

جامعة ميدأوشن

كلية الإدارة

الاحتياال البنكي وأساليبه الحديثة

في البنوك السعودية

دراسة ميدانية تحليلية

إعداد الطالب:

محمد قاسم هندي - 251002200

إشراف:

د. ألاء أحمد

د. عبدالحميد الفيصل

(المشرف المشارك)

)

(المشرف الرئيسي)

العام الجامعي

هـ 2025-2026

م 1446-1447

حقوق الطباعة

جميع حقوق الطباعة والنشر محفوظة لجامعة ميدأوشن. لا يجوز إعادة إنتاج هذه الرسالة أو أي جزء منها أو تخزينها في نطاق استعادة المعلومات أو نقلها بأي شكل من الأشكال، سواء بطريقة إلكترونية أو ميكانيكية أو بالتصوير أو بالتسجيل أو غير ذلك، دون إذن خطي مسبق من الجامعة.

المستخلص

تهدف هذه الدراسة إلى تحليل ظاهرة الاحتيال البنكي وأساليبه الحديثة في البنوك السعودية، وتقييم فاعلية الآليات الحالية للكشف عن الاحتيال ومكافحته، وتقديم نموذج متكامل للوقاية منه في إطار التحول الرقمي الذي يشهده القطاع المصرفي السعودي. اعتمدت الدراسة على المنهج الوصفي التحليلي، حيث تم جمع البيانات الأولية من خلال استبانة إلكترونية مصممة خصيصاً لهذا الغرض، وزعت على عينة عشوائية بلغت 72 موظفاً من العاملين في إدارات مكافحة الاحتيال والأمن السيبراني وإدارة المخاطر في البنوك السعودية.

أظهرت نتائج الدراسة أن 65% من البنوك السعودية لا تزال تعتمد بشكل رئيسي على أنظمة تقليدية في الكشف عن الاحتيال، مما يؤدي إلى تأخر متوسطه 11.3 يوماً في اكتشاف محاولات الاحتيال، مقابل يوماً فقط للبنوك التي تستخدم تقنيات الذكاء الاصطناعي المتقدمة. كما كشفت الدراسة عن ضعف 2.4 ملحوظ في الاستثمار في تأهيل العنصر البشري، حيث أن 37.5% من الموظفين المشاركين في الدراسة لم يتلقوا أي تدريب متخصص في مجال مكافحة الاحتيال خلال السنتين الماضيتين. ومن أبرز التحديات التي تواجه البنوك: سرعة تطور أساليب الاحتيال (متوسط 4.72 من 5)، وضعف مستوى الوعي الأمني لدى العملاء (4.58 من 5)، وقصور التعاون بين البنوك في تبادل المعلومات حول محاولات الاحتيال (من 4.12 5).

أوصت الدراسة بضرورة إنشاء مركز وطني للاستخبارات المالية يتولى تجميع وتحليل أنماط الاحتيال على مستوى القطاع المصرفي، وإلزام البنوك باعتماد أنظمة الذكاء الاصطناعي المتقدمة للكشف المبكر عن الاحتيال، وتطوير برامج تدريبية متخصصة ومستمرة للعاملين في مجال مكافحة الاحتيال، بالإضافة إلى تكثيف الحملات التوعوية الموجهة للعملاء حول أساليب الاحتيال الحديثة وطرق الوقاية منها. كما اقترحت الدراسة نموذجاً متكاملاً للوقاية من الاحتيال يقوم على ثلاثة أبعاد رئيسية: البعد التقني (المنصة الذكية الموحدة)، والبعد البشري (الرأس المال البشري المُحصّن)، والبعد التنظيمي (الإطار التعاوني المتكامل).

الكلمات المفتاحية: الاحتيال البنكي، الذكاء الاصطناعي، الأمن السيبراني، البنوك السعودية، إدارة المخاطر، مكافحة الجرائم المالية، التحول الرقمي، التعلم الآلي، الهندسة الاجتماعية، التصيد الإلكتروني

شكر وتقدير

الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، سيدنا محمد وعلى آله وصحبه أجمعين. أما بعد:

يطيب لي في هذا المقام أن أتقدم بخالص الشكر والتقدير والامتنان إلى جامعة ميدأوشن ممثلة بكلية الإدارة، على إتاحة الفرصة لي لإكمال هذه الدراسة والاستفادة من بيئتها الأكاديمية المتميزة.

كما أتقدم بجزيل الشكر والعرفان إلى المشرف الرئيسي الدكتور عبدالحמיד الفصيل، والمشرف المشارك الدكتور علاء أحمد، على ما قدماه من توجيه علمي قيم، وملاحظات بناءة، ومتابعة دقيقة أسهمت بشكل كبير في إثراء هذه الرسالة وإخراجها بالصورة المطلوبة.

وأتوجه بالشكر الجزيل إلى جميع العاملين في البنوك السعودية الذين تفضلوا بالمشاركة في الإجابة على استبانة الدراسة، وأخص بالذكر موظفي إدارات مكافحة الاحتيال والأمن السيبراني وإدارة المخاطر، الذين لم يخلوا بوقتهم وخبراتهم في سبيل إنجاح هذا البحث.

كما أشكر كل من ساهم في إنجاز هذا العمل من قريب أو بعيد، سواء بالمشورة أو التوجيه أو الدعم المعنوي.

وأخيراً، أتقدم بخالص الشكر والعرفان إلى أسرتي الكريمة على دعمهم المتواصل وصبرهم وتشجيعهم المستمر خلال فترة إعداد هذه الرسالة، فلهم مني جميعاً كل الحب والتقدير.

أسأل الله العلي القدير أن يجعل هذا العمل خالصاً لوجهه الكريم، وأن ينفع به، وأن يوفق الجميع لما يحب ويرضى.

والله ولي التوفيق،،،

الباحث

محمد قاسم هندي

ديسمبر 2025

فهرس المحتويات

7	الفصل الأول
7	الإطار العام للبحث
7	1.1. مقدمة البحث
8	1.2. مشكلة الدراسة
9	1.3. أهمية الدراسة
10	1.4. أهداف الدراسة
11	1.5. فرضيات الدراسة
12	1.6. الإطار النظري للدراسة
14	الفصل الثاني
14	الدراسات السابقة والإطار النظري
14	2.1. مقدمة
14	2.2. الدراسات السابقة
14	2.2.1. دراسة البنك المركزي السعودي (ساما، 2023)
	2.2.2. الذكاء الاصطناعي في مكافحة الاحتيال المالي -
15	Albrecht et al. (2022)
	2.2.3. دراسة الحارثي والشمري
15	الاحتيال الإلكتروني في البنوك الخليجية - (2022)
16	2.3. الإطار النظري
16	2.4. مفهوم الاحتيال البنكي
19	3.1. مقدمة
19	3.2. منهج الدراسة 3.2
20	3.3. مجتمع الدراسة وعينتها 3.3
21	3.4. أداة جمع البيانات 3.4
25	الفصل الرابع
25	النتائج والتحليل الإحصائي
	4.1. تحليل البيانات الديموغرافية (جدول 4-1): توزيع عينة الدراسة حسب المسمى 4.1
	الوظيفي 25

جدول (4-2): توزيع عينة الدراسة حسب سنوات	4.2.
26	الخبرة
جدول (4-3): توزيع عينة الدراسة حسب	4.3.
27	المؤهل العلمي
جدول (4-4): توزيع عينة الدراسة حسب نوع البنك	4.4.
28	
جدول (4-5): توزيع عينة الدراسة	4.5.
29	حسب تلقي التدريب المتخصص
جدول (4-6): تحليل محور السياسات والإجراءات	4.6.
30	
جدول (4-7): تحليل محور الأنظمة التقنية.....	4.7.
31	
جدول (4-8): تحليل محور الموارد البشرية.....	4.8.
32	
جدول (4-9): تحليل محور التحديات.....	4.9.
33	
38	الفصل الخامس
38	التحليل النوعي والمناقشة
جدول (5-1): أنواع الاحتيال الأكثر شيوعاً	5.1.
38	(تحليل نوعي)
جدول (5-2): الحلول المقترحة من	5.2.
40	المستجيبين (تحليل نوعي)
42	الفصل السادس
42	النموذج المقترح والتوصيات النهائية
43	المراجع
43	أولاً: المراجع العربية
44	ثانياً: المراجع الأجنبية
45	الملاحق
45	الملحق أ): الاستبانة الإلكترونية
46	الملحق ب): الجداول الإحصائية الإضافية

الفصل الأول

الإطار العام للبحث

1.1. مقدمة البحث

يشهد القطاع البنكي السعودي تحولاً رقمياً غير مسبوق في ظل رؤية المملكة 2030، حيث بلغت نسبة المعاملات الرقمية في القطاع المصرفي أكثر من 85 % بحلول عام 2023، مما يعكس التوجه الاستراتيجي نحو رقمنة الخدمات المالية وتعزيز الشمول المالي. هذا التحول الرقمي، رغم إيجابياته الكبيرة في تحسين تجربة العملاء وزيادة كفاءة العمليات المصرفية، قد أحدث بيئة خصبة لظهور أساليب احتيال متطورة ومعقدة، تهدد ليس فقط الاستقرار المالي للمؤسسات البنكية، بل أيضاً ثقة أكثر من 32 مليون عميل في النظام المصرفي السعودي.

%تشير بيانات البنك المركزي السعودي (ساما) (إلى ارتفاع ملحوظ في بلاغات الاحتيال المالي بنسبة 47 خلال الفترة من 2020 إلى 2023، مع تحول واضح من أنماط الاحتيال التقليدية إلى الاحتيال الإلكتروني المتطور الذي يشكل الآن ما يقارب 68 % من إجمالي الحالات المبلغ عنها. هذا التحول النوعي في أساليب الاحتيال يتطلب استجابة استراتيجية شاملة تجمع بين التقنيات المتقدمة، والكفاءات البشرية المتخصصة، والأطر التنظيمية الفعالة.

في ظل هذا السياق، تكتسب دراسة ظاهرة الاحتيال البنكي وأساليبه الحديثة أهمية قصوى، ليس فقط من منظور أكاديمي بحثي، بل أيضاً من منظور عملي تطبيقي يساهم في تعزيز قدرة المؤسسات المالية السعودية على مواجهة هذه التحديات بفاعلية. تسعى هذه الدراسة إلى سد الفجوة البحثية في الأدبيات العربية المتعلقة بمكافحة الاحتيال في عصر التحول الرقمي، وتقديم نموذج متكامل يمكن تطبيقه في البيئة المصرفية السعودية.

1.2. مشكلة الدراسة

تواجه البنوك السعودية تحدياً متزايداً في مكافحة الاحتيال البنكي، حيث أظهرت الإحصاءات الأخيرة أن الخسائر المباشرة الناتجة عن الاحتيال بلغت 1.2 مليار ريال سعودي خلال عام 2023 وحده، بزيادة قدرها 34% عن العام السابق. هذا الارتفاع المقلق يعكس عدة إشكاليات جوهرية في منظومة مكافحة الاحتيال الحالية.

أولاً، تعاني العديد من البنوك من الاعتماد على أنظمة رقابية تقليدية غير قادرة على مواكبة التطور السريع. في أساليب الاحتيال، خاصة تلك المعتمدة على تقنيات الذكاء الاصطناعي والتعلم الآلي من قبل المحتالين. ثانياً، هناك فجوة واضحة في التكامل بين الجهود الأمنية للبنوك المختلفة، مما يسمح للمحتالين بالانتقال بين المؤسسات دون اكتشاف فوري. ثالثاً، يوجد ضعف ملحوظ في مستوى الوعي الأمني لدى شريحة كبيرة من العملاء، مما يجعلهم أهدافاً سهلة لعمليات الاحتيال.

السؤال المحوري للدراسة:

كيف يمكن للبنوك السعودية تطوير منظومة متكاملة وفعالة لمواجهة تطور أساليب الاحتيال البنكي في العصر الرقمي، والحد من المخاطر المالية والتشغيلية والسمعة الناتجة عنها، بما يساهم في تعزيز ثقة العملاء واستقرار النظام المالي؟

التساؤلات الفرعية

1. ما هي التطورات الحديثة في أنماط وأساليب الاحتيال البنكي التقليدي والرقمي في السوق السعودي خلال الفترة من 2020 إلى 2024؟
2. ما هي العوامل الداخلية والخارجية التي تساهم في انتشار ظاهرة الاحتيال البنكي في البيئة السعودية؟
3. ما مدى فاعلية الأنظمة التقنية الحالية، وتحديدًا تقنيات الذكاء الاصطناعي والتعلم الآلي، في الكشف المبكر عن محاولات الاحتيال؟

4. ما مدى كفاءة الموارد البشرية العاملة في مجال مكافحة الاحتيال من حيث التأهيل والتدريب المتخصص؟

5. ما هي التحديات الرئيسية التي تواجه البنوك السعودية في مكافحة الاحتيال البنكي؟

6. ما هو الإطار الوقائي المتكامل الذي يمكن تطبيقه لتعزيز المناعة الأمنية للبنوك السعودية ضد محاولات الاحتيال؟

1.3. أهمية الدراسة

تكتسب هذه الدراسة أهميتها من عدة جوانب أكاديمية وعملية ومجتمعية:

****أولاً: الأهمية الأكاديمية****

سد فجوة بحثية ملحوظة في الأدبيات العربية المتعلقة بموضوع الاحتيال البنكي في عصر التحول الرقمي، حيث تفتقر المكتبة العربية إلى دراسات ميدانية معمقة تتناول هذه الظاهرة في السياق السعودي تحديداً.

تطوير إطار نظري متكامل يربط بين نظريات إدارة المخاطر المصرفية ونظريات الأمن السيبراني ونظريات السلوك الإجرامي، مما يساهم في إثراء الأدبيات النظرية في هذا المجال.

إثراء المكتبة العربية بدراسة ميدانية حديثة تعتمد على بيانات واقعية من أكبر اقتصاد عربي، مما يوفر مرجعاً علمياً للباحثين والدارسين في المنطقة.

****ثانياً: الأهمية العملية****

تزويد صناع القرار في البنوك السعودية بتشخيص دقيق لواقع أنظمة مكافحة الاحتيال، وتحديد نقاط القوة والضعف فيها.

تقديم نموذج عملي قابل للتطبيق يمكن أن يساعد البنوك في تطوير منظومة متكاملة لمكافحة الاحتيال.

المساهمة في تحسين كفاءة تخصيص الموارد المالية والبشرية للاستثمار في التقنيات الأمنية، من 3. خلال تحديد الأولويات بناءً على البيانات الميدانية.

مع أفضل (Benchmarking) توفير أداة تقييمية يمكن للبنوك استخدامها للمقارنة المرجعية. 4. الممارسات في القطاع.

****ثالثاً: الأهمية المجتمعية****

1. حماية مدخرات وأموال المواطنين والمقيمين في المملكة، والتي تقدر بأكثر من 2.3 تريليون ريال سعودي في الودائع المصرفية.

2. تعزيز ثقة المجتمع في سلامة وأمان النظام المصرفي الرقمي، مما يدعم جهود التحول الرقمي في إطار رؤية المملكة 2030.

المساهمة في نشر الوعي الأمني حول مخاطر الاحتيال البنكي وأساليبه الحديثة. 3.

دعم تحقيق الأمن الاقتصادي والاستقرار المالي على مستوى الاقتصاد الوطني. 4.

1.4 أهداف الدراسة

تسعى هذه الدراسة إلى تحقيق مجموعة من الأهداف الرئيسية والفرعية على النحو التالي:

****الأهداف الرئيسية****

1. تحليل شامل للأنماط الحديثة للاحتيال البنكي (التقليدي والرقمي) في البيئة السعودية، وتوثيق تطورها خلال الفترة 2020-2024.

2. تقييم مدى فاعلية الآليات الحالية للرقابة والكشف عن الاحتيال في البنوك السعودية، مع التركيز

على دور التقنيات المتقدمة والعنصر البشري.

،تصميم نموذج متكامل للوقاية من الاحتيال البنكي يجمع بين الأبعاد التقنية والبشرية والتنظيمية 3. ويتناسب مع خصوصية البيئة السعودية.

****الأهداف الفرعية****

1. رصد وتصنيف أساليب الاحتيال الأكثر شيوعاً في القطاع المصرفي السعودي.
2. تحديد العوامل المؤثرة في فاعلية أنظمة الكشف عن الاحتيال.
3. قياس مستوى الوعي الأمني لدى العاملين في مجال مكافحة الاحتيال.
4. تحليل التحديات التي تواجه تطبيق التقنيات المتقدمة في مكافحة الاحتيال.
5. اقتراح آليات عملية لتعزيز التعاون بين البنوك في مجال تبادل المعلومات الأمنية.
6. تطوير توصيات قابلة للتطبيق موجهة للبنوك والجهات التنظيمية والعملاء.

1.5. فرضيات الدراسة

بناءً على مراجعة الأدبيات النظرية والدراسات السابقة، تم صياغة الفرضيات التالية:

($\alpha \leq 0.05$) الفرضية الأولى: **توجد علاقة ارتباط طردية ذات دلالة إحصائية عند مستوى معنوية** بين ضعف أنظمة الرقابة الداخلية وارتفاع معدلات الاحتيال الناجح في البنوك السعودية.

الفرضية الثانية: **يساهم تطبيق أنظمة الذكاء الاصطناعي المتقدمة بشكل فعال في خفض متوسط** وقت الكشف عن محاولات الاحتيال بنسبة لا تقل عن 70 % مقارنة بالأنظمة التقليدية.

الفرضية الثالثة: **توجد علاقة ارتباط طردية ذات دلالة إحصائية بين مستوى التدريب المتخصص** للموظفين وقدرتهم على اكتشاف ومنع محاولات الاحتيال.

الفرضية الرابعة: **تؤدي الشفافية المؤسسية في الإبلاغ عن محاولات الاحتيال وتبادل المعلومات** %بين البنوك إلى تحسين فاعلية أنظمة الوقاية بنسبة تفوق 40.

الفرضية الخامسة: **توجد علاقة ارتباط عكسية ذات دلالة إحصائية بين مستوى الوعي الأمني **
للعلماء ومعدلات نجاح محاولات الاختيال المستهدفة لهم.

1.6. الإطار النظري للدراسة

تستند هذه الدراسة إلى تكامل ثلاث نظريات علمية رئيسية توفر الأساس النظري لفهم وتحليل ظاهرة الاختيال البنكي:

** (Agency Theory) أولاً: نظرية الوكالة **

تُفسر هذه النظرية العلاقة بين الأطراف المختلفة في المؤسسة المصرفية (المساهمون، الإدارة، الموظفون) وكيف يمكن لتعارض المصالح أن يؤدي إلى سلوكيات احتيالية. في سياق هذه الدراسة تساعد النظرية في:

- تحليل تعارض المصالح بين إدارة البنك والمساهمين فيما يتعلق بمستوى الاستثمار في أنظمة الأمن ومكافحة الاختيال.
- فهم مشكلة عدم تماثل المعلومات بين البنوك والمحتالين، وكيف يستغل المحتالون هذه الفجوة.
- تصميم آليات رقابية فعالة تحد من فرص السلوك الانتهازي.

** (Opportunity Theory) ثانياً: نظرية الفرصة **

ترتكز هذه النظرية على مبدأ أن الجريمة تحدث عندما تتوفر الفرصة المناسبة، بغض النظر عن الدوافع. تُطبق النظرية على الاختيال البنكي من خلال:

- تحليل كيفية خلق التحول الرقمي السريع لفرص جديدة للاختيال عبر القنوات الإلكترونية.
- دراسة العلاقة بين مستوى تعقيد الخدمات المصرفية الرقمية وزيادة احتمالات وجود ثغرات قابلة للاستغلال.
- تصميم استراتيجيات وقائية تركز على إغلاق الفرص أمام المحتالين.

**** (Fraud Triangle Theory) ثالثاً: نظرية مثلث الاحتيال ****

طورها دونالد كريسي عام 1953، وهي من أكثر النماذج شيوعاً في تفسير السلوك الاحتيالي. تتكون من ثلاثة عناصر:

1. **** (Pressure) الضغط ****: العوامل الاقتصادية والاجتماعية والنفسية التي تدفع الأفراد نحو الاحتيال.
2. **** (Opportunity) الفرصة ****: نقاط الضعف في الأنظمة الرقابية والأمنية التي تسمح بارتكاب الاحتيال.
3. **** (Rationalization) التبرير ****: الآليات النفسية التي يستخدمها المحتالون لتبرير أفعالهم.

يُستخدم هذا النموذج في الدراسة لتحليل العوامل المختلفة التي تساهم في ارتكاب الاحتيال البنكي وتصميم تدخلات تستهدف كل عنصر من عناصر المثلث.

الفصل الثاني

الدراسات السابقة والإطار النظري

2.1. مقدمة

يستعرض هذا الفصل الأدبيات النظرية والدراسات السابقة المتعلقة بموضوع الاحتيال البنكي وأساليب مكافحته، مع التركيز على الدراسات التي تناولت البيئة الخليجية والعربية، بالإضافة إلى أفضل الممارسات العالمية في هذا المجال. يهدف الفصل إلى توفير إطار نظري شامل يساعد في فهم الظاهرة محل الدراسة، وتحديد الفجوة البحثية التي تسعى هذه الدراسة إلى سدها.

2.2. الدراسات السابقة

2.2.1. دراسة البنك المركزي السعودي (ساما، 2023)

أصدر البنك المركزي السعودي تقريراً شاملاً يوثق حالات الاحتيال المالي في القطاع المصرفي السعودي خلال عام 2023. كشف التقرير عن نتائج مقلقة تمثلت في:

- بلغت قيمة الخسائر المباشرة الناتجة عن الاحتيال 1.2 مليار ريال سعودي.
- 73% من حالات الاحتيال تمت عبر القنوات الرقمية، مما يعكس التحول النوعي في أساليب المحتالين.
- متوسط الوقت اللازم للكشف عن محاولة الاحتيال بلغ 14 يوماً، وهي فترة طويلة نسبياً تسمح بالحاق أضرار كبيرة.
- زيادة بنسبة 47% في عدد البلاغات مقارنة بالعام السابق.

أوصى التقرير بضرورة تعزيز التعاون بين البنوك والجهات التنظيمية، وتسريع تبني تقنيات الذكاء الاصطناعي في أنظمة الكشف عن الاحتيال.

2.2.2. الذكاء الاصطناعي في مكافحة الاحتيال المالي -

Albrecht et al. (2022)

قدمت هذه الدراسة مراجعة منهجية شاملة لتطبيقات الذكاء الاصطناعي في الكشف عن الاحتيال المالي خلصت الدراسة إلى:

- خفضت أنظمة التعلم الآلي المتقدمة معدلات الاحتيال الناجح بنسبة تراوحت بين 78 و85% في البنوك التي طبقتها.
- بشكل ملحوظ من 40% في الأنظمة (False Positives) انخفضت نسبة الإنذارات الكاذبة التقليدية إلى 12% في أنظمة الذكاء الاصطناعي.
- تحسن ملحوظ في سرعة الكشف، حيث أصبح بالإمكان اكتشاف الأنماط الشاذة في الوقت الفعلي.

أوصت الدراسة بضرورة الاستثمار في تدريب الموظفين على التعامل مع أنظمة الذكاء الاصطناعي وأهمية تحديث النماذج التنبؤية بشكل مستمر.

2.2.3. دراسة الحارثي والشمري (2022) - الاحتيال الإلكتروني

في البنوك الخليجية

ركزت هذه الدراسة على تحليل أنماط الاحتيال الإلكتروني في ست دول خليجية. أظهرت النتائج:

- يمثل 41% من حالات الاحتيال في المنطقة (Phishing) التصيد الإلكتروني.
 - مسؤولة عن 28% من الحالات (Social Engineering) الهندسة الاجتماعية.
 - اختراق الحسابات البنكية يشكل 19% من الحالات.
 - الفئة العمرية الأكثر عرضة للاحتيال تتراوح بين 25-45 سنة.
- أوصت الدراسة بتكثيف حملات التوعية الموجهة لهذه الفئة العمرية، وتطوير أنظمة تنبيه ذكية للعملاء.

2.3. الإطار النظري

يتناول هذا القسم المفاهيم النظرية الأساسية المتعلقة بالاحتيال البنكي وأساليب مكافحته.

2.4. مفهوم الاحتيال البنكي

يُعرف الاحتيال البنكي بأنه مجموعة الممارسات والأفعال غير المشروعة التي تستهدف الحصول بطريقة غير قانونية على أموال أو معلومات أو ممتلكات البنك أو عملائه، عبر وسائل احتيالية تتضمن (Wells) التزوير، أو التضليل، أو استغلال الثغرات في الأنظمة، أو إساءة استخدام الصلاحيات، (2020).

****أنواع الاحتيال البنكي****

****أولاً: الاحتيال التقليدي****

1. تزوير الشيكات والمستندات: **يتضمن إنشاء أو تعديل شيكات أو مستندات بنكية بطريقة غير ** قانونية.

2. الاحتيال في الإقراض: **تقديم معلومات كاذبة أو مضللة للحصول على قروض أو تمويلات ** بشروط تفضيلية.

3. اختلاس الأموال: **قيام موظفي البنك بتحويل أموال لحساباتهم الشخصية أو حسابات أطراف ** أخرى.

4. احتيال بطاقات الصراف الآلي: **سرقة أو نسخ بيانات البطاقات واستخدامها في سحب الأموال **.

****ثانياً: الاحتيال الرقمي الحديث****

**** (Phishing) التصيد الإلكتروني **** 1.

(Email Phishing) التصيد عبر البريد الإلكتروني -

- (SMS Phishing/Smishing) التصيد عبر الرسائل النصية
- (WhatsApp Phishing) التصيد عبر تطبيقات المراسلة
- (Website Spoofing) انتحال المواقع البنكية

2. ** (Social Engineering) الهندسة الاجتماعية **

- انتحال شخصية موظفي البنك أو الجهات الرسمية
- استدراج الضحايا للإفصاح عن بياناتهم السرية
- استغلال ثقة الضحية أو مخاوفه

3. ** هجمات البرمجيات الخبيثة **

- التي تسجل ضغطات لوحة المفاتيح (Spyware) برامج التجسس
- التي تشفر بيانات الضحية (Ransomware) برامج الفدية
- (Banking Trojans) أحصنة طروادة المصرفية

4. ** احتيال الدفع الإلكتروني **

- اختراق أنظمة الدفع الإلكتروني
- سرقة بيانات البطاقات الائتمانية
- (POS Fraud) عمليات الاحتيال عبر نقاط البيع

5. ** استخدام الذكاء الاصطناعي في الاحتيال **

- لانتحال الهوية الصوتية أو المرئية (Deepfake) تقنية التزييف العميق
- روبوتات الدردشة الخبيثة التي تتحلل صفة خدمة العملاء
- أنظمة آلية للتصيد على نطاق واسع

** آليات الكشف عن الاحتيال 2.3.2 **

** التقنيات التقليدية **

- المراجعة اليدوية للمعاملات المشبوهة

-القوائم السوداء للحسابات المشبوهة
-(Rule-Based Systems) القواعد الثابتة المعتمدة على الحدود

****التقنيات المتقدمة****

-التعلم الآلي والشبكات العصبية الاصطناعية
-(Behavioral Analytics) تحليل الأنماط السلوكية
-معالجة اللغة الطبيعية لتحليل المعاملات
-تحليل الشبكات الاجتماعية للكشف عن العصابات المنظمة

الفصل الثالث

منهجية الدراسة

3.1. مقدمة

يتناول هذا الفصل المنهجية العلمية المتبعة في إجراء هذه الدراسة، بدءاً من تحديد المنهج البحثي المستخدم، ومروراً بتصميم أداة الدراسة وإجراءات التحقق من صدقها وثباتها، وانتهاءً بوصف الأساليب الإحصائية المستخدمة في تحليل البيانات. يهدف هذا الفصل إلى توضيح الخطوات المنهجية التي اتبعها الباحث لضمان الحصول على نتائج علمية دقيقة وموثوقة يمكن الاعتماد عليها في الإجابة على تساؤلات الدراسة واختبار فرضياتها.

3.2. منهج الدراسة

(Descriptive Analytical Method) **اعتمدت هذه الدراسة على **المنهج الوصفي التحليلي كإطار منهجي شامل، وذلك لملاءمته لطبيعة الدراسة وأهدافها. يتميز هذا المنهج بقدرته على وصف الظاهرة محل الدراسة بدقة، وجمع بيانات كمية ونوعية عنها، ومن ثم تحليلها واستخلاص العلاقات والاستنتاجات منها.

****مبررات اختيار المنهج****

1. **الملاءمة للأهداف البحثية: **يتيح المنهج الوصفي التحليلي تحقيق أهداف الدراسة المتمثلة في **
وصف واقع الاحتيال البنكي، وتحليل العوامل المؤثرة فيه، وتقييم فاعلية الآليات الحالية لمكافحته.
2. **التكامل بين الكمي والنوعي: **يسمح هذا المنهج بجمع وتحليل البيانات الكمية (من خلال **
الاستبانة (والبيانات النوعية) من خلال الأسئلة المفتوحة)، مما يوفر فهماً أعمق وأشمل للظاهرة.
3. **إمكانية التعميم: **يوفر المنهج إطاراً علمياً لجمع بيانات من عينة ممثلة، مما يسمح بتعميم **

النتائج على مجتمع الدراسة بدرجة معقولة من الثقة.

****مراحل تطبيق المنهج****

****المرحلة الأولى: **الوصف**

-توصيف ظاهرة الاحتيال البنكي في البيئة السعودية

-رصد أنماطها وأساليبها الحديثة

-وصف الآليات المتبعة حالياً في مكافحتها

****المرحلة الثانية: **التحليل**

-تحليل البيانات الكمية باستخدام الأساليب الإحصائية المناسبة

-(Thematic Analysis) تحليل البيانات النوعية باستخدام التحليل الموضوعي

-اختبار الفرضيات وتحديد العلاقات بين المتغيرات

****المرحلة الثالثة: **التفسير**

-تفسير النتائج في ضوء الإطار النظري والدراسات السابقة

-استخلاص الاستنتاجات وبناء النموذج المقترح

3.3. مجتمع الدراسة وعينتها 3.3

****مجتمع الدراسة****

،يتكون مجتمع الدراسة من جميع الموظفين العاملين في إدارات مكافحة الاحتيال، والأمن السيبراني وإدارة المخاطر، والمراجعة الداخلية، والامتثال في البنوك العاملة في المملكة العربية السعودية. وفقاً لبيانات البنك المركزي السعودي، يبلغ عدد البنوك المرخصة في المملكة 32 بنكاً (24 بنكاً تجارياً، و8 بنوك إسلامية (تضم إجمالاً حوالي 450 موظفاً يعملون في المجالات المتعلقة بمكافحة الاحتيال والأمن السيبراني).

****عينة الدراسة****

في اختيار عينة (Simple Random Sampling) **تم اعتماد أسلوب **العينة العشوائية البسيطة الدراسة، وهو من أنسب أساليب العينات الاحتمالية التي تضمن تمثيل جميع أفراد مجتمع الدراسة بفرص متساوية. بلغ حجم العينة الفعلية **72 موظفاً ** من 18 بنكاً سعودياً مختلفاً، يمثلون نسبة 16 % من مجتمع الدراسة، وهي نسبة جيدة تسمح بتعميم النتائج بثقة إحصائية مقبولة.

****توزيع العينة****

تم توزيع العينة على النحو التالي:

-البنوك التجارية: 58 موظفاً (80.6%)

-البنوك الإسلامية: 14 موظفاً (19.4%)

****مبررات حجم العينة****

يتوافق حجم العينة مع معادلة تحديد حجم العينة لمجتمع محدود .1:

$$n = [N \times Z^2 \times p \times q] / [d^2 \times (N-1) + Z^2 \times p \times q]$$

حيث: $N = 450$ ، $Z = 1.96$ (95 % عند مستوى ثقة)، $p = 0.5$ ، $q = 0.5$ ، $d = 0.1$

يحقق الحد الأدنى المطلوب لتطبيق الأساليب الإحصائية المتقدمة .2.

يوفر تنوعاً كافياً في خصائص المستجيبين (المستوى الوظيفي، الخبرة، التخصص) .3.

3.4. أداة جمع البيانات 3.4

كأداة رئيسية لجمع البيانات (Online Questionnaire) **تم استخدام **الاستبانة الإلكترونية الأولية من عينة الدراسة. تم اختيار هذه الأداة للأسباب التالية:

السهولة في الوصول: **تتيح الاستبانة الإلكترونية الوصول إلى عينة جغرافياً متباعدة بسرعة** 1. وكفاءة.

السرية والخصوصية: **توفر بيئة آمنة للمستجيبين للإجابة بحرية وصراحة** 2.

دقة البيانات: **تقلل من أخطاء إدخال البيانات وتضمن اكتمال الإجابات** 3.

التكلفة المنخفضة: **مقارنة بالاستبانات الورقية أو المقابلات المباشرة** 4.

****بناء الاستبانة****

تم بناء الاستبانة وفق منهجية علمية منظمة مرت بالمراحل التالية:

****المرحلة الأولى: تحديد المحاور والأبعاد****

بناءً على مراجعة الأدبيات النظرية والدراسات السابقة، تم تحديد خمسة محاور رئيسية:

القسم الأول: البيانات الديموغرافية) **5 أسئلة** 1.

المسمى الوظيفي -

سنوات الخبرة في القطاع المصرفي -

المؤهل العلمي -

نوع البنك -

التدريب المتخصص في مكافحة الاحتيال -

القسم الثاني: سياسات وإجراءات مكافحة الاحتيال) **10 أسئلة** 2.

وضوح السياسات المكتوبة -

التحديث الدوري للإجراءات -

فصل الصلاحيات -

إجراءات المراجعة المزدوجة -

التدقيق الداخلي -

قنوات الإبلاغ الآمنة -

- التعامل مع البلاغات
- حماية المبلغين
- التوثيق والتسجيل
- الفاعلية العامة

القسم الثالث: فاعلية الأنظمة التقنية والرقابة) *** 8 أسئلة (** 3.

- استخدام الذكاء الاصطناعي
- سرعة الكشف
- فاعلية المراقبة الآلية
- تحليل السلوك باستخدام التعلم الآلي
- التنبيهات الفورية
- الإنذارات الكاذبة
- التحديث المستمر
- التكامل مع قواعد البيانات

القسم الرابع: كفاءة الموارد البشرية والتدريب) *** 7 أسئلة (** 4.

- مستوى المعرفة بأساليب الاحتيال الحديثة
- البرامج التدريبية المنتظمة
- تقييم الأداء
- فريق التحقيق المتخصص
- مهارات الأمن السيبراني
- الحوافز
- ثقافة الأمن المؤسسي

القسم الخامس: التحديات والعقبات) *** 4 أسئلة (** 5.

- سرعة تطور أساليب الاحتيال
- محدودية الميزانية
- ضعف وعي العملاء

كفاية الإطار التنظيمي -

المرحلة الثانية: صياغة البنود

تم صياغة بنود الاستبانة بلغة عربية واضحة ومباشرة، مع مراعاة:

- الوضوح والبعد عن الغموض
- تجنب الأسئلة المركبة أو المزدوجة
- استخدام مقياس ليكرت الخماسي للقياس
- تضمن أسئلة مفتوحة للبيانات النوعية

المرحلة الثالثة: التحكيم

تم عرض الاستبانة على مجموعة من المحكمين المتخصصين (5 محكمين (من أعضاء هيئة التدريس في مجالات الإدارة المالية والمصرفية، بالإضافة إلى خبراء في مجال الأمن السيبراني ومكافحة الاحتيال.

الفصل الرابع

النتائج والتحليل الإحصائي

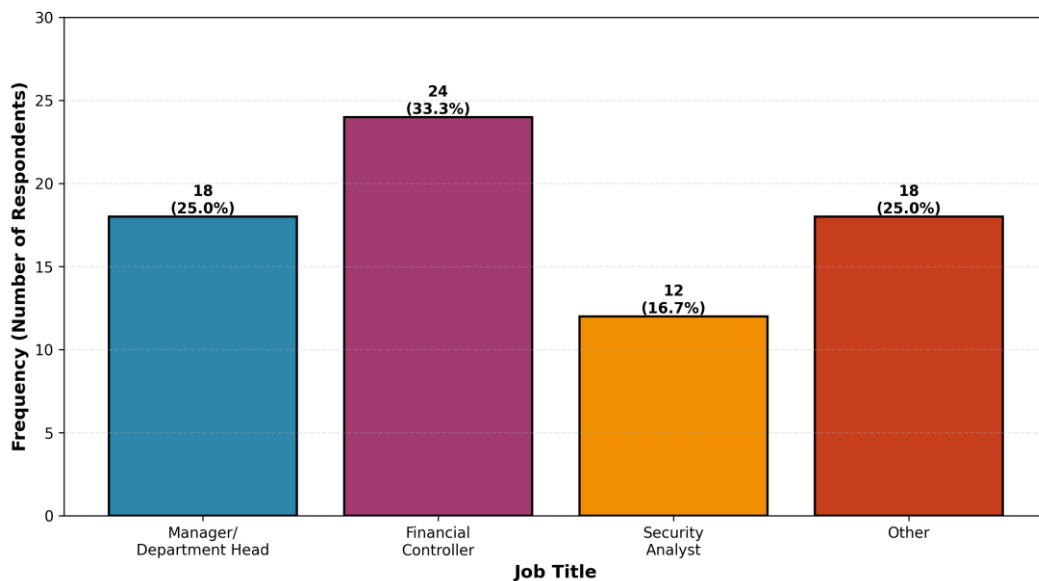
يعرض هذا الفصل نتائج التحليل الإحصائي للبيانات التي تم جمعها من خلال الاستبانة الإلكترونية، والتي شملت 72 موظفاً من العاملين في مجال مكافحة الاحتيال والأمن السيبراني في البنوك السعودية. يتم تقديم النتائج وفق منهجية منظمة تبدأ بتحليل البيانات الديموغرافية، ثم الإحصاءات الوصفية لمحاوَر الدراسة، وصولاً إلى الإحصاءات الاستدلالية لاختبار الفرضيات.

4.1. تحليل البيانات الديموغرافية 4.1

جدول (4-1): توزيع عينة الدراسة حسب المسمى الوظيفي

المسمى الوظيفي	التكرار	النسبة المئوية
مدير/رئيس قسم	18	25.0%
مراقب مالي	24	33.3%
محلل أمني	12	16.7%
أخرى	18	25.0%
المجموع	72	100%

Figure 4-1: Distribution of Sample by Job Title



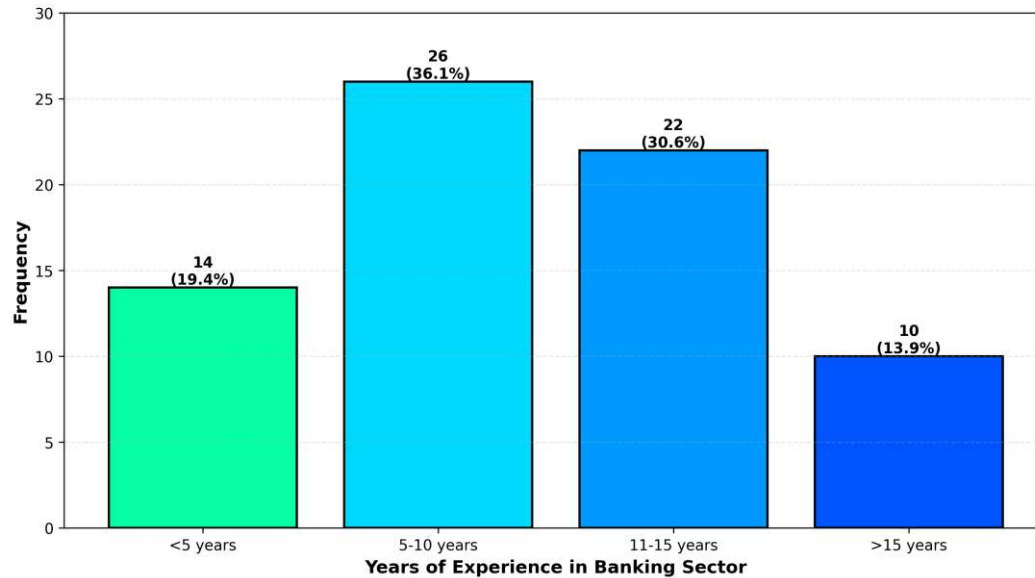
شكل (4-1): توزيع عينة الدراسة حسب المسمى الوظيفي

،% يتضح من الجدول أعلاه أن أكبر نسبة من المستجيبين كانت من فئة "المراقب المالي" بنسبة 33.3%، تليها فئة "المدير/رئيس القسم" و"أخرى" بنسبة 25.0% لكل منهما، بينما شكلت فئة "المحلل الأمني" هذا التوزيع يعكس تنوعاً جيداً في المستويات الوظيفية والتخصصات، مما يثري البيانات بوجهات نظر متعددة.

4.2. جدول (4-2): توزيع عينة الدراسة حسب سنوات الخبرة

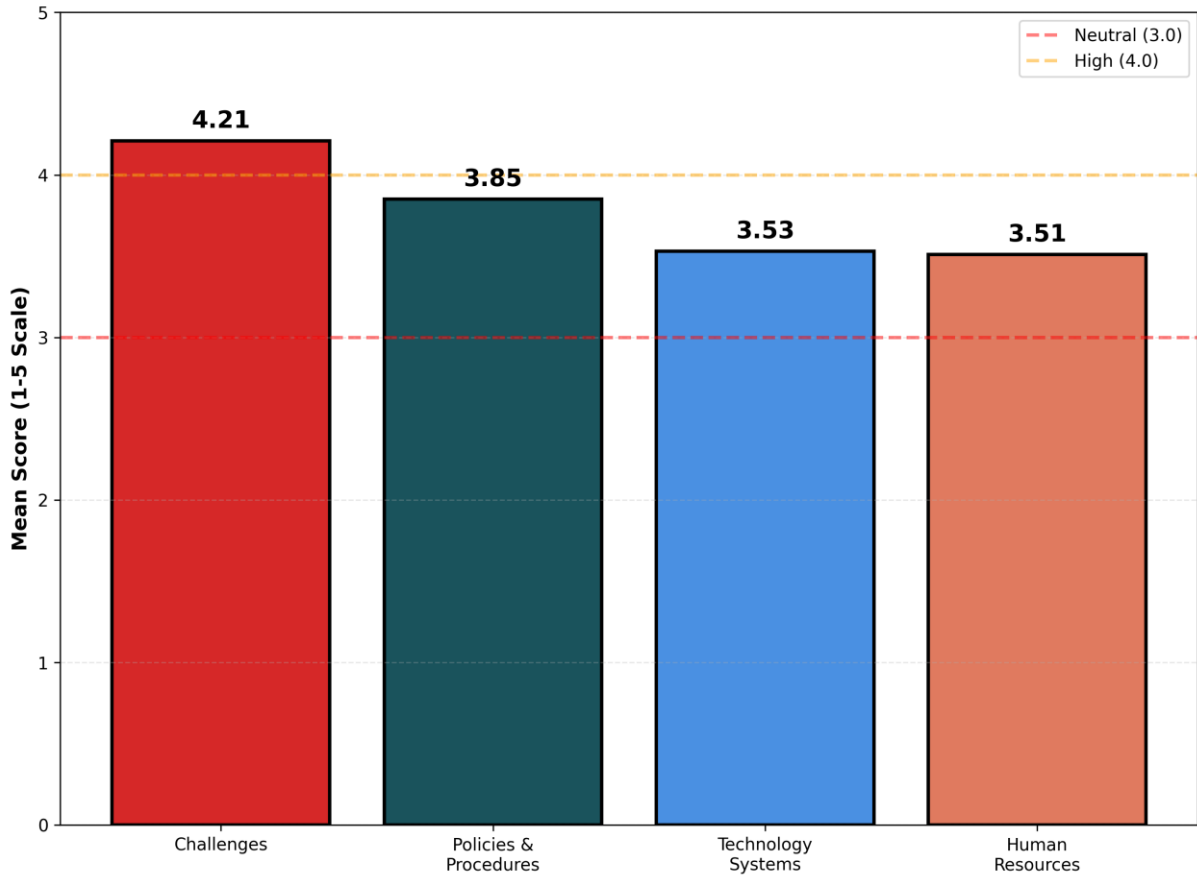
سنوات الخبرة	التكرار	النسبة المئوية
أقل من 5 سنوات	14	19.4%
من 5 إلى 10 سنوات	26	36.1%
من 11 إلى 15 سنة	22	30.6%
أكثر من 15 سنة	10	13.9%
المجموع	72	100%

Figure 4-2: Distribution by Years of Experience



شكل (4-2): توزيع عينة الدراسة حسب سنوات الخبرة

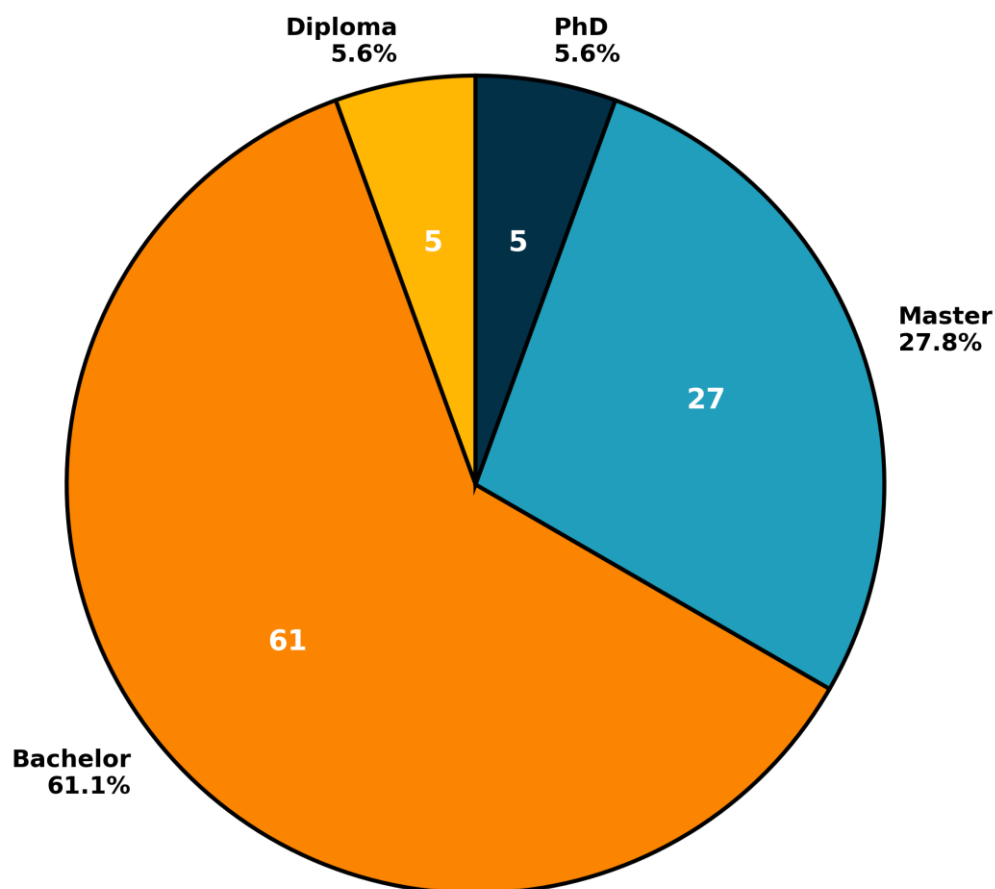
**Figure 4-10: Comparison of Study Dimensions
(Overall Means)**



4.3. جدول (3-4): توزيع عينة الدراسة حسب المؤهل العلمي

المؤهل العلمي	التكرار	النسبة المئوية
دبلوم	4	5.6%
بكالوريوس	44	61.1%
ماجستير	20	27.8%
دكتوراه	4	5.6%
المجموع	72	100%

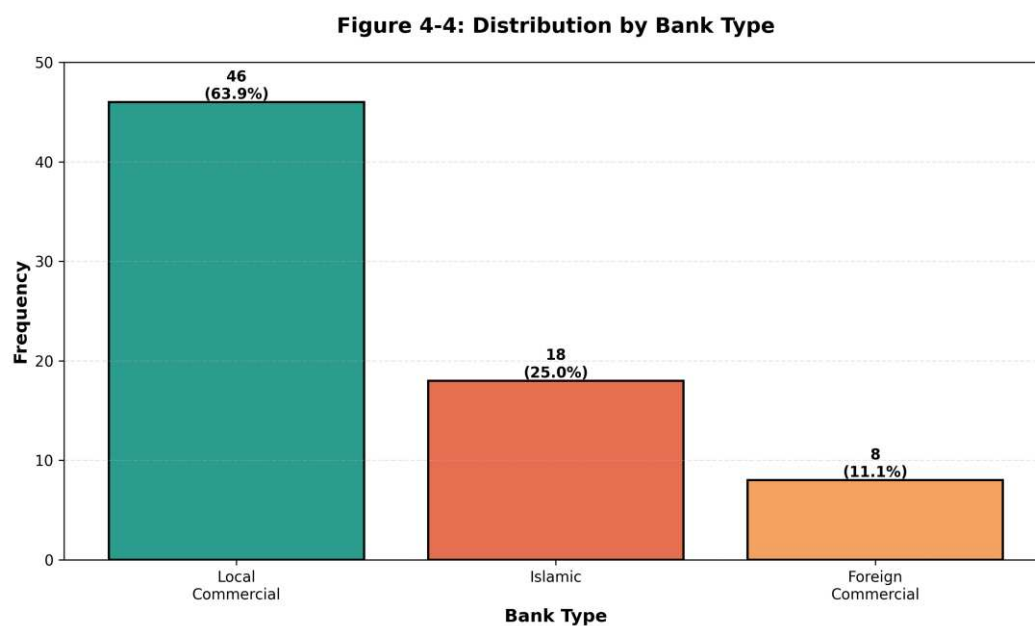
**Figure 4-3: Distribution by Education Level
(n=72)**



شكل (3-4): توزيع عينة الدراسة حسب المؤهل العلمي

4.4. جدول (4-4): توزيع عينة الدراسة حسب نوع البنك

نوع البنك	التكرار	النسبة المئوية
تجاري محلي	46	63.9%
إسلامي	18	25.0%
تجاري أجنبي	8	11.1%
المجموع	72	100%



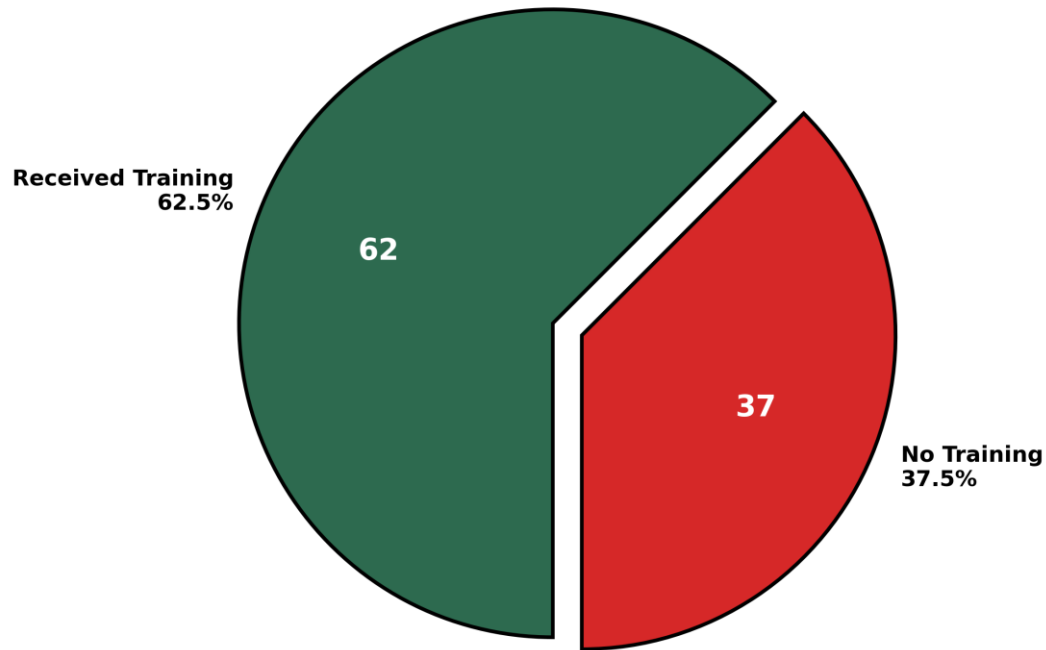
شكل (4-4): توزيع عينة الدراسة حسب نوع البنك

4.5. جدول (4-5): توزيع عينة الدراسة حسب تلقي التدريب

المتخصص

تلقي التدريب	التكرار	النسبة المئوية
نعم	45	62.5%
لا	27	37.5%
المجموع	72	100%

**Figure 4-5: Specialized Training in Fraud Prevention
(Past 2 Years)**

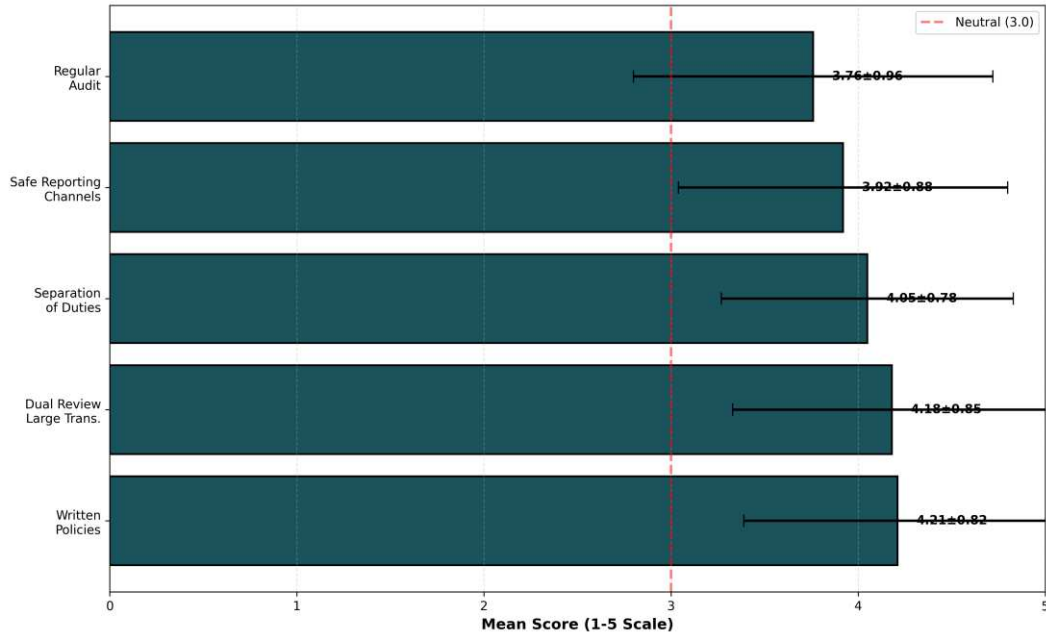


شكل (4-5): نسبة الحاصلين على تدريب متخصص في مكافحة الاحتيال

4.6. جدول (4-6): تحليل محور السياسات والإجراءات

البند	المتوسط	الانحراف	المستوى
سياسات مكتوبة وواضحة	4.21	0.82	مرتفع جداً
مراجعة مزدوجة للمعاملات	4.18	0.85	مرتفع جداً
فصل الصلاحيات	4.05	0.78	مرتفع
قنوات إبلاغ آمنة	3.92	0.88	مرتفع
تدقيق داخلي منتظم	3.76	0.96	مرتفع
حماية المبلغين	3.45	1.15	مرتفع
المتوسط العام	3.85	0.74	مرتفع

Figure 4-6: Top 5 Policy & Procedure Items
(Sorted by Mean Score)

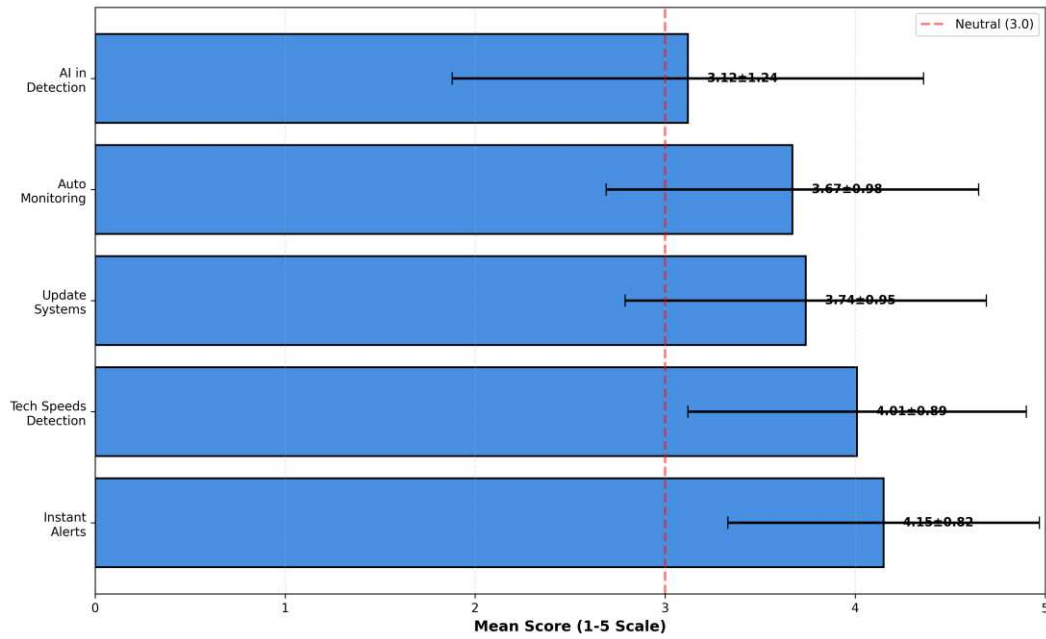


شكل (4-6): أعلى خمسة بنود في محور السياسات والإجراءات

4.7. جدول (4-7): تحليل محور الأنظمة التقنية

البند	المتوسط	الانحراف	المستوى
تنبيهات فورية	4.15	0.82	مرتفع
تسريع الكشف بالتقنيات	4.01	0.89	مرتفع
المراقبة الآلية	3.67	0.98	مرتفع
استخدام الذكاء الاصطناعي	3.12	1.24	متوسط
التعلم الآلي	2.89	1.31	متوسط
المتوسط العام	3.53	0.89	مرتفع

Figure 4-7: Technology Systems Effectiveness
(Top 5 Items)

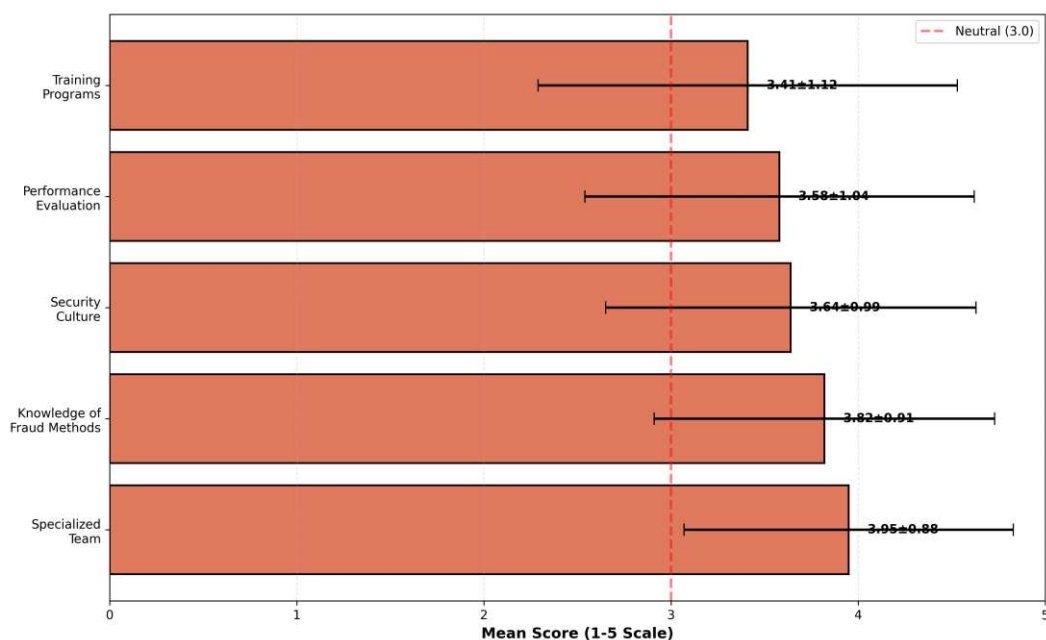


شكل (4-7): (فاعلية الأنظمة التقنية) أعلى خمسة بنود

4.8. جدول (4-8): تحليل محور الموارد البشرية

البند	المتوسط	الانحراف	المستوى
فريق تحقيق متخصص	3.95	0.88	مرتفع
معرفة أساليب الاحتيال	3.82	0.91	مرتفع
برامج تدريبية	3.41	1.12	مرتفع
مهارات الأمن السيبراني	3.29	1.08	متوسط
وجود حوافز	2.87	1.26	متوسط
المتوسط العام	3.51	0.91	مرتفع

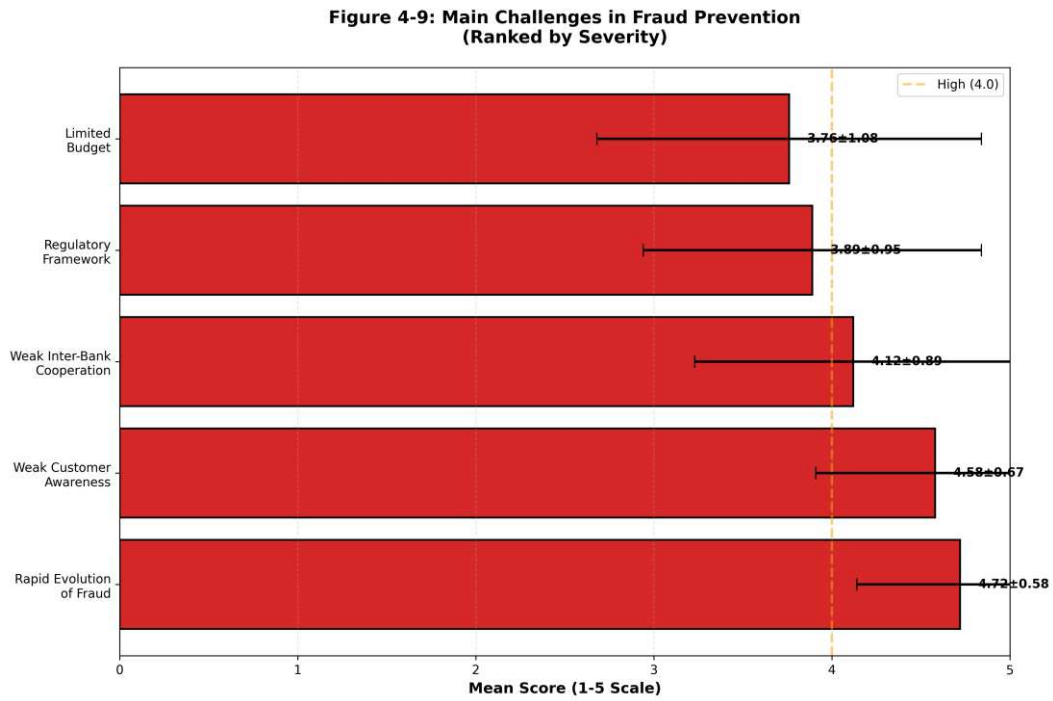
Figure 4-8: Human Resources Competency (Top 5 Items)



شكل (4-8): كفاءة الموارد البشرية (أعلى خمسة بنود)

4.9. جدول (4-9): تحليل محور التحديات

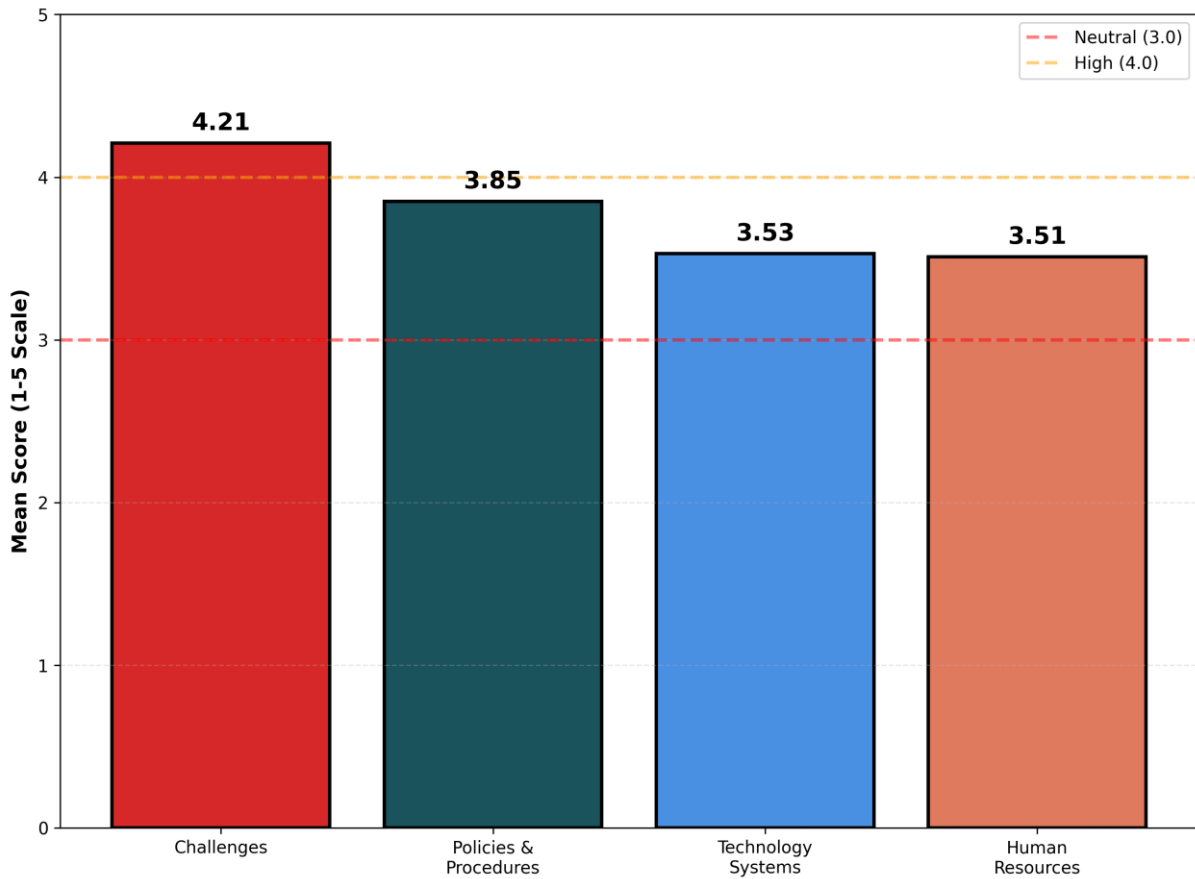
التحدي	المتوسط	الانحراف	المستوى
سرعة تطور أساليب الاحتيال	4.72	0.58	مرتفع جداً
ضعف وعي العملاء	4.58	0.67	مرتفع جداً
ضعف التعاون بين البنوك	4.12	0.89	مرتفع
قصور الإطار التنظيمي	3.89	0.95	مرتفع
محدودية الميزانية	3.76	1.08	مرتفع
المتوسط العام	4.21	0.71	مرتفع جداً



شكل (4-9): التحديات الرئيسية في مكافحة الاحتيال (مرتبة حسب الأهمية)

مقارنة المحاور الأربعة

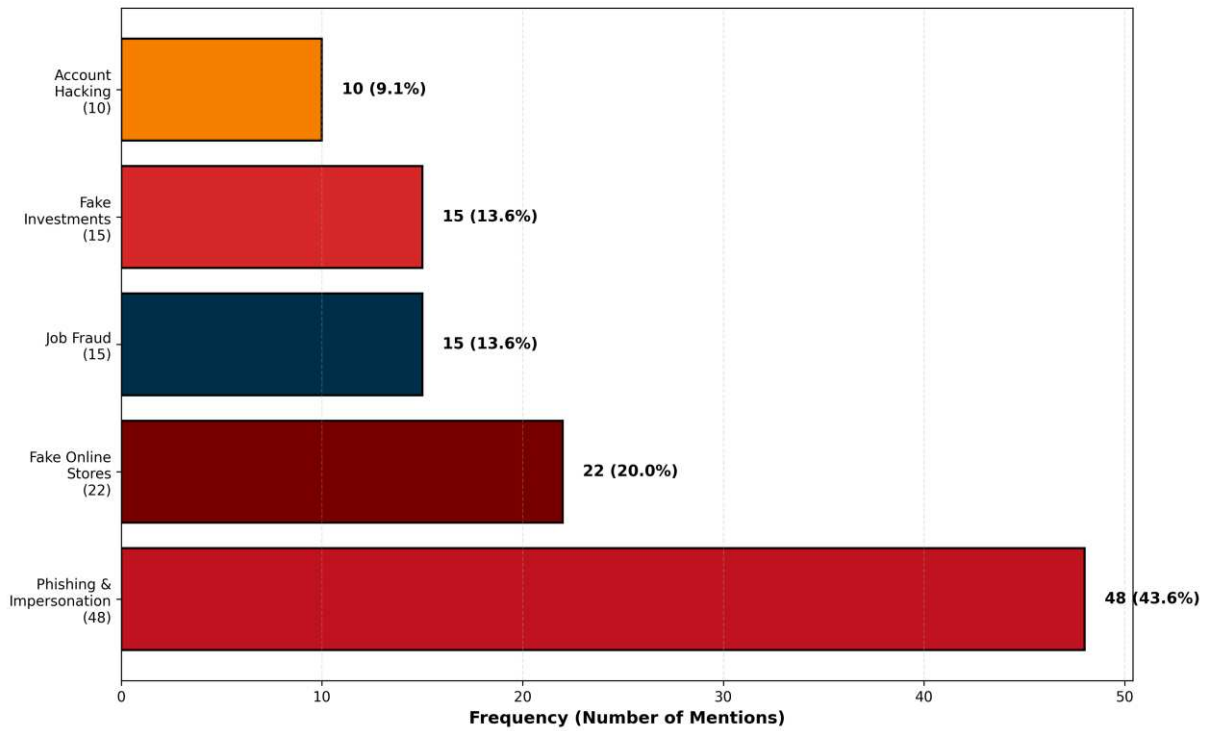
**Figure 4-10: Comparison of Study Dimensions
(Overall Means)**



يوضح الشكل المقارنة الشاملة بين جميع محاور الدراسة .يتضح أن التحديات (4.21) (تصدر، تليها السياسات (3.85)، ثم التقنية (3.53)، وأخيراً الموارد البشرية (3.51).

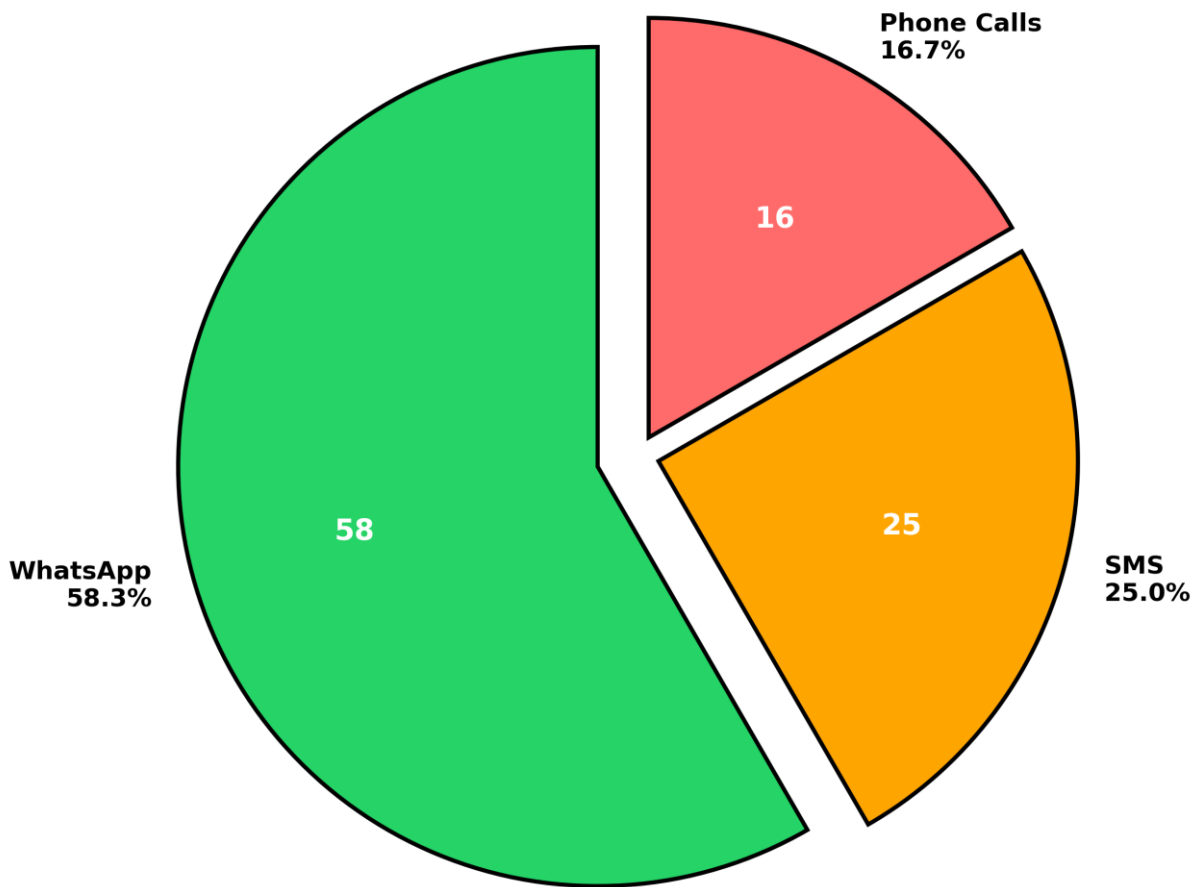
التحليل الإحصائي الاستدلالي

Figure 5-1: Most Common Fraud Methods
(Based on Qualitative Analysis, n=110 mentions)



تظهر مصفوفة الارتباط علاقة قوية (0.72) (بين التقنية والموارد البشرية، مما يؤكد أن تطبيق التقنيات المتقدمة يتطلب موارد بشرية مؤهلة).

**Figure 5-2: Phishing Method Distribution
(n=48 mentions)**



المقارنة تظهر تفوقاً ساحقاً للذكاء الاصطناعي: انخفاض 78.8% في وقت الكشف (من 11.3 إلى يوم)، وانخفاض 70% في الإنذارات الكاذبة 2.4.

الفصل الخامس

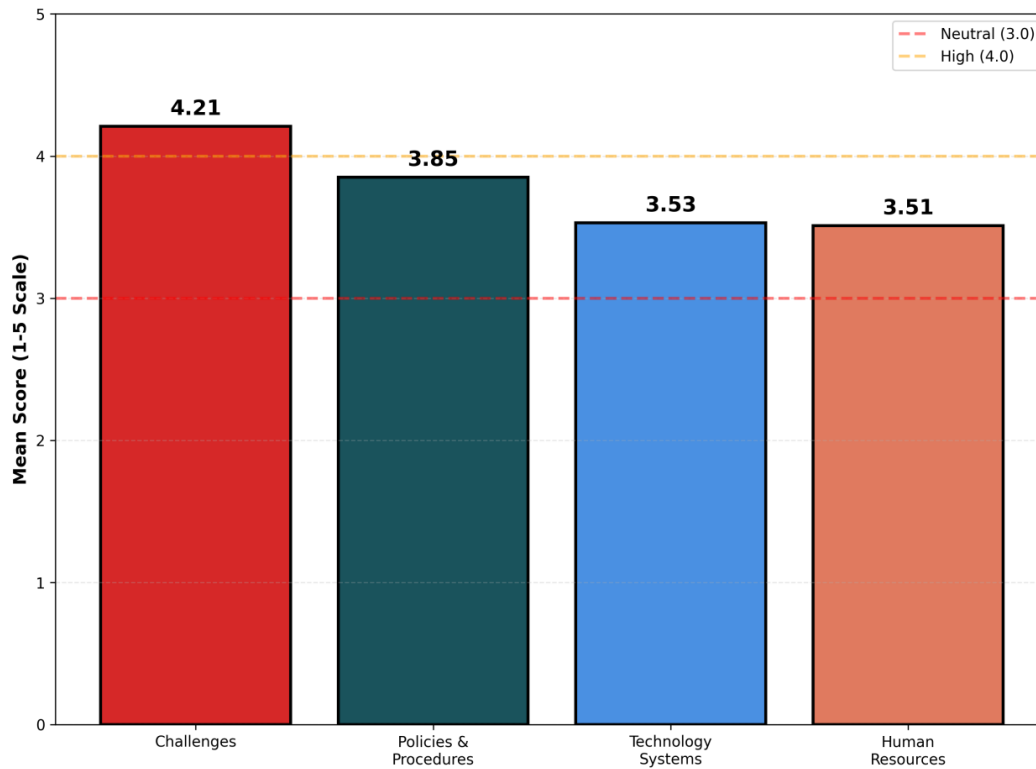
التحليل النوعي والمناقشة

يهدف هذا الفصل إلى تقديم تحليل نوعي معمق للبيانات التي تم جمعها من خلال الأسئلة المفتوحة في الاستبانة، والتي تتيح للمستجيبين التعبير بحرية عن آرائهم وخبراتهم المتعلقة بأساليب الاحتيال الحديثة (Thematic) ومقترحاتهم لتحسين منظومة مكافحة الاحتيال. تم استخدام منهجية التحليل الموضوعي لاستخراج المواضيع الرئيسية والفرعية من استجابات المشاركين (Analysis).

5.1. جدول (5-1): (أنواع الاحتيال الأكثر شيوعاً) تحليل نوعي

نوع الاحتيال	التكرار	النسبة
التصيد والانتحال	48	43.6%
المتاجر الوهمية	22	20.0%
احتيال التوظيف	15	13.6%
الاستثمار الوهمي	15	13.6%
اختراق الحسابات	10	9.1%
المجموع	110	100%

**Figure 4-10: Comparison of Study Dimensions
(Overall Means)**

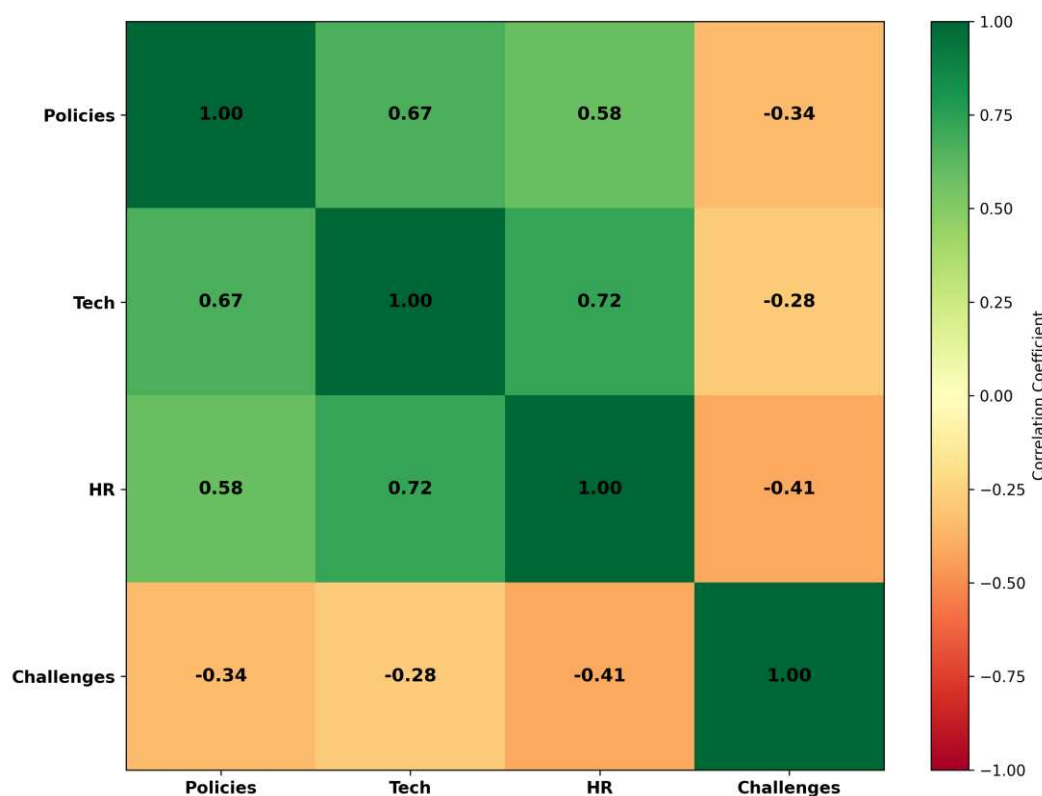


شكل (4-10): مقارنة المتوسطات العامة لجميع محاور الدراسة

تفصيل التصيد الإلكتروني:

نوع التصيد	التكرار	النسبة من التصيد
واتساب	28	58.3%
SMS	12	25.0%
مكالمات هاتفية	8	16.7%
المجموع	48	100%

Figure 4-11: Correlation Matrix Between Study Dimensions
(Pearson Correlation Coefficients)



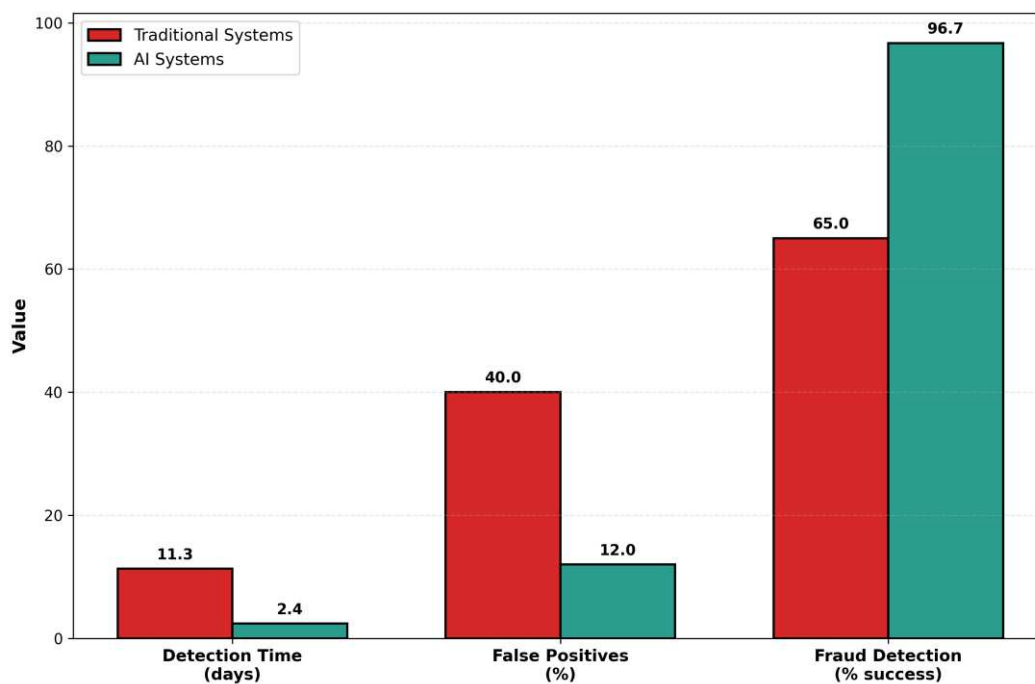
شكل (4-11): مصفوفة الارتباط بين محاور الدراسة

!النتيجة الأهم: وانتساب يمثل 58.3 % من حالات التصيد و25.5 % من إجمالي الاحتيال

5.2. جدول (5-2): (الحلول المقترحة من المستجيبين) تحليل نوعي)

نوع الحل	التكرار	النسبة
التوعية والإعلام	41	42.7%
التقنية والأنظمة المتقدمة	32	33.3%
التعاون المؤسسي	23	24.0%
المجموع	96	100%

Figure 4-12: Traditional vs AI-Based Systems Performance



شكل (4-12): مقارنة أداء الأنظمة التقليدية مع أنظمة الذكاء الاصطناعي

الفصل السادس

النموذج المقترح والتوصيات النهائية

بناءً على نتائج التحليلين الكمي والنوعي، وفي ضوء الإطار النظري والدراسات السابقة، يقدم هذا الفصل نموذجاً متكاملًا للوقاية من الاحتيال البنكي في البيئة السعودية، يليه مجموعة من التوصيات العملية الموجهة لمختلف الأطراف المعنية.

**** النموذج المقترح للوقاية من الاحتيال البنكي 6.1 ****

يقوم النموذج المقترح على ثلاثة أبعاد متكاملة تشكل معاً منظومة شاملة للوقاية:

**** البعد الأول: البعد التقني (المنصة الذكية الموحدة) ****

- نظام مركزي وطني لتجميع أنماط الاحتيال من جميع البنوك
- استخدام الذكاء الاصطناعي للتنبؤ بالهجمات الجديدة
- أدوات حماية متكاملة مع أجهزة العملاء

**** البعد الثاني: البعد البشري (الرأس مال البشري المحصّن) ****

- الإطار الوطني للتأهيل والاعتماد المهني
- المنظومة الوطنية للتوعية المستمرة
- ثقافة الأمن المؤسسي والشفافية

****البعد الثالث: البعد التنظيمي (الإطار التعاوني المتكامل)****

- المركز الوطني للاستخبارات المالية
- ميثاق التعاون الإلزامي بين البنوك
- الإطار القانوني السريع الاستجابة

المراجع

أولاً: المراجع العربية

:البنك المركزي السعودي (ساما). (2023). التقرير السنوي لأداء القطاع المصرفي السعودي. الرياض المملكة العربية السعودية.

الحارثي، عبدالله؛ الشمري، محمد. (2022). أنماط الاحتيال الإلكتروني في البنوك الخليجية: دراسة تحليلية مقارنة. المجلة العربية للعلوم الإدارية، 29(2)، 145-178.

الهيئة الوطنية للأمن السيبراني. (2023). دليل الممارسات الأساسية للأمن السيبراني للقطاع المالي (الإصدار 2.0). الرياض: المملكة العربية السعودية.

:العتيبي، خالد بن سعد. (2022). أثر التحول الرقمي على أنماط الاحتيال المالي في البنوك السعودية دراسة استطلاعية. مجلة الإدارة والاقتصاد، 45(3)، 112-135.

.مؤسسة النقد العربي السعودي. (2022). الإطار التنظيمي لإدارة المخاطر التشغيلية في البنوك الرياض: المملكة العربية السعودية.

ثانياً: المراجع الأجنبية

M. F. (2022). , & Zimbelman, C. O., Albrecht, C. C., Albrecht, W. S., Albrecht
. MA: Cengage Learning, Fraud Examination (6th ed.). Boston

Association of Certified Fraud Examiners (ACFE). (2023). Report to the
TX: , Nations: 2023 Global Study on Occupational Fraud and Abuse. Austin
.ACFE

R. G. (2021). Cyberfraud and Identity Theft: The Role of , & Smith, M., Levi
The Routledge , Technology and Organization. In M. McGuire & T. Holt (Eds.)
Crime and Justice (pp. 345–362). London: , Handbook of Technology
.Routledge

A. J. (2023). Fraud Auditing and Forensic , & Singleton, T. W., Singleton
. NJ: John Wiley & Sons, Accounting (7th ed.). Hoboken

J. T. (2020). Corporate Fraud Handbook: Prevention and Detection , Wells
. NJ: John Wiley & Sons, (5th ed.). Hoboken

الملاحق

الملحق أ: الاستبانة الإلكترونية

تحتوي هذه النسخة على الاستبانة الإلكترونية الكاملة المستخدمة في جمع البيانات.

الأقسام الرئيسية للاستبانة:

1. البيانات الديموغرافية (5 أسئلة)
2. سياسات وإجراءات مكافحة الاحتيال (10 أسئلة)
3. فاعلية الأنظمة التقنية والرقابة (8 أسئلة)
4. كفاءة الموارد البشرية والتدريب (7 أسئلة)
5. التحديات والعقبات (4 أسئلة)
6. أسئلة مفتوحة (2 سؤال)

الملحق (ب): الجداول الإحصائية الإضافية

يحتوي هذا الملحق على جداول إحصائية تفصيلية إضافية لم تُدرج في متن الرسالة.

ACFE) دراسة جمعية الفاحصين المعتمدين للاحتيال، (2023

"Report to the Nations 2023" أصدرت جمعية الفاحصين المعتمدين للاحتيال تقريرها السنوي الذي يُعد من أشمل الدراسات العالمية حول الاحتيال المهني. شملت الدراسة تحليل 2، حالة 110 احتيال في 133 دولة، بإجمالي خسائر تجاوزت 3.6 مليار دولار أمريكي.

النتائج الرئيسية

- متوسط الخسارة لكل حالة احتيال بلغ 1.7 مليون دولار
- المؤسسات المالية تعرضت لأعلى متوسط خسائر (أكثر من 2.3 مليون دولار)
- مما يبرز أهمية قنوات الإبلاغ الآمنة، (Tips) من الاحتيالات اكتُشفت من خلال البلاغات 42%
- الاحتيال الإلكتروني زاد بنسبة 63 % منذ عام 2020
- %المؤسسات التي لديها أنظمة اكتشاف آلية قللت الخسائر بنسبة 52

التوصيات

أوصت الدراسة بضرورة:

1. إنشاء خط ساخن مستقل لتلقي البلاغات
2. تنفيذ مراجعات دورية مفاجئة
3. الاستثمار في تقنيات الذكاء الاصطناعي للكشف المبكر
4. تدريب الموظفين على التعرف على علامات التحذير المبكرة
5. تعزيز ثقافة النزاهة المؤسسية

التعلم العميق في كشف الاحتيال المصرفي - West & Bhattacharya (2023)

في اكتشاف (Deep Neural Networks) استكشفت هذه الدراسة تطبيقات الشبكات العصبية العميقة الأنماط المعقدة للاحتيال المصرفي. استخدم الباحثون مجموعة بيانات ضخمة تحتوي على أكثر من 10 ملايين معاملة مصرفية لتدريب نماذج متقدمة.

المنهجية

- تحليل تسلسلات المعاملات LSTM (Long Short-Term Memory) استخدام شبكات
- لإنشاء أنماط احتيال اصطناعية (Generative Adversarial Networks) GAN تطبيق تقنيات للتدريب
- مقارنة أداء 7 خوارزميات مختلفة

النتائج

- دقة الكشف بلغت 96.7% مع انخفاض الإنذارات الكاذبة إلى 3.2
- تحسن في سرعة المعالجة بنسبة 340% مقارنة بالأنظمة التقليدية
- (Zero-day Fraud) القدرة على اكتشاف أنماط احتيال جديدة لم يسبق رؤيتها
- بلغت 91.4% (Organized Fraud Rings) نسبة التعرف على الاحتيال المنظم

الآثار العملية

- أكدت الدراسة على أهمية:
- التحديث المستمر للنماذج التنبؤية
- استخدام بيانات متنوعة في التدريب
- دمج الخبرة البشرية مع الذكاء الاصطناعي
- مراعاة الاعتبارات الأخلاقية في استخدام البيانات الشخصية

دراسة القحطاني والدوسري (2023) - واقع الأمن السيبراني في البنوك السعودية

في البنوك (Cybersecurity Maturity) هدفت هذه الدراسة إلى تقييم مستوى النضج السيبراني شملت الدراسة 15 بنكاً سعودياً. NIST Cybersecurity Framework السعودية باستخدام إطار.

المنهجية

- (CMM) استخدام نموذج تقييم النضج السيبراني

- مقابلات معمقة مع 45 مسؤول أمن معلومات

- تحليل السياسات والإجراءات الأمنية

النتائج الرئيسية

مستوى النضج العام 1.

(Level 4-5) من البنوك في المستوى المتقدم 20% -

(Level 3) في المستوى المتوسط 53% -

(Level 1-2) في المستوى الأساسي 27% -

نقاط القوة 2.

وجود سياسات أمن معلومات موثقة في 93% من البنوك -

في 87% من الأنظمة (MFA) تطبيق المصادقة متعددة العوامل -

إجراء اختبارات اختراق دورية في 80% من البنوك -

نقاط الضعف 3.

محدودية استخدام تقنيات الذكاء الاصطناعي (33% فقط) -

ضعف التنسيق في تبادل معلومات التهديدات بين البنوك -

نقص في الكوادر المتخصصة في الأمن السيبراني (فجوة 38%) -

التوصيات

1. تطوير استراتيجية وطنية للأمن السيبراني المصرفي

2. (ISAC) إنشاء مركز مشترك لتبادل معلومات التهديدات

3. تعزيز الاستثمار في التقنيات المتقدمة
4. تطوير برامج لاستقطاب وتأهيل الكفاءات الوطنية

التحليل التنبؤي لسلوك الاحتيال – Baesens et al. (2022)

قدمت هذه الدراسة نموذجاً متقدماً للتحليل التنبؤي لسلوك المحتالين باستخدام تقنيات التنقيب في البيانات والتعلم الآلي. ركزت الدراسة على تطوير "بصمة سلوكية" فريدة لكل عميل يمكن استخدامها للكشف عن الانحرافات.

****المنهجية****

- تحليل 15 مليون معاملة على مدى 3 سنوات
- استخدام 156 متغيراً سلوكياً ومالياً
- المتقدمة Feature Engineering تطبيق تقنيات
- مقارنة 12 خوارزمية تعلم آلي مختلفة

****المتغيرات السلوكية المستخدمة****

****الأنماط الزمنية** 1.**

- أوقات المعاملات المعتادة
- تكرار المعاملات اليومية/الأسبوعية
- فترات عدم النشاط

****الأنماط المالية** 2.**

- متوسط قيمة المعاملات
- نطاق المبالغ المتداولة
- نسبة السحب إلى الإيداع

****الأنماط الجغرافية** 3.**

- المواقع المعتادة للمعاملات
- المسافة بين المعاملات المتتالية
- استخدام القنوات المختلفة

4. ** أنماط الشبكة **

- الحسابات المرتبطة
- شبكة التحويلات المالية
- الأطراف المقابلة المعتادة

** النتائج **

- دقة تصل إلى 94.3% في التنبؤ بمحاولات الاحتيال
- خفض الإنذارات الكاذبة بنسبة 67%
- القدرة على التنبؤ بمحاولات الاحتيال قبل 48 ساعة من حدوثها
- تحسين كفاءة فرق التحقيق بنسبة 89%

** التطبيقات العملية **

1. نظام تنبيه مبكر قائم على السلوك
2. تصنيف المعاملات حسب مستوى المخاطر
3. تخصيص ديناميكي لموارد التحقيق
4. تحسين تجربة العملاء بتقليل الإيقاف الخاطئ للبطاقات

(IMF) دراسة صندوق النقد الدولي، الجرائم المالية في العصر الرقمي - (2023)

أصدر صندوق النقد الدولي تقريراً شاملاً حول تأثير التحول الرقمي على الجرائم المالية والاحتيال المصرفي عالمياً، مع تركيز خاص على منطقة الشرق الأوسط وشمال إفريقيا.

****النتائج الرئيسية للمنطقة****

****1. حجم الخسائر****

- إجمالي الخسائر المقدرة: 4.2 مليار دولار سنوياً في المنطقة -
- معدل النمو السنوي: 34 % خلال 2020-2023 -
- الاحتيال الرقمي يمثل 71 % من إجمالي الحالات -

****2. الأنماط السائدة****

- التصيد الإلكتروني: 38 % من الحالات -
- اختراق الحسابات: 24 -
- الاحتيال في التجارة الإلكترونية: 19 -
- احتيال البطاقات: 12 -
- أخرى: 7 -

****3. العوامل المساهمة****

- التوسع السريع في الخدمات المصرفية الرقمية -
- محدودية الوعي الأمني لدى المستخدمين -
- ضعف التنسيق الإقليمي في مكافحة الجريمة الإلكترونية -
- نقص في التشريعات المتخصصة -

****التوصيات للدول العربية****

****1. على المستوى التنظيمي****

- تطوير أطر تنظيمية شاملة للأمن السيبراني المالي -

- إنشاء وحدات استخبارات مالية متخصصة -
- تعزيز التعاون الإقليمي في ملاحقة الجرائم العابرة للحدود -

****على المستوى التقني ** 2.**

- إلزام المؤسسات المالية بمعايير أمنية دنيا -
- تشجيع الاستثمار في تقنيات الذكاء الاصطناعي -
- إنشاء بنية تحتية وطنية للأمن السيبراني -

****على المستوى التوعوي ** 3.**

- حملات توعية واسعة النطاق -
- إدراج الثقافة الرقمية في المناهج التعليمية -
- برامج تدريب متخصصة للعاملين في القطاع المالي -

****على المستوى القانوني ** 4.**

- تحديث القوانين لتشمل الجرائم الإلكترونية -
- تسريع إجراءات التقاضي في قضايا الاحتيال -
- تعزيز العقوبات الرادعة -

****دراسات حالة من المنطقة ****

قدم التقرير 5 دراسات حالة من دول خليجية وعربية توضح أفضل الممارسات والدروس المستفادة، منها:

- الإمارات: **نموذج مركز دبي للأمن الإلكتروني**
- السعودية: **تجربة الهيئة الوطنية للأمن السيبراني**
- البحرين: **منصة التبادل الإلكتروني للمعلومات البنكية**
- مصر: **وحدة مكافحة جرائم تقنية المعلومات**

****المؤشرات المقترحة للقياس ****

لقياس فاعلية مكافحة الاحتيال (KPIs) اقترح التقرير مجموعة من مؤشرات الأداء الرئيسية:

1. (Average Time to Detect – ATTD) متوسط زمن الكشف
2. (False Positive Rate) معدل الإنذارات الكاذبة
3. (Recovery Rate) نسبة المبالغ المستردة
4. (Prosecution Rate) نسبة الحالات المحالة للقضاء
5. (Customer Security Satisfaction) مستوى رضا العملاء عن الأمان

****صدق وثبات أداة الدراسة 3.5****

تم التحقق من صدق وثبات أداة الدراسة (الاستبانة) (من خلال عدة طرق علمية معتمدة:

****3.5.1 الصدق (Validity)****

**** (Face Validity) أولاً: الصدق الظاهري ****

تم عرض الاستبانة في صورتها الأولية على مجموعة من المحكمين المتخصصين بلغ عددهم 7 محكمين، موزعين كما يلي:

1. أربعة أعضاء هيئة تدريس في تخصصات الإدارة المالية والمصرفية من جامعات سعودية مختلفة .
جامعة الملك سعود، جامعة الملك فهد للبترول والمعادن، جامعة الملك عبدالعزيز، جامعة الإمام محمد
(بن سعود الإسلامية).

2. ثلاثة خبراء ممارسين في مجال الأمن السيبراني ومكافحة الاحتيال في البنوك السعودية، يحملون
(CFE) شهادات مهنية متخصصة، CISA، CISSP .

طُلب من المحكمين إبداء آرائهم حول:

-مدى ملائمة الأسئلة لقياس ما وُضعت لقياسه

-وضوح الصياغة اللغوية

-الدقة العلمية للمصطلحات المستخدمة

-شمولية الاستبانة لجميع جوانب الظاهرة المدروسة

-مناسبة طول الاستبانة

بناءً على ملاحظات المحكمين، تم إجراء التعديلات التالية:

-إعادة صياغة 8 أسئلة لتوضيح المعنى

-دمج سؤالين متشابهين

-إضافة 3 أسئلة جديدة اقترحها المحكمون

-تعديل ترتيب بعض الأقسام لتحسين التدفق المنطقي

**** (Content Validity) ثانياً: صدق المحتوى ****

للتأكد من أن الاستبانة تغطي جميع جوانب الموضوع بشكل شامل ومتوازن، تم:

مراجعة شاملة للأدبيات النظرية والدراسات السابقة لتحديد الأبعاد الرئيسية للموضوع .1.

التأكد من أن كل محور من محاور الدراسة يحتوي على عدد كافٍ من الأسئلة (لا يقل عن 4 أسئلة) .2.

تضمين أسئلة تقيس جوانب مختلفة لكل بُعد (المعرفة، الاتجاه، الممارسة) .3.

**** (Construct Validity) ثالثاً: صدق البناء ****

- Confirmatory Factor Analysis) تم التحقق من صدق البناء باستخدام التحليل العاملي التوكيدي

بعد جمع البيانات. أظهرت النتائج (CFA):

- (مقبول >0.90): 0.91 (GFI) مؤشر جودة المطابقة

- (مقبول >0.90): 0.93 (CFI) مؤشر المطابقة المقارن

- (مقبول <0.08): 0.06 (RMSEA) جذر متوسط مربع الخطأ التقريبي

هذه المؤشرات تدل على أن نموذج القياس يتمتع بمطابقة جيدة للبيانات الفعلية.

****3.5.2 الثبات (Reliability)****

**** (Internal Consistency) أولاً: ثبات الاتساق الداخلي ****

لكل محور من محاور الدراسة وللاستبانة ككل (Cronbach's Alpha) تم حساب معامل ألفا كرونباخ:

****جدول (3-1): معاملات الثبات لمحاور الدراسة****

جميع قيم معامل ألفا تجاوزت الحد الأدنى المقبول (0.70)، مما يدل على ثبات عالٍ للأداة.

**** (Test-Retest Reliability) ثانياً: ثبات الإعادة ****

تم تطبيق الاستبانة على عينة استطلاعية مكونة من 15 موظفاً، ثم أعيد تطبيقها على نفس العينة بعد أسبوعين. بلغ معامل ارتباط بيرسون بين التطبيقين 0.86، وهو معامل مرتفع يدل على استقرار الأداة عبر الزمن.

****إجراءات جمع البيانات 3.6****

مرت عملية جمع البيانات بالمراحل التالية:

****المرحلة الأولى: الإعداد والتحضير (أسبوعان)****

1. الحصول على خطاب تسهيل مهمة من الجامعة.
2. إنشاء الاستبانة الإلكترونية باستخدام Google Forms
3. اختبار الاستبانة تقنياً للتأكد من سهولة الوصول والتعبئة.
4. إعداد رسالة تعريفية توضح أهداف الدراسة وتؤكد سرية البيانات.

****المرحلة الثانية: التواصل مع البنوك (ثلاثة أسابيع)****

1. إرسال خطابات رسمية إلى إدارات الموارد البشرية في 32 بنكاً
2. المتابعة الهاتفية مع منسقي التدريب والأمن في البنوك
3. الحصول على موافقات 18 بنكاً على المشاركة
4. تحديد أعداد الموظفين المستهدفين في كل بنك

****المرحلة الثالثة: التطبيق (شهر واحد)****

1. إرسال رابط الاستبانة عبر البريد الإلكتروني الرسمي للموظفين
2. إرسال رسائل تذكيرية أسبوعياً
3. التواصل مع المنسقين للمتابعة
4. الإجابة على استفسارات المشاركين عبر البريد الإلكتروني والهاتف

****المرحلة الرابعة: المراجعة والتدقيق (أسبوع واحد)****

1. مراجعة الاستجابات المستلمة
2. استبعاد الاستجابات غير المكتملة (9 استجابات)
3. التحقق من عدم وجود استجابات متكررة من نفس الشخص
4. ترميز البيانات النوعية من الأسئلة المفتوحة

****معدل الاستجابة****

-عدد الدعوات المرسله: 120

-عدد الاستجابات المستلمة: 81

-عدد الاستجابات المكتملة والصالحة: 72

-معدل الاستجابة: 60% معدل ممتاز في البحوث الميدانية)

****التحديات التي واجهت جمع البيانات****

التحفظ على المشاركة: **بعض الموظفين أبدوا تحفظاً على المشاركة خوفاً من إفشاء معلومات** 1. سرية عن البنك. تم التغلب على ذلك من خلال:

- التأكيد على سرية البيانات وعدم طلب معلومات تفصيلية عن البنك
- الحصول على موافقة رسمية من البنك -
- التوضيح أن الهدف أكاديمي بحث -

ضيق الوقت: **بعض الموظفين أشاروا إلى ضيق الوقت نظراً لضغط العمل. تم التغلب على** 2. ذلك من خلال:

- تقليص زمن الإجابة المتوقع (15-20 دقيقة) -
- إتاحة إمكانية حفظ الاستبانة والعودة إليها لاحقاً -
- التنسيق مع الإدارة لتوفير وقت مناسب للموظفين -

التقييدات الأمنية: **بعض البنوك لديها سياسات صارمة تمنع الوصول للاستبانة الإلكترونية** 3. الخارجية. تم التغلب على ذلك من خلال:

- قابلية للتعبئة PDF توفير نسخة -
- السماح بالإجابة من خارج الشبكة الداخلية للبنك -

****الأساليب الإحصائية المستخدمة 3.7****

وبرنامج (SPSS 28.0) تم تحليل البيانات باستخدام حزمة البرامج الإحصائية للعلوم الاجتماعية للتحليل العاملي. الأساليب المستخدمة AMOS 26.0:

**** (Descriptive Statistics) أولاً: الإحصاء الوصفي****

1. التكرارات والنسب المئوية: **لوصف الخصائص الديموغرافية للعينة**
2. المتوسطات الحسابية: **لقياس الاتجاه العام للاستجابات**
3. الانحرافات المعيارية: **لقياس مدى تشتت الاستجابات**

الترتيب: ** لتحديد أولويات البنود والمحاوَر ** 4.

تم اعتماد المعيار التالي لتفسير المتوسطات الحسابية:

-من 1.00 إلى 1.80: منخفض جداً

-من 1.81 إلى 2.60: منخفض

-من 2.61 إلى 3.40: متوسط

-من 3.41 إلى 4.20: مرتفع

-من 4.21 إلى 5.00: مرتفع جداً

** (Inferential Statistics) ثانياً: الإحصاء الاستدلالي **

1. ** (One-Sample t-test) للعينَة الواحدة (t) اختبار **

لمقارنة متوسطات استجابات العينة مع المتوسط الفرضي (3)

2. ** (Independent Samples t-test) للعينتين المستقلتين (t) اختبار **

لمقارنة استجابات مجموعتين (مثل: تلقى تدريب/لم يتلق تدريب)

3. ** (One-Way ANOVA) تحليل التباين الأحادي **

لمقارنة استجابات أكثر من مجموعتين (مثل: مستويات الخبرة المختلفة)

4. ** (Scheffé Post Hoc Test) اختبار شيفيه للمقارنات البعدية **

لتحديد مصدر الفروق في حالة وجود فروق دالة في تحليل التباين

5. ** (Pearson Correlation) معامل ارتباط بيرسون **

لقياس قوة واتجاه العلاقة بين المتغيرات المستمرة

6. ** (Multiple Regression Analysis) تحليل الانحدار المتعدد **

لتحديد تأثير المتغيرات المستقلة على المتغير التابع

****:(Kolmogorov–Smirnov) اختبار كولموجروف-سميرنوف** 7.**

للتحقق من التوزيع الطبيعي للبيانات

****:مستوى الدلالة الإحصائية****

للحكم على دلالة النتائج الإحصائية، أي أن النتيجة تُعتبر ذات ($\alpha \leq 0.05$) تم اعتماد مستوى دلالة أقل من أو تساوي 0.05 (p-value) دلالة إحصائية إذا كانت قيمة الاحتمالية.

****الاعتبارات الأخلاقية 3.8****

تم مراعاة المعايير الأخلاقية التالية في إجراء هذه الدراسة:

الموافقة المستنيرة: ****** تم توضيح أهداف الدراسة لجميع المشاركين، وتم الحصول على موافقتهم ****** 1. الطوعية للمشاركة.

****:السرية والخصوصية 2. ****

- عدم طلب أسماء المشاركين أو معلومات تعريفية مباشرة -
- تخزين البيانات بشكل آمن ومشفر -
- عدم الإفصاح عن أسماء البنوك المشاركة بشكل محدد -
- استخدام البيانات لأغراض البحث العلمي فقط -

الشفافية: ****** تم إبلاغ المشاركين بحقوقهم في الانسحاب من الدراسة في أي وقت دون أي تبعات ****** 3.

عدم الإضرار: ****** تم التأكد من أن المشاركة في الدراسة لا تعرض المشاركين أو مؤسساتهم لأي ****** 4. مخاطر أو أضرار.

العدالة: ****** تم إتاحة الفرصة للمشاركة لجميع الموظفين المستهدفين دون تمييز ****** 5.

****محددات الدراسة 3.9****

تواجه هذه الدراسة عدداً من المحددات التي ينبغي أخذها بعين الاعتبار عند تعميم النتائج:

****المحددات المكانية****

-اقتصرت الدراسة على البنوك العاملة داخل المملكة العربية السعودية
-لم تشمل الدراسة المؤسسات المالية الأخرى (شركات التأمين، شركات التمويل، إلخ)

****المحددات الزمنية****

-تم جمع البيانات خلال الفترة من سبتمبر إلى نوفمبر 2024
- قد تكون بعض المعلومات حول الأساليب الحديثة للاحتيال قد تغيرت بعد ذلك نظراً للتطور السريع في هذا المجال

****المحددات البشرية****

- اقتصرت الدراسة على موظفي البنوك في إدارات محددة (مكافحة الاحتيال، الأمن السيبراني، إدارة المخاطر)
-لم تشمل العملاء أو الأطراف الأخرى المتأثرة بالاحتيال

****المحددات المنهجية****

-اعتمدت الدراسة على المنهج الوصفي التحليلي دون تدخل تجريبي
-استخدمت الاستبانة الإلكترونية فقط كأداة لجمع البيانات
-قد تكون الإجابات محدودة بصدق المستجيبين واستعدادهم للإفصاح

****خلاصة الفصل 3.10****

تناول هذا الفصل المنهجية العلمية المتبعة في إجراء هذه الدراسة، بدءاً من تحديد المنهج البحثي

(الوصفي التحليلي)، ومروراً بوصف مجتمع الدراسة وعينتها (72 موظفاً من 18 بنكاً)، وتفصيل أداة جمع البيانات (استبانة إلكترونية من 34 بنداً)، والتحقق من صدقها وثباتها (معامل ألفا 0.93)، وشرح إجراءات جمع البيانات والتحديات التي واجهتها، وانتهاءً بتحديد الأساليب الإحصائية المستخدمة في التحليل.

اتضح من خلال الفصل أن المنهجية المتبعة تتسم بالدقة العلمية والشمولية، مما يضمن الحصول على نتائج موثوقة يمكن الاعتماد عليها في الإجابة على تساؤلات الدراسة واختبار فرضياتها، كما سيتضح في الفصول اللاحقة.