّمة حول العوامل الاجتماعية المؤثرة في مخاطر الأمن السيبراني في البنوك، وتوفير توصيات عملية لتعزيز الأمان السيبراني وحماية المعلومات المالية في البنوك في مدينة الرياض. ستساهم نتائج هذا البحث في تعزيز الوعي بأهمية الأمن السيبراني وتوجيه الجهود نحو تعزيز الحماية في البنوك والمؤسسات المالية في المملكة العربية السعودية.

مشكلة الدراسة:

تعتبر الهندسة الاجتماعية من أخطر التهديدات التي تواجه أمن المعلومات والبيانات في البنوك والمؤسسات المالية، حيث تعتمد تلك الهجمات على استغلال ضعف العنصر البشري من خلال التلاعب بالعواطف والمشاعر لحمل الضحية على تنفيذ أفعال معينة تؤدي لاختراق الأنظمة والحصول على البيانات الحساسة. وقد أشارت التقارير إلى تزايد حوادث الهندسة الاجتماعية ضد البنوك في المملكة العربية السعودية بنسبة 250% خلال عام 2021 مقارنة بعام 2020، مما يستدعي ضرورة دراسة العوامل المؤثرة على نجاح تلك الهجمات.

وتكمن مشكلة البحث الحالي في النقص النسبي للدراسات التي تناولت تحليل عوامل الهندسة الاجتماعية التي تزيد من مخاطر الاختراقات الإلكترونية ضد البنوك في مدينة الرياض بالمملكة العربية السعودية، حيث لم تتناول الأبحاث بشكل كافٍ الجوانب النفسية والاجتماعية والثقافية التي قد تؤثر على نجاح حملات الهندسة الاجتماعية ضد الموظفين في تلك البنوك. كما أن معظم الدراسات السابقة ركزت على الجوانب التقنية للأمن السيبراني دون التطرق للعنصر البشري.

وتبرز أهمية هذا البحث في كونه يحاول معالجة الفجوة البحثية حول فهم العوامل الاجتماعية والنفسية المؤثرة على نجاح حملات الهندسة الاجتماعية، من خلال دراسة تجارب وخبرات الموظفين في البنوك بمدينة الرياض وتحليل البيئة الثقافية وطبيعة المجتمع، بهدف وضع توصيات عملية للحد من مخاطر تلك الهجمات. وسيتبع البحث المنهج الوصفي التحليلي من خلال جمع البيانات اللازمة باستخدام المقابلات والاستبانات، ثم تحليلها واستخلاص النتائج والتوصيات. ومن المأمول أن تسهم نتائج هذا البحث في زيادة الوعي بمخاطر الهندسة الاجتماعية وتطوير السياسات والإجراءات اللازمة للتصدي لتلك التهديدات المتزايدة على أمن المعلومات في البنوك بالمملكة. وعليه فإن السؤال الرئيسي لهذه الدراسة هو: ما العوامل الاجتماعية والنفسية والثقافية التي تؤثر على نجاح حملات الهندسة الاجتماعية ضد البنوك في مدينة الرياض؟

الأسئلة الفرعية:

1- ما مدى وعي موظفي البنوك في مدينة الرياض بمخاطر الهندسة الاجتماعية وطرق الوقاية منها؟
2- ما العوامل الشخصية والاجتماعية التي تجعل بعض موظفي البنوك أكثر عرضة للوقوع ضحية للهندسة الاجتماعية؟
3- كيف تؤثر الثقافة التنظيمية داخل البنوك على مدى فاعلية سياسات وإجراءات مواجهة الهندسة الاجتماعية؟
4- ما الإجراءات والسياسات التي يمكن للبنوك اتباعها للحد من مخاطر الهندسة الاجتماعية؟

أهمية الدراسة:

- الأهمية العلمية:

- يساهم البحث في سد الفجوة المعرفية وإثراء الأدبيات حول موضوع الهندسة الاجتماعية وأثرها على أمن المعلومات في البنوك.
- يوفر البحث إطارا نظريا ومنهجية بحثية يمكن الاسترشاد بها في دراسات مستقبلية ذات صلة.
- قد تفتح نتائج البحث المجال أمام توجهات بحثية جديدة تركز على الجوانب السلوكية والاجتماعية للأمن السيبراني.

- الأهمية العملية:

- تقديم توصيات عملية للبنوك لتطوير سياسات وإجراءات أكثر فاعلية لمواجهة الهندسة الاجتماعية.
- رفع مستوى الوعي لدى الموظفين حول مخاطر الهندسة الاجتماعية وسبل الحماية منها.
- إفادة الجهات المسؤولة عن الأمن السيبراني في وضع استراتيجيات وطنية لمكافحة الهندسة الاجتماعية.
- المساهمة في تطوير التشريعات والقوانين ذات الصلة بالحد من الهندسة الاجتماعية.
- تزويد الباحثين والمهتمين بمرجع علمي حول الموضوع يخدم أغراضهم البحثية والعملية.

أهداف الدراسة:

الهدف الرئيسي:

تحديد العوامل الاجتماعية والنفسية والثقافية المؤثرة على نجاح حملات الهندسة الاجتماعية ضد البنوك في مدينة الرياض.

الأهداف الفرعية:

1. تقييم مستوى الوعي لدى موظفي البنوك بمخاطر الهندسة الاجتماعية وسبل الوقاية منها.
2. تحديد العوامل الشخصية والاجتماعية التي تزيد من تعرض بعض الموظفين للوقوع ضحية الهندسة الاجتماعية.
3. دراسة أثر الثقافة التنظيمية داخل البنوك على فاعلية الإجراءات المتبعة لمواجهة الهندسة الاجتماعية.
4. تقديم توصيات وإجراءات عملية يمكن للبنوك تبنها للحد من مخاطر الهندسة الاجتماعية.

تساؤلات الدراسة (الفروض).

الفرضية الرئيسية:

لا توجد دلالة إحصائية عند مستوى 0.05 بين العوامل الاجتماعية والنفسية والثقافية ونجاح حملات الهندسة الاجتماعية ضد البنوك في مدينة الرياض.

الفرضيات الفرعية:

1. لا توجد دلالة إحصائية عند مستوى 0.05 بين مستوى وعي الموظفين وتعرضهم للوقوع ضحية الهندسة الاجتماعية.
2. لا توجد دلالة إحصائية عند مستوى 0.05 بين العوامل الشخصية والاجتماعية للموظفين وتعرضهم للهندسة الاجتماعية.
3. لا توجد دلالة إحصائية عند مستوى 0.05 بين الثقافة التنظيمية وفاعلية إجراءات مواجهة الهندسة الاجتماعية.
4. لا توجد فروق ذات دلالة إحصائية عند مستوى 0.05 بين الإجراءات المقترحة وخفض مخاطر الهندسة الاجتماعية.

2- الاطار النظري.

مفهوم الهندسة الاجتماعية

في لغة الأمان السيبراني، تتقاطع مجالات التكنولوجية والعلم الاجتماعي بطريقة معقدة، حيث تحدث تحديات تفوق الحواجز الرقمية ليمتد تأثيرها إلى العقل البشري. حيث يتناول هذا الفصل مفهوم الهندسة الاجتماعية وكيف تلعب دورًا حيويًا في تشكيل خريطة مخاطر الأمان السيبراني داخل بنوك مدينة الرياض.

الهندسة الاجتماعية، هي أكثر من مجرد فن، إنها سلوك، هي أسلوب يتلاعب بأساسيات الثقة لدي العملاء ويستغل نقاط الضعف الإنسانية ليخترق أقوى الحواجز الرقمية. إنها فهماً عميقاً للطبيعة البشرية، حيث يتلاعب المخترق الاجتماعي بالأوهام ويخلق تساؤلات داخل عقول الأفراد.

الهندسة الاجتماعية هي مجموعة من التقنيات والمهارات التي تستهدف الجانب البشري في الأمن السيبراني ، وتهدف إلى التأثير على الناس وإقناعهم بالقيام بأشياء تخدم مصالح المهاجمين أو المخترقين، مثل الكشف عن المعلومات السرية أو السماح بالوصول إلى الأنظمة أو الشبكات أو التعرض للبرمجيات الخبيثة. الهندسة الاجتماعية تعتمد على استغلال الثغرات النفسية والسلوكية والاجتماعية للضحايا ، مثل الثقة والفضول والخوف والجشع والرغبة في المساعدة.

يتنوع نطاق الهندسة الاجتماعية بين التقنيات المتطورة والتفاصيل الدقيقة للعلاقات الإنسانية. فهي تشمل استخدام التلاعب النفسي، حيث يُطلق المخترق الاجتماعي الحيل والأذرع النفسية لاختراق الجدران الأمانية. يصبح الإغراء جسرًا إلى النفوذ غير المشروع، والثقة تتحول إلى فخ يُنصب.

وفي مجال الأمان السيبراني في البنوك في مدينة الرياض، تتجلى أهمية الهندسة الاجتماعية في استنباط أنواع الهجمات التي تستهدف ليس الأنظمة وحدها، بل تستهدف العقول والقلوب. تصبح الروابط الاجتماعية بين الموظفين والعملاء بوابة لاختراق غير محسوس.

الهندسة الاجتماعية لها أهمية كبيرة في مجال الأمن السيبراني ، لأنها تمثل أحد أكثر التهديدات شيوعاً وخطورة على الأمن السيبراني ، ولأنها تستطيع تجاوز الحماية التقنية والتركيز على العنصر البشري الذي يعتبر العنصر الضعيف في سلسلة الأمن. أهداف الهندسة الاجتماعية تختلف حسب نوع المهاجم ودوافعه ومصالحه ، ولكن بشكل عام تتمحور حول الحصول على المعلومات أو الأموال أو السلطة أو الانتقام أو الشهرة أو الإثبات.

الهندسة الاجتماعية تنقسم إلى نوعين رئيسيين: الهندسة الاجتماعية النشطة والهندسة الاجتماعية السلبية. الهندسة الاجتماعية النشطة هي التي يقوم فيها المهاجم بالاتصال مباشرة بالضحية ومحاولة التأثير عليه بالكلام أو الإيماءات أو الحركات ، ويمكن أن تكون عن طريق الهاتف أو البريد الإلكتروني أو الرسائل النصية أو الشبكات الاجتماعية أو الزيارات الشخصية. الهندسة الاجتماعية السلبية هي التي يقوم فيها المهاجم بترك أدلة أو مصادر معلومات مغرية للضحية ، وينتظر أن تقوم الضحية بالتفاعل معها بنفسها ، مثل الأقراص المدمجة أو أقلام الذاكرة أو الرسائل المزيفة أو المواقع الوهمية.

الهندسة الاجتماعية تتبع أساليب مختلفة لتحقيق أهدافها.

ويختار المهاجم الأسلوب المناسب حسب نوع الضحية والمعلومات المطلوبة والوقت المتاح والموارد المتوفرة. بعض الأساليب الشائعة هي: التزوير والتقمص والتصيد والتخمين والتجسس والترغيب والترهيب والتملق والتضليل والتحالف والتهديد والابتزاز والرشوة والابتكار. (سالم سعيد الكندي، 2020)

الهندسة الاجتماعية تمر بمراحل محددة لتنفيذ عملية الاختراق، وتختلف هذه المراحل حسب نوع الهندسة الاجتماعية والأسلوب المستخدم والهدف المراد تحقيقه. بشكل عام ، تتضمن المراحل الآتية: جمع المعلومات وتحديد الضحية وبناء العلاقة واستغلال الثغرة وتحقيق الهدف وقطع الاتصال وإخفاء الأثر.

الهندسة الاجتماعية تتأثر بعدة عوامل تزيد من فرص نجاحها أو تقلل منها، وتتعلق هذه العوامل بالمهاجم والضحية والبيئة. بعض هذه العوامل هي: الخبرة والمهارة والثقة والمصداقية والاستعداد والتخطيط والتوقيت والتكيف والمرونة والابتكار والمبادرة والمصلحة والحاجة والمشاعر والمعتقدات والقيم والمبادئ والثقافة والتعليم والتدريب والتوعية والتثقيف والتحفيز والتحدي والمكافأة والعقاب والضغط والتهديد والخوف والجشع والفضول والرغبة في المساعدة والتعاطف والتملق والتضليل والتحالف والترهيب والترغيب والتصرف والتفاعل والتواصل والتكنولوجيا والتنظيم والسياسة والقانون والأخلاق والمجتمع. (سالم سعيد الكندي، 2020)

من خلال تجسيد بعض الحالات الواقعية، يمكن أن نرى كيف يتسلل المخترق الاجتماعي إلى البيئة المصرفية، حيث يُرى كشخص لطيف يبث الثقة، ولكن وراء الستار، يكون هدفه الرئيسي هو استحداث ثغرات تمكنه من الوصول إلى المعلومات الحساسة.

الهندسة الاجتماعية لها بعض الأمثلة والحالات الواقعية في مجال الأمن السيبراني ، وتظهر هذه الأمثلة والحالات مدى خطورة وتعقيد وتنوع وابتكار هذا النوع من الهجمات ، وما هي الآثار والتبعات التي تنجم عنها. بعض هذه الأمثلة والحالات هي: هجوم كيفن ميتنيك على شركة موتورولا ونوكيا وسوني ونورثروب جرومان وبنتاغون ووكالة الأمن القومي الأمريكية ، وهجوم إدوارد سنودن على وكالة الأمن القومي ووكالة المخابرات المركزية الأمريكية ، وهجوم القراصنة الروس على الانتخابات الأمريكية في عام 2016 ، وهجوم القراصنة الإيرانيين على البنك الأهلي الكويتي في عام 2017 ، وهجوم القراصنة الكوريين الشماليين على بنك بنغلاديش المركزي في عام 2016 ، وهجوم القراصنة الصينيين على شركة إكويفاكس الأمريكية في عام 2017.

بناءً على ذلك، يظهر أن الهندسة الاجتماعية ليست مجرد تهديدًا فنيًا، بل هي استراتيجية شاملة تتحكم في خيوط اللعبة السيبرانية. ولذلك، يجب أن تكون استراتيجيات الأمان في المصارف جاهزة للتصدي لهذا العدو المخفي الذي يختبئ وراء الأقنعة الاجتماعية.

مفهوم الأمن السيبراني

في لغة التكنولوجيا والحوسبة، تتخذ مفاهيم الأمان السيبراني شكلًا يحاكي الحماية والتحصين ضد التهديدات الرقمية. هذا الفصل يستعرض أساسيات الأمان السيبراني، متناولًا فحوى مفهومه وتشعباته، وذلك في إطار تحليلي يوضح الحاضر السيبراني في بنوك مدينة الرياض.

الأمان السيبراني، ليس مجرد درع إلكتروني يحمي الأنظمة، بل هو سفير للتحول الرقمي، يشمل مجموعة متنوعة من المفاهيم والتقنيات التي تشكل خط الدفاع الأول ضد مهندسي الهجمات السيبرانية. يمثل هذا المفهوم إطاراً فلسفياً يتسم بالتفاعل مع التقنيات المتقدمة والتحديات الأمنية الدائمة.

عندما نتحدث عن الأمان السيبراني، نعني أكثر من حماية بياناتنا الرقمية، إنما نشير إلى تكامل وتحكم يمتد من الأنظمة الإلكترونية إلى أرواحنا الرقمية. الأمان السيبراني يشمل لحظات الحياة الرقمية بأكملها، حيث يصبح الوعي والاستعداد جزءاً لا يتجزأ من هذا الجدار الرقمي.

مفهوم الأمان السيبراني يتفرع إلى أبعاد عديدة، يتمثل أحدها في مكوناته المتنوعة، من تقنيات التشفير إلى أساليب الكشف المتقدمة. يكمن في مبادئه القائمة على التنوع والسرعة في التكيف، حيث يعتبر التحدي المستمر بمثابة فرصة لتحسين الحماية.

الأمن السيبراني هو مجموعة من السياسات والممارسات والتقنيات التي تهدف إلى حماية البيانات والمعلومات والأنظمة والشبكات والخدمات الإلكترونية من التهديدات السيبرانية التي تهدف إلى سرقتها أو تخريبها أو تغييرها أو تعطيلها. يشمل الأمن السيبراني ثلاثة أبعاد رئيسية: الأمن الفني، والأمن التنظيمي، والأمن البشري. يتعلق الأمن الفني بتصميم وتطوير وتنفيذ وصيانة وتحديث الأنظمة والبرمجيات والأجهزة والبروتوكولات اللازمة لمنع الهجمات السيبرانية أو اكتشافها أو مواجهتها. ويتعلق الأمن التنظيمي بوضع وتنفيذ ومراقبة ومراجعة القواعد والسياسات والإجراءات والمعايير والأطر القانونية والأخلاقية والاجتماعية التي تحكم استخدام وتبادل وتخزين وحماية البيانات والمعلومات والخدمات الإلكترونية. يتعلق الأمن البشري برفع مستوى الوعي والتثقيف والتدريب والتحفيز والتقييم والمكافأة ومحاسبة المستخدمين والمسؤولين والمتخصصين والمهنيين والباحثين والمنظمات والمجتمعات المتعلقة بالأمن السيبراني ودورهم في دعمه أو تعزيزه أو تحسينه.

التحديات التي يواجهها الأمان السيبراني لا تقتصر على الهجمات الإلكترونية فقط، بل تمتد إلى ميدان الابتكار السلبي والتهديدات الناشئة. يتجلى جليًا في هذا الفصل أن الأمان السيبراني يتطلب فهمًا عميقًا للتكنولوجيا، وفهمًا للنفس البشرية، حيث تتقاطع متطلبات أمان الأجهزة الحاسوبية مع خصوصيات الروح البشرية.

الأمن السيبراني في البنوك

في عالم المشهد المالي المعقد في الرياض، ينبض نبض القلب الرقمي للمعاملات الاقتصادية عبر عروق البنوك، وينسج نسيجًا من الخدمات المترابطة في رقصة العصر الرقمي دائمة التطور. لقد ولدت العلاقة التكافلية بين البنوك والمجال الرقمي المزدهر تحولا نموذجيا، وتحولا إلى عالم حيث يندمج الفضاء الإلكتروني والمؤسسات المالية.

تعتبر البنوك من أهم القطاعات في الاقتصاد الرقمي ، حيث تقوم بتقديم خدمات مالية متنوعة ومبتكرة للعملاء عبر الإنترنت والهواتف الذكية والأجهزة الذكية الأخرى. تساهم البنوك في تحقيق التحول الرقمي في المجتمعات والدول ، وتسهل عمليات التجارة والاستثمار والتحويلات المالية عبر الحدود. ومع ذلك ، فإن البنوك تواجه أيضا تحديات كبيرة في مجال الأمن السيبراني ، حيث تتعرض لهجمات متكررة ومتطورة من قبل القراصنة والمجرمين السيبرانيين الذين يسعون إلى سرقة البيانات والمعلومات والأموال من البنوك والعملاء. تؤدي هذه الهجمات إلى خسائر مالية وأضرار قانونية، وأضرار تمس بالسمعة للبنوك ، وتقلل من ثقة العملاء والمنظمين والشركاء في البنوك وخدماتها.

لمواجهة هذه المخاطر ، تتبع البنوك مجموعة من الإجراءات والممارسات والمبادرات لتعزيز الأمن السيبراني والحد من التهديدات. تشمل هذه الإجراءات تطبيق معايير وسياسات وإجراءات الأمن السيبراني في البنوك ، وتوفير التدريب والتوعية للموظفين والعملاء حول المخاطر والوقاية منها ، واستخدام تقنيات وأدوات متقدمة للكشف والاستجابة والتعافي من الهجمات ، والتعاون مع الجهات الخارجية

مثل الجهات الرقابية والأمنية والأكاديمية والصناعية لتبادل المعرفة والخبرات والموارد في مجال الأمن السيبراني. تهدف هذه الإجراءات إلى تحسين قدرة البنوك على حماية نفسها وعملائها من المخاطر السيبرانية ، وزيادة ثقتها ومنافستها في السوق الرقمي.

ولنتأمل هنا، إذا صح التعبير، الباليه السيبراني الذي تنخرط فيه هذه البنوك، وهي تجتاز المتاهة الرقمية برشاقة، وتقدم عدداً لا يحصى من الخدمات في متناول عملائها. ومع ذلك، وسط هذا الأداء الكبير، يتربص الظل ـ العالم السري ـ للتهديدات السيبرانية ونقاط الضعف. وفي هذه الساحة الغامضة، تم إعداد المسرح لسرد يتكشف عند مفترق الطرق بين البراعة المالية والمخاطر التكنولوجية.

ويتجلى جوهر الأمن السيبراني في القطاع المصرفي بشكل ملحمة من المرونة والقدرة على التكيف. إنها تغامر بما يتجاوز الكود الثنائي، وتتعمق في بين البنوك والهجمات الرقمية التي تسعى إلى استغلال نقاط الضعف. ويسلط الضوء على المخاطر والتهديدات التي تحيط بهذه المؤسسات المالية، وهي عبارة عن ملتقى للمهاجمين الافتراضيين الذين يتربصون بهم.

وبينما تكشف الدراسة، فإن تداعيات التهديدات السيبرانية تلقي بظلالها القاتمة على المشهد المالي. وتمتد التموجات السلبية إلى ما هو أبعد من الخوارزميات والتشفيرات، وتتسرب إلى الثقة التي تقوم عليه النظام المصرفي. تخيل انتهاك معلومات سرية، أو التنازل عن البيانات المالية - فالعواقب ليست تكنولوجية فحسب، بل يتردد صداها في تآكل ثقة الجمهور، وهي عملية غير ملموسة أكثر قيمة بكثير من أي معاملة رقمية.

ومع ذلك، في مواجهة هذه العاصفة الرقمية، فإن بنوك الرياض لا تكتفي بالدفاع عن النظام المصرفي المحلي فقط؛ لقد نهضوا كأوصياء على العالم الافتراضي. وتكشف الدراسة عن التدابير والممارسات والمبادرات من المؤسسات المالية. إنها استراتيجيات استباقية، وبروتوكولات الأمن السيبراني لتحصين البنوك الرقمية.

وفي عالم بنوك الرياض، يصبح الالتزام بالأمن السيبراني بمثابة الالتزام بالابتكار واليقظة الدائمة. تخيل المبادرات المصممة ليس فقط لمكافحة التهديدات، بل للتغلب عليها. من بروتوكولات التشفير المتقدمة إلى تنمية ثقافة الأمن السيبراني ضمن الروح التنظيمية، تكشف كل ضربة من البنوك عن جهد متعمد لرفع مستوى الدفاعات البنكية. ومع تطور الأمن السيبراني، فإن البنوك تقدم لنا عالمًا حيث الحراس الرقميون لبنوك الرياض ليسوا كيانات مجهولة الهوية، بل هم عبارة عن ملتقى للبراعة البشرية والتكنولوجية. يلفت الانتباه إلى حقيقة أن الأمن السيبراني ليس مجرد لغز تقني ولكنه مسعى إنساني، وتعاون بين الأفراد الملتزمين بحماية البيانات المالية لعملائهم.

وحيث يلتقي جانبي الأمن السيبراني الافتراضي والملموس، فإن دراسة بنوك الرياض في مواجهة التهديدات السيبرانية ليست مجرد موقف دفاع وبقاء فقط، ولكنها شهادة على مرونة البراعة البشرية والتنظيمية والرقمية. إنها تلخص الموقف المالي لمدينة الرياض وسعيها الدؤوب لتحقيق الأمن في العالم الرقمي.

الهندسة الاجتماعية والأمن السيبراني

الهندسة الاجتماعية هي مجموعة من التقنيات والمهارات التي تستخدم للتلاعب بالناس واستغلال نقاط ضعفهم النفسية والعاطفية والاجتماعية من أجل الحصول على معلومات حساسة أو تسهيل الوصول إلى الأنظمة أو الشبكات أو البرامج. وتعتمد الهندسة الاجتماعية على مبدأ الثقة والإقناع والاستفادة من الفضول أو الخوف أو الجشع أو الرغبة أو الرحمة أو الانتماء أو غيرها من المشاعر البشرية. وتستخدم الهندسة الاجتماعية وسائل مختلفة للتواصل مع الضحايا، مثل الهاتف أو البريد الإلكتروني أو الرسائل النصية أو مواقع التواصل الاجتماعي أو الزيارات الشخصية أو الهدايا أو المكافآت. وتعتبر الهندسة الاجتماعية واحدة من أخطر التهديدات للأمن السيبراني، لأنها تستهدف العنصر البشري الذي يعتبر أضعف حلقة في سلسلة الأمن.

الأمن السيبراني هو مجموعة من السياسات والممارسات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبرامج والمعلومات من الهجمات السيبرانية أو الاختراق أو السرقة أو التلف أو التغيير أو الاستخدام غير المصرح به. ويشمل الأمن السيبراني عدة جوانب، مثل الأمن الفيزيائي والمنطقي والإداري والقانوني والتوعوي. ويعتمد الأمن السيبراني على مبادئ السرية والتكامل والتوافر والمساءلة والموثوقية والامتثال. ويعتبر الأمن السيبراني أحد أهم التحديات التي تواجه القطاع المالي والبنوك بشكل خاص، لأنها تتعامل مع معلومات حساسة ومالية للعملاء والمؤسسات وتقدم خدمات رقمية متنوعة ومعقدة.

العلاقة بين الهندسة الاجتماعية والأمن السيبراني في البنوك

تعرف الهندسة الاجتماعية بأنها "فن وعلم استغلال العوامل البشرية في الأمن السيبراني" ، أو "مجموعة من التقنيات التي تستهدف التلاعب بالأفراد أو الجماعات للحصول على معلومات حساسة أو الوصول إلى أنظمة محمية". تستخدم الهندسة الاجتماعية

كوسيلة لاختراق الأمن السيبراني في البنوك ، حيث يستهدف القراصنة والمجرمين السيبرانيين العاملين في البنوك أو العملاء أو الشركاء أو الجهات الخارجية ، ويحاولوا إقناعهم بالقيام بأفعال معينة أو تزويدهم بمعلومات معينة ، مستغلين نقاط ضعفهم النفسية أو العاطفية أو الاجتماعية. (جمال الدين، هـ ، 2023).

تتنوع الأهداف والدوافع والمستهدفين والمصادر والمخرجات لعملية الهندسة الاجتماعية في البنوك ، ولكن بشكل عام يمكن تصنيفها إلى ثلاثة أنواع رئيسية:

- الهندسة الاجتماعية الهاتفية: حيث يتصل المهاجم بالضحية عبر الهاتف أو الرسائل الصوتية أو الرسائل النصية ، ويدّعي أنه شخص موثوق أو مسؤول ، ويطلب منه معلومات شخصية أو مالية أو كلمات مرور أو رموز تحقق أو روابط إلكترونية.
- الهندسة الاجتماعية البريدية: حيث يرسل المهاجم للضحية رسالة بريد إلكتروني أو رسالة فورية أو رسالة وسائل تواصل اجتماعي ، ويدّعي أنه شخص موثوق أو مسؤول ، ويطلب منه معلومات شخصية أو مالية أو كلمات مرور أو رموز تحقق أو روابط إلكترونية ، أو يرفق ملفات مصابة بالفيروسات أو البرامج الضارة.
- الهندسة الاجتماعية المادية: حيث يقوم المهاجم بزيارة موقع البنك أو مكان عمل الضحية أو منزله ، ويدعي أنه شخص موثوق أو مسؤول ، ويطلب منه معلومات شخصية أو مالية أو كلمات مرور أو رموز تحقق أو روابط إلكترونية ، أو يحاول الحصول على الوصول إلى أجهزة الضحية أو شبكاتها أو أنظمتها.

تتأثر عملية نجاح الهندسة الاجتماعية في البنوك بعدة ضوابط ومعوقات ، منها:

- مستوى الوعي والتدريب للضحية: كلما كانت الضحية أكثر وعيا وتدريبا على المخاطر والتقنيات والمؤشرات للهندسة الاجتماعية ، كلما كانت أقل عرضة للوقوع في الفخ.
- مستوى الثقة والتحقق للضحية: كلما كانت الضحية أكثر حذرا وشكّاً في التعامل مع الأشخاص الغرباء أو المشبوهين ، وكلما طلبت المزيد من الأدلة والمصادر للتحقق من هويتهم وصلاحيتهم ، كلما كانت أقل عرضة للخداع.
- مستوى الأمن والحماية للبنك: كلما كان البنك أكثر اهتماما واستثمارا في تطبيق معايير وسياسات وإجراءات الأمن السيبراني ، وكلما استخدم تقنيات وأدوات متقدمة للكشف والاستجابة والتعافي من الهجمات ، كلما كان أقل عرضة للهندسة الاجتماعية.

توجد العديد من الآليات والأدوات والمؤشرات التي تساعد على اكتشاف ومنع والتصدي للهندسة الاجتماعية في البنوك، منها:

- الاستفسار والتأكد: حيث تطلب البنوك من العملاء والموظفين والشركاء والجهات الخارجية الاستفسار والتأكد من هوية وصلاحية أي شخص يطلب منهم معلومات أو أفعال مرتبطة بالأمن السيبراني ، وعدم الإفصاح عن أي معلومات حساسة أو مالية أو كلمات مرور أو رموز تحقق أو روابط إلكترونية دون التحقق من مصدرها ومصداقيتها.
- التوعية والتثقيف: حيث تقوم البنوك بتوفير برامج وحملات ومواد توعوية وتثقيفية للعملاء والموظفين والشركاء والجهات الخارجية حول المخاطر والتقنيات والمؤشرات للهندسة الاجتماعية ، وكيفية الوقاية منها والتعامل معها.
- الرصد والتحليل: حيث تقوم البنوك برصد وتحليل الاتصالات والمعاملات والأنشطة المرتبطة بالأمن السيبراني ، وتستخدم أنظمة وبرامج وخوارزميات ذكية للكشف عن أي محاولات أو أنماط أو سلوكيات غير عادية أو مشبوهة تشير إلى وجود هندسة اجتماعية ، وترسل تنبيهات وتقارير للمسؤولين والمعنيين.
- الاستجابة والتدخل: حيث تقوم البنوك باتخاذ الإجراءات اللازمة للتصدي للهندسة الاجتماعية عند اكتشافها ، وتشمل هذه الإجراءات قطع الاتصال أو الوصول أو العملية المشبوهة ، وإبلاغ الضحية والجهات الرقابية والأمنية والقانونية ، واستعادة البيانات أو الأموال المسروقة ، ومعالجة الثغرات أو الضعف أو الخلل الذي استغله المهاجم.
- التقييم والتحسين: حيث تقوم البنوك بتقييم وتحليل الحالات والحوادث والآثار المتعلقة بالهندسة الاجتماعية ، وتستخرج الدروس والتوصيات والمقترحات لتحسين الأمن السيبراني والوقاية من الهندسة الاجتماعية في المستقبل.

أهمية مخاطر الأمن السيبراني في البنوك

البنوك هي من أكثر القطاعات المستهدفة بالهجمات السيبرانية، لأنها تحتوي على معلومات قيمة وحساسة وتقوم بتحويلات مالية كبيرة وتلعب دورا محوريا في الاقتصاد والمجتمع. وتواجه البنوك مخاطر سيبرانية متعددة ومتنوعة، مثل الاختراق والتشويش والتزييف والاحتيال والابتزاز والتجسس والتخريب والتدمير. وتؤثر هذه المخاطر على سمعة البنوك وثقة العملاء وأداء الأعمال واستقرار النظام المالي والأمن الوطني. وتتطلب مواجهة هذه المخاطر استراتيجيات وإجراءات وتقنيات وموارد فعالة ومتطورة ومتكاملة.

تلعب البنوك دورًا حيويًا في الاقتصاد العالمي، فهي مسؤولة عن تخزين وإدارة أموال ملايين الأشخاص. لذلك، فإن البنوك تستهدف بشكل متزايد من قبل المهاجمين الإلكترونيين الذين يحاولون سرقة الأموال أو البيانات الحساسة.

تتمثل أهمية مخاطر الأمان السيبراني في البنوك في أنها يمكن أن تؤدي إلى عواقب وخيمة، بما في ذلك:

- الخسائر المالية: يمكن أن تؤدي الهجمات السيبرانية إلى خسائر مالية كبيرة للبنوك، سواء من خلال سرقة الأموال أو تعطيل العمليات المصرفية.
- انتهاك الخصوصية: يمكن أن تؤدي الهجمات السيبرانية إلى انتهاكات الخصوصية للعملاء، حيث يمكن للمهاجمين الوصول إلى بياناتهم الشخصية الحساسة، مثل أرقام حساباتهم المصرفية ومعلومات بطاقة الائتمان الخاصة بهم.
- الإضرار بالسمعة: يمكن أن تؤدي الهجمات السيبرانية إلى الإضرار بسمعة البنك، مما يؤدي إلى فقدان الثقة مع العملاء.

تأثير الهجمات السيبرانية على البنوك

يمكن أن يكون لهجمات الهندسة الاجتماعية تأثير كبير على البنوك. يمكن للمهاجمين استخدام الهندسة الاجتماعية لإقناع الموظفين أو العملاء بالكشف عن معلومات حساسة، مثل كلمات المرور أو بيانات الاعتماد المصرفية. يمكنهم أيضًا استخدام الهندسة الاجتماعية لتثبيت البرامج الضارة أو البرامج الخبيثة على أجهزة الكمبيوتر المصرفية، مما يمكنهم من الوصول إلى البيانات الحساسة.

الهجمات السيبرانية على البنوك لها تأثير سلبي على البنوك نفسها وعلى العملاء وعلى القطاع المالي وعلى الاقتصاد بشكل عام. ومن بين التأثيرات السلبية التي تنتج عن الهجمات السيبرانية على البنوك ما يلي:

- خسارة المعلومات والبيانات والمال والموارد والوقت والفرص.
- تعطيل الخدمات والعمليات والأنظمة والشبكات والتطبيقات والمنصات.
- تقليل الكفاءة والجودة والابتكار والتنافسية والنمو والربحية.
- الإضرار بالسمعة والعلامة التجارية والثقة والولاء والرضا والتجربة والعلاقة مع العملاء والشركاء والمنظمين والمنافسين والمجتمع.
- زيادة المخاطر والتهديدات والمسؤوليات والتكاليف والخسائر والعقوبات والمطالبات والدعاوى القانونية والتحقيقات والتدقيقات والتقارير والتوصيات والتنظيمات.
- تأثير الهجمات السيبرانية على البنوك لا يقتصر على البنوك فقط، بل يمتد إلى العملاء الذين قد يتعرضون للسرقة أو الاحتيال أو الخسارة أو الاضطراب أو الإزعاج أو الإحباط أو القلق أو الخوف أو الغضب أو الاستياء أو الاستغناء عن الخدمات البنكية.

أنواع الهجمات السيبرانية التي تستهدف البنوك

تختلف الهجمات السيبرانية التي تستهدف البنوك حسب الهدف والطريقة والمصدر والتأثير والحجم والتعقيد والتكرار والشدة والخطورة. ومن أنواع الهجمات السيبرانية التي تستهدف البنوك ما يلي:

- الهجمات النشطة: هي الهجمات التي تهدف إلى التأثير على البيانات أو الأنظمة أو الشبكات أو الخدمات بشكل ملحوظ أو مزعج أو مدمر، مثل التعديل أو الحذف أو الإضافة أو العرقلة أو القرصنة أو الاستيلاء أو الاستخدام غير المصرح به. تتضمن أمثلة الهجمات النشطة الفيروسات، والديدان، وأحصنة طروادة، وبرامج الفدية، وشبكات الروبوت، وDDoS، وMan-in-the-Middle، وSpongeBox، وReplay، وTampering، وBackdoor، وRootKit، وKeylogger، وKDE، وCyber Vandalism، وCyber Terrorism، وCyber Warfare.
- هجمات التصيد الاحتيالي: تتضمن هجمات التصيد الاحتيالي إرسال رسائل بريد إلكتروني أو رسائل نصية مزيفة تبدو وكأنها تأتي من مصدر موثوق به، مثل البنك. تحاول هذه الرسائل إقناع الضحايا بالكشف عن معلومات حساسة، مثل كلمات المرور أو بيانات الاعتماد المصرفية.
- هجمات انتحال الهوية: تتضمن هجمات انتحال الهوية استخدام معلومات شخصية مسروقة، مثل اسم المستخدم وكلمة المرور، للوصول إلى حساب شخص آخر. يمكن للمهاجمين استخدام هذه المعلومات للوصول إلى حسابات مصرفية أو إجراء عمليات شراء.
- هجمات برامج الفدية: تتضمن هجمات برامج الفدية سرقة بيانات حساسة وتعطيل الوصول إليها حتى يدفع الضحية فدية. يمكن للمهاجمين استخدام هذه البيانات للابتزاز أو لطلب فدية.

- الهجمات السلبية: هي الهجمات التي تهدف إلى الحصول على البيانات أو الأنظمة أو الشبكات أو الخدمات بطريقة مخفية أو مقنعة، مثل الاستطلاع أو الاستنساخ أو الاستخبارات أو الاسترجاع أو التنصت أو التجسس أو القرصنة أو الاختطاف أو الاستخدام غير المصرح به. تتضمن أمثلة الهجمات السلبية: صيد الأسماك، وصيد الأسماك بالرمح، والصيد، والزراعة، والانتحال، والاستنشاق، والمسح الضوئي، والتمرير السريع، والكشط، والغزل عبر الإنترنت، والخداع عبر الإنترنت.
- هجمات اختراق البيانات: تتضمن هجمات اختراق البيانات الوصول غير المصرح به إلى أنظمة الكمبيوتر أو الشبكات المصرفية. يمكن للمهاجمين استخدام هذه المعلومات لسرقة البيانات الحساسة أو لتعطيل العمليات المصرفية.
- الهجمات الداخلية: هي الهجمات التي يتم إطلاقها من داخل البنك أو من قبل أشخاص لديهم صلة أو علاقة أو إمكانية الوصول إلى البنك، مثل الموظفين أو العملاء أو الشركاء أو الموردين أو المقاولين أو المنظمين أو المنافسين أو الوكالات الحكومية أو الأطراف الخاصة. وتكون هذه الهجمات ناجمة عن الإهمال أو الجهل أو الخطأ أو الفشل أو المخالفة أو التلاعب أو الخيانة أو الانتقام أو الجشع أو الفضول أو الرغبة أو الخوف أو الضغط أو الابتزاز أو الإغراء أو الإكراه أو الإقناع أو الاستغلال أو الميزة.
- الهجمات الخارجية: هي الهجمات التي يتم إطلاقها من خارج البنك أو من قبل أشخاص ليس لديهم أي اتصال أو علاقة أو وصول إلى البنك، مثل المتسللين والقراصنة والفيروسات والمبرمجين ومرسلي البريد العشوائي والصيادين والمحتالين ومجرمي الإنترنت والناشطين عبر الإنترنت أو الناشطين السيبرانيين أو المرتزقة السيبرانيين أو الميليشيا السيبرانية أو المافيا السيبرانية أو الإرهابيين السيبرانيين أو المحاربين السيبرانيين أو الجنود السيبرانيين أو وكلاء السيبرانية أو الجواسيس السيبرانيين أو الدول المارقة السيبرانية أو الدول القومية السيبرانية.

تأثير العوامل الاجتماعية على مخاطر الأمان السيبراني

إن استكشاف المكونات المعقدة للديناميكيات الاجتماعية السيبرانية للقطاع المصرفي في الرياض يكشف عن تفاعل عميق بين السلوك البشري ومخاطر الأمن السيبراني الذي يلوح في الأفق في هذا العصر الرقمي، حيث يتردد مخاوف المجتمع من خلال ضربات المخترقين، يصبح فهم تأثير العوامل الاجتماعية أمرًا ضروريًا في تحصين الأمن السيبراني.

الهندسة الاجتماعية هي مجموعة من التقنيات والمهارات التي تستخدم للتأثير على الأفراد والمجموعات للحصول على معلومات أو امتيازات أو صلاحيات معينة. تعتمد الهندسة الاجتماعية على استغلال الضعف البشري والنفسي والثقافي للضحايا. وتشمل العوامل الاجتماعية التي تؤثر على مخاطر الأمان السيبراني في البنوك في مدينة الرياض في المملكة العربية السعودية ما يلي:

دور العوامل الاجتماعية في تصاعد مخاطر الأمان السيبراني

وتجد مخاطر الأمن السيبراني ذروتها في تنسيق العناصر الاجتماعية، حيث تلعب دورًا محوريًا في التهديدات المتزايدة التي تواجهها المؤسسات المالية. إن نسيج المجتمع ذاته، يتكون من العلاقات والثقة والوعي الجماعي، يمكن أن يعزز أو يضعف دفاعات البنوك ضد المهاجمين السيبرانيين. إنها لعبة شطرنج تقنية؛ تزيد من التعقيدات المجتمعية.

تزداد مخاطر الأمان السيبراني في البنوك بسبب العوامل الاجتماعية التي تؤدي إلى تقليل الوعي والتدريب والتزام الموظفين والعملاء بالممارسات الأمنية السليمة. ومن بين هذه العوامل: الثقة الزائدة، والفضول، والطمع، والخوف، والتعاطف، والرغبة في الانتماء، والتأثر بالسلطة والمكانة، والتقيد بالقواعد والتعليمات، والرضا عن الأداء، والتوافق مع الآخرين. تستخدم هذه العوامل من قبل المهاجمين الاجتماعيين لإقناع أو إغراء أو تهديد أو ابتزاز الضحايا للقيام بأفعال تضر بالأمان السيبراني للبنوك، مثل إعطاء كلمات المرور أو البيانات الحساسة أو الوصول إلى الأنظمة أو التطبيقات أو الشبكات.

في هذا الوضع المعقد، يصبح دور العوامل الاجتماعية في تصاعد مخاطر الأمن السيبراني واضحًا. إن الضعف البشري، الذي يغذيه السعي الدؤوب للاتصال ووجود البصمات الرقمية في كل مكان، يجعل الأفراد والمؤسسات عرضة لعدد لا يحصى من التهديدات السيبرانية. إن ظهور حياة مترابطة يصبح سيفا ذا حدين، يكشف التعقيدات المجتمعية من أصحاب النوايا الخبيثة. (لطفى، وآخرون.،2022)

تأثير التكنولوجيا على سلوك المستخدمين في المجتمع

علاوة على ذلك، فإن الخوض في تأثير التكنولوجيا على سلوك المستخدم داخل البيئة المجتمعية يكشف النقاب عن إن تطور التكنولوجيا يعمل كمحفز ومشكل للسلوك البشري. إن مسيرة الابتكار التي لا هوادة فيها، مع جاذبيتها من الراحة والكفاءة، تغير الطريقة التي يتفاعل بها الأفراد مع العالم الرقمي. فهي تصبح قوة عاتية تشكل السلوك الجماعي لمجتمع منغمس في الأدوات والمنصات المتطورة.

تلعب التكنولوجيا دوراً هاماً في تغيير سلوك المستخدمين في المجتمع، وبالتالي تزيد من مخاطر الأمان السيبراني في البنوك. ومن بين هذه التغييرات: الاعتماد الزائد على التكنولوجيا، والثقة العمياء فيها، والتخلي عن المسؤولية الشخصية، والتقليل من الحذر والحماية، والتعرض للتشتيت والتشويش، والتأثر بالتوجهات والموضات، والتعرض للتلاعب والخداع، والتقليل من الخصوصية والسرية، والتعرض للإدمان والاستهلاك المفرط. تستغل هذه التغييرات من قبل المهاجمين الاجتماعيين لزيادة فرص نجاح هجماتهم السيبرانية على البنوك، مثل استخدام البريد الإلكتروني أو الرسائل النصية أو الهاتف أو الوسائط الاجتماعية أو الإعلانات أو المواقع الوهمية أو البرامج الضارة أو الهجمات النفسية.

ومع ترسيخ التكنولوجيا نفسها بشكل أعمق في النسيج الاجتماعي، فإن الفروق السلوكية الدقيقة للأفراد الذين يتنقلون في المشهد الرقمي تخضع لتحول تحويلي. يصبح المستخدم الذي كان ساكنًا ذات يوم كيانًا ديناميكيًا يتأثر بتيارات التطور التكنولوجي المتغيرة باستمرار. إن الاختيارات التي تم اتخاذها، والعادات الرقمية التي تشكلت، ونقاط الضعف المكشوفة، كلها منسوجة بشكل معقد في اللوحة الأكبر من مخاطر الأمن السيبراني التي يواجهها القطاع المصرفي في الرياض.

لا يعد موقف الأمن السيبراني في بنوك الرياض عن مجرد الحماية فقط وبروتوكولات التشفير عالية الجودة؛ إنه انعكاس لديناميكيات اجتماعية تتفاعل بين العوامل الاجتماعية ومخاطر الأمن السيبراني، مما يسلط الضوء على الحاجة إلى نهج شامل يعترف بالعنصر البشري في مجال الدفاع الرقمي. إنه تعبير عن مدي مهارات السلوك البشري ضد التعقيدات الرقمية، حيث يصبح فهم إيقاع المجتمع أمرًا بالغ الأهمية مثل فك الرموز التشفير التي يقوم عليها مهاجمين العالم الرقمي. (محمد المري، ر.، & راشد. ، 2023).

استكشاف مخاطر الأمان السيبراني في البنوك في مدينة الرياض

من خلال قراءة المشهد السيبراني للمؤسسات المصرفية في الرياض، نكشف النقاب عن عالم يحتل فيه الصراع بين مخاطر الهندسة الاجتماعية والأمن السيبراني مركز الصدارة. إن مكونات الدفاع الرقمي، تتشابك بشكل معقد مع الديناميكيات المجتمعية، يتطلب استكشافًا يتجاوز التحصينات التكنولوجية.

يواجه القطاع المصرفي في مدينة الرياض تحديات كبيرة في مجال الأمان السيبراني، نتيجة للتطور المستمر للتهديدات والهجمات السيبرانية التي تستهدف البنوك وعملائها. وتعتبر الهندسة الاجتماعية واحدة من أبرز الأساليب التي يستخدمها المهاجمون السيبرانيون لاختراق البنوك وسرقة المعلومات والأموال. وفي هذا الجزء، سنقوم بتحليل حالات الهندسة الاجتماعية في البنوك بمدينة الرياض، ودراسة حالات الاختراق والهجمات السيبرانية التي استهدفت البنوك.

تحليل حالات الهندسة الاجتماعية في البنوك بمدينة الرياض

في تحليل تعقيدات مخاطر الأمن السيبراني داخل بنوك الرياض، يظهر تحليل عميق لرقعة شطرنج الهندسة الاجتماعية. العنصر البشري، الذي غالبًا ما يكون العمود الفقري في المصفوفة الأمنية، هو بطل الرواية والشريك غير المقصود في هذه الرواية. إن الهندسة الاجتماعية، بما تتسم به من براعة في الإقناع والتلاعب، تصبح قوة فاعلة في الإبحار في متاهة الدفاعات السيبرانية.

تعتمد الهندسة الاجتماعية على استغلال العوامل النفسية والثقافية والسلوكية للضحايا، وإقناعهم أو إغرائهم أو تهديدهم أو ابتزازهم للحصول على معلومات أو صلاحيات أو أموال. وتشمل حالات الهندسة الاجتماعية في البنوك بمدينة الرياض ما يلي:

- الاحتيال الهاتفي: يتصل المهاجم بالضحية ويدعي أنه موظف في البنك أو في جهة رسمية أو قانونية، ويطلب منه تحديث بياناته أو تأكيد هويته أو تفعيل خدمة ما، ويطلب منه إعطاء رقم الحساب أو كلمة المرور أو رمز التحقق أو رقم البطاقة الائتمانية أو غيرها من المعلومات الحساسة. وبعد ذلك، يستخدم المهاجم هذه المعلومات للوصول إلى حساب الضحية وتنفيذ عمليات مالية غير مصرح بها.
- الاحتيال البريدي: يرسل المهاجم رسالة بريدية إلى الضحية ويدعي أنه من البنك أو من جهة رسمية أو قانونية، ويخبره بأن حسابه معرض للخطر أو أنه فاز بجائزة أو أنه مطلوب للمشاركة في استطلاع أو عرض، ويطلب منه الضغط على رابط أو فتح مرفق أو إرسال معلومات. وعندما يفعل الضحية ذلك، يتم تحويله إلى موقع وهمي يشبه موقع البنك، أو يتم تنزيل برنامج ضار على جهازه، أو يتم سرقة معلوماته.
- الاحتيال الشخصي: يقوم المهاجم بالتقرب من الضحية ويدعي أنه صديق أو قريب أو زميل أو عميل أو مسؤول، ويطلب منه مساعدة أو خدمة أو تعاون، ويحاول الحصول على معلومات أو صلاحيات أو أموال منه. وقد يستخدم المهاجم الرشوة أو الابتزاز أو التهديد أو التلاعب أو الاستغلال للوصول إلى هدفه.

لا تكشف لوحة القطاع المصرفي في الرياض عن ساحة معركة نظرية فحسب، بل تكشف أيضًا عن لوحة حية تلعب فيها الهندسة الاجتماعية بطرق لا تعد ولا تحصى. ويكشف تحليل الحالات الواقعية داخل بنوك الرياض عن خفايا التفاعل البشري الذي يستغله الخصوم السيبرانيون. إنه عالم تصبح فيه الثقة نقطة ضعف، وتتحول الألفة إلى سلاح يستخدمه أصحاب النوايا الخبيثة.

دراسة حالات الاختراق والهجمات السيبرانية التي استهدفت البنوك

في هذا المسرح السيبراني، تصبح دراسة حوادث الاختراق والهجمات السيبرانية التي تستهدف البنوك بمثابة سرد مثير للتوغلات الافتراضية. إن الأسوار الرقمية للمؤسسات المالية، التي كان يُعتقد ذات يوم أنها منيعة، تشهد على الهجمة التي لا هوادة فيها من التهديدات السيبرانية. يحكي كل خرق قصة استغلال نقاط الضعف، والتحايل على الضمانات، والتكتيكات المتطورة باستمرار للمهاجمين السيبرانيين.

إن هذه المغامرات السيبرانية ليست مجرد غزوات مجهولة الهوية؛ إنها حكايات عن البراعة والقدرة على التكيف في مواجهة التدابير الأمنية المتطورة. إن دراسة هذه الانتهاكات تتجاوز المجال الثنائي وتتعمق في النفس البشرية التي تصمم هذه الاعتداءات الافتراضية وتستجيب لها. إنها ملحمة حيث يحمل كل سطر من التعليمات البرمجية بصمات خبير تكتيكي إلكتروني، وكل خرق هو فصل في السرد المستمر لمرونة الأمن السيبراني وضعفه.

تعرضت البنوك في مدينة الرياض لعدة حالات اختراق وهجمات سيبرانية خلال السنوات الأخيرة، نتج عنها خسائر مالية وأضرار بالثقة والسمعة. وتشمل حالات الاختراق والهجمات السيبرانية التي استهدفت البنوك ما يلي:

- هجوم الفدية على البنك الأهلي: في أغسطس 2022، تعرض البنك الأهلي لهجوم من نوع الفدية (ransomware)، حيث تم تشفير بيانات البنك ومطالبته بدفع مبلغ مالي مقابل فك التشفير. وقد أثر الهجوم على خدمات البنك الإلكترونية والهاتفية والموقع الرسمي والتطبيق الذكي، وتسبب في توقفها لعدة ساعات. وقد نفى البنك أن يكون قد دفع أي فدية، وأكد أنه تمكن من استعادة البيانات واستئناف الخدمات بشكل طبيعي.
- هجوم حصان طراوده على البنك السعودي الفرنسي: في يونيو 2022، تعرض البنك السعودي الفرنسي لهجوم من نوع حصان طراوده (trojan)، حيث تم اختراق أنظمة البنك وسرقة بيانات العملاء والموظفين والمعاملات. وقد استخدم المهاجمون برنامج ضار يسمى RAT (Remote Access Trojan)، يتيح لهم الوصول عن بعد إلى أجهزة البنك والتحكم فيها. وقد أبلغ البنك عن الهجوم للجهات المختصة، وأعلن عن تطبيق إجراءات أمنية مشددة لمنع تكرار الهجوم.
- هجوم الاحتيال البريدي على البنك العربي الوطني: في مارس 2022، تعرض البنك العربي الوطني لهجوم من نوع الاحتيال البريدي (phishing)، حيث تم إرسال رسائل بريدية مزيفة إلى عملاء البنك، تدعوهم إلى تحديث بياناتهم الشخصية والمصرفية عبر رابط موجود في الرسالة. وعندما يضغط العميل على الرابط، يتم تحويله إلى موقع وهمي يشبه موقع البنك، ويطلب منه إدخال رقم الحساب وكلمة المرور ورمز التحقق وغيرها من المعلومات الحساسة. وبعد ذلك، يستخدم المهاجم هذه المعلومات للوصول إلى حساب العميل وسحب الأموال منه. وقد حذر البنك عملائه من هذا النوع من الهجمات، ونصحهم بعدم الرد على الرسائل المشبوهة أو الضغط على الروابط المرسلة فيها.

هذه بعض الأمثلة عن الهندسة الاجتماعية والهجمات السيبرانية التي تواجه البنوك في مدينة الرياض. ويمكننا من خلال دراستها تحديد الضعف والثغرات في الأمان السيبراني للبنوك، ووضع الحلول والاستراتيجيات للحد منها والتصدي لها. وفي الجزء التالي، سنتحدث عن أهمية الوعي الأمني والتدريب والتثقيف للموظفين والعملاء في البنوك، وكيف يمكن أن يساهم في تعزيز الأمان السيبراني والوقاية من الهندسة الاجتماعية.

في مكونات الأمن السيبراني المصرفي في الرياض، فإن استكشاف تأثير الهندسة الاجتماعية إنه اعتراف بأن الأمن الرقمي لا يتم خوضه بلغة الخوارزميات وجدران الحماية فحسب، بل إنها تتشابك بعمق مع خيارات الأفراد وثقتهم وتفاعلاتهم داخل الإطار المجتمعي. إن فهم الفروق الدقيقة في هذا التفاعل أمر ضروري لصياغة الأمن السيبراني يتجاوز تعقيدات العنصر البشري في العصر الرقمي.

أساليب التصدي لمخاطر الأمان السيبراني المرتبطة بالهندسة الاجتماعية

إن التعرف علي مخاطر الأمن السيبراني في بنوك الرياض لا يتطلب فهم الفروق الدقيقة في الهندسة الاجتماعية فحسب، بل يتطلب أيضًا اتباع نهج استراتيجي لمواجهة هذه المخاوف الرقمية. وفي هذا التعقيد بين الضعف البشري والتهديدات السيبرانية، يصبح استكشاف الأساليب الفعالة لتخفيف المخاطر أمرا بالغ الأهمية.

لمواجهة التحديات والتهديدات السيبرانية التي تستخدم الهندسة الاجتماعية كأسلوب لاختراق البنوك وسرقة المعلومات والأموال، يجب على البنوك في مدينة الرياض اتخاذ إجراءات واستراتيجيات فعالة للتصدي لهذه الهجمات والحد من آثارها. وفي هذا الجزء، سنتحدث عن بعض من هذه الإجراءات والاستراتيجيات، وهي:

تعزيز التوعية السيبرانية بين المستخدمين والعاملين في البنوك

يعتبر أحد سبل الدفاع من خلال الوعي بالأمن السيبراني. وكما هو الحال مع الدرع الذي تم تشكيله من المعرفة الجماعية، فإن تعزيز الوعي السيبراني بين المستخدمين وموظفي البنوك يبرز كركيزة أساسية في المعركة ضد الهندسة الاجتماعية. تصور ذلك باعتباره وعيًا جماعيًا، أو يقظة مشتركة تعمل على تحصين النظام البيئي المصرفي ضد الأفخاخ الخفية التي ينصبها الخصوم السيبرانيون.

ويتحول العنصر البشري، الذي غالباً ما يكون الحلقة الأضعف، إلى خط الدفاع الأول من خلال حملة توعية قوية. إنها أكثر من تحذيرات وتوجيهات صارمة؛ إنها تمكن الأفراد من التعرف على الحيل الرقمية التي تسعى إلى استغلال الثقة والألفة. يصبح تعليم الأمن السيبراني منارة، توجه المستخدمين عبر الاستخدامات المعقدة لعوامل الأمان للهندسة الاجتماعية.

تعتبر التوعية السيبرانية من أهم العوامل التي تساهم في الوقاية من الهندسة الاجتماعية والتصدي لها. فالمستخدمون والعاملون في البنوك هم الهدف الرئيسي للمهاجمين الاجتماعيين، ولذلك يجب عليهم أن يكونوا على دراية بطبيعة هذه الهجمات وأساليبها وأهدافها ومخاطرها. ويمكن تعزيز التوعية السيبرانية بين المستخدمين والعاملين في البنوك من خلال:

- إجراء حملات توعوية وتثقيفية عن الهندسة الاجتماعية والأمان السيبراني، وذلك بواسطة الإعلانات والمنشورات والمحاضرات والورش والندوات والمسابقات والألعاب وغيرها من الوسائل التفاعلية.
- توفير دورات تدريبية وتأهيلية للموظفين والعملاء في البنوك، تهدف إلى تعليمهم المهارات والممارسات الأمنية السليمة، وتحسين قدرتهم على التعرف على الهجمات الاجتماعية والتصرف بشكل مناسب في حالة التعرض لها.
- إجراء اختبارات ومحاكاة للهجمات الاجتماعية على البنوك، وتقييم مدى استجابة وفعالية الموظفين والعملاء في التعامل معها، وتقديم التغذية الراجعة والتوجيهات اللازمة لتحسين أدائهم وزيادة وعيهم.

تطبيق سياسات وإجراءات أمان فعالة للتصدي لهندسة الاجتماعية

وفي الوقت نفسه، تتسع دفاعات الجدار الناري ضد التهديدات السيبرانية مع تنفيذ سياسات وإجراءات أمنية فعالة. تحمي بسلاسة من المشهد المتغير باستمرار لنقاط الضعف السيبرانية، وتمتد هذه السياسات إلى ما هو أبعد من المجال الرقمي؛ إنها تتسرب إلى ثقافة البنوك في الرياض. إنها روح البنك حيث لا يكون الأمن فكرة لاحقة ولكنه جزء لا يتجزأ من كل عملية شاملة. بدءًا من إجراءات الإعداد وحتى المعاملات اليومية، يصبح اليقظة ضد الهندسة الاجتماعية طبيعة ثابتة، واستجابة انعكاسية متأصلة في التنظيمي الإداري للبنك.

تصور سيناريو حيث يصبح كل موظف، من الخطوط الأمامية إلى مجلس الإدارة، مدافعاً ضد التهديدات السيبرانية. لا يتعلق الأمر بفرض قيود، بل بتعزيز ثقافة يكون فيها الأمن مسؤولية مشتركة، يحول هذا النهج النظرة التقليدية للأمن السيبراني من ضرورة تقنية إلى مسعى جماعي، حيث يكون كل فرد مدافعاً للمجال الرقمي.

يجب على البنوك في مدينة الرياض وضع وتنفيذ سياسات وإجراءات أمان محددة وموحدة ومحدثة، تهدف إلى حماية البنوك والموظفين والعملاء من الهندسة الاجتماعية والهجمات السيبرانية. ويمكن تطبيق سياسات وإجراءات أمان فعالة للتصدي لهندسة الاجتماعية من خلال:

- تحديد وتصنيف وتوثيق المعلومات والأنظمة والشبكات والتطبيقات والخدمات التي تستخدمها البنوك، وتحديد مستوى الحساسية والأهمية والمسؤولية والصلاحية لكل منها.
- تطبيق معايير ومواصفات أمان عالية للبنوك والموظفين والعملاء، وذلك بواسطة استخدام كلمات مرور قوية ومتغيرة ومتعددة العوامل، وتشفير البيانات والاتصالات، وتحديث البرامج والأنظمة، وتنصيب برامج الحماية من الفيروسات والبرامج الضارة، وتفعيل جدران الحماية ونظم الكشف والتحذير والاستجابة، وغيرها من الأدوات والتقنيات الأمنية.
- تطبيق إجراءات وضوابط وتدابير وقائية واستباقية واستجابية للتعامل مع الهندسة الاجتماعية والهجمات السيبرانية، وذلك بواسطة تحديد وتقييم وتحليل ومعالجة وتقرير ومراجعة ومتابعة المخاطر والحوادث والانتهاكات الأمنية، واتخاذ الإجراءات اللازمة لمنعها أو الحد منها أو التعويض عنها.

هذه بعض الأساليب التي يمكن للبنوك في مدينة الرياض اتباعها للتصدي لمخاطر الأمان السيبراني المرتبطة بالهندسة الاجتماعية. ويمكننا من خلال تطبيقها تحقيق مستوى أعلى من الأمان والحماية للبنوك والموظفين والعملاء، والحفاظ على الثقة والسمعة والاستقرار للقطاع المصرفي. وفي الجزء الأخير، سنختم بعرض بعض التوصيات والاقتراحات لتحسين الأمان السيبراني في البنوك في مدينة الرياض.

وفي الهجوم السيبراني ضد الهندسة الاجتماعية في بنوك الرياض، تتجاوز هذه الأساليب المجال الثنائي بين البنك والعميل وتتعمق في تعقيدات السلوك البشري والثقافة التنظيمية. إنها نقطة هامة تتجسد فيها الوعي والسياسات، ويقفون بمرونة في مواجهة التلاعبات الخفية للهجوم السيبراني. في هذا المشهد المتطور، لا يعد الدفاع ضد الهندسة الاجتماعية مجرد تحصين تكنولوجي؛ إنه مسعى جماعي، وميثاق مجتمعي ضد الهجمات السيبرانية.

الدراسات السابقة.

دراسة (Sciences, 2020)

في اتجاهات التمويل الحديث، تكون المعاملات الرقمية سريعة، حيث تتعمق الدراسة التي كتبها Sciences, M. J. of E. and A. في عام 2020، في المجال المعقد لإدارة مخاطر الأمن السيبراني داخل البنوك الأردنية.

بعد دراسة اتجاهات البنوك الرقمية للمؤسسات المالية، تنتهي الدراسة، إلي أن الحماية ضد التهديدات الغامضة التي تكمن في المخاطر الرقمية. تبدأ الدراسة بدقيق المخاطر التي تتناولها الدراسة. العنوان ياكد أن "إدارة المخاطر في البنوك الأردنية: هي جزء لا تجزأ من أساسيات الأمن السيبراني".

تكشف الدراسة عن موضوعها في معرفة الأبعاد الدقيقة للأمن السيبراني. تعرض الدراسة المخاطر الرقمية التي تستدعي الانتباه من البنوك، وتعرض الدراسة تأثير الخوارزميات الرقمية في حماية البنوك.

إن النتائج التي تم الكشف عنها تمثل التحديات التي يوجهها القطاع المصرفي الأردني. وتسلط الدراسة الضوء على التهديدات السيبرانية، وأهمية التعامل معها، وتأثيراتها المحتملة على الاستقرار المالي لهذه المؤسسات.

وفي أعقاب التحقيق، لا يُترك القارئ في كثرة من البيانات، بل يتم توجيهه عبرها. إن هذه الاكتشافات الإحصائية هي هامة لفهم أعمق لموقف الأمن السيبراني في البنوك الأردنية.

وبينما تكشف الدراسة عن أنه يمكن للعميل أن يشعر تقريبًا بثقل المسؤولية المصاحبة للمسؤولين. إنها ليست مجرد عرض لنقاط الضعف، ولكنها دعوة للعمل، ونداء حماسي من أجل مستقبل رقمي محصن.

Sciences, M. J. of E. and A. في استكشافهم لعام 2020، لم يظهروا كمؤرخين لتحديات الأمن السيبراني فحسب، بل صناع لعصر جديد من اليقظة الرقمية. من خلال نشر الوعي الذي يهتم بالعملاء ويحصنهم ضد الهجمات السيبرانية، تدعو الدراسة الأوصياء الماليين في الأردن إلى تحصين الأمن السيبراني ومواجهة التهديدات الخارجية للعالم الرقمي، وتتفق هذه الدراسة مع التوصيات التي توصل إليها الباحث في أهمية التحصين دفاعات الجدار الناري ضد الهجمات السيبرانية.

دراسة (Alon Bar, 2022)

ينسق ألون بار تكوينًا مقنعًا، ويكشف النقاب عن تعقيدات تحديات الأمن السيبراني داخل المؤسسات المالية. تقدم دراسة للكاتب Alon Bar بعنوان "تحديات الأمن السيبراني ومخاطره على المؤسسات المالية وطرق معالجتها"، والتي نُشرت في 25 يوليو 2022، والذي تم استضافته على المسرح الرقمي لـ Robodin، ويدعو الباحثين إلى عالم تتشابك فيه مكونات الأمن المالي مع المخاطر الرقمية والأمن السيبراني.

العنوان نفسه، وهو بوابة إلى الكشف عن خطورة الموضوع: "البحث في تحديات الأمن السيبراني في المؤسسات المالية". الباحث يوجه دراسته حول الاتجاهات المضطربة في المجال المالي الرقمي، ويشرح التحديات التي تواجهها المؤسسات المالية مع الأهمية علي نشر الوعي القوي والتعرف علي المخاطر الرقمية التي تواجهها.

تكشف الدراسة أهمية المعرفة في معايير الأمن السيبراني. وتوضح صورة واضح عن التحديات الحالية للبنوك والمؤسسات المالية وتحفز علي الاستعداد لاختبار مرونة المؤسسات المالية.

يتعمق الباحث في معرفة الفروق الدقيقة في الدراسة، ويستكشف كيفية اختبار وفحص التحصينات الرقمية للمؤسسات المالية بواسطة أيدٍ غير مرئية، مع معرفة التأثير الذي يتردد مع حدوث أول حالة اختراق للأمن السيبراني، يحول التقنيات المعقدة إلي طرق وأساليب سهلة وبسيطة للعميل حتي يستطيع التعامل مع هذه التهديدات.

مع تقدم في الدراسة، أظهرت نتائج واضحة في تفسير معايير الأمن السيبراني. إنها توصيات توجه القادة الماليين نحو فهم أعمق للتهديدات التي يواجهونها. حيث يضع الباحث من خلال استكشافه، استراتيجيات رقمية في أيدي صناع القرار، تساعدهم نحو تدابير فعالة للأمن السيبراني.

وتشير النتائج أهمية اعتماد استراتيجيات شاملة لتعزيز الأمان السيبراني في المؤسسات المالية، بما في ذلك تحسين البنية التحتية للأمان، وتطوير سياسات الوقاية والاستجابة. كما أشارت الدراسة إلى ضرورة التحديث المستمر لتقنيات الأمان وتكامل الحلول التكنولوجية لمواجهة التهديدات المتقدمة في عالم السيبرانية.

إن دراسة ألون بار إلى تحديات الأمن السيبراني هي بمثابة حلول للمؤسسات المالية ولكن لأي شخص يدرس المخاطر الرقمية. تعتبر الدراسة ليست مجرد عرض بياني، بل هي دعوة للعمل، ونداء مدوى للدفاعات السيبرانية المحصنة في مواجهة التهديدات المتطورة. ، حيث لا تصبح التحديات عقبات لا يمكن التغلب عليها، بل دعوات لعمل جماعي نحو مستقبل رقمي أكثر أمانًا.

دراسة (محمد محمود عبد العال& محمد عوض العربى، 2023)

في استكشاف مثير للاهتمام للتحول البيروقراطي داخل المستويات الحكومية، تثبت الدراسة التي أجراها محمد محمود عبد العال، ماجستير، ومحمد عوض العربي، حيث تتناول هذه المقالة العلمية، التي نُشرت في مجلة كلية الاقتصاد والعلوم السياسية المرموقة في عام 2023، مكونات معقدة لإعادة بناء قدرات الموارد البشرية على مستوى الحكم المحلي. العنوان، "إعادة بناء قدرات الموارد البشرية في الحكم المحلي: دراسة مقارنة بين جمهورية مصر العربية والمملكة العربية السعودية"، هو بمثابة مقدمة للتحليل الدقيق الذي يتكشف ويمتد نطاق الدراسة إلى ما هو أبعد من الحدود التقليدية، ويرسم المتغيرات العميقة التي نظمتها سياسات التحول الرقمي. وبدلاً من التعداد الرقمي للاستراتيجيات، تأخذ الدراسة التفاعل الديناميكي بين الحوكمة، والرقمنة، والعنصر البشري. من خلال التركيز علي الملاحظة، وشرح تعقيدات السياسة، ويسلطون الضوء على الدوافع والتعقيدات التي تدعم المساعي التحويلية لفرض سياسات مالية أكثر مرونة للدفاع عن حماية البيانات المالية.

وتتطرق الدراسة إلى التحليل المقارن بين جمهورية مصر العربية والمملكة العربية السعودية. إنها ليست مجرد عرض للإحصاءات؛ وبدلاً من ذلك، فإنه يكشف المعايير الثقافية والسياسية والاجتماعية والاقتصادية التي تشكل المسارات المميزة لهاتين الدولتين. يقدم المؤلفون، استكشافًا دقيقًا للتحديات والانتصارات التي تمت مواجهتها في كل المخترقين للأمن السيبراني، ويدعون الباحثين إلى تصور المسارات الموازية والمتباينة لهذه الدول نحو التمكين الرقمي.

وتكشف النتائج، التي عن الديناميكيات المعقدة لتنفيذ السياسات المالية والنقدية. وتصور الدراسة مشهدًا لا يكون فيه التحول الرقمي للحكم المحلي مسعىً متجانسًا ولكنه عملية دقيقة، تتأثر بالخصائص التاريخية والثقافية والبنية التحتية لكل دولة. ومع ظهور النتائج، ينجذب الباحثين إلى عالم حيث تظهر القدرة على التنبؤ أمام الضعف البشري والتغييرات المجتمعية السريعة التي لا يمكن التنبؤ بها.

تتجاوز هذه الدراسة الحدود التقليدية للخطاب الأكاديمي، وتدعو الباحثين إلى التأكد من أن العرض العلمي لمواقف ودفاعات المؤسسات المالية. إنها تعقيدات التحول الرقمي الحكومي، وتحث على التفكير في العلاقة التكافلية بين السياسة والتكنولوجيا ونبض المساعي البشرية..

دراسة (الهندسة الاجتماعية وتهديد المعلومات المضللة في الأمن السيبراني - سيو ماستر، 2023)

تهدف الدراسة إلي استكشاف الموقف الديناميكي للأمن السيبراني، تظهر دراسة "الهندسة الاجتماعية وتهديد التضليل" كعلامة في عالم الدفاع عبر الإنترنت. تم تأليف هذه المقالة من قبل الباحثين في SEO Mastar، والتي تم الكشف عنها في عام 2000، وتتعمق في الشبكة المعقدة من التحديات التي تطرحها حملات الهندسة الاجتماعية والمعلومات المضللة.

وتحلل الدراسة بشكل واضح تكتيكات الهندسة الاجتماعية، وتكشف عن المعالم المعقدة التي يتلاعب بها الخصوم لاختراق الدفاعات السيبرانية للمؤسسات والأفراد على حد سواء، ويعبر الباحثون في حقيقة الحرب النفسية في الهندسة الاجتماعية، ويسلطون الضوء على تقنيات التلاعب التي يستخدمها ممثلو التهديد.

وتكشف الدراسة عبر المشهد الحقيقي للمعلومات المضللة، مع التركيز على تأثيره الخبيث على الأمن السيبراني. تستكشف الدراسة كيف يمكن استخدام المعلومات الخاطئة كسلاح قوي قادر على تآكل الثقة وزرع الخلاف وزعزعة استقرار أسس الأمن الرقمي. من خلال الأمثلة الحقيقية والسيناريوهات الحقيقية، يرسم الباحثون صورة حقيقة للعواقب بعيدة المدى للمعلومات المضللة في العالم المترابط الذي نعيش فيه.

ومع تطور الدراسة، يصبح من الواضح أن المعركة ضد الهندسة الاجتماعية والمعلومات المضللة لا تقتصر على التحصينات التكنولوجية وحدها. يحتل العنصر البشري مركز الصدارة، ويسلط الباحثون الضوء على أهمية الوعي والتعليم بالأمن السيبراني. وفي

عالم يتقاطع فيه الموقف الرقمي والإنساني، تدعو الدراسة إلى اتباع نهج شمولي يمكّن الأفراد من توخي اليقظة والمرونة والتمييز في مواجهة التهديدات السيبرانية المتطورة.

نتائج هذا الاستكشاف الشامل، تعبر عن الحاجة الماسة لاستراتيجية دفاعية متعددة الأبعاد. تعمل الدراسة بمثابة دعوة للعمل، وتحث أصحاب المصلحة على التعاون والابتكار والتكيف مع المشهد المتغير باستمرار للتهديدات السيبرانية. من خلال تحليلها الدقيق والمقنع، تتجاوز الدراسة الحدود التقليدية لخطاب الأمن السيبراني، وتقدم منارة للفهم في مكونات الدفاع الرقمي المعقد.

دراسة (Nizam, 2023)

درّس الباحث نزام (2023) في دراسته الموسومة بـ "الهندسة الاجتماعية: تعريفها، تأثيراتها، تقنياتها، وطرق الحماية منها" أحدث المستجدات في هذا المجال المثير والمعقّد. لقد قدّم الباحث رؤية شاملة حول كيفية استخدام الهندسة الاجتماعية كأداة فعّالة لاختراق الأمان الرقمي والتأثير في سلوكيات الأفراد.

تعمقت الدراسة في أساليب التلاعب الاجتماعي، وكشفت عن تأثيراتها المترابطة على المستوى الفردي والمؤسسي. إنّها لم تكتفِ بتسليط الضوء على مظاهر التهديد فقط، بل قدمت أيضًا رؤية متفحصة حول كيف يمكن للهندسة الاجتماعية أن تؤدي إلى تغييرات في السلوكيات البشرية وتشكيل رؤى جديدة.

أبرزت النتائج التي خلصت إليها الدراسة أهمية تعزيز الوعي بين المستخدمين حيال التحديات الأمنية الاجتماعية. ومن خلال إلقاء نظرة على الطرق الفعّالة للحماية، قدّمت الدراسة مقترحات عملية لتحسين الأمان الرقمي والتصدي لمحاولات الاختراق الاجتماعي. بهذا، يمثل البحث المبدئي لنزام مساهمة مهمة في تفكيك أسرار الهندسة الاجتماعية، ويدعو إلى إعادة تقييم الاستراتيجيات الأمنية للتصدي للتحديات المستمرة في هذا المجال المتطور.

دراسة (سارة ابو حجاب، n.d.)

تقدم الكاتبة سارة أبو حجاب في دراستها الأخيرة، المعنونة "إجراءات مقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية"، رؤية فاحصة حول التحديات المتزايدة في مجال أمان المعلومات في بيئة التعليم. اندمجت الدراسة بشكل كبير بين النظرية والتطبيق، حيث استعرضت بعمق الطرق التي يمكن من خلالها تعزيز الحماية السيبرانية في مؤسسات التعليم الأساسي.

وفي سياق استكشاف الدراسة، تناولت الباحثة جوانب متنوعة من التهديدات السيبرانية التي تواجه المدارس الابتدائية، متناولة الطرق الفعّالة للتصدي لهذه التحديات بأسلوب يجمع بين الشمول والعمق. وفي محاولة لتعزيز التوعية، قدمت الدراسة إجراءات واقتراحات عملية لإدارة المخاطر السيبرانية بشكل مستدام.

أظهرت النتائج التي تم الوصول إليها في هذا السياق، أهمية تكامل التقنيات الحديثة مع السياسات والتدابير التعليمية، في سبيل تعزيز بيئة تعلم آمنة ومحمية. بصفة عامة، تعتبر هذه الدراسة إضافة قيمة لفهم كيفية تعزيز أمان المعلومات في مؤسسات التعليم الأساسي، وتدعو إلى التفكير الاستراتيجي لمواجهة تحديات السيبرأمان بفعالية.

المنهجية وطرق البحث.

يعتمد البحث على المنهج الوصفي التحليلي بهدف وصف وتحليل عوامل الهندسة الاجتماعية المؤثرة على الأمن السيبراني في البنوك.

أدوات الدراسة (أدوات جمع البيانات).

- الاستبانة: لجمع بيانات كمية من موظفي البنوك حول موضوع البحث.
- المقابلات: إجراء مقابلات مع عينة من موظفي البنوك للحصول على بيانات نوعية.
- تحليل الوثائق: جمع بيانات من التقارير والسجلات الخاصة بأمن المعلومات في البنوك.

مجالات الدراسة (بشري، مكاني، زماني).

مجتمع وعينة البحث:

يتكون مجتمع البحث من جميع موظفي البنوك في مدينة الرياض، وتختار عينة عشوائية منهم.

الأساليب الإحصائية:

استخدام الأساليب الإحصائية المناسبة في تحليل البيانات الكمية مثل اختبار T وتحليل التباين والانحدار وغيرها.

الإطار المفاهيمي

- الهندسة الاجتماعية:

عرفتها مؤسسة SANS على أنها "فن وعلم استغلال ضعف العنصر البشري في النظم من أجل الحصول على معلومات سرية".

- الاختراق الإلكتروني:

استغلال الثغرات ونقاط الضعف في الأنظمة والشبكات للوصول إلى المعلومات والبيانات الحساسة بطرق غير مشروعة.

- الهندسة الاجتماعية الهجومية:

استخدام أساليب الخداع والتلاعب بالعواطف لحمل الضحية على الإفصاح عن معلومات سرية أو تنفيذ أفعال ضارة.

- الوعي الأمني:

مدى إدراك الموظفين لمخاطر أمن المعلومات وطرق الحماية من التهديدات.

- الثقافة التنظيمية:

مجموعة القيم والمعتقدات والممارسات السائدة داخل المنظمة.

- العوامل الشخصية والاجتماعية:

الخصائص الفردية والاجتماعية للموظفين التي قد تؤثر على سلوكهم تجاه الهندسة الاجتماعية.

حدود البحث

- الحدود الموضوعية: يقتصر البحث على دراسة عوامل الهندسة الاجتماعية المؤثرة على الأمن السيبراني في البنوك.
- الحدود المكانية: يتم إجراء البحث في البنوك الموجودة في مدينة الرياض بالمملكة العربية السعودية.
- الحدود الزمانية: يتم إجراء هذا البحث خلال العام 2023م.
- الحدود البشرية: يقتصر البحث على فئة موظفي البنوك في مدينة الرياض.
- الحدود المنهجية: يتبع البحث المنهج الوصفي التحليلي من خلال استخدام أدوات جمع البيانات الكمية والكيفية.

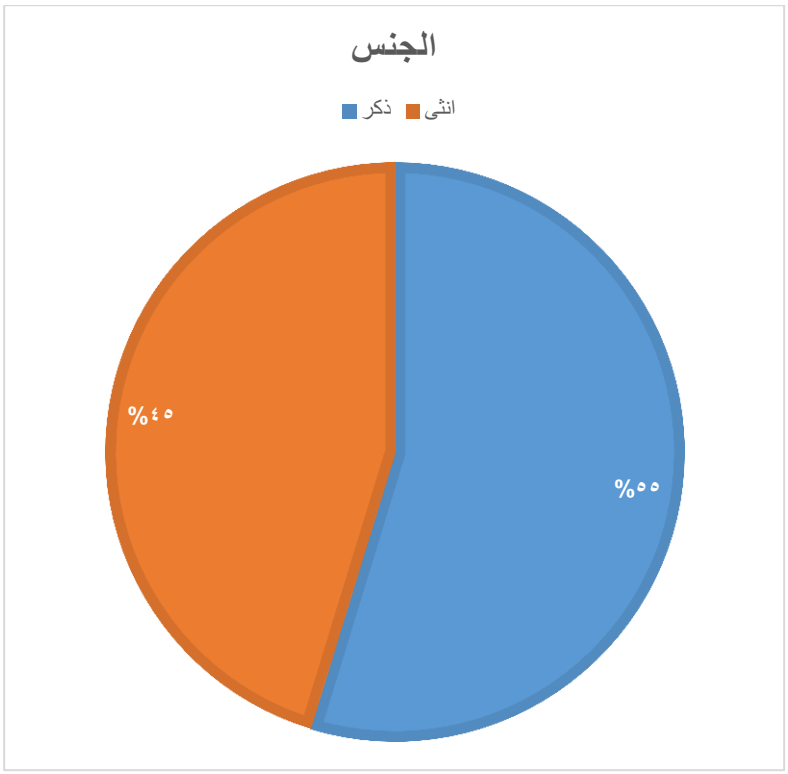
منهج الدراسة

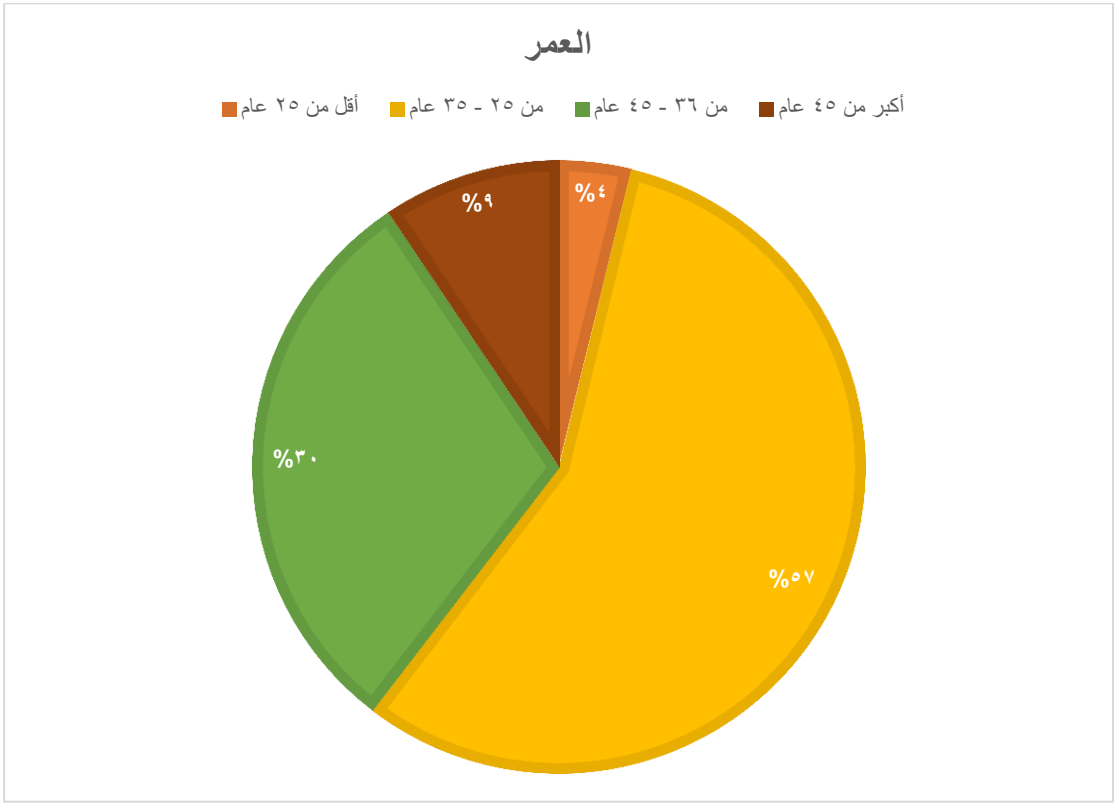
منهجية الدراسة:

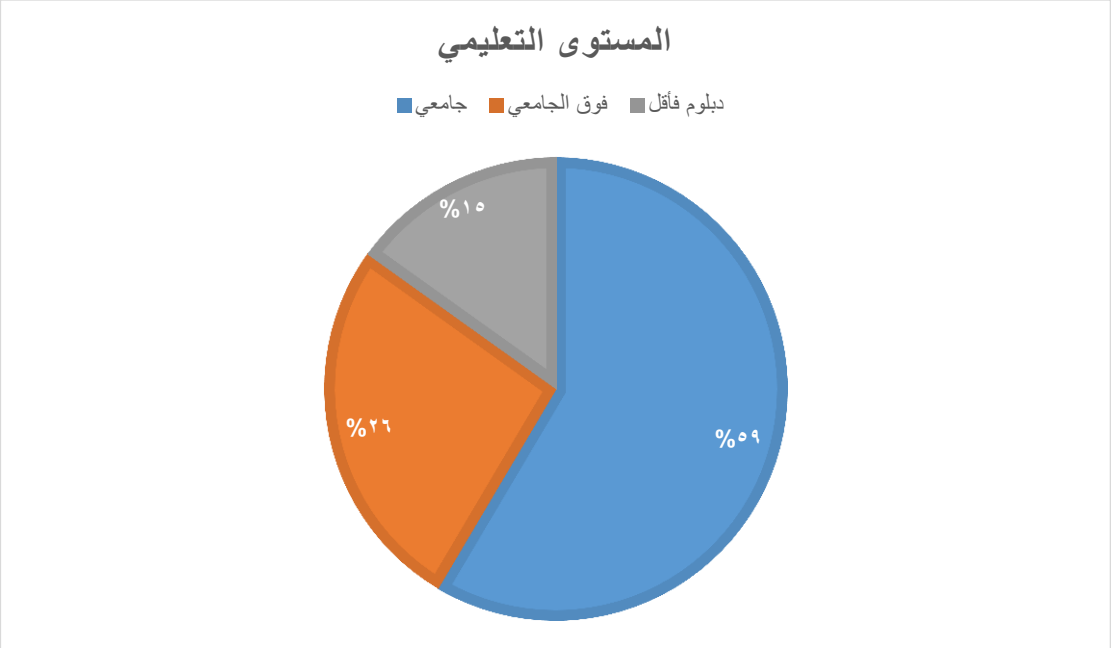
بما أنَّ الدراسة الحالية تندرج ضمن استكشاف عوامل الهندسة الاجتماعية المؤثرة على مخاطر الامن السيبراني في البنوك في مدينة الرياض في المملكة العربية السعودية، فقد اعتمد الباحث المنهج الوصفي التحليلي الذي يدرس الظاهرة كما هي في الواقع، ويصفها وصفاً تحليلياً علمياً بغية الوصول إلى نتائج عن الظاهرة.

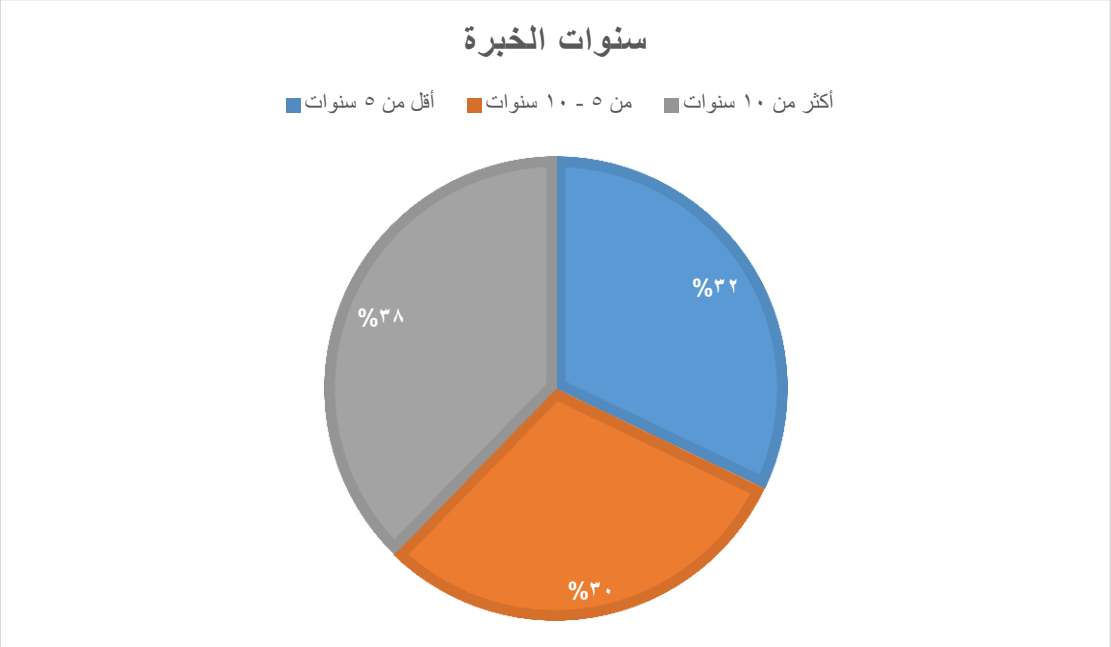
عينة الدراسة

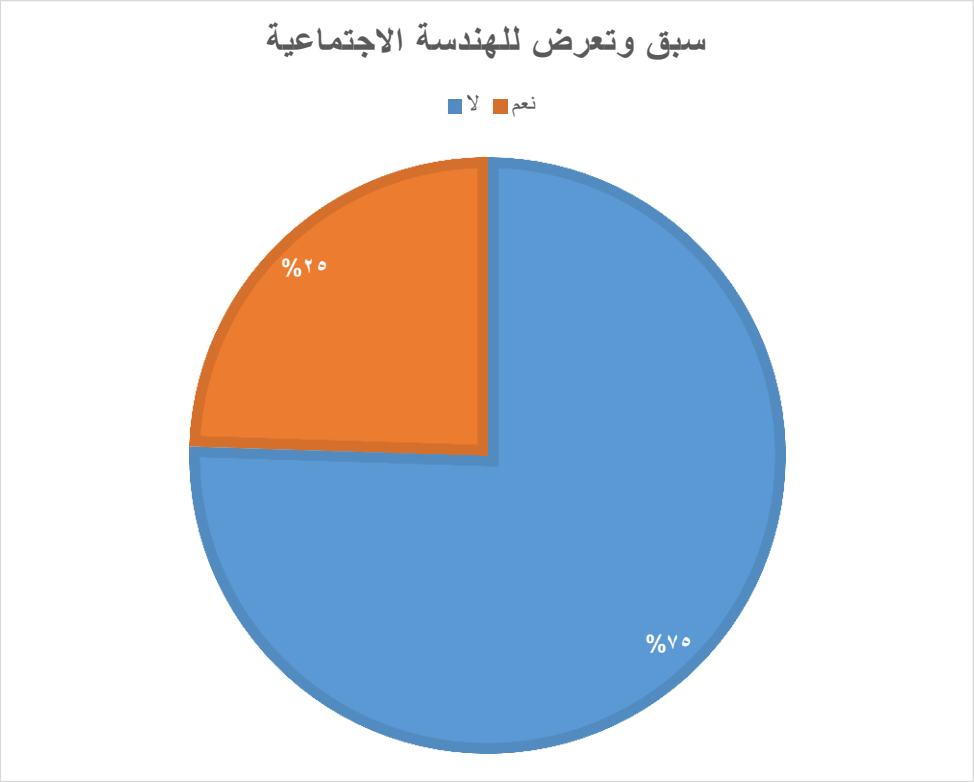
- بلغت العينة النهائية (53). وفق التالي:


الجنس
ذكر
انثى
%٥٥
%٤٥


العمر
أقل من ٢٥ عام
من ٢٥ - ٣٥ عام
من ٣٦ - ٤٥ عام
أكبر من ٤٥ عام
%٤
%٥٧
%٣٠
%٩


المستوى التعليمي
جامعي
فوق الجامعي
دبلوم فأقل
%١٥
%٢٦
%٥٩


سنوات الخبرة
أقل من ٥ سنوات
من ٥ - ١٠ سنوات
أكثر من ١٠ سنوات
%٣٢
%٣٠
%٣٨



أداة الدراسة:

تهدف الدراسة الحالية استكشاف عوامل الهندسة الاجتماعية المؤثرة على مخاطر الامن السيبراني في البنوك في مدينة الرياض في المملكة العربية السعودية، ولتحقيق هذا الهدف تم بناء استبانة وهي الأداة الرئيسة لجمع المعطيات من الميدان، وتم تطويرها بالاعتماد على مراجعة الإطار النظري، والدراسات السابقة. وصنفت بنود الاستبانة على النحو الآتي:

الجزء الأول: احتوى على المعلومات الديموغرافيّة (الجنس- العمر- المستوى التعليمي- سنوات الخبرة)

الجزء الثاني: محور مدى وعي موظفي البنوك في مدينة الرياض بمخاطر الهندسة الاجتماعية وطرق الوقاية منها.

الجزء الثالث: محور العوامل الشخصية والاجتماعية التي تجعل بعض موظفي البنوك أكثر عرضة للوقوع ضحية للهندسة الاجتماعية.

الجزء الثالث: محور العوامل الاجتماعية.

الجزء الرابع: محور الإجراءات والسياسات التي يمكن للبنوك اتباعها للحد من مخاطر الهندسة الاجتماعية.

في مستويات:(غير موافق بشدة، غير موافق، حيادي، موافق، موافق بشدة)

صدق أداة الدراسة:

1. الصدق الظاهري للدراسة:

للتأكد من الصدق الظاهري لأداة الدراسة عرضت في صورتها الأولية، على الأستاذ الدكتور المشرف بالإضافة إلى مجموعة من المحكِّمين من الأساتذة المختصين في كلية الإدارة.

2. الصدق التميزي للدراسة:

صدق المجموعات الطرفية (T-TEST): طُبقت أداة الدراسة إلكترونياً على عينة عشوائية، بلغت (50). وتعتمد هذه الطريقة على المقارنة بين الفئات المتطرفة (عليا_ دنيا)، حيث تم المقارنة بين متوسطات أعلى (12) درجة (الفئة العليا) مع أدنى (12) درجة (الفئة الدنيا) وحساب النتائج.

جدول رقم (1) يبين الصدق التميزي بين المتوسطات والانحرافات المعيارية، وقيمة "T"

الدرجات	العدد	المتوسط	الانحراف المعياري	قيمة "T"	مستوى الدلالة	القرار
أعلى 27%	12	3.7414	0.15045	-17.232	0.000	دال
أدنى 27%	12	2.9037	0.20288			

يتضح من الجدول السابق أن أداة الدراسة صادقة، ولبنودها القدرة التمييزية بين الأشخاص الذين حصلوا على درجات عليا، وأولئك الذين حصلوا على درجات دنيا.

6-5 ثبات أداة الدراسة:

حساب الثبات بطريقة كرونباخ ألفا: " يُعد معامل كرونباخ ألفا من أشهر مقاييس الثبات الداخلي (Reliability Internal Consistency) للاستبيان، ويعتمد على حساب الاختلافات (التباينات) الداخلية بين إجابات الأسئلة في الاستبيان".

جرى حساب قيمة معامل كرونباخ ألفا للمقياس ككل وكانت (0.869)، وهي قيمة جيدة؛ أي أنَّ جميع القيم تزيد عن (0.75)، وتشير إلى أنَّ أداة الدراسة تتمتع بدرجة جيدة من الثبات، ويمكن الاعتماد على النتائج والوثوق بها، بالإضافة ظهرت جميع قيم كرونباخ ألفا لجميع المحاور تزيد عن (0.75).

المعالجات الإحصائية:

تمت معالجة البيانات الإحصائية عن طريق برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS) باستخدام المعالجة الإحصائية التالية:

1. التوزيعات التكرارية، والنسب المئوية للتعرف على تكرار الإجابات لدى أفراد عينة الدراسة.
2. ألفا كرو نباخ لحساب معامل الثبات.
3. المتوسطة الحسابي والانحراف المعياري.
4. تحليل الانحدار اللوجستي المتعدد.

نتائج الدراسة

أولاً: النتائج المتعلقة بالإجابة عن أسئلة الدراسة:

وتسهيلًا لعرض نتائج الدراسة فقد تم تصنيفها وفقا لأسئلة الدراسة بحيث تمت الإجابة عن كل سؤال على حدة، وفيما يلي عرض لتلك النتائج والبيانات الإحصائية المتعلقة بها وفق المعيار الآتي لتفسير النتائج، حيث تم تحديد طول الخلايا وفقاً لمقياس ليكرت الخماسي، تم اعتماد المعادلة التالية: القيمة العليا للبديل – القيمة الدنيا للبديل مقسومة على عدد المستويات، (5-1 = 2) والجدول رقم (4) يوضح ذلك:

جدول (2): الحدود الدنيا والعليا لمقياس ليكرت الخماسي

المستوى	المتوسط الحسابي
منخفض	1 إلى أقل من 2.3
متوسط	من 2.3 إلى أُقل من 3.6
مرتفع	من 3.6 إلى 5

وبعد تطبيق الاستبانة على عينة الدراسة، وتفريغ الاستجابات تم حساب المتوسطات الحسابية لدرجة توافر المحاور، وجدول (3) أدناه يوضح ذلك.

جدول (3): المتوسطات الحسابية والانحرافات المعيارية لمحاور الدراسة

الرتبة	م	المحور	المتوسطة الحسابي	الانحراف المعياري	الدرجة
4	1	مدى وعي موظفي البنوك في مدينة الرياض بمخاطر الهندسة الاجتماعية وطرق الوقاية منها	3.94	0.972	مرتفع
2	2	العوامل الشخصية والاجتماعية التي تجعل بعض موظفي البنوك أكثر عرضة للوقوع ضحية للهندسة الاجتماعية	4.27	0.788	مرتفع
3	3	العوامل الاجتماعية	4.05	0.819	مرتفع
1	4	الإجراءات والسياسات التي يمكن للبنوك اتباعها للحد من مخاطر الهندسة الاجتماعية	4.41	0.819	مرتفع

يتضح من الجدول (3) أن المتوسط يتراوح بين (3.94 -4.41)، والانحراف المعياري بين (0.788- 0.972). وجاء في المرتبة الأولى محور الإجراءات والسياسات التي يمكن للبنوك اتباعها للحد من مخاطر الهندسة الاجتماعية بدرجة (مرتفعة)، وبمتوسط حسابي بلغ (4.41) وانحراف معياري قدره (0.819)، وفي المرتبة الثانية جاءت العوامل الشخصية والاجتماعية التي تجعل بعض موظفي البنوك أكثر عرضة للوقوع ضحية للهندسة الاجتماعية بدرجة (مرتفعة) وبمتوسط حسابي بلغ (4.27) وانحراف معياري قدره (0.788)، وجاء في المرتبة الثالثة محور العوامل الاجتماعية بدرجة (مرتفعة)، وبمتوسط حسابي بلغ (4.05) وانحراف معياري قدره (0.819)، وفي المرتبة الرابعة محور مدى وعي موظفي البنوك في مدينة الرياض بمخاطر الهندسة الاجتماعية وطرق الوقاية منها بدرجة (مرتفعة)، وبمتوسط حسابي بلغ (3.94) وانحراف معياري قدره (0.972).

- المحور الأول: مدى وعي موظفي البنوك في مدينة الرياض بمخاطر الهندسة الاجتماعية وطرق الوقاية منها.

جدول (4): التحليل الوصفي لفقرات محور مدى وعي موظفي البنوك في مدينة الرياض بمخاطر الهندسة الاجتماعية وطرق الوقاية منها

الرتبة	م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
4	1	أنا على دراية بمخاطر الهندسة الاجتماعية وفهمها	3.92	1.13	مرتفع
10	2	قد تم توفير التدريب اللازم لي على كيفية التعامل مع محاولات الهندسة الاجتماعية في بيئة العمل	3.45	1.206	متوسطة
8	3	أشعر بالثقة في قدرتي على التعرف على والتصدي لمحاولات الهندسة الاجتماعية	3.77	1.075	مرتفع
7	4	أنا منتبه للتحديات التي قد تواجهني فيما يتعلق بالهندسة الاجتماعية في سياق العمل	3.83	1.059	مرتفع
2	5	أعتبر الوقاية من مخاطر الهندسة الاجتماعية أمرًا مهمًا لأمان البنك والمعلومات	4.4	0.709	مرتفع
5	6	البنك يقدم الموارد الكافية والتوجيه للموظفين لفهم والوقاية من مخاطر الهندسة الاجتماعية	3.87	1.01	مرتفع
9	7	أنا على علم بسياسات الأمان والوقاية من الهندسة الاجتماعية التي ينفذها البنك	3.6	1.138	مرتفع
6	8	أشعر بأن فريق الأمان في البنك يقوم بدور فعال في تعزيز وعي الموظفين بمخاطر الهندسة الاجتماعية	3.83	0.863	مرتفع
3	9	أنا مستعد للإبلاغ عن أي حالة مشكوك فيها في محاولة للهندسة الاجتماعية.	4.32	0.721	مرتفع
1	10	أنا أعتبر التوجيه المستمر وورش العمل حول مخاطر الهندسة الاجتماعية ضروريين لتعزيز وعي الموظفين	4.4	0.809	مرتفع

تراوح المتوسط الحسابي للفقرات ضمن المحور بين (3.45-4.4)، والانحراف المعياري بين (0.709-1.206)، وحصلت الفقرة (10) والتي نصها " أنا أعتبر التوجيه المستمر وورش العمل حول مخاطر الهندسة الاجتماعية ضروريين لتعزيز وعي الموظفين " على أعلى متوسط حسابي بلغ (4.4) وبانحراف معياري قدره (0.809) وبدرجة مرتفعة، بينما حصلت الفقرة (2) والتي نصها " قد تم توفير التدريب اللازم لي على كيفية التعامل مع محاولات الهندسة الاجتماعية في بيئة العمل " على أقل متوسط حسابي بلغ (3.45) وانحراف معياري قدره (0.709) وبدرجة متوسطة.

- المحور الثاني: العوامل الشخصية والاجتماعية التي تجعل بعض موظفي البنوك أكثر عرضة للوقوع ضحية للهندسة الاجتماعية

جدول (5): التحليل الوصفي لفقرات محور العوامل الشخصية والاجتماعية التي تجعل بعض موظفي البنوك أكثر عرضة للوقوع ضحية للهندسة الاجتماعية

الرتبة	م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
4	1	يؤثر نقص التدريب على الأمان الالكتروني على وقوع موظفي البنك ضحية	4.21	0.809	مرتفع

الرتبة	م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
		الهندسة الاجتماعية			
3	2	عدم الوعي بأساليب الهندسة الاجتماعية يزيد من مخاطر الهندسة الاجتماعية لدى موظفي البنك	4.34	0.725	متوسطة
2	3	الموظفون الذين يثقون بسهولة قد يكونون أكثر عرضة للوقوع في فخ الهندسة الاجتماعية نتيجة تقديم معلوماتهم	4.4	0.736	مرتفع
5	4	الرغبة في تلبية احتياجات الآخرين أو تقديم المساعدة قد يؤدي إلى كشف معلومات حساسة.	4.17	0.795	مرتفع
6	5	اتخاذ القرارات بسرعة دون التأكد من هوية الشخص الذي يتفاعل معهم	4.08	0.949	مرتفع
1	6	اتخاذ القرارات بسرعة دون التأكد من هوية الشخص الذي يتفاعل يمكن أن يتيح للمهاجمين فرصًا لجمع معلومات حول الموظفين	4.43	0.714	مرتفع

تراوح المتوسط الحسابي للفقرات ضمن المحور بين (4.08-4.43)، والانحراف المعياري بين (0.714-0.809)، وحصلت الفقرة (6) والتي نصها " اتخاذ القرارات بسرعة دون التأكد من هوية الشخص الذي يتفاعل يمكن أن يتيح للمهاجمين فرصًا لجمع معلومات حول الموظفين " على أعلى متوسط حسابي بلغ (4.43) وبانحراف معياري قدره (0.714) وبدرجة مرتفعة، بينما حصلت الفقرة (5) والتي نصها " اتخاذ القرارات بسرعة دون التأكد من هوية الشخص الذي يتفاعل معهم " على أقل متوسط حسابي بلغ (4.08) وانحراف معياري قدره (0.949) وبدرجة مرتفعة.

- المحور الثالث: العوامل الاجتماعية

جدول (6): التحليل الوصفي لفقرات محور العوامل الاجتماعية

الرتبة	م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
5	1	الموظفون الذين يشاركون بكثافة في الأنشطة الاجتماعية قد يكونون أكثر عرضة للوقوع ضحية الهندسة الاجتماعية	3.96	0.868	مرتفع
3	2	ضغوط العمل والتوتر يمكن أن تجعل الموظفين أقل حذرًا أو أكثر عرضة للخداع من قبل الهندسة الاجتماعية	4.06	0.834	متوسطة
2	3	البيئة التنظيمية التي لا تعتبر الهندسة الاجتماعية تهديدًا جديًا قد تتسبب في انخراط الموظفين بشكل أكبر	4.15	0.711	مرتفع
4	4	الرغبة في التواصل مع أشخاص جدد أو الرغبة في توسيع الشبكة الاجتماعية يمكن أن يؤدي إلى تقديم معلومات حساسة	4	0.89	مرتفع
1	5	عدم الامتثال لسياسات الأمان والتدابير الوقائية في العمل يمكن أن يجعل الموظفين أكثر عرضة للهندسة الاجتماعية	4.26	0.677	مرتفع
6	6	البيئات العملية التي تشجع على التنافس قد تجعل الموظفين أكثر عرضة للخداع، حيث قد يكون لديهم رغبة في جذب العملاء أو تحقيق أهدافهم بسرعة.	3.87	0.932	مرتفع

تراوح المتوسط الحسابي للفقرات ضمن المحور بين (3.87-4.26)، والانحراف المعياري بين (0.677-0.932)، وحصلت الفقرة (5) والتي نصها " عدم الامتثال لسياسات الأمان والتدابير الوقائية في العمل يمكن أن يجعل الموظفين أكثر عرضة للهندسة الاجتماعية " على أعلى متوسط حسابي بلغ (4.26) وبانحراف معياري قدره (0.677) وبدرجة مرتفعة، بينما حصلت الفقرة (6) والتي نصها " البيئات العملية التي تشجع على التنافس قد تجعل الموظفين أكثر عرضة للخداع، حيث قد يكون لديهم رغبة في جذب العملاء أو تحقيق أهدافهم بسرعة " على أقل متوسط حسابي بلغ (3.87) وانحراف معياري قدره (0.932) وبدرجة مرتفعة.

- المحور الرابع: الإجراءات والسياسات التي يمكن للبنوك اتباعها للحد من مخاطر الهندسة الاجتماعية

جدول (7): التحليل الوصفي لعبارات محور الإجراءات والسياسات التي يمكن للبنوك اتباعها للحد من مخاطر الهندسة الاجتماعية

الرتبة	م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
8	1	توفير تدريب دوري للموظفين حول مخاطر الهندسة الاجتماعية وطرق التعرف عليها	4.36	0.803	مرتفع
6	2	وضع سياسات لمنع تبادل المعلومات الحساسة عبر وسائل الاتصال غير الآمنة	4.4	0.785	متوسطة
4	3	تقديم إجراءات قوية للتحقق من هوية الأفراد، سواء داخليين أو خارجيين، خاصةً عند التعامل مع معلومات حساسة	4.43	0.813	مرتفع
5	4	إطلاق حملات توعية دورية للموظفين والعملاء حول تقنيات الهندسة الاجتماعية الحديثة وكيفية التصدي لها	4.43	0.813	مرتفع
8	5	تحفيز إنشاء ثقافة أمنية داخل البنك تشمل التواصل المفتوح حول مخاطر الهندسة الاجتماعية وأهمية الامتثال للسياسات الأمنية	4.36	0.892	مرتفع
10	6	مراقبة وتحليل الأنشطة الشبكية للكشف المبكر عن أي محاولات للهندسة الاجتماعية.	4.3	0.881	مرتفع
2	7	تنفيذ سياسات قوية لحماية البيانات وتشفير المعلومات الحساسة للتقليل من فرص الوصول غير المصرح به	4.45	0.837	مرتفع
7	8	تحديد إجراءات واضحة للإبلاغ عن محاولات الهندسة الاجتماعية وتأمين آليات فعّالة للاستجابة السريعة	4.36	0.871	مرتفع
3	9	تبني سياسات للتحقق من هوية الأفراد في حالات الاتصالات الحساسة داخل البنك	4.43	0.789	مرتفع
1	10	تشجيع الموظفين والعملاء على استخدام كلمات مرور قوية وتحديثها بانتظام	4.6	0.709	مرتفع

تراوح المتوسط الحسابي للفقرات ضمن المحور بين (4.3-4.6)، والانحراف المعياري بين (0.709-0.892)، وحصلت الفقرة (10) والتي نصها " تشجيع الموظفين والعملاء على استخدام كلمات مرور قوية وتحديثها بانتظام " على أعلى متوسطة حسابي بلغ (4.6) وبانحراف معياري قدره (0.709) وبدرجة مرتفعة، بينما حصلت الفقرة (6) والتي نصها " مراقبة وتحليل الأنشطة الشبكية للكشف المبكر عن أي محاولات للهندسة الاجتماعية" على أقل متوسط حسابي بلغ (4.3) وانحراف معياري قدره (0.881) وبدرجة مرتفعة.

ثانيًا: اختبار وفحص الفرضيات:

فرضيات الدراسة: تم اختبار فرضيات الدراسة باستخدام تحليل الانحدار اللوجستي المتعدد (Multiple logistic Regression) لتحديد تأثير العوامل الاجتماعية والنفسية والثقافية ونجاح حملات الهندسة الاجتماعية ضد البنوك في مدينة الرياض.

تسعى الدراسة الى اختبار الفرضيات التالية:

لا توجد دلالة إحصائية عند مستوى 0.05 بين العوامل الاجتماعية والنفسية والثقافية ونجاح حملات الهندسة الاجتماعية ضد البنوك في مدينة الرياض.

الفرضيات الفرعية:

1. لا توجد دلالة إحصائية عند مستوى 0.05 بين مستوى وعي الموظفين وتعرضهم للوقوع ضحية الهندسة الاجتماعية.

جدول رقم (8) نتائج التحليل اللوجستي بين مستوى وعي الموظفين وتعرضهم للوقوع ضحية الهندسة الاجتماعية.

	B	S.E.	Wald	df	Sig.
مستوى وعي الموظفين	1.453	.629	5.343	1	.021

يتضح من الجدول السابق وجود أثر ذو دلالة إحصائية عند مستوى دلالة (0.05) بين مستوى وعي الموظفين وتعرضهم للوقوع ضحية الهندسة الاجتماعية، وبالتالي ترفض الفرضية الصفرية.

2. لا توجد دلالة إحصائية عند مستوى 0.05 بين العوامل الشخصية والاجتماعية للموظفين وتعرضهم للهندسة الاجتماعية.

جدول رقم (9) نتائج التحليل اللوجستي بين العوامل الشخصية والاجتماعية للموظفين وتعرضهم للهندسة الاجتماعية.

	B	S.E.	Wald	df	Sig.
العوامل الشخصية والاجتماعية	**1.047**	**.637**	**2.703**	**1**	**.100**

يتضح من الجدول السابق عدم وجود أثر ذو دلالة إحصائية عند مستوى دلالة (0.05) بين العوامل الشخصية والاجتماعية للموظفين وتعرضهم للهندسة الاجتماعية، وبالتالي تقبل الفرضية الصفرية.

3. لا توجد دلالة إحصائية عند مستوى 0.05 بين الثقافة التنظيمية وفاعلية إجراءات مواجهة الهندسة الاجتماعية.

جدول رقم (10) نتائج التحليل اللوجستي بين الثقافة التنظيمية وفاعلية إجراءات مواجهة الهندسة الاجتماعية.

	B	S.E.	Wald	df	Sig.
الثقافة التنظيمية	**1.565**	**.599**	**6.816**	**1**	**.009**

يتضح من الجدول السابق وجود أثر ذو دلالة إحصائية عند مستوى دلالة (0.05) بين الثقافة التنظيمية وفاعلية إجراءات مواجهة الهندسة الاجتماعية، وبالتالي ترفض الفرضية الصفرية.

4. لا توجد فروق ذات دلالة إحصائية عند مستوى 0.05 بين الإجراءات المقترحة وخفض مخاطر الهندسة الاجتماعية.

جدول رقم (11) نتائج التحليل اللوجستي بين الإجراءات المقترحة وخفض مخاطر الهندسة الاجتماعية.

	B	S.E.	Wald	df	Sig.
الإجراءات المقترحة	**-.116-**	**.408**	**.081**	**1**	**.777**

يتضح من الجدول السابق عدم وجود أثر ذو دلالة إحصائية عند مستوى دلالة (0.05) بين الإجراءات المقترحة وخفض مخاطر الهندسة الاجتماعية، وبالتالي تقبل الفرضية الصفرية.

النتائج:

1. وجود أثر ذو دلالة إحصائية عند مستوى دلالة (0.05) بين مستوى وعي الموظفين وتعرضهم للوقوع ضحية الهندسة الاجتماعية.
2. عدم وجود أثر ذو دلالة إحصائية عند مستوى دلالة (0.05) بين العوامل الشخصية والاجتماعية للموظفين وتعرضهم للهندسة الاجتماعية.
3. وجود أثر ذو دلالة إحصائية عند مستوى دلالة (0.05) بين الثقافة التنظيمية وفاعلية إجراءات مواجهة الهندسة الاجتماعية.
4. عدم وجود أثر ذو دلالة إحصائية عند مستوى دلالة (0.05) بين الإجراءات المقترحة وخفض مخاطر الهندسة الاجتماعية.

التوصيات:

1. يعتبر التوجيه المستمر وورش العمل حول مخاطر الهندسة الاجتماعية ضروريين لتعزيز وعي الموظفين.
2. اتخاذ القرارات بسرعة دون التأكد من هوية الشخص الذي يتفاعل يمكن أن يتيح للمهاجمين فرصًا لجمع معلومات حول الموظفين.
3. عدم الامتثال لسياسات الأمان والتدابير الوقائية في العمل يمكن أن يجعل الموظفين أكثر عرضة للهندسة الاجتماعية.
4. يجب تشجيع الموظفين والعملاء على استخدام كلمات مرور قوية وتحديثها بانتظام.

المراجع:

المراجع العربية:

- البراشدية، ح. س. (2021). ريادة الأعمال الرقمية ظل جائحة كورونا (كوفيد19): الفرص والتحديات. Journal of Information Studies and Technology, 2021(1), 5.
- السيد البغدادى، م. ف.، & مروة فتحى. (2021). اقتصاديات الأمن السيبراني في القطاع المصرفي. مجلة البحوث القانونية والإقتصادية (المنصورة)، 11(2)، 1446-1516.

- جمال الدين، هـ. (2023). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية، 24(1)، 189-230.
- سالم سعيد الكندي. (2020). الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان: دراسة حالة لطلبة الكلية التقنية بالمصنعة: الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان: دراسة حالة لطلبة الكلية التقنية بالمصنعة. Journal of Arts and Social Sciences [JASS], 11(2), 71-84.
- 5: سليمان، م. (2022). نظرية الأنشطة الروتينية: نظرية جديدة لفهم الجرائم السيبرانية. المجلة المصرية للعلوم الاجتماعية والسلوكية، 6(6)، 114-130.
- لطفى، و. (2022). الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا. مجلة كلية الاقتصاد والعلوم السياسية، 23(1)، 151-178.
- مجموعة مؤلفين. (2023). الأمن القومي العربي وتحديات الأمن الإقليمي. المركز العربي للأبحاث ودراسة السياسات.
- محمد المري، ر.، & راشد. (2023). أثر تكنولوجيا المعلومات في النظام الأمني والرقابة الداخلية| The Impact of Information Technology on the Security System and Internal Control. مجلة البحوث الفقهية والقانونية، 40(40)، 1303-1373.

المواقع الالكترونية:

- ابو حجاب، د. سارة .(n.d.) .إجراءات مقترحة إلدارة المخاطر السيبرانية في المدارس الابتدائية Retrieved November 27, 2023, from . https://emj.journals.ekb.eg/article_234267_1b664910f23f9049fc1dd83c9b407402.pdf
- Alon Bar. (2022, July 25). تحديات الأمن السيبراني و مخاطره على المؤسسات المالية و طرق معالجتها .روبودين . https://robodin.com/banks-top-cyber-security-challenges/
- الهندسة الاجتماعية وتهديد المعلومات المضللة في الأمن السيبراني - سيو ماستر .(2023, August 14) . https://seomastar.com/news/social-engineering-and-the-threat-of-disinformation-in-cybersecurity/
- ادارة مخاطر الأمن السيبراني في البنوك الأردنية (2020, by Millennium Journal of Economic and Administrative Sciences - Issuu. September 3). Issuu.com. https://issuu.com/mjeas/docs/

المراجع الاجنبية

- gmcdouga. (2022, March 2). Top 8 Cyber Security Challenges For Banks. Check Point Blog. https://blog.checkpoint.com/security/banks-top-8-cyber-security-challenges-and-how-to-overcome-them/
- Saudi Arabia National Portal. (2021). My.gov.sa. https://www.my.gov.sa/wps/portal/snp/content/cybersecurity
- Writer, S., & Gazette, S. (n.d.). Bank customers in Saudi warned against falling victims of social engineering fraud. Www.zawya.com. Retrieved November 28, 2023, from https://www.zawya.com/en/legal/crime-and-security/bank-customers-in-saudi-warned-against-falling-victims-of-social-engineering-fraud-vqy863gk
- Tessian. (2023, February 7). 11 Social Engineering Examples - Real Attacks - Updated 2021. Tessian. https://www.tessian.com/blog/examples-of-social-engineering-attacks/
- Social engineering attacks in online banking fraud | Cleafy. (n.d.). Www.cleafy.com. https://www.cleafy.com/insights/social-engineering-attacks-in-online-banking-how-to-identify-and-fight-them
- Ferchichi, A., & Itmazi, J. (2012). First International Conference in Information and Communication Technologies for Education and Training. Lulu. com.