

دور إدارة مخاطر تكنولوجيا المعلومات في الحد من مخاطر المعاملات

المصرفية

(دراسة حالة على عملاء البنوك المصرفية في المملكة العربية السعودية)

الطلاب	أفنان المطيري	20212005091
	ريم القحطاني	20222005571
	عبدالله المطيري	20212005185
	أسامة هادي	20222005724
	نوف الشهراني	20222005554
	فيصل المطيري	20212005116
	العزوف العتيبي	20212005071
	عمر الحميدي	20212005048
قائد الفريق	وجدان المطيري	20212005126
إشراف	د. وليد سليمان	د. فاطمة مصطفى

شكروعرفان

بسم الله الرحمن الرحيم، والحمد لله رب العالمين الذي وفقنا وأعاننا على إنهاء هذا البحث والخروج به بهذه الصورة المتكاملة ، كما نتقدم بالشكر لكل من الدكتور وليد سليمان والدكتورة فاطمة مصطفى ، فأنتم أساس نجاح هذا البحث وخروجه على هذه الصورة المتقدمة .

كما نشكر عائلتنا التي ساندتنا وقدمت لنا الكثير من الدعم على جميع الأصعدة، ونشكر الزملاء وكل من قدم لنا الدعم المادي أو المعنوي .

ونسأل الله أن يوفقنا و يسدد خطانا وأن يؤتينا علما ينفعنا في الدنيا والآخرة .

قائمة المحتويات

الجزء	الفصل	المحتوى	رقم الصفحة
	التمهيد	• شكر وعرفان • قائمة المحتويات • قائمة الجداول	1 2 3
1	الفصل الأول مشكلة البحث	• المقدمة ومشكلة الدراسة • الدراسات السابقة والإطار النظري. • المنطلقات النظرية للدراسة • المنهجية وطرق البحث • أدوات الدراسة • مجالات الدراسة • الاطار الزمني للدراسة	4 6 10 11 11 11 11
2	الفصل الثاني الإطار النظري لمخاطر المعاملات المصرفية الإلكترونية	• مفهوم الخدمات المصرفية الإلكترونية • صور الخدمات المصرفية الإلكترونية. • أنواع المخاطر التي تتعرض لها البنوك من جراء الخدمات المصرفية الالكترونية. • أساليب مواجهة مخاطر تطبيق الإدارة الالكترونية في مجال الخدمات المصرفية .	12 12 14 17
3	الفصل الثالث الإطار النظري للاحتيالات البنكية وتطور الإدارة الإلكترونية في المملكة العربية السعودية	• (الاحتياالات البنكية)طرق متعددة لاختراق حسابات العملاء • واقع الاحتيال الإلكتروني في بيئة الأعمال السعودية • أبرز طرق الاحتيال المالي في المملكة العربية السعودية. • تطور النظام المصرفي في المملكة العربية السعودية	21 23 23 24
4	الفصل الرابع الدراسة العملية وإجراءاتها المنهجية	• استمارة الاستبانة وعينة الدراسة • اختبار ثبات الاستبانة • تحليل البيانات الديموغرافية لعينة الدراسة • المتوسطات والانحرافات المعيارية لمتغيرات الدراسة • اختبار فرضيات الدراسة • ملخص النتائج والتوصيات	26 27 28 29 34 36
5	ملاحق الدراسة	• قائمة المراجع العربية • قائمة المراجع الأجنبية • ملاحق الدراسة • ملخص البحث باللغة العربية • ملخص البحث باللغة الإنجليزية	38 39 40 42 43

قائمة الجداول

رقم الجدول	عنوان الجدول	رقم الصفحة
1	درجات قياس ليكرت الخماسي (Likert)	26
2	نتائج اختبار معامل الثبات بطريقة كرونباخ ألفا على محاور الدراسة المختلفة	27
3	نتائج البيانات الديموغرافية والشخصية لعينة الدراسة	28
4	أسئلة محور الإجراءات العملية في متغير إدارة مخاطر تكنولوجيا المعلومات	29
5	أسئلة محور الإجراءات الاحترازية في متغير إدارة مخاطر تكنولوجيا المعلومات	30
6	أسئلة محور الاحتمالات البنكية في متغير إدارة مخاطر تكنولوجيا المعلومات	32
7	أسئلة محور المتغير التابع (الحد من مخاطر المعاملات المصرفية)	33
8	نتائج اختبار تحليل الإنحدار الخطي المتعدد للتحقق من أثر إدارة مخاطر تكنولوجيا المعلومات على الحد من مخاطر المعاملات المصرفية	34

دور إدارة مخاطر تكنولوجيا المعلومات في الحد من مخاطر المعاملات المصرفية

المقدمة :

يعتبر موضوع إدارة المخاطر من الموضوعات التي استحوذت على اهتمام المؤسسات المالية و البنكية، وذلك لما شهدته الصناعة المالية و المصرفية من المشكلات و الأزمات المالية التي أدت إفلاس وإغلاق العديد منها، كما أن تزايد العولمة المالية و البنكية وانخراط المصارف في الأسواق المالية العالمية ، وتنامي سوق الائتمان البنكي وتنوعه من ناحية أخرى، كل هذه الأسباب أدت إلى زيادة المخاطر على البنوك والمصارف ولا سيما المخاطر المتعلقة بتقنية وتكنولوجيا المعلومات، خاصة وأن هذا القطاع يواجه مشكلة المخاطر التقنية أكثر من غيره.

وبما أن جميع البنوك والمصارف في عصرنا الحالي تعتبر من أساسات اقتصاد الدول. حيث تعتمد هذه البنوك على أنظمة تقنية لمعالجة وحفظ معلوماتها بحيث تستطيع أداء مهامها والمنافسة لتقديم مختلف خدماتها في أفضل صورة كخدمات الاونلاين وبطاقات الائتمان والعمليات الإلكترونية وغيرها. وعلى الرغم من الفوائد والمميزات هذه إلا أنه يوجد العديد من المخاطر التي تؤثر على مختلف مجالات البنك وهنا يأتي دور تحديد ومعرفة وإدارة المخاطر حيث تلعب إدارة المخاطر دوراً هاماً في حماية أصول المعلومات للبنوك، وبالتالي مهمتها، حيث تحميها من المخاطر المتعلقة بتكنولوجيا المعلومات.

تعتبر عملية إدارة المخاطر الفعالة مكوناً مهماً لتقنية المعلومات حيث يجب أن يكون الهدف الرئيسي لعملية إدارة المخاطر في المؤسسة (البنوك) هو حماية المؤسسة وقدرتها على أداء مهمتها، وليس فقط أصول تقنية المعلومات الخاصة بها.

مشكلة الدراسة :

لم تعد المخاطر للمصارف البنكية تقتصر على مخاطر التعثر الائتماني ومخاطر السوق فقط ، بل أصبح لدينا نوع جديد من المخاطر وهي مخاطر المعاملات المصرفية وخاصة المعاملات الإلكترونية الحديثة ، وهنا ظهرت الحاجة لتأسيس طرق جديدة للتعامل معها .

أهمية الدراسة :

- تعد إدارة مخاطر الخدمات المصرفية من إحدى المواضيع الهامة والجديرة بالإهتمام وتكمن أهميتها في مايلي :
- تعد هذه الدراسة خطوة تجاه فهم أعمق في مجال الخدمات المصرفية وتحليل مخاطرها وتأثيراتها ، حيث تدخل الصناعة المصرفية عصر تكنولوجيا جديد .
 - تعتبر عمليات تطوير وتحديث الخدمات المصرفية وسيلة يعتمد عليها المصرف من أجل الوصول إلى تحسين الأداء المادي .
 - تحسين مستوى الخدمات المصرفية في البنوك من أجل القدرة على المنافسة .

أهداف الدراسة :

تهدف هذه الدراسة إلى إعداد آلية فعالة للتعامل مع مخاطر تكنولوجيا المعلومات المستخدمة في المصارف البنكية وذلك لإحباط هذه المخاطر قبل حدوثها أو التخفيف من أثرها في حال وقوعها. وتشمل الأهداف الرئيسية لهذه الدراسة ما يلي:

- 1.إعداد إطار نظري يوضح طبيعة المخاطر المرتبطة بتكنولوجيا المعلومات والتي قد تتعرض لها المصارف البنكية
- 2.إعداد إطار نظري يمكن الجهات المعنية من التنبؤ بالمخاطر واعتماد إجراءات استباقية للتصدي لها.
- 3.اقتراح سلسلة إجراءات يمكن اتباعها في حال التعرض للخطر.
- 4.إصدار توصيات للجهات المعنية لحثهم على احترام مبادئ التصرف السليم الذي يقلل فرص التعرض للمخاطر.
- 5.إعداد مقترح يمكن الجهات المعنية من تقييم مدى قوة الإجراءات الاحترازية التي تتبعها المؤسسة المصرفية .

أسئلة الدراسة :

تسعى الدراسة إلى الإجابة على بعض الأسئلة المحورية التي من شأن الإجابة عليها إثراء الساحة العلمية وتطوير المعارف ذات الصلة بإدارة المخاطر المتعلقة بتكنولوجيا المعلومات المستخدمة في مجال الصيرفة البنكية، ومن أبرز من هذه التساؤلات ما يلي:

1. ماهي أبرز المخاطر التي قد تتعرض لها المؤسسات المصرفية البنكية؟
2. كيف يكمن التنبؤ بالمخاطر المرتبطة بتكنولوجيا المعلومات والتعاطي معها قبل حدوثها؟
3. ماهي الإجراءات العملية التي ينبغي اتباعها في حالة حدوث الخطر؟
4. ماهي أبرز الإجراءات الاحترازية التي ينبغي للمؤسسات المصرفية تبنيها؟
5. كيف يمكن تقييم فعالية أنظمة الأمان المرتبطة بتكنولوجيا المعلومات؟ من خلال الإجابة على هذه التساؤلات سيتمكن الباحثون المشرفون على هذه الدراسة من إعداد آلية فعالة لإدارة المخاطر المرتبطة بتكنولوجيا المعلومات المستخدمة في المصارف البنكية.

الدراسات السابقة :

لا يزال هناك نقص حاد في الدراسة البحثية التي تطرقت لموضوع إدارة مخاطر تكنولوجيا المعلومات المستخدمة في المصارف البنكية، لذلك ستشكل هذه الدراسة إضافة نوعية للمحتوى العلمي المتعلق بهذا المجال. فيما يلي بعض الدراسات التي تم نشرها في هذا السياق نوردتها موجزة لوضع إطار نظري لقبولة هذه الدراسة .

(1)دراسة :حميمش نرجس 2016-2017

- العنوان: دور تدقيق أنظمة تكنولوجيا المعلومات والاتصال في الحد من مخاطر المعاملات المصرفية الإلكترونية في الجزائر (حالة مجموعة من البنوك الجزائرية 2017)

- الهدف من الدراسة: التعرف على طبيعة وواقع المعاملات المصرفية الإلكترونية في الجزائر وتوضيح مختلف المخاطر الناتجة عنها ,وتوضيح مساهمة التدقيق في الحد من هذه المخاطر .

- اجراءات الدراسة: استخدمت الباحثة المنهج الوصفي على مجموع البنوك العمومية والخاصة ، عن طريق تحليل آراء العينة حول علاقة تدقيق أنظمة تكنولوجيا المعلومات والاتصال بمخاطر المعاملات المصرفية البنكية

- استنتاجات الدراسة: أن المعاملات المصرفية الإلكترونية في الجزائر لاتزال غير ناضجة ومتطورة مقارنة بالواقع العالمي لكونها حديثة عهد من جهة وعدم قوة المنافسة من جهة أخرى.

(2)دراسة: خالد محمود القطناني ٢٠٠٤

- العنوان: أثر خصائص البيئة التقنية وتكنولوجيا المعلومات في مخاطر الرقابة التشغيلية "دراسة تحليلية في المصارف الأردنية"

- الهدف من الدراسة: التعرف على بعض خصائص البيئة التقنية وتكنولوجيا المعلومات (الخصائص الإدارية، خصائص الملاءمة، خصائص الأمن والسلامة) وقياس مدى توافرها في المصارف الأردنية، بالإضافة إلى تحديد مدى تأثير هذه الخصائص في مخاطر الرقابة التشغيلية في المصارف الأردنية

- اجراءات الدراسة: استخدم الباحث المنهج الوصفي الاستقرائي فيما يتعلق بالبيانات الخاصة بالإطار النظري للدراسة ، أما بيانات الدراسة الميدانية فقد تم جمعها باستخدام أسلوب قائمة الاستقصاء (الاستبانة) التي تم تصميمها لأغراض الدراسة

- استنتاجات الدراسة: توصل الباحث الى أنه توجد فروق ذات دلالة إحصائية بين آراء العاملين في دوائر الرقابة الداخلية في المصارف الأردنية والمدققين الخارجيين لهذه المصارف بشأن مدى توافر خصائص البيئة التقنية والتكنولوجية لنظم المعلومات في المصارف الأردنية.

(3)دراسة: دراسة العازمي(2022)

-العنوان: دور تفعيل حوكمة تكنولوجيا المعلومات في تأمين المعلومات الحاسبية من المخاطر الإلكترونية في ظل عصر الرقمنة دراسة تطبيقية علي البنوك التجارية الكويتية."

-الهدف من الدراسة : ركزت هذه الدراسة على المخاطر التي تشكل تهديدا حقيقيا لأنظمة تكنولوجيا المعلومات المستخدمة في المصارف البنكية كما تناولت أيضا مصادر هذه المخاطر ومعدلات حدوثها

- اجراءات الدراسة : يعتمد البحث على إتباع كل من المنهج الاستقرائي والمنهج الاستنباطي حيث تتبع المنهج

الاستقرائي في تحديد الأبعاد المختلفة لحوكمة تكنولوجيا المعلومات ودورها في تأمين المعلومات الحاسبية

في ضوء إدارة المخاطر الإلكترونية في البنوك الكويتية محل الدراسة من خلال استقراء البحوث والكتابات

والرسائل والدوريات العلمية. كما يتم استخدام المنهج الاستنباطي من خلال تفسير وتحليل نتائج البيانات والإطار النظري لدور حوكمة تكنولوجيا المعلومات في تأمين المعلومات الحاسبية في ضوء إدارة المخاطر الإلكترونية في البنوك الكويتية من خلال دراسة تطبيقية على البنوك الكويتية باستخدام التقارير والقوائم المالية والنشرات الإحصائية المنشورة.

- استنتاجات الدراسة: وأوصى العازمي في ختام دراسته بعدة أمور من أبرزها توفير إجراءات أمان حماية كافية للوقاية من فيروسات الحاسوب، تأهيل الموظفين وإكسابهم الخبرة اللازمة للتعاطي مع المخاطر، واستخدام أحدث التقنيات لتقييم أنظمة الأمان.

(4)دراسة: سلطاني و صفيح (2022)

-العنوان: " إدارة مخاطر الخدمات المصرفية الإلكترونية في المصارف الإسلامية: دراسة حالة مصرف الراجحي السعودي"

-الهدف من الدراسة : واقع إدارة المخاطر التي قد تتعرض لها الخدمات المصرفية الإلكترونية وخاصة الإسلامية منها، واقتصرت الدراسة على بنك الراجحي السعودي

- إجراءات الدراسة: تم الاعتماد على المنهج الوصفي التحليلي للإحاطة بالجوانب المتعلقة بالمصارف الإسلامية والمخاطر التي تتعرض لها، إضافة إلى ما يتعلق بالخدمات المصرفية الإلكترونية ومخاطرها، كما تم الاعتماد أيضا على أسلوب دراسة الحالة للتعرف على واقع الخدمات المصرفية الإلكترونية في المصارف الإسلامية وواقع إدارة المخاطر التي تصاحبها.

- استنتاجات الدراسة: توصلت الدراسة إلى عدت نتائج من أبرزها نجاح بنك الراجحي في تطبيق إجراءات أمن تكنولوجيا المعلومات المقترحة من طرف لجنة بازل في ما يخص الصيرفة الإلكترونية، كما خلص الباحثان إلى أن المصارف الإسلامية تتبنى أساليب وقائية وأخرى علاجية ناجحة في حالة حدوث الخطر. إضافة إلى ذلك توصل الباحثان إلى أن خدمات الصيرفة الإلكترونية لا تأتي بمخاطر جديدة لكنها قد تؤثر سلبا على المخاطر المتعلقة بالعمليات التشغيلية، الأهداف الإستراتيجية و الوضعية القانونية وكذلك السمعة. ومما أوصى به الباحثان الاستثمار في تكنولوجيا المعلومات، ضرورة وجود أقسام داخلية معنية بتكنولوجيا المعلومات للاستغناء عن خدمات الأطراف الخارجية، زيادة دورات التكوين على تكنولوجيا المعلومات، تنظيم دورات تحسيسية لتعريف الموظفين على أهمية وكيفية التعااطي مع الخدمات المصرفية الإلكترونية.

(5)دراسة: ليندكفيست و خيلتاش (2022)

- العنوان: "أثر الذكاء الاصطناعي على مقاربة المصارف لإدارة المخاطر

- الهدف من الدراسة: سعت الدراسة إلى الإجابة على سؤالين جوهريين هما:

• كيف يمكن للمؤسسات في القطاع المصرفي التخفيف من المخاطر التي تنطوي عليها حلول الذكاء الاصطناعي وفقاً لإطار إدارة المخاطر الديناميكي؟

• كيف يؤثر تطبيق الذكاء الاصطناعي على إدارة المخاطر في البنوك من منظور متعدد المستويات؟

- إجراءات الدراسة: استخدمت الدراسة إطارين نظريين لتحليل البيانات. تم استخدام الإطار الأول، وهو الإطار الديناميكي لإدارة المخاطر، لتحليل التغيرات في عملية إدارة المخاطر استنادا إلى موقعها الفريد داخل المجتمع.

أعطى الإطار الثاني، المنظور متعدد المستويات، الدراسة فهما شاملا لتأثير الذكاء الاصطناعي كمحرك للتحويل الاجتماعي والتقني.

- استنتاجات الدراسة: وتوصل الباحثان إلى أن إدخال الذكاء الاصطناعي في الأنظمة المصرفية يؤدي إلى التعرف على المزيد من المخاطر التي يجب التعاطي معها. كما يبرز التحليل الحاجة على مزيد من التكامل الرأسي داخل المنظمة ، حيث تتوفر الكفاءات التي يمكن الاستفادة منها أثناء فحص المخاطر.

المنطلقات النظرية للدراسة :

تعد إدارة المخاطر من أهم الأمور التي تضعها المؤسسات المصرفية على رأس أولوياتها لما لها من بالغ الأثر في نجاح المصرف وديمومة خدماته. ويعرف الباحث يوسف (2008) إدارة المخاطر على أنها " كافة الاجراءات التي تقوم بها إدارات المصارف من أجل وضع حدود للأثار السلبية الناجمة عن تلك المخاطر." وتتشعب هذه المخاطر إلى عدة أنواع من ضمنها المخاطر التشغيلية والمخاطر الائتمانية والمخاطر السياسية والاجتماعية والتكنولوجية. في هذه الدراسة ستركز البحث على مخاطر تكنولوجيا المعلومات وكيفية إدارتها. وتعتبر تكنولوجيا المعلومات العمود الفقري للمعاملات المصرفية والبنية التحتية التي لا غنى عنها لمزاولة العمليات التشغيلية وكذلك لا غنى عنها لتأمين المصرف وخدماته. ويؤكد هذا ما قاله الباحثان شارما و ميتال (2018) حيث قالوا أن النمو التطور في مجال التكنولوجيا أديا إلى تحول محوري في العمليات والأنظمة المصرفية كافة، ويضيف شارما و ميتال أن الاستخدام الفعال نجح في تسهيل إدارة المعاملات المصرفية بشكل دقيق وفعال خاصة في البنوك ذات قاعدة عملاء كبيرة.

أن الدور المحوري الذي تلعبه تكنولوجيا المعلومات في قطاع المصارف البنكية يجعل من الحتمي وضع آلية فعالة لإدارة المخاطر المرتبطة بهذه التكنولوجيا ومن أبرز مسؤوليات إدارة مخاطر عمليات تكنولوجيا المعلومات حسب ما أوردته الوكالة الفيدرالية لتمويل الإسكان (2017) ما يلي:

- تحديد مخاطر تكنولوجيا المعلومات وقياسها ومراقبتها والسيطرة عليها .
- تنفيذ هيكل تنظيمي لتكنولوجيا المعلومات مناسب لدعم الأنشطة التجارية للمؤسسة.
- الحفاظ على الوثائق الحالية للأنظمة المعمول بها ، والحفاظ على فهم مرضي لكيفية دعم كل نظام من هذه الأنظمة للعمليات المرتبطة به.

- التأكد من أن عملية الاستعانة بأطراف خارجية تتوافق مع الخطط الاستراتيجية للمؤسسة وتتم إدارتها بشكل مناسب .
- إنشاء بيئة رقابية فعالة من خلال تحديد الفعال للمخاطر وتقييمها وإدارتها ومراقبتها.
- إنشاء وصيانة بيئات تشغيل آمنة مادية ومنطقية.
- توفير الاستمرارية التشغيلية والمرونة المرضية .
- توفير عدد كافٍ من الموظفين واختيارهم بشكل فعال و المحافظة على تعاقبهم بشكل مرض وتدريبهم بشكل جيد .
- الاستعانة بمستشارين ومراجعين خارجيين مؤهلين عند الضرورة.

المنهجية وطرق البحث:

باعتبار الدراسة تأتي في إطار الدراسات الاقتصادية فقد تم الاعتماد على المنهجين الوصفي والتحليلي ، حيث تم التطرق للإطار العام التعريفي والجانب القانوني للموضوع بإتباع المنهج الوصفي ، وإتباع المنهج التحليلي لتحليل نتائج الدراسة وتفسيرها .

أدوات الدراسة:

- -مصادر أولية : تتمثل في الاستبيان .
- -مصادر ثانوية : تتمثل في الكتب والمراجع والدوريات والمؤتمرات .

مجالات الدراسة:

تركز الدراسة على المخاطر التي تتعرض لها المعاملات المصرفية في البنوك المملكة العربية السعودية ، وقد امتدت الدراسة على سنة 2022 - 2023.

الاطار الزمني للدراسة :

المهمة	البداية	النهاية	فترة انجاز المهمة
اختيار العنوان	2022/9/13	2022/9/28	15
الفصل الأول : المقدمة	2022/10/1	2022/10/31	30
الفصل الثاني الاطار النظري للدراسة	2022/10/31	2022/11/5	5
الفصل الثالث نظريات وعينة الدراسة	2022/11/6	2022/11/21	15
الفصل الرابع تحليل البيانات	2022/11/22	2022/11/27	5
الفصل الخامس النتائج	2022/11/28	2022/12/8	10
مراجعة الدراسة وسرد المراجع	2022/12/20	2022/12/31	11

الفصل الثاني

الإطار النظري لمخاطر المعاملات المصرفية الإلكترونية

مفهوم الخدمات المصرفية الإلكترونية:

التي عرفت بأنها: "تقديم البنوك لخدمات مصرفية تقليدية أو مبتكرة من خلال شبكات اتصال إلكترونية، تقتصر صلاحيات الدخول إليها على المشاركين فيها وفقا لشروط العضوية التي تحددها البنوك ،فهي جميع الآليات الإلكترونية التي تمكن من ممارسة جميع الأنشطة والأعمال داخل الشركات أو بين الشركات وعملائها وموزعيها ومورديها بصورة أسرع وأكثر دقة وعبر نطاق أو مدى زمني ومكاني أوسع.

صور الخدمات المصرفية الإلكترونية:

1- البطاقات الائتمانية : هي بطاقة بلاستيكية صغيرة الحجم شخصية، تصدرها المصارف أو منشآت التمويل الدولية تمنح للأشخاص الذين لهم حسابات مصرفية و هي من أشهر الخدمات المصرفية الحديثة، و بموجب هذه البطاقة يستطيع المتعاملين الحاملين لهذه البطاقة الحصول على ائتمانا مجانيا متفق عليه مع المصرف يقومون بسداده بعد مدة ، فهي عبارة عن مستند يعطيه مصدره لشخص طبيعي أو معنوي بناءا على عقد بينهما يمكنه من شراء السلع والخدمات ممن يعتمد المستند دون دفع الثمن حالا لتضمنه التزام المصدر بالدفع كما يمكنه أيضا من سحب النقود من المصارف

2- البطاقات غير الائتمانية: هي تلك البطاقات التي لا تتيح لحاملها فرصة الحصول على الائتمان (قرض) ، و تنقسم بدورها إلى :

3- البطاقة المدينة (بطاقات الدفع): و هي البطاقات التي تعتمد على وجود أرصدة فعلية للعميل لدى البنك في صورة حسابات جارية لمقابلة المسحوبات المتوقعة للزبون حامل البطاقة ، حيث تسمح له بتسديد مشترياته ، و يتم السحب في البنك مباشرة عكس البطاقات الائتمانية ، فإن الزبون يحوّل الأموال العائدة له إلى البائع عند استعماله لهذه البطاقة ، و تتميز هذه البطاقات بأنها توفر الوقت و الجهد للعملاء و كذلك زيادة إيرادات البنك المصدر لها .

4- بطاقة الدفع مقدما: و هذه البطاقة تقوم على أساس تثبيت مبلغ محدد بحيث يمكن الدخول في البطاقة بذلك المبلغ ، ليتم التخفيض التدريجي لمبلغ البطاقة كلما تم استعمالها ، ومن أمثلة البطاقات المتداولة ، بطاقات النداء الهاتفية ، و بطاقات النقل الداخلي العام .

5- البطاقة الذكية: الكروت الذكية عن بطاقة بلاستيكية ذات مواصفات و مقاييس معينة محددة من قبل منظمة " ISO و تحتوي تلك البطاقة على رقاقة الكترونية Chip ، تعمل كشبه حاسب آلي بحيث يمكن تخزين بعض البيانات عليها و استرجاعها . فيتم عليها تخزين جميع البيانات الخاصة بحاملها ، مثل الاسم ، العنوان ، المصرف المصدر لها ، أسلوب الصرف ، المبلغ المنصرف و تاريخه ، تاريخ حياة العميل المصرف .

6- النقود الإلكترونية: تعرف على أنها عبارة عن منتجات دفع متنوعة مخصصة للمستهلك تستخدم لدفع المستحقات بطرق إلكترونية ، فهي عبارة عن مجموعة بروتوكولات وتوقيعات رقمية تتيح للرسالة الإلكترونية أن تحل فعليا محل العملات التقليدية ، وبسبب تنوع هذه المنتجات فقد يصعب إعطاء فكرة عنها إلا عن طريق تحديد صورها المتمثلة في:

- الصورة الأولى: هي البطاقة المدفوعة مسبقا والتي يمكن استخدامها لأغراض متنوعة ويطلق عليها اسم البطاقة المخزنة القيمة أو محفظة النقود الإلكترونية ELECTRIC PURSES .

- الصورة الثانية: هي آليات الدفع مخزنة القيمة أو سابقة الدفع التي تسمح بالدفع من خلال شبكة الحاسوب الآلية ، المتعارف عليها باسم نقود الشبكة Net Money ، أو النقود السائلة الرقمية Digital Cash .

وعليه فإن أهم ما يميز النقود الإلكترونية هو قيمتها المسددة مسبقا ، والتي تكون مختزنة بداخلها .

7- الشيك الإلكتروني : يعرف بأنه رسالة إلكترونية مؤمنة وموثقة تحمل التزاما قانونيا بالدفع وهو ذات الالتزام في الشيكات الورقية ، أي أنه وثيقة إلكترونية تحل محل الشيكات الورقية ولكن بشكل وتنسيق إلكتروني ، حيث يتم إرسال هذه الرسالة عبر البريد الإلكتروني المؤمن من مصدر الشيك إلى حامله ، هذا الأخير الذي يحصل على مستحقاته بعد تقديم الشيك للمصرف عبر الانترنت ، والذي يحمل توقيعاً رقمياً مشفراً يصعب تزويره و هنا تظهر أهمية التوقيع الإلكتروني ، والذي أصبح اليوم معترف به قانوناً في بعض البلدان ، ليس فقط في قضايا النقد والائتمان ، بل تجاوز ذلك إلى مختلف المعاملات والعقود الإلكترونية بالرغم من ذلك فإنه لا توجد تشريعات وقوانين تحمي التوقيع الإلكتروني.

8- السفينة الإلكترونية : هي محرّر شكلي ثلاثي الأطراف معالج إلكتروني بصورة كلية أو جزئية يتضمن الأمر الصادر من شخص يسمى الساحب إلى شخص آخر يسمى المسحوب عليه بأن يدفع مبلغ من النقود إلى شخص ثالث يسمى المستفيد أثناء الاطلاع أو في تاريخ محدد .

9- استخدام أجهزة الصراف الآلي : عبارة عن استخدام وسيط بين المتعاملين يتلقى طلبات وبيانات كل منهما ويتحقق منها عن طريق موقعه على الشبكة ، ويتولى عملية عرض السلعة أو الخدمة والتسليم والوفاء لقاء عمولة معينة ، وهو ما يساهم في ربح الوقت و تقليل التكاليف .

10- المقاصة الإلكترونية : هذه الخدمة تسمح بتحويل النقود من حساب الزبائن إلى حسابات أخرى في أي فرع لأي مصرف في البلد ، مثل دفع المرتبات الشهرية من حساب صاحب العمل إلى حساب الموظفين ، كما تطورت هذه الخدمة بحيث أصبحت تشمل نظام التسوية الإجمالية بالوقت الحقيقي ، حيث أصبحت التسوية الإلكترونية

للمدفوعات بين المصارف المختلفة تتم نظام المدفوعات الإلكترونية للمقاصة .

أنواع المخاطر التي تتعرض لها البنوك من جراء الخدمات المصرفية الإلكترونية :

رغم ما حققه تطبيق الإدارة الإلكترونية في مجال الخدمات المصرفية من مزايا ومن تخطي لعيوب تقديم هذه الخدمات بطريقة تقليدية سواء من حيث السرعة أو الجودة ، إلا أن ذلك قد أفرز أنواع أخرى من المخاطر منها :

أولاً: المخاطر القانونية: وهي تلك المخاطر الناجمة عن عدم التحديد الواضح للحقوق و الالتزامات القانونية الناتجة عن الخدمات المصرفية الإلكترونية لاسيما و أن العديد من وسائل أداء تلك العمليات المصرفية لا زالت في مرحلة التطوير مثل السجلات و التوقيعات و العقود الإلكترونية و قواعد إرسال و تلقي السجلات الإلكترونية، و الاعتراف بسلطات و قواعد التصديق الإلكتروني، و إحكام السرية و الإفصاح، وتبرز أهم التحديات القانونية متمثلة في تحدي قبول القانون للتعاقدات الإلكترونية، أمن المعلومات، وسائل الدفع، التحديات الضريبية، إثبات الشخصية، التوقيع الإلكتروني، أنظمة الدفع النقدي المال الرقمي أو الإلكتروني، سرية المعلومات، أمن المعلومات من مخاطر إجرام التقنية العالية، خصوصية العميل، المسؤولية عن الأخطاء والمخاطر، التعاقدات المصرفية الإلكترونية ،مسائل الملكية الفكرية لبرمجيات وقواعد معلومات البنك أو المستخدمة من موقع البنك أو المرتبطة بها،علاقات وتعاقدات البنك مع الجهات المزودة للتقنية أوالموردة لخدماتها أو مع المواقع الحليفة مشاريع الاندماج والمشاركة والتعاون المعلوماتية.

تحدث هذه المخاطر نتيجة عدم احترام القوانين أو القواعد أو الضوابط المقررة خاصة تلك المتعلقة بمكافحة غسيل الأموال أو نتيجة عدم التحديد الواضح للحقوق والالتزامات القانونية الناتجة عن الخدمات المصرفية الالكترونية ومن ذلك عدم وضوح ما إذا كانت هناك قواعد لحماية المستهلكين في بعض الدول أو لعدم المعرفة القانونية لبعض الاتفاقيات المبرمة باستخدام وسائل الوساطة الالكترونية

ثانياً: المخاطر التقنية: تحدث هذه المخاطر من احتمال الخسارة الناتجة عن خلل في شمولية النظام أو من برنامج إلكتروني غير ملائم للعمليات المصرفية الالكترونية. أو من أخطاء العملاء،فهي مخاطر ناتجة عن سوء عمل النظام الالكتروني نتيجة سوء استخدام هذا النظام، أو سوء مراقبة البرامج في حد ذاتها و نتيجة عدم توفر وسائل التأمين الكافية للنظم أو عدم تصميمها أو إنجازها ،مما يفرض خطأ في تشغيل البرمجيات وتتمثل فيمايلي :

1-عدم التأمين الكافي للنظم :وهي تتعلق بعدم توافر وسائل الأمن الكافية لنظم حسابات البنك ،مما يتيح إمكانية اختراقها ،حيث يتم التعرف على المعلومات الخاصة بالعملاء و استغلالها سواء أكان ذلك خارج البنك أو من العاملين فيه .

2-عدم ملائمة تصميم النظم أو انجاز عمل أو أعمال الصيانة :وهي تنشأ بسبب عدم كفاءة النظم أو إخفاءها لمواجهة متطلبات المستخدمين وعدم السرعة في حل مشاكل الصيانة ،لاسيما إذا تم الاعتماد على مصادر خارج البنك لتقديم الدعم الفني بشأن البنية التحتية اللازمة أو نتيجة عدم كفاية البرمجيات أو الموظفين القائمين على تلك الأعمال . لاسيما وأن عدم إلمام موظفي البنوك بالاستخدام الأمثل للتكنولوجيا الحديثة يؤدي إلى القصور في أداء العمليات الالكترونية بشكل صحيح، وهو ما يؤثر على سمعة المصرف التي تبدأ بالانحطاط من اللحظة التي يعجز فيها عن إدارة أنظمتها المستخدمة ،مما يولد عند الزبون القناعة الكافية أن هذا المصرف لا يستطيع أن يوفر الحد الأدنى من الأمان المطلوب، فإذا ما واجهت أحد المصارف مشاكل في خدماتها الالكترونية فقد يؤدي ذلك إلى فقدان الثقة بها، ليتوافر على إثره رأي عام سلبي اتجاه المصرف ، الأمر الذي قد يمتد إلى التأثير على مصارف أخرى، نتيجة عدم مقدرة البنك على إدارة نظمه بكفاءة أو حدوث اختراق مؤثر لها وقد بدأت المصارف تطرح مخاطر ناجمة عن اتساع الهوة في علاقتها مع العملاء مما جعلها تتعرض لعمليات نصب مختلفة، ذلك أن الخدمة المصرفية عبر الانترنت يكون من الصعب مراقبتها بصورة دقيقة، و هو ما يؤثر على حجم السيولة النقدية سواء بالزيادة أو بالنقصان لصعوبة مراقبتها من طرف البنك المركزي، وحتى يمكن التحكم و الحد من هذه المخاطر لابد من إتباع إجراءات التقنين و ذلك بالترخيص القانوني للطرق و المعاملات الالكترونية، كما لابد من التنسيق الدولي لتنظيم هذه المعاملات.

3-إساءة العملاء استخدام نظام الدفع : ينتج هذا الخطر نتيجة عدم إحاطة العملاء بإجراءات التأمين الوقائية، وكذا نتيجة سماحهم لعناصر أخرى بالدخول إلى حسابات عملاء آخرين و استخدام معلوماتهم الشخصية، بالإضافة إلى استخدام أحد العملاء رقم بطاقته في برنامج غير محمي قد يسمح للغير بالحصول على معلومات وافية عن حسابه ،كذلك يؤدي تسرب فيروسات في البرامج والحواسب المتصلة بالانترنت إلى إتلاف البرامج والأنظمة ،وتوزيعها للمستهلك النهائي بطريقة مشوهة وغير سليمة ،مما يلحق ضرر بالعميل من جهة وبالمصرف من جهة أخرى .من خلال إمكانية إتلاف وتدمير المعلومات الأساسية للمصارف .

ثالثا:مخاطر خرق أنظمة الأمن والحماية (الجرائم الإلكترونية): يعد الأمن المعلوماتي من أهم المخاطر التي تواجه تطبيق الإدارة الإلكترونية في مجال تقديم الخدمات المصرفية ،فبرغم وجود مجموعة من الأساليب المضادة لهذه الاختراقات إلا أن مشكلة أمن المعلومات لازالت تشكل هاجسا في ظل انتشار الجرائم الإلكترونية

التي تتمثل في كل سلوك سلبي أو إيجابي يتم بموجبه الاعتداء على البرامج والمعلومات للاستفادة منها بأية صورة كانت ، والتي من بينها :

1- مخاطر تبييض الأموال :لقد وضعت اللجنة الأوروبية لغسيل الأموال تعريفا لهذه العملية و حددت عناصرها حيث عرفت في دليلها الصادر عام 1990 بأنها "عملية تحويل الأموال المحصل عليها من أنشطة جرمية لتجنب المسؤولية القانونية عن الاحتفاظ بمحصلات هذا الجرم".

2- مخاطر السلب بالقوة الالكترونية:حيث يتم استخدام الحاسب في التلاعب بالمعلومات و ذلك بإدخال بيانات زائفة من جانب المتحايل باختلاق دائنين كأجور يجب دفعها أو فواتير يجب سدادها.و ذلك عن طريق اختلاق مدينين غير حقيقيين يجب عليهم سداد فواتير صادرة عن الحاسب، أما المدين المعتدى عليه فلن يتمكن من إثبات كونه غير مدين لوجود فواتير معلوماتية، و هكذا يستغل المتحايل طرق الدفع الآلية للحصول على أموال غير شرعية.

3-مخاطر السطو على أرقام البطاقات :أصبح السطو على أرقام البطاقات عبر شبكة الانترنت عملية سهلة، لذلك تزايدت هذه الحوادث التي أعقبتها عمليات الابتزاز لإرجاع تلك الأرقام أو لعدم نشرها أو لعدم استخدامها ونذكر من هذه الجرائم مايلي :

- تجاوز الحامل لرصيده بالسحب خلال أجهزة الصراف الآلي و تقع هذه الجريمة عندما يقوم حامل البطاقة بالسحب من الآلية للنقد بمبلغ يزيد عن رصيده، أو يتجاوز الحد الأقصى المصرح له به.
- إساءة استعمال بطاقات الوفاء: قد يقدم العميل بشراء سلع و خدمات تتجاوز قيمتها المبلغ الذي يضمه البنك أو الجهة المصدرة كحد أقصى لها.
- استخدام بطاقة انتهت مدة صلاحيتها :لكل بطاقة مدة صلاحية معينة، و بعد مرور هذه المدة لابد على العميل بردها للبنك أو الجهة المصدرة لها و ذلك إما لتجديدها أو التخلي عنها . بموجبها بائتمان للعميل .
- استعمال البطاقة المسروقة أو المفقودة من قبل الغير .
- السحب ببطاقات الكترونية مزورة: حيث يقوم الغير بتزوير البطاقات عن طريق بطاقات ائتمان مسروقة، و استبدال بياناتها، كما قد يتم ذلك بالتواطؤ مع صاحب البطاقة الذي يتركها للغير لاستعمالها.

أساليب مواجهة مخاطر تطبيق الإدارة الإلكترونية في مجال الخدمات المصرفية

تفاديا للمخاطر الناجمة عن تطبيق الإدارة الإلكترونية في مجال الخدمات المصرفية ، لابد من اتخاذ بعض التدابير الاحترازية التي تحول دون عرقلة عملية التطبيق ، منها ما يتعلق بتقدير المخاطر ومنها ما يتضمن الرقابة على التعرض للمخاطر ، في حين يتطرق البعض منها لوضع حد لتلك المخاطر :

أولاً: تقدير المخاطر: يبدأ البنك بتقدير المخاطر التي يمكن أن يتعرض لها بعد الوقوف على أهميتها المالية ليتسنى له تحديد تلك المخاطر ، وبعد ذلك يقوم مجلس إدارة البنك بتحديد الخسائر المالية التي من الممكن أن تلحق البنك في حالة تعرضه لمثل هذه المخاطر ، ومن ثم يقوم بدراسة وافية لتلك المخاطر دون أن يخرج في مراحل تقديره لها عن المراحل الثلاثة التالية :

- تحديد المخاطر التي يمكن للمصرف أن يتعرض لها.
- وضع حدود قصوى لما يمكن للمصرف تحمله من خسائر نتيجة التعامل مع هذه المخاطر من قبل مجلس إدارة المصارف.
- مقارنة الخطر مع غيره من المخاطر و تحديد قدرة و إمكانية مواجهته.

ثانياً : الرقابة على التعرض للمخاطر: تشمل هذه الرقابة مجموعة من المجالات نذكر منها :

1-تنفيذ سياسات وإجراءات التأمين:وتستهدف هذه السياسة مايلي :

- تحديد شخصية المتعامل مع النظم المختلفة .
- ضمان عدم إجراء تعديلات على رسائل العملاء أثناء عمليات الدفع .
- ضمان الحفاظ على سرية المعاملات المالية المختلفة للزبائن والعملاء .
- الاحتفاظ بقاعدة بيانات مركزية للتتبع عمليات غسيل الأموال .
- ضمان ما تم تسديده من صاحب البطاقة .

2-الرقابة على المصارف: وهي رقابة تمارس من طرف جهات من خارج البنك تابعة للبنك المركزي أو السلطة النقدية للدولة ، بحيث تقوم هذه السلطات الرقابية بمهمة متابعة امتثال البنوك للأوامر والتعليمات الصادرة عن

البنك المركزي و الهيئات التابعة له و من ثم معالجة التجاوزات المسجلة بحكم القانون أو بحكم التنظيم، وكذا فتح أبواب الحوار مع البنوك للبحث في القضايا التي تعرقل السير الحسن للمؤسسة المصرفية أو تحد من فعالية لجنة الرقابة أو لمعالجة أي قصور في التنظيم الاحترازي بفعل المحيط المصرفي، ثم اتخاذ إجراءات مناسبة سريعة لتصحيح الوضع، مثلا تعتمد سلطة الرقابة (Profil) إستراتيجية بعد تقييم الاحتياجات المالية لمواجهة المخاطر، مفادها العناية بالبنوك التي تتميز بشكل محدد من المخاطرة الإجمالية أو لاحتلالها موقعا حساسا أو لمزاولتها نشاطا هاما في الاقتصاد الوطني.

3- تدقيق الحسابات : يتم تدقيق الحسابات بالاستفادة من الخبراء و الشركات المتخصصة ، أين يستطيع المصرف أن يوكل مهام التدقيق في الحسابات العائدة له لموظفين أو لشركات خاصة مختصة بأعمال التدقيق ، وذلك بهدف الوقوف على الأخطاء التي كانت لديه ليتمكن في المستقبل من تجنبها أو التقليل منها، أما إذا تم اختيار خبراء التدقيق من موظفي المصرف فمن المستحسن أن يكونوا مستقلين عن إدارة الخدمات المصرفية ليتمكنوا من القيام بعملهم بشكل أفضل وأكثر استقلالية ، بالرغم من أن القوانين تفترض تعيين مدقق خارجي فأكثر على المؤسسات، إلا أنه في قطاع البنوك يتعين الحصول على موافقة السلطة الرقابية المختصة إلى جانب قرار الجمعية العمومية، ويحق

للسلطات الرقابية الحصول منه على أي بيانات أو إيضاحات لازمة مع الحق في أن تكلفه بمهام تراها ضرورية

على البنك المعني لأغراض رقابية، في حين يخول له الرجوع إلى السلطات الرقابية ضمن متطلبات العمل.

ثالثا: الحد من التعرض للمخاطر : حتى يمكن التغلب على المخاطر التي تعترض تطبيق الإدارة الإلكترونية في مجال

تقديم الخدمات المصرفية ،لابد من اتخاذ الإجراءات التالية :

1-وضع سياسات وإجراءات للحماية :

يحتاج المصرف للحد من المخاطر القيام ببعض الأمور المهمة ومنها أن يستخدم نظام حماية على درجة عالية من التقنية للقيام بمهامه بشكل جيد بالإضافة إلى ما يلقي على عاتق المصرف من أعمال الرقابة على النظام المصرفي ،وحتى يستطيع هذا النظام القيام بعمله وفق الشكل المطلوب منه ويتمكن من المحافظة على سرية

المعلومات المزوّدة له ، إلا أن ما تتطلبه عملية الحماية هو تفعيل العناصر كلها المكملّة لعملية الحماية التي أكدت لجنة بازل على إقرار اقتراح يتضمن استخدام عدة طرق لحماية النظام الإلكتروني منها على سبيل المثال :

- استخدام كلمة المرور و التشفير .
- القيام بمراقبة الفيروسات ومنعها من الدخول .
- منع أي عمل غير مشروع من الدخول إلى الأنظمة الإلكترونية المستخدمة سواء كانت من داخل أو خارج البنك

2- إحاطة العملاء بكل قواعد عمليات الدفع :

لابد من إرشاد وتثقيف العملاء بشكل مستمر عن قواعد وطرق استخدام أدوات الدفع وخاصة عند تبني أدوات حديثة ومحاولة إعلامهم بمختلف الإجراءات الكيفية لحل الأخطاء وذلك من خلال نشر المصرف للمعلومات على موقعه في شبكة الانترنت أو بأي طريقة أخرى .

3--تدعيم الاتصالات بين المستويات المختلفة في المصرف :

على المصرف أن يعمل كل ما بوسعه لتدعيم الاتصالات ما بين مجلس الإدارة والإدارة العليا وبين مختلف الأقسام وكذا بين العاملين بشأن سلامة أداء نظم الدفع ، وأن يوفر عنصر الكفاءة في موارده البشرية من خلال تدريبهم المستمر على مختلف الأنظمة وكيفية التعامل مع مختلف الاختلالات إن حدثت.

الفصل الثالث

الاحتيالات البنكية وتطور الإدارة الإلكترونية في المملكة العربية السعودية

«الاحتيالات البنكية».. طرق متجددة لاختراق حسابات العملاء

خطط حكومية لحماية البيانات

محمد الغامدي - اليوم 2021/05/14

"دعا مختصون إلى المحافظة على البيانات البنكية للعملاء والحذر من الطرق المتجددة التي يلجأ إليها المحتالون عبر الإنترنت لسرقة البيانات والأموال البنكية، خاصة في ظل ما تبذله الدولة من جهود حثيثة وإحكام الرقابة وفرض الأنظمة والتشريعات، لتضمن حماية أموال العملاء وبياناتهم من أي عملية نصب أو تحايل مصرفي، والجهود لسد الثغرات أمام العصابات لعدم سرقة أموال عملاء البنوك.

أفادت المحامية راوية المالكي بأن أن عملية الاحتيال المالي غالباً تكون من جهات غير مرخصة ومجهولة والتواصل مع الضحايا يتم عن طريق أرقام دولية في الغالب ويقومون بإيهام الضحية (المحول) بأن لديهم فروعاً

داخل المملكة ويعطيه رقم حسابات محلية لأفراد أو مؤسسات (المحول إليه) لتحويل المبلغ على حساباتهم البنكية، وفي هذه الحالة الأشخاص المحولة إليهم المبالغ المالية في الحقيقة هم ضحايا أيضا. وأضافت إنه يجب على كل شخص يحول له أموال أن يعرف مصدرها ويتصل بالبنك وإخباره عن المبلغ الذي وصل إليه وفي حال عدم معرفته بالشخص المحول عليه أن يتقدم ببلاغ لحماية نفسه وحتى لا يخضع للمساءلة القانونية، ولفتت إلى أن التوعية من خلال البنوك السعودية والبنك المركزي السعودي وهيئة السوق المالية مستمرة، فيما تبذل جهودا حثيثة في نشر الوعي بالاحتيال المالي وسبل الوقاية منه من خلال إقامة حملات توعوية سنوية للحد منها.

وأوضحت المالكي أن المتضرر بإمكانه أن يسترد حقه بالكامل، عند إحالة دعواه للمحكمة الجزائية ضد الشخص المحول إليه المبلغ المالي، مشيرة إلى أن المحكمة ستنظر في دعواه كحق عام وهو جريمة غسل الأموال والاحتيال المالي وكحق خاص يترافع فيه المتضرر لنفسه لإعادة ما تم أخذه من أموال.

أكد الخبير الاقتصادي فهد الأحمدى أن عصر «الكاش» شارب على الانتهاء، فيما أن عمليات القرصنة لا تقتصر على سرقة النقود التقليدية بل تمتد لتشمل سرقة البيانات البنكية والأرقام السرية، مضيفا إن أعظم مصدر لتسريب البيانات البنكية هو «أصحاب الحسابات نفسها»، مشيرا إلى أن المحتال «المحترف» يمكنه الاستيلاء عليها عبر تقنية البلوتوث أو الواي فاي أو من خلال صورة أرسلها الضحية عبر برامج التواصل الاجتماعي.

وحت الخبير الأحمدى عملاء البنوك بالحذر عند طلب بياناتهم البنكية خاصة أن موظف البنك لا يطلب تلك البيانات، مشددا على عدم التعامل مع موظف عبر الهاتف أو البريد الإلكتروني أو ووسائل التواصل الاجتماعي وأضاف الأحمدى: في الأغلب يأتي اتصال مزيف من دولة لا يعرفها الشخص ولا يعرف مفتاحها الدولي، وعبر هاتف متحرك «وليس أرضيا» أو من محتال يدعي أنه مكلف من البنك بتحديث معلوماتك، فيما يلجأ المحتال إلى إرسال بريد إلكتروني خال من شعار الشركة واسمها الرسمي لا يتضمن علامة القفل https ويصل عبر خدمة بريدية عامة مثل Hotmail، gmail، Outlook وليس نطاقا مستقلا أو موقعا خاصا بالشركة.

وقال الأحمدى إن أكثر طرق الاحتيال إيلا ما هي استغلال العواطف الدينية لتوريث الضحية بمنتجات مالية تزيد فوائدها عن البنوك التقليدية وبكلام أكثر صراحة: لا تأخذ قرضا بفائدة ظالمة لمجرد أنه «شرعي» مضيفا إن من أكثر الطرق المعروفة: هي أن تتلقى اتصالا من شركة قانونية مزيفة، أو مكتب محاماة وهمي، يدعي قدرته

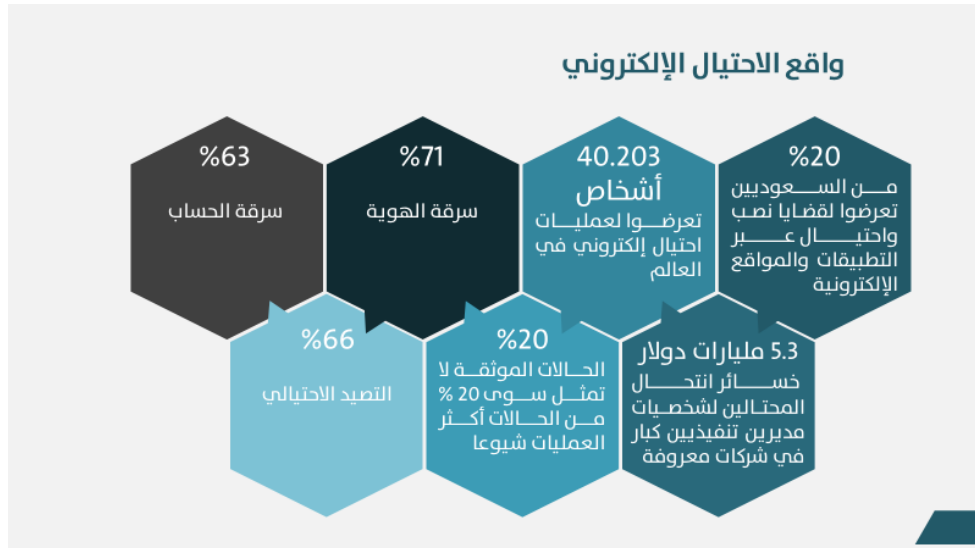
على استعادة حقل المنهوب» ولكنهم يحتاجون فقط إلى رقم الحساب الذي تمت منه عملية الاحتيال.»

وحذر الأحمدى من عدم الدخول في مساهمات وهمية، أو دعوات توظيف الأموال، أو إغراءات بمنح أرباح خيالية أكبر من البنوك، مشيراً إلى أنه رغم النصائح المتكررة إلا أن طرق الاحتيال متجددة، فيما يبقى خط الدفاع الأول ضد الاحتيال هو الوعي والحذر والاحتفاظ بالأرقام السرية والشك في كل من يطلب البيانات المالية.

وأبان الأحمدى أن من طرق الاحتيال استخدام أسماء البنوك لتكون مدخلا للاحتيال على العميل بطريقة إلكترونية فيما يتسبب التهاون في عدم التحقق من شخصية المحتال وعدم فهم الطرق الاحتيالية إلى فقد الأموال.

واقع الاحتيال الإلكتروني في بيئة الأعمال السعودية:

مع تطور الوسائل التقنية التي يمكن من خلالها الحصول على الخدمات والمنتجات المالية، تتطور أساليب الاحتيال المالي وتتجدد بين فترة وأخرى متخذة أشكالاً وصوراً متعددة؛ إلا أن هدفها واحد وهو الاحتيال على الأفراد و الكيانات الاقتصادية للحصول على بياناتهم المالية والشخصية وسرقة أموالهم ومدخراتهم ولكن مهما تعددت أساليب الاحتيال، من الضروري معرفة أن تجنب عمليات الاحتيال المالي تبدأ بعدم الاستجابة إلى أي طرف مجهول يطلب منك الإفصاح عن بياناتك المالية والشخصية مهما بدا واثقاً؛ فالثقة سلاح المحتال لطمأنتك وإقناعك بمصداقيته فنلاحظ ان المجرمين يأخذون الأموال من الضحايا بطريقة خداعية سهلة تجعل الضحية يدفع بمحض ارادته و من ثم يصدّم بان ماله قد اخذ منه بطريقة خداعية و يكون هناك صعوبة ولا يستطيع استرجاعه في غالب الاحيان.



أبرز طرق الاحتيال المالي في المملكة العربية السعودية :

- قيام جهات مجهولة تدعي أنها مؤسسات رسمية مثل البنوك أو مؤسسات حكومية كالبنك المركزي السعودي بالاتصال على هاتفك الجوال أو إرسال رسائل نصية أو بريد إلكتروني تطلب منك إفشاء بيانات بطاقتك الائتمانية أو الأرقام السرية لحساباتك المصرفية أو الإفصاح عن رمز التحقق الذي يصل إلى جوالك من الجهة المالية بحجة تحديث بياناتك أو فوزك بجائزة أو وجود مشكلة بحسابك المصرفي يستلزم حلها.
- استغلال الحاجات النفسية لدى الأفراد مثل رغبتهم بالثراء السريع أو الفوز بجوائز مالية أو عينية.
- التعامل مع جهات غير مرخصة وأفراد يعملون بطريقة غير نظامية يعرضون خدمات تتعلق بمنح القروض بشروط وأسعار أفضل، أو سداد القروض والمتعثرات المالية بلا شروط منطقية إذ قد يقومون بالتسديد عنك مقابل توقيعك على مستندات تلزمك بدفع مبالغ أكبر.
- تعرض بيانات حساباتك البنكية وبطاقتك الائتمانية إلى التسريب بسبب عدم وجود برامج حماية في حاسبك الآلي أو الجوال عند استخدام القنوات الإلكترونية للمصارف أو استخدام مواقع تسوق إلكترونية غير موثوقة عند الشراء.
- “التسول الإلكتروني” وهو نظام جديد اتبعه المحتالون بغاية التسول عبر مواقع التواصل الاجتماعي لذا فقد حددت المملكة عقوبة سجن بهذه الجريمة أيضا. وهو محاولة الحصول على الضحية من تصميم مواقع و إرسال رسائل نصية توحى أنها للتبرع مثل منصة احسان وغيرها .

- إرسال روابط مزيفة لا استقدام العمالة المنزلية أو استخراج رخصة قيادة و خصوصاً الناء أصبح أيضاً مشهوراً مؤخراً، و يكمن هذا في ان ارسال مثل هذه الروابط يساعد المجرمين على اختراق حسابات ضحاياهم و هذا من خلال نقر الضحية و الولوج الى الرابط المرسل اليه ليرى انه تم اختراق حسابه.
- شراء المنتجات من غير تسليمها أي ان المحتالين يبيعون سلع مزيفة بأسعار قد تكون رخيصة في بعض الأحيان و لا تكون البضاعة موجودة أصلاً فلا يتم تسليم البضاعة بتاتا بل تتم سرقة الأموال فقط.

تطور النظام المصرفي في المملكة العربية السعودية :-

تقارير شهرية للحد من التحايلات البنكية

عبد الرحمن المصباحي – عكاظ-الجمعة 11 نوفمبر 2022

"واصل البنك المركزي السعودي (ساما) مكافحته للاحتيال المالي، بعد أن وجه تعميماً إلى كافة البنوك والمصارف المحلية، والبنوك الأجنبية والرقمية، طالبا بضرورة عمل تقييم دقيق للوضع الحالي لإجراءات مكافحة الاحتيال، لتحديد مواطن الضعف في البنك، مع تقييم مستوى النضج، وتزويده بتقارير شهرية حيالها وذلك اعتباراً من شهر نوفمبر الجاري.

وجه البنك المركزي في تعميم حديث، إلزام كافة البنوك والمصارف بوضع خطة عمل لتحقيق درجة النضج كحد أدنى لضوابط دليل مكافحة الاحتيال، وذلك خلال 9 أشهر من تاريخ التعميم الصادر خلال الشهر الجاري، وذلك بعد تقييم الوضع الحالي في بيئة البنك بشكل دقيق، مع تزويد البنك المركزي بها في نهاية شهر نوفمبر الجاري.

واشترط البنك المركزي على البنوك والمصارف الالتزام التام بمتطلبات دليل مكافحة الاحتيال المالي في موعد أقصاه 29 يونيو من عام 2023، مع إعداد تقرير سنوي مفصل من إدارة المراجعة الداخلية، ولها الاستعانة ببيوت الخبرة يوضح مدى الالتزام بمتطلبات دليل مكافحة الاحتيال المالي ابتداء من نهاية الربع الرابع من العام القادم 2023.

لجأت هيئة السوق المالية، بالتعاون مع هيئة الاتصالات إلى حجب معظم تلك المواقع؛ بهدف حماية الزوار ممن قد تنطلي عليهم حيلة التداول من خلال تلك المواقع أو تقديم معلوماتهم الشخصية والمصرفية إليها، خصوصاً أن 26 موقعاً منها لجأت إلى انتحال شخصية شركات مصرفية كبرى أو جهات حكومية لاستقطاب شرائح من

الأفراد قليلي الخبرة في المجال التقني.

قامت العديد من البنوك خلال الفترة الأخيرة، بتحديث أنظمتها عبر تفعيل خدمة الاتصال الآلي على المستفيد عند رغبته الدخول من جهاز رقمي جديد، وتهدف هذه الخدمة إلى الحد من التحايل، خصوصاً أن معظم حالات الاحتيال التي حدثت أخيراً كان سببها الدخول على الحساب البنكي للضحية عبر إرسال رابط وهمي لشركات أو حكومات، وسحب كافة أرصدته، وجاءت الخطوة الأخيرة بالاتصال على أصحاب الحسابات من قبل البنوك لتأكيد دخولهم من أجهزة جديدة للحد من عمليات الاحتيال."

الفصل الرابع

الدراسة العملية وإجراءاتها المنهجية

1. استمارة الاستبانة وعينة الدراسة:-

تُعد أداة الدراسة أحد الوسائل التي يستخدمها الباحث لحصوله على المعلومات المطلوبة من المصادر المعنية في بحثه، ومنها الاستبانات كما في هذه الدراسة، وقد اعتمد الباحث في إعداد أداة الدراسة على ما استخدم في الدراسات السابقة من أدوات ومقاييس، تناول فيها متغيرات مثل إدارة مخاطر تكنولوجيا المعلومات، والحد من مخاطر المعاملات المصرفية، ومنها دراسة (عوض وآمال، 2014)، ودراسة (هاشم، وأماني، 2012).

وقد تكونت الاستبانة من المتغيرات التي مثلت دور إدارة مخاطر تكنولوجيا المعلومات في الحد من مخاطر المعاملات المصرفية، فضلاً عن أسئلة تخص المتغيرات الديموغرافية للمشاركين في الدراسة، وقد تم تحديد الأسئلة في ضوء كل متغير كما يلي:

- 1- محور المتغيرات الديموغرافية: وكان عدد الأسئلة 3 أسئلة.
- 2- محور المتغير المستقل (إدارة مخاطر تكنولوجيا المعلومات): وتتضمن 3 محاور فرعية، وهي الإجراءات العملية، والإجراءات الاحترازية، والاحتمالات البنكية، وكان عدد الأسئلة 13 سؤال.
- 3- محور المتغير التابع (الحد من مخاطر المعاملات المصرفية): وكان عدد الأسئلة 4 أسئلة.

وقد استخدم الباحث مقياس ليكرت (Likert) الخماسي لإجابات الفقرات كما يلي:

الجدول رقم 1: درجات مقياس ليكرت الخماسي (Likert)

موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
5	4	3	2	1

وبعد إعداد الاستبانة تم عرضها على عدد من السادة المحققين والمحكمين، وأخذ الباحث بملاحظاتهم وآرائهم لتكون الاستبانة بشكلها النهائي كما في الملحق.

أما بخصوص عينة الدراسة فكانت على عملاء البنوك المصرفية في المملكة العربية السعودية، وعددهم 62 عينة، وبعد الانتهاء من مرحلة إجراء الاستبيان، أُخضعت الاستبيانات إلى مرحلة الفرز، والتدقيق، والتحليل الدقيق عبر البرنامج الإحصائي SPSS إصدار نسخة 28.

2. اختبار ثبات الاستبانة:-

يقصد بالثبات هو أن تعطي الاستبانة النتيجة نفسها عند إعادة توزيعها أكثر من مرة تحت نفس الظروف والشروط، أو بعبارة أخرى أن تعطي قراءات متقاربة عند استخدامها في كل مرة، وعدم تغييرها بشكل كبير عند إعادة توزيعها على أفراد العينة عدة مرات خلال فترات زمنية معينة، لأن الأداة المتذبذبة لا يمكن الاعتماد عليها ولا الأخذ بنتائجها، وإلا ستكون نتائج الدراسة غير مطمئنة ومضللة.

وقد تم التحقق من ثبات استبانة الدراسة باستخدام طريقة الثبات بطريقة الاتساق الداخلي (consistency)، والذي يشير إلى قوة الارتباط بين الفقرات في أداة الدراسة، وذلك باستخدام معادلة كرونباخ ألفا (Cronbach Alpha)، ويعتمد هذا الأسلوب على مدى توافر الاتساق في أداء الأفراد من فقرة إلى أخرى وإلى جميع فقرات الاستبانة، ونتائج الجدول رقم 2 توضح ذلك:

الجدول رقم 2: نتائج اختبار معامل الثبات بطريقة كرونباخ ألفا على محاور الدراسة المختلفة

محاور الدراسة	عدد الفقرات	قيمة ألفا كرونباخ
الإجراءات العملية	3	330.7
الإجراءات الاحترازية	5	250.8
الاحتمالات البنكية	5	0.660
الدرجة الكلية للمتغير المستقل	13	170.8
الحد من مخاطر المعاملات المصرفية	4	600.8
الدرجة الكلية للمحاور مجتمعة	17	0.885

المصدر: من إعداد الباحث وفق البرنامج الإحصائي (SPSS)

يتضح من نتائج الجدول 2 أن قيمة معامل ألفا كرونباخ كانت مقبولة لمحاور الدراسة الأربعة، وكانت أقل الدرجات لمحور الاحتمالات البنكية بقيمة 0.660، إلا أنها تُعد قيمة مقبولة نسبياً، فيما كانت أعلى الدرجات لمحور الحد من مخاطر المعاملات المصرفية بقيمة 0.860، بينما بلغت قيمة معامل ألفا للثبات الكلي للمحاور مجتمعة 0.885، وهي قيمة مرتفعة تدل على أن المقياس يتمتع بدرجة عالية من الثبات.

ولتفسير نتائج الدراسة، ومناقشتها قام الباحث بتقسيم التحليل الإحصائي إلى ثلاثة أجزاء: أولاً تحليل البيانات الشخصية والمتغيرات الديموغرافية لأفراد الدراسة، وثانياً: تحليل النسب المئوية، والاتجاه، والوسط الحسابي، والانحراف المعياري لاستجابات المشاركين في عينة الدراسة، وأخيراً اختبار فرضية الدراسة كما يلي:

3. تحليل البيانات الديموغرافية لعينة الدراسة

الجدول رقم 3: نتائج البيانات الديموغرافية والشخصية لعينة الدراسة

النسبة المئوية	العدد	الجنس
53.2	33	أنثى

46.8	29	ذكر
		العمر
11.3	7	أقل من 20 عاماً
19.4	12	أكثر من 40 عاماً
69.4	43	من 20 إلى 40 عاماً
		المؤهل الدراسي
50.0	31	بكالوريوس
24.2	15	ثانوية عامة
9.7	6	دبلوم
16.1	10	دراسات عليا

المصدر: من إعداد الباحث وفق البرنامج الإحصائي (SPSS)

توضح نتائج الجدول رقم 3 النسبة المئوية، والتكرارات لبيانات المشاركين في الدراسة، وهي الجنس، والعمر، والمؤهل الدراسي، وكما هو واضح فقد كانت نسبة المشاركين متقاربة جداً بين الذكور، والإناث مع أفضلية طفيفة للإناث بنسبة 53.2% مقابل 46.8% للذكور، فيما كانت الفئة العمرية الأكثر مشاركة من 20 إلى 40 عاماً بنسبة 69.4% مما يعطي دلالة واضحة على توفر عنصر الشباب بشكل أكبر في عينة الدراسة، وأخيراً؛ فقد كان نصف المشاركين في الدراسة من حملة البكالوريوس بنسبة 50.0% مقابل 24.2% لحملة الثانوية العامة، فيما بلغت نسبة حاملي الدراسات العليا 16.1%، والدبلوم 9.7%، وهذه النسب تشير إلى مدى التنوع التي تتمتع به عينة الدراسة، واختلاف الثقافات، والمؤهلات بين أفراد المشاركين.

4. المتوسطات والانحرافات المعيارية لمتغيرات الدراسة:-

1.4. محاور الإجراءات العملية (إدارة مخاطر تكنولوجيا المعلومات)

الجدول رقم 4: أسئلة محور الإجراءات العملية في متغير إدارة مخاطر تكنولوجيا المعلومات

الفقرات	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة	المتوسط الحسابي	الانحراف المعياري	اتجاه الرأي
يتبع البنك أساليب متقدمة لإدارة مخاطر تكنولوجيا المعلومات	0	3	7	33	19	4.10	0.783	أوافق
	0	4.8	11.3	53.2	30.6			

أوافق	0.779	4.18	20	37	2	2	1	تكرار	يعمل البنك باستمرار على تحسين أداء إدارة مخاطر تكنولوجيا المعلومات
			32.3	59.7	3.2	3.2	1.6	نسبة مئوية	
أوافق	1.006	3.94	19	29	6	7	1	تكرار	يوفر البنك الاستشارات، والنصائح اللازمة للعملاء للحد من مخاطر تكنولوجيا المعلومات
			30.6	46.8	9.7	11.3	1.6	نسبة مئوية	
أوافق	0.696	4.07	المتوسط والانحراف المعياري الإجمالي للمتغير						

المصدر: من إعداد الباحث وفق البرنامج الإحصائي (SPSS)

ملاحظة (1-1.79 لا أو افق بشدة، 1.80-2.59 لا أو افق، 2.60-3.39 محايد، 3.40-4.19 أو افق، 4.20-5 أو افق بشدة)

يتضح من خلال نتائج جدول رقم 4 أن المتوسطات الحسابية لفقرات محور الإجراءات العملية في متغير إدارة مخاطر تكنولوجيا المعلومات قد جاءت متقاربة، وتراوح ما بين 3.94 إلى 4.18 على مقياس ليكرت الخماسي، وكانت القيمة الإجمالية للمتوسط الحسابي للمحور 4.07، مما يشير إلى أن اتجاه الرأي لدى المشاركين في الاستبيان كان بالموافقة على الإجراءات العملية التي يتخذها البنك للحد من مخاطر المعاملات الإلكترونية، وتكنولوجيا المعلومات، إذ جاءت في المرتبة الأولى الفقرة ونصها: "يعمل البنك باستمرار على تحسين أداء إدارة مخاطر تكنولوجيا المعلومات" بمتوسط حسابي 4.18 وانحراف معياري 0.779، فيما حصلت الفقرة نصها: "يوفر البنك الاستشارات، والنصائح اللازمة للعملاء للحد من مخاطر تكنولوجيا المعلومات" على المرتبة الأخيرة، بمتوسط حسابي 3.94 وانحراف معياري 1.006، وهو ما يعكس مدى التقارب في وجهات نظر أفراد عينة الدراسة حول الفقرات المتعلقة بمحور الإجراءات العملية في متغير إدارة مخاطر تكنولوجيا المعلومات.

2.4. محور الإجراءات الاحترازية (إدارة مخاطر تكنولوجيا المعلومات)

الجدول رقم 5: أسئلة محور الإجراءات الاحترازية في متغير إدارة مخاطر تكنولوجيا المعلومات

الفقرات	لا أوافق بشدة	لا أوافق	محايد	أوافق بشدة	المتوسط الحسابي	الانحراف المعياري	اتجاه الرأي
يقوم البنك بإحاطة العملاء بالإجراءات الوقائية للحد من مخاطر تكنولوجيا المعلومات	1	7	5	34	3.89	0.960	أوافق
	1.6	11.3	8.1	54.8			
تكرار	1	3	5	37	4.03	0.829	أوافق

			25.8	59.7	8.1	4.8	1.6	نسبة مئوية	يقوم البنك بتحديث التطبيقات البنكية الموجودة على أجهزة المحمول باستمرار لحماية حسابات العملاء
أوافق	1.047	3.60	12	24	18	5	3	تكرار	يتمتع العاملون بالبنك بالخبرة اللازمة لتقليل مخاطر استخدام تكنولوجيا المعلومات
			19.4	38.7	29.0	8.1	4.8	نسبة مئوية	
محايد	1.176	3.27	11	16	18	13	4	تكرار	يوفر البنك أنظمة بديلة في حالة تعطل النظام الأصلية
			17.7	25.8	29.0	21.0	6.5	نسبة مئوية	
أوافق	1.000	3.87	16	30	11	2	3	تكرار	يتبع البنك الإجراءات اللازمة لحماية البرامج، والتطبيقات من المحاولات غير العادية للاختراق، والهاكرز
			25.8	48.4	17.7	3.2	4.8	نسبة مئوية	
أوافق	0.773	3.73	المتوسط والانحراف المعياري الإجمالي للمتغير						

المصدر: من إعداد الباحث وفق البرنامج الإحصائي (SPSS)

ملاحظة (1-1.79 لا أو افق بشدة، 1.80-2.59 لا أو افق، 2.60-3.39 محايد، 3.40-4.19 أو افق، 4.20-5 أو افق بشدة)

يتضح من خلال نتائج جدول رقم 5 أن المتوسطات الحسابية لفقرات محور الإجراءات الاحترازية في متغير إدارة مخاطر تكنولوجيا المعلومات قد جاءت متفاوتة، وتراوح ما بين 3.27 إلى 4.03 على مقياس ليكرت الخماسي، وكانت القيمة الإجمالية للمتوسط الحسابي للمحور 3.73، مما يشير إلى أن اتجاه الرأي لدى المشاركين في الاستبيان كان بالموافقة على الإجراءات الاحترازية التي يتخذها البنك للحد من مخاطر المعاملات الإلكترونية، وتكنولوجيا المعلومات، ولكن بدرجات متفاوتة إذ جاءت في المرتبة الأولى الفقرة ونصها: "يقوم البنك بتحديث التطبيقات البنكية الموجودة على أجهزة المحمول باستمرار لحماية حسابات العملاء" بمتوسط حسابي 4.03 وانحراف معياري 0.829، فيما حصلت الفقرة نصها: "يوفر البنك أنظمة بديلة في حالة تعطل النظام الأصلية" على المرتبة الأخيرة، بمتوسط حسابي 3.27 وانحراف معياري 1.176، مما يعكس عدم الاقتناع الكامل للمشاركين في الاستبانة بقدرة البنك على مواجهة تعطل نظم التشغيل الأصلية، وهذه القيم تعكس وجود بعض التفاوت في

وجهات نظر أفراد عينة الدراسة حول الفقرات المتعلقة بمحور الإجراءات الاحترازية في متغير إدارة مخاطر تكنولوجيا المعلومات.

3.4. محور الاحتمالات البنكية (إدارة مخاطر تكنولوجيا المعلومات)

الجدول رقم 6: أسئلة محور الاحتمالات البنكية في متغير إدارة مخاطر تكنولوجيا المعلومات

الفقرات	لا أوافق بشدة	لا أوافق	محايد	أوافق بشدة	أوافق بشدة	المتوسط الحسابي	الانحراف المعياري	اتجاه الرأي
يُعد التعرض للاحتتمالات البنكية أمراً شائعاً في ظل بيئة تكنولوجيا المعلومات	1	4	4	27	26	4.18	0.933	أوافق
	1.6	6.5	6.5	43.5	41.9			
تكرار	1	4	6	24	27	4.16	0.961	أوافق

			43.5	38.7	9.7	6.5	1.6	نسبة مئوية	يُعد الاحتيال عن طريق الرسائل النصية أشهر طرق الاحتيالات البنكية
أوافق بشدة	0.801	4.69	50	9	1	0	2	تكرار	لا أقوم بالرد إطلاقاً على أي رسالة تأتي من رقم مجهول فيها طلب لبعض بياناتي البنكية
			80.6	14.5	1.6	0	3.2	نسبة مئوية	
محايد	1.114	4.06	29	17	9	5	2	تكرار	أقوم بالإبلاغ فوراً عن أية محاولة للاحتيال الإلكتروني
			46.8	27.4	14.5	8.1	3.2	نسبة مئوية	
أوافق	1.011	4.16	26	28	3	2	3	تكرار	يقوم البنك بالحفاظ على سرية معلومات العملاء لتفادي عمليات الاحتيال الإلكتروني
			41.9	45.2	4.8	3.2	4.8	نسبة مئوية	
أوافق بشدة	0.480	4.25	المتوسط والانحراف المعياري الإجمالي للمتغير						

المصدر: من إعداد الباحث وفق البرنامج الإحصائي (SPSS)

ملاحظة (1-1.79 لا أو افق بشدة، 1.80-2.59 لا أو افق، 2.60-3.39 محايد، 3.40-4.19 أو افق، 4.20-5 أو افق بشدة)

يتضح من خلال نتائج جدول رقم 6 أن المتوسطات الحسابية لفقرات محور الاحتيالات البنكية في متغير إدارة مخاطر تكنولوجيا المعلومات قد جاءت متقاربة، وتراوح ما بين 4.06 إلى 4.69 على مقياس ليكرت الخماسي، وكانت القيمة الإجمالية للمتوسط الحسابي للمحور 4.25، مما يشير إلى أن اتجاه الرأي لدى المشاركين في الاستبيان كان بالموافقة بشدة على مدى خطورة الاحتيالات البنكية، والوعي الكامل بها، إذ جاءت في المرتبة الأولى الفقرة ونصها: " لا أقوم بالرد إطلاقاً على أي رسالة تأتي من رقم مجهول فيها طلب لبعض بياناتي البنكية" بمتوسط حسابي 4.69 وانحراف معياري 0.801، فيما حصلت الفقرة نصها: " أقوم بالإبلاغ فوراً عن أية محاولة للاحتيال الإلكتروني" على المرتبة الأخيرة، بمتوسط حسابي 4.06 وانحراف معياري 1.114، مما يعكس عدم الاقتناع الكامل للمشاركين في الاستبانة بقدرة البنك على مواجهة تعطل نظم التشغيل الأصلية، وهو ما يعكس مدى التقارب في وجهات نظر أفراد عينة الدراسة حول الفقرات المتعلقة بمحور الاحتيالات البنكية في متغير إدارة مخاطر تكنولوجيا المعلومات.

4.4. محور المتغير التابع (الحد من مخاطر المعاملات المصرفية)

الجدول رقم 7: أسئلة محور المتغير التابع (الحد من مخاطر المعاملات المصرفية)

الفقرات	لا أوافق بشدة	لا أوافق	محايد	أوافق بشدة	المتوسط الحسابي	الانحراف المعياري	اتجاه الرأي
يقوم البنك بتوضيح المعاملات المصرفية الأكثر تعرضاً لمخاطر تكنولوجيا المعلومات للعملاء	تكرار	4	7	12	23	16	أوافق
	نسبة مئوية	6.5	11.3	19.4	37.1	25.8	
يقوم البنك بعمل نظام لرقابة وأمن المعاملات المصرفية الإلكترونية التي تتم من خلال أساليب تكنولوجيا المعلومات	تكرار	0	2	15	34	11	أوافق
	نسبة مئوية	0	3.2	24.2	54.8	17.7	
يتم توفير معلومات لعملاء البنك حول المعاملات المصرفية الإلكترونية وكيفية استخدامها بطريقة صحيحة	تكرار	1	4	11	31	15	أوافق
	نسبة مئوية	1.6	6.5	17.7	50.0	24.2	
يتخذ البنك اتباع كافة الإجراءات الممكنة لتفادي مخاطر المعاملات المصرفية الإلكترونية المرتبطة بتكنولوجيا المعلومات	تكرار	2	0	14	32	14	أوافق
	نسبة مئوية	3.2	0	22.6	51.6	22.6	
				المتوسط والانحراف المعياري الإجمالي للمتغير			أوافق
					3.83	0.784	

المصدر: من إعداد الباحث وفق البرنامج الإحصائي (SPSS)

ملاحظة (1-1.79 لا أو افاق بشدة، 1.80-2.59 لا أو افاق، 2.60-3.39 محايد، 3.40-4.19 أو افاق، 4.20-5 أو افاق بشدة)

يتضح من خلال نتائج جدول رقم 7 أن المتوسطات الحسابية لفقرات محور المتغير التابع (الحد من مخاطر المعاملات المصرفية) قد جاءت متقاربة للغاية، وتراوح ما بين 3.65 إلى 3.90 على مقياس ليكرت الخماسي، وكانت القيمة الإجمالية للمتوسط الحسابي للمحور 3.83، مما يشير إلى أن اتجاه الرأي لدى المشاركين في الاستبيان كان بالموافقة على ما يقوم به البنك للحد من مخاطر المعاملات المصرفية المرتبطة بتكنولوجيا

المعلومات، إذ جاءت في المرتبة الأولى الفقرة ونصها: " يتخذ البنك يتبع كافة الإجراءات الممكنة لتفادي مخاطر المعاملات المصرفية الإلكترونية المرتبطة بتكنولوجيا المعلومات " بمتوسط حسابي 3.90 وانحراف معياري 0.863، فيما حصلت الفقرة نصها: " يقوم البنك بتوضيح المعاملات المصرفية الأكثر تعرضاً لمخاطر تكنولوجيا المعلومات للعملاء " على المرتبة الأخيرة، بمتوسط حسابي 3.65 وانحراف معياري 1.175، وهو ما يعكس مدى التقارب في وجهات نظر أفراد عينة الدراسة حول الفقرات المتعلقة بمتغير الحد من مخاطر المعاملات المصرفية.

5. اختبار فرضية الدراسة

هل يوجد أثر ذو دلالة إحصائية لإدارة مخاطر تكنولوجيا المعلومات على الحد من مخاطر المعاملات المصرفية في المملكة العربية السعودية؟

الجدول رقم 8: نتائج اختبار تحليل الانحدار الخطي المتعدد للتحقق من أثر إدارة مخاطر تكنولوجيا المعلومات على الحد من مخاطر المعاملات المصرفية

محاو ر إدارة مخاطر تكنولوجيا المعلومات	بيتا	ت المحسوبة	مستوى الدلالة	ر	2ر	ف المحسوبة	مستوى الدلالة
الإجراءات العملية	0.077	0.654	0.515	0.796	0.633	33.356	>0.001**
الإجراءات الاحترازية	0.626	5.197	<0.001**				
الاحتمالات البنكية	0.205	2.310	0.024*				

* ذات دلالة إحصائية عند مستوى دلالة أقل من 0.05

** ذات دلالة إحصائية عند مستوى دلالة أقل من 0.01

تم عمل اختبار الانحدار الخطي المتعدد للتحقق من أثر إدارة مخاطر تكنولوجيا المعلومات على الحد من مخاطر المعاملات المصرفية، وكما هو واضح من نتائج الجدول رقم 8: أظهرت نتائج التحليل الإحصائي وجود تأثير ذي دلالة إحصائية عند مستوى معنوية $\alpha \geq 0.0$ ، فقد بلغت قيمة معامل الارتباط (ر) 0.796، وهذا يؤكد وجود ارتباط إيجابي قوي بين إدارة مخاطر تكنولوجيا المعلومات بمحاورها الثلاث والحد من مخاطر المعاملات المصرفية ، أما قيمة معامل التحديد (ر2) فقد بلغت 0.633: أي أن تطبيق إدارة مخاطر تكنولوجيا المعلومات بمحاورها الثلاث قد فسر ما مقداره 63.3% من التباين الحاصل في الحد من مخاطر المعاملات المصرفية ، أما النسبة الباقية والتي تبلغ 37.7% فإنها تُعزى لمتغيرات أخرى لم تدخل في نموذج الانحدار.

إضافة إلى ذلك، فقد بينت قيمة معامل التحديد (بيتا) حجم الأثر لكل محور على حدة، وكانت القيم كالتالي: 0.077، 0.626، 0.205 لمحاور الإجراءات العملية، والإجراءات الاحترازية، والاحتياطات البنكية على التوالي، وبمستوى دال إحصائياً لكل من محوري الإجراءات الاحترازية، والاحتياطات البنكية؛ وهو ما يعني أن الزيادة بمقدار وحدة واحدة في تطبيق الإجراءات الاحترازية يؤدي إلى الحد من مخاطر المعاملات المصرفية ، بنسبة 62.6%، وكذلك الزيادة بمقدار وحدة واحدة في وعي العملاء بالاحتياطات البنكية يؤدي إلى الحد من مخاطر المعاملات المصرفية بنسبة 20.5%، بينما تؤدي الزيادة بمقدار وحدة واحدة في تطبيق الإجراءات العملية إلى الحد من مخاطر المعاملات المصرفية بنسبة 7%.

وبناء على ما سبق تم قبول فرضية الدراسة والتي تنص على: يوجد أثر ذو دلالة إحصائية لإدارة مخاطر تكنولوجيا المعلومات على الحد من مخاطر المعاملات المصرفية في المملكة العربية السعودية.

ملخص النتائج والتوصيات

1. توصلت الدراسة إلى أن استجابة المشاركين في الدراسة لفقرات محوري الإجراءات العملية، والإجراءات الاحترازية في متغير إدارة مخاطر تكنولوجيا المعلومات جاءت مرتفعة، وذات دلالة إيجابية؛ وتعكس موافقة أغلب المشاركين في الاستبيان عليها حيث كان المتوسط الحسابي للمحورين 4.07، و3.73 على التوالي.

2. وتوصلت الدراسة أيضاً إلى أن استجابة المشاركين في الدراسة لفقرات محور الاحتمالات البنكية في متغير إدارة مخاطر تكنولوجيا المعلومات جاءت مرتفعة، وذات دلالة إيجابية؛ وتعكس درجة الموافقة عليها بشدة من أغلب المشاركين في الاستبيان عليها حيث كان المتوسط الحسابي للمحور 4.25.

3. كما توصلت الدراسة إلى وجود أثر قوي لإدارة مخاطر تكنولوجيا المعلومات على الحد من مخاطر المعاملات المصرفية، إذ أظهرت نتائج التحليل وجود ارتباط إيجابي وقوي جداً بين تطبيق محاور مخاطر تكنولوجيا المعلومات (وتحديداً الإجراءات الاحترازية، والاحتمالات البنكية)، والحد من مخاطر المعاملات المصرفية، إذ إن الزيادة بمقدار وحدة واحدة في تطبيق الإجراءات الاحترازية يؤدي إلى الحد من مخاطر المعاملات المصرفية، بنسبة 62.6%، وكذلك الزيادة بمقدار وحدة واحدة في وعي العملاء بالاحتمالات البنكية يؤدي إلى الحد من مخاطر المعاملات المصرفية بنسبة 20.5%،

وفي النهاية؛ فهذه قائمة بأهم التوصيات المستخلصة من هذه الدراسة:

1. ضرورة العمل على زيادة الإجراءات العملية المتخذة بواسطة البنوك (مثل تقديم الاستشارات، والنصائح اللازمة للعملاء، وغيرها) للحد من مخاطر المعاملات المصرفية المرتبطة بتكنولوجيا المعلومات.
2. ضرورة زيادة الإجراءات الاحترازية المتخذة بواسطة البنوك (مثل توفير أنظمة بديلة للنظم الأصلية حال تعطلها) للحد من مخاطر المعاملات المصرفية المرتبطة بتكنولوجيا المعلومات.
3. ضرورة قيام المصارف، والبنوك في المملكة بزيادة وعي العملاء بالإجراءات الاحترازية اللازمة (مثل الإبلاغ فوراً عن أية محاولة للاحتيال الإلكتروني) للحد من مخاطر المعاملات المصرفية المرتبطة بتكنولوجيا المعلومات.
4. ضرورة توعية المواطن السعودي بأهمية وموثوقية المعاملات المصرفية الإلكترونية.
5. ضرورة الاهتمام برفع كفاءة موظفي البنوك بما يكفي لإدارة المخاطر المرتبطة بتكنولوجيا المعلومات.
6. ضرورة الاهتمام بتدريب الموظفين على استخدام تكنولوجيا المعلومات، مع تطوير وتحديث النظم والمعدات المستخدمة من خلال دورات التدريب المستمرة للعاملين.

7. ضرورة القيام بتحديث الخدمات المصرفية المقدمة للعملاء باستمرار، ومواكبة التطورات التكنولوجية الهائلة في المجال المصرفي.

8. ضرورة قيام البنوك بتعزيز كافة الإجراءات الأمنية اللازمة داخل البنك، وخارجه للحد من مخاطر المعاملات المصرفية المرتبطة بتكنولوجيا المعلومات.

9. ضرورة القيام بدراسات أخرى مشابهة على عينات دراسة مختلفة، وأكثر عدداً لتأكيد نتائج هذه الدراسة، وكذلك الخروج بتوصيات أخرى للحد من مخاطر المعاملات المصرفية المرتبطة بتكنولوجيا المعلومات.

قائمة المراجع:

المراجع العربية:

1. العازمي، ع. ا. (2022). دور تفعيل حوكمة تكنولوجيا المعلومات في تأمين المعلومات المحاسبية من المخاطر الالكترونية في ظل عصر الرقمنة دراسة تطبيقية على البنوك التجارية الكويتية. المجلة العلمية للدراسات والبحوث المالية والإدارية، 13(2)، 1115-1155.
2. سلطاني، الهاشي، صفيح، & صادق. (2022). إدارة مخاطر الخدمات المصرفية الإلكترونية في المصارف الإسلامية: دراسة حالة مصرف الراجحي السعودي. مجلة الاقتصاد و التنمية البشرية، 13(1)، 91-104.
3. عبد الرحمن المصباحي. (2022). تقارير شهرية للحد من التحايلات البنكية ، عكاظ.
4. محمد الغامدي . (2021). «الاحتيالات البنكية» طرق متجددة لاختراق حسابات العملاء ، اليوم.
5. مريم عثمانى. (2019). تطبيق الإدارة الإلكترونية في مجال الخدمات المصرفية بين ضرورة الانفتاح ومخاطر النجاح.
6. حميمش نرجس ، قالون جيلاني. (2017). دور تدقيق أنظمة تكنولوجيا المعلومات والاتصال في الحد من مخاطر المعاملات المصرفية الإلكترونية في الجزائر .
7. نزهة غالي. (2017). السفتجة الإلكترونية وقواعد قانون الصرف في التشريع الجزائري ، مجلة العلوم الإجتماعية ، العدد 25 .
8. حمو محمد وحمو علي . (2017). مكانة الصيرفة الإلكترونية في الجزائر ، مجلة دراسات في الاقتصاد والتجارة المالية ، العدد 02 ، 200 جامعة الجزائر 03 .
9. رشيد فراح وكريمة فرحي . (2015). متطلبات الأعمال الإلكترونية في العالم العربي بين الواقع وضرورة التحسين ، مجلة علوم الإقتصاد والتسيير والتجارة ، العدد 32 ، ص 151.
10. مريم خوبيزي . (2015). واقع إستخدام وسائل الدفع الإلكترونية في الجهاز المصرفي الجزائري وكيفية إدارة المخاطر الناتجة عنها وفقا لنموذج بازل الدولية للرقابة المصرفية ، مجلة الدراسات المالية والمحاسبية والإدارية ، العدد الرابع ، ص 41 .
11. عوض ، آمال محمد محمد. (2014). دور حوكمة تكنولوجيا المعلومات في ضبط مخاطر الأنشطة المصرفية الإلكترونية في البنوك السعودية. الفكر المحاسبي، مج 18 ، ع 4 ، 1 - 51 .

12. هاشم، أماني هاشم السيد حسن. (2012). تفعيل دور لجان المراجعة في الحد من المخاطر المصرفية الإلكترونية: دراسة ميدانية.مجلة التجارة والتمويل، ع 1، 301 - 367 .
13. رشيد بوعافية.(2012).آلية الدفع الإلكتروني بإستعمال بطاقة الإنتمان عبر شبكة الأنترنت، مجلة الاقتصاد الجديد، العدد 07 .
14. خالد محمود القطناني.(2004).أثر خصائص البيئة التقنية وتكنولوجيا المعلومات في مخاطر الرقابة التشغيلية دراسة تحليلية في المصارف الأردنية .

English Resources:

- 1-Lindqvistpontus, P., & Khailtash, D. (2022). The Impact of AI on Banks' Risk Management Approach . KTH Royal Institute of Technology.
- 2-Sharma, R., & Mittal, A. (2018). ROLE OF IT IN BANKING SECTOR & CHALLENGES. Indian Journal of Economics & Business, 17(3), 41-53.

ملاحق الدراسة :

الاستبيان :

المتغير المستقل إدارة مخاطر تكنولوجيا المعلومات

المحور الأول: الإجراءات العملية

مضمون العبارة / درجة الاتفاق	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
1. يتبع البنك أساليب متقدمة لإدارة مخاطر تكنولوجيا المعلومات					
2. يتم تقييم مخاطر تكنولوجيا المعلومات بالبنك بصفة دورية وصحيحة					
3. يعمل البنك باستمرار على تحسين أداء إدارة مخاطر تكنولوجيا المعلومات					
4. يوفر البنك الاستشارات، والنصائح اللازمة للعملاء للحد من مخاطر تكنولوجيا المعلومات					

المحور الثاني: الإجراءات الاحترازية

مضمون العبارة / درجة الاتفاق	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
1. يقوم البنك بإحاطة العملاء بالإجراءات الوقائية للحد من مخاطر تكنولوجيا المعلومات					
2. يقوم البنك بتوفير النظم الرقابية التي يمكن أن تؤدي إلى تخفيف مخاطر تكنولوجيا المعلومات					
3. يقوم البنك بتحديث وتغيير نظم رقابة تكنولوجيا المعلومات باستمرار لتواكب أية متغيرات جديدة					
4. يتمتع العاملون بالبنك بالخبرة اللازمة لتقليل مخاطر استخدام تكنولوجيا المعلومات					
5. يوفر البنك أنظمة بديلة في حالة تعطل النظام الأصلية					
6. يتبع البنك الإجراءات اللازمة لحماية البرامج، والتطبيقات من المحاولات غير العادية للاختراق، والهكرز					

المحور الثالث: الاحتيالات البنكية

مضمون العبارة / درجة الاتفاق	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
1. يُعد التعرض للاحتيالات البنكية أمراً شائعاً في ظل بيئة تكنولوجيا المعلومات					
2. يُعد الاحتيال عن طريق الرسائل النصية أشهر طرق الاحتيالات البنكية					
3. لا أقوم بالرد إطلافاً على أي رسالة تأتي من رقم مجهول فيها طلب لبعض بياناتي البنكية					
4. أقوم بالإبلاغ فوراً عن أية محاولة للاحتيال الإلكتروني					
5. يقوم البنك بالحفاظ على سرية معلومات العملاء لتفادي عمليات الاحتيال الإلكتروني					

المتغير التابع: الحد من مخاطر المعاملات المصرفية

مضمون العبارة / درجة الاتفاق	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
1. يقوم البنك بتوضيح المعاملات المصرفية الأكثر تعرضاً لمخاطر تكنولوجيا المعلومات للعملاء					
2. يقوم البنك بعمل نظام لرقابة وأمن المعاملات المصرفية الإلكترونية التي تتم من خلال أساليب تكنولوجيا المعلومات					
3. يتم توفير معلومات لعملاء البنك حول المعاملات المصرفية الإلكترونية وكيفية استخدامها بطريقة صحيحة					
4. يتبع البنك يتبع كافة المحاولات الممكنة لتفادي مخاطر المعاملات المصرفية الإلكترونية في بيئة تكنولوجيا المعلومات					

<https://forms.gle/1RidnBEJU73PygiG6>

الخاتمة

ملخص الدراسة باللغة العربية

تُعد إدارة المخاطر الإلكترونية أحد مصادر القلق الكبيرة للمؤسسات المالية والمصرفية بسبب المشاكل والأزمات العديدة التي واجهتها، وتُعد البنوك الأكثر عرضة بشكل خاص للمخاطر التقنية ومخاطر تكنولوجيا المعلومات، لأنها تعتمد على الأنظمة الفنية لتخزين المعلومات ومعالجتها. ونظراً للدور الهام الذي تلعبه البنوك في اقتصاد البلدان، من خلال تقديمها للعديد من الخدمات مثل الخدمات المصرفية عبر الإنترنت وبطاقات الائتمان والمعاملات الإلكترونية، فإن إدارة المخاطر تُعد جزءاً مهماً من أنظمة حماية البنوك وأصول معلوماتها يساعد على حمايتهم من المخاطر المتعلقة بتكنولوجيا المعلومات، إضافة إلى ذلك؛ يجب أن يكون لدى البنوك عملية فعالة لإدارة المخاطر لحماية المؤسسة ورسالتها، وليس فقط أصول تكنولوجيا المعلومات، لذا فلا بد من إيجاد طرق جديدة للتعامل مع مخاطر المعاملات المصرفية، وخاصة المعاملات الإلكترونية الحديثة. ومن هنا كانت أهمية هذه الدراسة في إعداد آلية فعالة للتعامل مع مخاطر تكنولوجيا المعلومات المستخدمة في المصارف البنكية وذلك لإحباط هذه المخاطر قبل حدوثها، أو التخفيف من أثرها في حال وقوعها.

وقد استخدم الباحث المنهج الوصفي الاستقرائي فيما يتعلق بالبيانات الخاصة بالإطار النظري للدراسة، كما استخدم أسلوب قائمة الاستقصاء (الاستبانة) لتجميع بيانات الدراسة، بالإضافة إلى ذلك؛ فقد تم الاعتماد على المنهجين الوصفي والتحليلي لتحليل نتائج الدراسة وتفسيرها. كما شملت أدوات الدراسة البحثية كلاً من المصادر الأولية؛ والتي تمثلت في الاستبيان، والمصادر الثانوية؛ والتي تمثلت في الكتب والمراجع والدوريات والمؤتمرات.

وقد توصلت الدراسة إلى وجود أثر قوي لإدارة مخاطر تكنولوجيا المعلومات على الحد من مخاطر المعاملات المصرفية؛ وتحديدًا اتباع الإجراءات الاحترازية، وتوعية العملاء بالاحتمالات البنكية التي من الممكن أن يتعرضوا لها؛ إذ يؤدي كلاً من ذلك إلى الحد من مخاطر المعاملات المصرفية بنسبة كبيرة.

وبناءً على ذلك؛ يُمكن القول بأن نتائج هذه الدراسة تعطي دلالة واضحة، وقوية لأهمية دور إدارة مخاطر تكنولوجيا المعلومات على الحد من مخاطر المعاملات المصرفية، وإمكانية تطبيق ذلك عملياً من خلال بعض التصورات المهنية مثل: زيادة اتخاذ الإجراءات العملية، والاحترازية المتخذة بواسطة البنوك للحد من مخاطر المعاملات المصرفية المرتبطة بتكنولوجيا المعلومات، والقيام بتوعية المواطن السعودي بأهمية وموثوقية المعاملات المصرفية الإلكترونية، وزيادة وعيه فيما يخص الاحتمالات البنكية التي من الممكن أن يتعرض لها، والاهتمام برفع كفاءة موظفي البنوك، وكذلك تحديث الخدمات المصرفية المقدمة للعملاء باستمرار، ومواكبة

التطورات التكنولوجية الهائلة المصاحبة لها، وأخيراً ضرورة قيام البنوك بتعزيز كافة الإجراءات الأمنية اللازمة داخل البنك.

English abstract:-

Cyber risk management is one of the significant concerns of financial and banking institutions due to the several problems and crises they have faced. Generally, Banks are the most vulnerable to technical and information technology (IT) risks because they rely on technical systems to store and process information. Given the critical role that banks play in the economies of countries by providing many services such as online banking, credit cards, and electronic transactions, risk management is an integral part of the protection systems of banks and their information assets that helps protect them from IT-related risks. In addition; Banks must have an effective risk management process in place to protect the organization and its mission, not just IT assets, therefore, new ways to deal with the risks of banking transactions, especially modern electronic transactions, must be found. Hence, the importance of this study in preparing an effective mechanism to deal with the risks of information technology used in banking banks to thwart these risks before they occur, or mitigate their impact.

The researcher used the descriptive and inductive approach concerning the data of the study's theoretical framework and used the survey list method (questionnaire) to collect the study data; in addition, the descriptive and analytical methods were relied on to analyze and interpret the results of the study. Also, the research study tools included two sources: first, primary sources, represented in the questionnaire. Second, secondary sources are represented in books, references, periodicals, and conferences.

The study found a strong impact of IT risk management on reducing the risks of banking transactions, precisely following precautionary measures, and educating customers about bank frauds that they may be exposed to, as both lead to reducing the risks of banking transactions by a large percentage.

Accordingly, it can be said that the results of this study give a clear and strong indication of the importance of the role of information technology risk management in reducing the risks of banking transactions and the possibility of applying this practically through some professional perceptions such as: increasing the practical and precautionary measures taken by banks to reduce the risks of banking transactions related to information technology, educating the Saudi citizen about the importance and reliability of electronic banking transactions, and increase his awareness regarding bank frauds that he may be exposed. Moreover, the current study pays attention to raising the efficiency of bank employees, updating banking services provided to customers continuously, keeping pace with the tremendous technological developments associated with them, and finally, the need for banks to strengthen all necessary security measures within the bank.