

جامعة ميدأوشن

كلية الإدارة

تخصص إدارة مخاطر

أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية دراسة
تطبيقية على مصرف الراجحي

إعداد الطالب

نورة مطلق مسفر الخامسي

233001453

إشراف/

د. الفصيل عبد الحميد محمد حسن

العام الدراسي:

2024



Contents

4	مقدمة:
4	مشكلة الدراسة:

5	أهمية الدراسة:
6	أهداف الدراسة:
6	تساؤلات الدراسة
7	فروض الدراسة:
7	نموذج الدراسة
8	الدراسات السابقة:
8	المنطلقات النظرية للدراسة:
19	المنهجية وطرق البحث:
20	مصادر جمع البيانات
20	أدوات الدراسة :
21	حدود الدراسة :
21	المراجع:

مقدمة:

أصبحت التكنولوجيا والاتصالات الرقمية جزءاً لا يتجزأ من حياتنا اليومية، ظهرت مخاطر الأمن السيبراني كتهديد متنام ينذر بعواقب وخيمة هذه المخاطر تتخذ أشكالاً متعددة، من اختراقات البيانات الحساسة إلى الاحتيال الإلكتروني والهجمات الموجهة لأنظمة البنية التحتية الحيوية. (محمد، 2019)

فعلى سبيل المثال، تعرض البيانات الشخصية والمالية لخطر السرقة من قبل قرصنة إلكترونيين يسعون إلى الحصول على معلومات حساسة لأغراض إجرامية كما أن الوصول غير المصرح به إلى أنظمة الحكومات والشركات يمكن أن يؤدي إلى تعطيل الخدمات الحيوية وإلحاق أضرار اقتصادية بالغة وفي بعض الحالات، قد تستخدم الهجمات السيبرانية لزعزعة الاستقرار السياسي والاجتماعي من خلال نشر المعلومات المضللة وتشويه السمعة. (بانقا، 2019)

إن هذه التهديدات تتطور باستمرار مع ظهور تقنيات متطورة للاختراق والاستغلال ولذلك، باتت حماية البيانات والأنظمة الحساسة أمراً بالغ الأهمية لمواجهة هذه المخاطر المتزايدة وتتطلب ذلك جهوداً مشتركة من قبل الحكومات والشركات والأفراد لتطوير استراتيجيات فعالة للأمن السيبراني، بما في ذلك تعزيز الوعي والتدريب والاستثمار في تقنيات الحماية المتقدمة إن المواجهة الناجحة لمخاطر الأمن السيبراني ستكون حاسمة في الحفاظ على الأمن والاستقرار في عالمنا المتصل رقمياً. (البغدادي، 2021)

كما تعد البطاقات المصرفية أداة مالية بالغة الأهمية في العصر الحديث، حيث أصبحت جزءاً لا يتجزأ من حياتنا اليومية هذه البطاقات تأتي بأشكال وأنواع متنوعة، كالبطاقات الائتمانية وبطاقات الخصم المباشر والبطاقات المسبقة الدفع، وتقدم مجموعة واسعة من الخدمات والمزايا للمستخدمين. (محمد، 2019)

البطاقات الائتمانية، على سبيل المثال، تتيح للحاملين القدرة على الشراء والسداد في وقت لاحق مع إمكانية الاستفادة من الائتمان المتاح وتسديد القيمة على أقساط أما بطاقات الخصم المباشر فتربط مباشرة بحساب المستخدم المصرفي، مما يمكنه من السحب النقدي والدفع المباشر من رصيده وهناك أيضاً البطاقات المسبقة الدفع التي يتم شحنها بمبالغ محددة مسبقاً، وتوفر مرونة في الإنفاق والتحكم بالمصروفات. (البغدادي، 2021)

إن استخدام البطاقات المصرفية يوفر للمستخدمين الراحة والأمان في إجراء المعاملات المالية، سواء أثناء السفر أو في حياتهم اليومية كما أنها تسهل عمليات الشراء عبر الإنترنت وتعزز الشمول

المالي من خلال إتاحة الخدمات المصرفية لفئات أوسع من السكان علاوة على ذلك، تساهم البطاقات في إدارة الأموال بشكل أكثر كفاءة وشفافية. (بانقا، 2019).

مشكلة الدراسة:

في ظل التطور الهائل في التكنولوجيا الرقمية والذي شمل كافة أنشطة المؤسسات المصرفية، برز بشكل ملحوظ مخاطر الأمن السيبراني على البنوك وعملائها. إن البطاقات المصرفية أصبحت أداة مالية بالغة الأهمية في حياتنا اليومية، حيث تقدم مجموعة واسعة من الخدمات والمزايا للمستخدمين. ويوفر استخدام هذه البطاقات الراحة والأمان في إجراء المعاملات المالية، سواء أثناء السفر أو في الحياة اليومية. كما تسهل عمليات الشراء عبر الإنترنت وتعزز الشمول المالي.

ومع ذلك، فإن التطور التكنولوجي الرقمي المتسارع قد أدى إلى ظهور مخاطر الأمن السيبراني على البنوك وعملائها. وهذا ما يدفع الباحث إلى دراسة أثر هذه المخاطر على استخدام البطاقات المصرفية، من خلال التركيز على حالة مصرف الراجحي كدراسة تطبيقية. إن فهم هذا الأثر سيساعد في تطوير إجراءات وتقنيات أمنية فعالة لحماية البطاقات المصرفية وتعزيز ثقة المستخدمين في استخدامها ووفقاً للدراسات السابقة المتعلقة بموضوع البحث، يرى الباحث أن مشكلة البحث يمكن صياغتها في السؤال الرئيسي التالي:

ما هو أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية؟ دراسة تطبيقية على مصرف الراجحي؟

أهمية الدراسة:

تستمد هذه الدراسة أهميتها من جانبين:

الأهمية العلمية:

تتناول متغيرات هامة مثل مخاطر الأمن السيبراني بأبعادها (مخاطر الامن السيبراني، مخاطر امن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية) واستخدام البطاقات المصرفية بأبعادها (البطاقات المصرفية)، والتي لم يتم دراستها على نطاق واسع ولذلك يؤمل أن تشكل الدراسة الحالية إضافة علمية حديثة تكون نقطة انطلاق للباحثين لإجراء الدراسات والبحوث المتعلقة بموضوع الدراسة الحالية.

الأهمية العملية:

تتعرز أهمية هذه الدراسة من خلال التطور التكنولوجي المستمر، والذي زاد من توقعات واحتياجات البنوك وأصبح من الضروري بالنسبة لها توفير حلول وأدوات متقدمة للسيطرة على مخاطر الأمن السيبراني والتخفيف منها ومن المؤمل أن تسلط هذه الدراسة ونتائجها وتوصياتها الضوء على هذه القضية وتكون بمثابة قاعدة معلومات لصناع القرار في مصرف الراجحي

أهداف الدراسة:

أجريت هذه الدراسة بهدف قياس أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية دراسة تطبيقية على مصرف الراجحي ويتفرع منه مجموعة من الأهداف الفرعية:

- التعرف على اثر مخاطر الامن السيبراني في استخدام البطاقات المصرفية
- التعرف على اثر مخاطر امن المعلومات في استخدام البطاقات المصرفية
- التعرف على اثر مخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية
- التعرف على اثر مخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية
- التعرف على اثر مخاطر الامن السيبراني في البطاقات المصرفية

تساؤلات الدراسة

السؤال الرئيسي الأول : ما هو أثر مخاطر الأمن السيبراني بأبعادها (مخاطر الامن السيبراني، مخاطر امن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية) واستخدام البطاقات المصرفية بأبعادها (البطاقات المصرفية)، دراسة تطبيقية على مصرف الراجحي وتتفرع منه عدة أسئلة فرعية كالتالي:

- السؤال الفرعي الأول: كيف يؤثر مخاطر الامن السيبراني في استخدام البطاقات المصرفية على مصرف الراجحي؟
- السؤال الفرعي الثاني: كيف يؤثر مخاطر امن المعلومات في استخدام البطاقات المصرفية على مصرف الراجحي؟
- السؤال الفرعي الثالث: كيف يؤثر مخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية على مصرف الراجحي؟

➤ السؤال الفرعي الرابع: كيف تؤثر المخاطر التشغيلية في استخدام البطاقات المصرفية على مصرف الراجحي؟

➤ السؤال الفرعي الخامس: كيف تؤثر مخاطر الامن السيبراني على البطاقات المصرفية على مصرف الراجحي؟

فروض الدراسة:

وللإجابة على أسئلة البحث وتحقيق أهدافه، تم صياغة الفرضيات التالية:

الفرضية الرئيسية الأولى: لا يوجد تأثير ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمخاطر الأمن السيبراني بأبعاده (مخاطر الامن السيبراني، مخاطر امن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية) دراسة تطبيقية على مصرف الراجحي ويتفرع منها الفرضيات الفرعية التالية:

1. **الفرضية الفرعية الأولى Ho1:** لا يوجد تأثير ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية بالتطبيق على مصرف الراجحي

2. **الفرضية الفرعية الثانية Ho2:** لا يوجد تأثير ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمخاطر امن المعلومات في استخدام البطاقات المصرفية بالتطبيق على مصرف الراجحي

3. **الفرضية الفرعية الثالثة Ho3:** لا يوجد تأثير ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية بالتطبيق على مصرف الراجحي

4. **الفرضية الفرعية الرابعة Ho4:** لا يوجد تأثير ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمخاطر التشغيلية في استخدام البطاقات المصرفية بالتطبيق على مصرف الراجحي

5. **الفرضية الرئيسية الثانية:** لا يوجد تأثير ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لاستخدام البطاقات المصرفية بأبعاده (البطاقات المصرفية) دراسة تطبيقية على مصرف الراجحي ويتفرع منها الفرضية الفرعية التالية:

1. **الفرضية الفرعية:** لا يوجد تأثير ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمخاطر الامن السيبراني في البطاقات المصرفية بالتطبيق على مصرف الراجحي

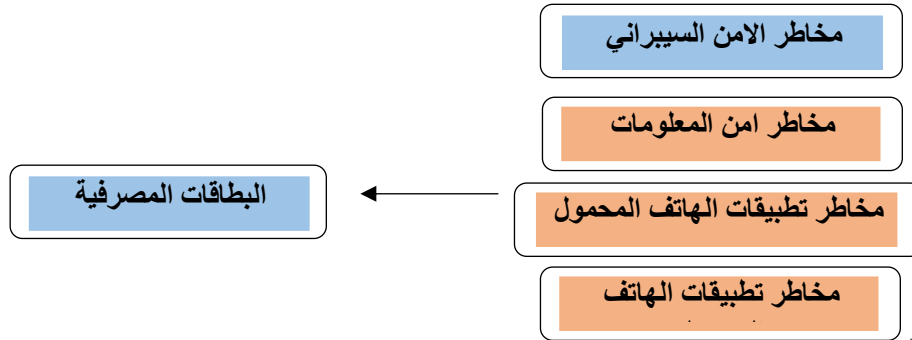
نموذج الدراسة

يوضح الشكل 1-1 النموذج المدروس مع متغيراته مخاطر التطبيق والمخاطر التشغيلية والمخاطر السيبرانية ومتغير تابع يتمثل في البطاقات المصرفية في مصرف الراجحي.

المتغير

المتغير المستقل

التابع



المصدر: إعداد الباحث

الدراسات السابقة:

1. دراسة محمد (2019) بعنوان:

"الأمن السيبراني في القطاع المصرفي - صندوق النقد العربي"

وترى هذه الدراسة أن التطور المذهل الذي شهدته صناعة التكنولوجيا المالية والفرص التي أتاحتها للبنوك لتحسين مستوى ونوع الخدمات المقدمة للعملاء من خلال ابتكار قنوات جديدة إلا أن هذه الفرص التي تركتها تكنولوجيا المعلومات والاتصالات تشكل تحدياً خاصاً ولكي تستمر البنوك في الابتكار مع بقائها عرضة لمخاطر الهجمات الإلكترونية يتعين على البنوك إجراء اختبار إجهاد لتحديد مدى تأثيرات أي عملية اختراق ناجحة على الأنظمة الإلكترونية لتلك البنوك بشكل نصف سنوي أو سنوي. كما تم ذكر المخاطر المتعلقة بالبرامج الإلكترونية التي تقوم بالمعاملات المصرفية الإلكترونية وضرورة تأمين هذه العمليات بتهيئة برامج الحماية لحمايتها من الاختراق واختبارها للتأكد من فعاليتها. كما تؤكد على أهمية وجود معايير محددة تنظم المخاطر الإلكترونية حيث تختلف

الآراء حول كيفية تنظيم المخاطر الإلكترونية حيث يرى البعض أن الطبيعة المتطورة للمخاطر الإلكترونية لا تخضع لتنظيم محدد وأنه يمكن معالجة القضايا الخاصة بالإنترنت من خلال الدفع الحالي الأحكام المتعلقة بالمخاطر التشغيلية والتكنولوجيات في هذا القسم.

2. دراسة بانقا (2019) بعنوان:

"مخاطر الهجمات الإلكترونية السيبرانية وآثارها الاقتصادية"

تم إجراء دراسة حالة لدول مجلس التعاون الخليجي بهدف توضيح أهمية المخاطر السيبرانية وكيفية إدارتها وكانت النتائج وأهمها تحسن أداء دول مجلس التعاون الخليجي في التعامل مع الجرائم السيبرانية إلا أنها أظهرت أن الدليل العالمي للأمن السيبراني يحدد القضايا القانونية والتنظيمية والتدريبية والتعاونية التي تحتاج إلى تطوير الحلول والقدرات ضد الهجمات السيبرانية

3. دراسة الشورة (2020) بعنوان:

"الأمن السيبراني في البنوك الإسلامية الأردنية"

وتبين هذه الدراسة أن التهديدات السيبرانية لا تزال في طور التطور وهذا دليل على ذكاء وإتقان القراصنة من خلال إيجاد نقاط ضعف وثغرات قد لا تكون مهمة أو ملحوظة لنا كمستخدمين للتكنولوجيا الرقمية وقد تكون هذه التهديدات من قبل القراصنة مادية بقصد الابتزاز أو معنوية أو لديها نية الإضرار بفرد أو مجتمع أو بلد بأكمله كما ترى هذه الدراسة أن سبب زيادة المخاطر السيبرانية في يعود إلى قلة الخبرة المهنية في هذا المجال ولا يزال الأمن السيبراني في فترة النمو والتطور وخاصة بعد إقرار مؤخراً لقانون الأمن السيبراني بالإضافة إلى توجيه البنك المركزي الذي يلزم البنوك بتبني سياسة الأمن السيبراني. وتؤكد هذه الدراسة على أهمية الأمن السيبراني وأنه ضرورة ملحة ويتطلب تعاون القطاعين العام والخاص لتطوير البنية التحتية الرقمية المتقدمة وزيادة الوعي والتتقيف في هذا المجال وتوصي باعتماده كمقرر جامعي.

4. دراسة الزيود (2020) بعنوان:

"إدارة مخاطر الأمن السيبراني في المصرف"

تناولت هذه الدراسة مفهوم المخاطر السيبرانية من كافة الجوانب وأنواع ومجالات التهديدات فبالإضافة إلى تنفيذ ومتابعة كافة التعليمات الصادرة في البنوك الإسلامية الأردنية وتلتزم المصارف بالسياسات المتعلقة بأمن المعلومات والأمن السيبراني كما تقوم البنوك بنشر إرشادات الحوكمة المؤسسية في تقاريرها السنوية ومن ناحية أخرى تبين هذه الدراسة أن السياسات المتبعة فيما يتعلق بالمخاطر السيبرانية بالإضافة إلى الحاجة إلى نشر المزيد من التوضيحات حول مدى المخاطر السيبرانية وقدرة البنوك على التعامل معها والتعامل مع هذه المخاطر تتطلب توضيحاً أكثر تفصيلاً وتبحث هذه الدراسة الإجراءات المتبعة في المصارف لإدارة المخاطر السيبرانية من خلال تحديد

وتأكيد إجراءات وأساليب إدارة المخاطر السيبرانية وفقاً لاعتبارات السرية وتوفير أصول السلامة والمعلومات الفنية ومتابعة تطبيق الإجراءات في كافة الفروع بالإضافة إلى تقييم المخاطر السيبرانية يقوم المصرف بإجراء المشاريع الفنية قبل إجراء التغييرات أو إدخال أطراف خارجية أو إطلاق خدمات جديدة وأخيراً مراجعة منهجية إدارة المخاطر السيبرانية وتوثيق التغييرات وفقاً لذلك إلى فترة زمنية محددة

5. دراسة السمحان 2020 بعنوان

"متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود

أجريت هذه الدراسة بهدف التعرف على متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود وقد شملت العينة المدروسة (5%) من أفراد المجتمع أي (478) فرداً وتم استخدام الوزن النسبي واختبار مربع كاي لاختبار الفرضيات وخلصت الدراسة إلى أن متطلبات الأمن السيبراني لحماية أنظمة المعلومات الجامعية تأتي في مقدمة المتطلبات المالية وأوصت هذه الدراسة بضرورة اهتمام جامعة الملك سعود بمتطلبات حماية أنظمة المعلومات الإدارية بالجامعة والتأكيد على وعي العاملين في كافة المؤسسات الحكومية وتطوير معاييرهم المهنية وخلق بنية تحتية لدخول ساحة صناعة البرمجيات العالمية والقدرة على المنافسة.

6. دراسة منصور 2021 بعنوان:

"تأثير الأمن السيبراني على الرقابة الداخلية وإنعكاسها على الوحدة الاقتصادية دراسة

استطلاعية لآراء عينة من المدققين والمحاسبين في وزارة التعليم العالي والبحث العلمي

تهدف هذه الدراسة إلى التعرف على أهمية الأمن السيبراني من خلال تأثيره على الرقابة الداخلية وقيمة الوحدة الاقتصادية من خلال تبني إطار حوكمة تكنولوجيا المعلومات (COBIT5) (وهو إطار معتمد لحوكمة وإدارة تكنولوجيا المعلومات بالاعتماد على المنهج الوصفي التحليلي للبيانات الأولية من خلال استبانة قدمت لعينة مكونة من (98) مدققاً ومحاسباً يعملون في التعليم العالي والبحث العلمي في العراق أجريت الدراسة بعد تحليل البيانات وتوصلت إلى وجود علاقة بين أبعاد ومتطلبات الأمن السيبراني والعمليات والإجراءات والمخاطر السيبرانية وحماية السرية والخصوصية واستراتيجية الأمن المنطقي في الأطر الحديثة للرقابة الداخلية (COBITS) وقيمة الوحدة الاقتصادية فضلاً عن حاجة الوحدة الاقتصادية إلى تبني أدوات فعالة لتقييم الضوابط الداخلية بشكل مستمر للحفاظ على أمن المعلومات من خلال تبني أطر الرقابة الداخلية الحديثة (COBITS) ومن خلال دمج الإجراءات والميزات في ضوء الأطر الحديثة لمنع اختراق الأنظمة الإلكترونية والجهود الرامية إلى التلاعب بمعلوماتها وتتناول هذه الدراسة مفهوم الأمن السيبراني وأثره على الرقابة الداخلية.

7. دراسة البغدادي 2021 بعنوان:

"اقتصاديات الأمن السيبراني في القطاع المصرفي"

تهدف هذه الدراسة إلى التعرف على اقتصاديات الأمن السيبراني في القطاع المصرفي من خلال تسليط الضوء على التحديات التي تواجه المجتمع لتحقيق الأمن السيبراني وآليات تعزيزه في البنوك الإلكترونية وذلك بالاعتماد على منهج تحليلي مقارن وهو ما تم تناوله في الأدبيات والدراسات السابقة. ومع تناول موضوع الدراسة ومن ثم للدراسات السابقة خلصت هذه الدراسة إلى أن الطبيعة المتطورة للمخاطر السيبرانية ليست منظمة بشكل خاص وأنه يمكن معالجة القضايا السيبرانية من خلال الأنظمة الحالية المتعلقة بالمخاطر التشغيلية والتكنولوجية. وفي نهاية البحث أوصى الباحث بضرورة وضع أسس للتحقيق في هذه المخاطر وإدارتها وتحديد دقيق لمسؤوليات الأطراف المختلفة ذات الصلة بها والحصول على ترخيص من البنك. وتوفير البيانات اللازمة لها.

8. دراسة الزيود (2021) بعنوان:

"أثر التدقيق الداخلي في الحد من مخاطر السيبرانية في البنوك التجارية"

أجريت هذه الدراسة بهدف التعرف على أثر التدقيق الداخلي على كفاءة التدقيق الداخلي وحياد التدقيق الداخلي والوضع التنظيمي للتدقيق الداخلي وتخطيط التدقيق الداخلي في الحد من المخاطر السيبرانية في المصارف وهدفت هذه الدراسة إلى استخدام الاستبانة كأداة دراسة لجمع البيانات من عينة الدراسة والتي يشمل مجتمع الدراسة المدققين الأجانب العاملين في مكاتب التدقيق الأجنبية حيث تم تحديد العينة بعدد (520) مدققاً و(235) مدققاً يقومون بأعمال التدقيق في البنوك التجارية و(235) استبانة لهم كما تبين أن عدد الاستبانات الصالحة للتحليل الإحصائي بلغ (169) بنسبة مئوية بلغت (0.72). وللإجابة عن أسئلة مشكلة البحث واختبار فرضيات البحث أجرى الباحث الاختبارات الإحصائية الوصفية والتي تم توضيحها بال تكرارات والنسب المئوية والمتوسط الحسابي والانحراف المعياري ودرجة الأهمية النسبية واختبار معامل الثبات ألفا كرونباخ وتحليل الانحدار المتعدد وتوصلت نتائج الدراسة الحالية إلى أنه بالنسبة للتدقيق الداخلي الكفاءة والوضع التنظيمي والتخطيط في الحد من المخاطر السيبرانية في البنوك التجارية كما توصلت الدراسة إلى عدم وجود تأثير للتدقيق الداخلي الحيادية في الحد من المخاطر السيبرانية في البنوك وتوصي هذه الدراسة بضرورة تشجيع إدارة البنوك على زيادة مستوى الوعي والمسؤولية تجاه المخاطر السيبرانية وأثرها على أدائها وقدراتها وتوصي برفع مستوى البنوك الوعي بأهمية تأثير التدقيق الداخلي في الحد من المخاطر السيبرانية.

9. دراسة أبو الهيجاء 2021 بعنوان:

"المخاطر السيبرانية من الناحية الاقتصادية والمالية"

وبهدف التعرف على عواقب المخاطر السيبرانية والواقع الجديد الذي تفرضه هذه المخاطر على القطاع الاقتصادي بشكل عام والقطاع المالي بشكل خاص اتبعت هذه الدراسة المنهج الوصفي من خلال مراجعة الدراسات والبحوث والإحصاءات والندوات والمصادر العلمية والمقالات التي تناولت موضوع الدراسة كما استخدمت هذه الدراسة الإحصائيات المنشورة على المواقع الإلكترونية لدعم نتائج الدراسة الحالية وتوصلت الدراسة إلى أن القطاعات الاقتصادية هي الأكثر عرضة للجرائم السيبرانية وخاصة القطاع المصرفي وبحسب البنك الدولي فإن قطاع الخدمات المالية يشهد هجمات إلكترونية أكثر (65%) من أي قطاع آخر وأوصت الدراسة بتطوير استراتيجية وطنية لنشر الوعي بالأمن السيبراني والمخاطر السيبرانية وتقبل مسؤولية جميع الأطراف فيما يتعلق بالأمن السيبراني وأهميته وضرورة التأمين المستقبلي ضد هذه المخاطر.

10. دراسة زوايب وحاج علي 2021 بعنوان:

"تأثير تكنولوجيا المعلومات والاتصال على المخاطر التشغيلية بالبنوك دراسة إستقصائية على عدد من البنوك التجارية الجزائرية"

أجريت هذه الدراسة بهدف إظهار أثر تكنولوجيا المعلومات والاتصالات على المخاطر التشغيلية وقد تم إعداد استبانة كأداة لجمع البيانات من موظفي البنوك التجارية في الجزائر وخلصت هذه الدراسة إلى وجود علاقة ارتباط بين استخدام تكنولوجيا المعلومات والاتصالات في البنوك التجارية والمخاطر التشغيلية مما يعني أنه كلما تصرف البنك بناءً عليها ومع التكنولوجيا العالية يتم التحكم في المخاطر التشغيلية والتنبيه بها وضمان حسن إدارتها وفي هذا البحث أوصى بمحاولة زيادة كفاءة العنصر البشري من خلال عقد دورات تدريبية في مجال تكنولوجيا المعلومات والاتصالات من أجل زيادة التحكم في أدوات التكنولوجيا الجديدة وتشكيل لجنة متخصصة لإدارة وتوقع المخاطر التشغيلية مع الأخذ في الاعتبار ما ورد في قرارات بازل بشأن إدارة المخاطر التشغيلية.

11. دراسة (أبو الخير (2022) بعنوان

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية"

أجريت هذه الدراسة بهدف اختبار أثر جودة التدقيق الداخلي في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية وفي البنوك الإلكترونية المسجلة في السوق المصري تم استخدام هذا الاستبيان كأداة للدراسة وتم استخدام هذا الاستبيان بين (1000) موظف تم توزيعهم باستخدام برنامج SPSS وأظهرت النتائج أن هناك تطور في المخاطر السيبرانية مما يجعل المؤسسات المالية وخاصة البنوك الإلكترونية تقوم بإجراء بحوث مستمرة ومكثفة من أجل اتخاذ

الإجراءات الوقائية ضد هذه المخاطر من خلال لوائح تجعل هذه الإجراءات لمجلس الإدارة وتوضح وتشجع وفي هذه الدراسة كان من الضروري محاولة تكثيف الوعي لدى العملاء من خلال البرامج السمعية والبصرية والندوات الثقافية لرفع مستوى الثقافة والأمن السيبراني بين هذه البنوك بهدف معرفة الضوابط والتعليمات المتعلقة بأمن أنظمة المعلومات والفضاء السيبراني

12. دراسة أميرهم (2022) بعنوان:

"أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على ترشيد قرارات المستثمرين

أجريت هذه الدراسة بهدف تحديد أثر جودة التدقيق الداخلي في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية وقد اقتصر عينة الدراسة على مسؤولي إدارة الخدمات ومسؤولي تكنولوجيا المعلومات ومسؤولي إدارة المخاطر في البنوك الإلكترونية على السوق المالية المصرية ولتحقيق أهداف البحث تم استخدام المنهج الوصفي التحليلي ويتكون مجتمع الدراسة من جميع العاملين في هذه الإدارة وقد تم اختيار عينة من 448 عاملاً وإعداد استبانة وتوزيعها على العينة المدروسة وتم استخدام برنامج SPSS لتحليل البيانات وبما أن الإجراءات أصبحت أكثر شفافية لمجالس إدارة تلك البنوك مما يؤدي إلى دعم الاستقرار المالي في تلك البنوك فقد أوصت هذه الدراسة بالعديد من التوصيات أهمها: بذل الجهود لزيادة وعي العملاء من خلال البرامج السمعية والبصرية والندوات التثقيفية لزيادة مستوى ثقافة الأمن السيبراني بين العملاء في القطاع المصرفي بهدف فهم الضوابط والتعليمات الخاصة بأمن أنظمة المعلومات والفضاء السيبراني.

13. دراسة قرزيز وزيدان (2022) بعنوان

دور أمن المعلومات في تحقيق جودة الخدمات المصرفية

أجريت هذه الدراسة بهدف إبراز مساهمة الأمن المعلوماتي في تحقيق جودة الخدمات المصرفية على مستوى المكتب الإقليمي للشلف وكأداة أولية لجمع البيانات شملت عينة البحث 55 موظفا لديهم معرفة بالأمن المعلوماتي بناء على عينة قصدية حيث تم استخدام برنامج SPSS لتحليل البيانات بين الأمن المعلوماتي وجودة الخدمات المصرفية وقد أظهرت النتائج وجود فرق ذي دلالة إحصائية عند مستوى 0.05 لجودة الخدمات المصرفية يعزى لمتغيرات السن والمستوى التعليمي والمهنة وتوصي هذه الدراسة بضرورة تدريب الموظفين وتمكينهم من البرامج والآليات الحديثة للتعامل مع التهديدات المصرفية وتحقيق جودة الخدمة بناء على قضايا تتعلق بالخصوصية والأمن والتوافر.

14. دراسة اشويقي وآخرون (2022) بعنوان

معوقات استخدام بطاقات الدفع الإلكتروني في المصاريف التجارية

أجريت هذه الدراسة بهدف فهم المشاكل التي تواجه المستهلك في استخدام بطاقات الدفع الإلكترونية في السوق الليبي والمصارف التجارية بالإضافة إلى معرفة وعي المصرف باستخدام بطاقات الدفع الإلكترونية في المصارف التجارية الليبية وذلك بالاعتماد على دراسة الأدبيات النظرية للموضوع. بالإضافة إلى المنهج الوصفي توصل البحث إلى عدة نتائج من خلال دراسة ميدانية على مستخدمي البطاقات الإلكترونية في مصرف تجارت ومصرف التنمية أجدابيا كان من أهمها أن مستخدمي هذه البطاقات يفضلون الدفع النقدي في أغلب المعاملات التجارية على الطرق الأخرى. كما أن هناك العديد من الأسباب التي تؤدي إلى انتشار استخدام البطاقات الإلكترونية ومن أهمها ضعف وسائل الدفع الإلكترونية والخوف من التقنيات وعدم إلمام المستخدمين بها ووجود مشاكل مع أجهزة الصرف الآلي بالإضافة إلى الانقطاعات المتكررة لشبكة الاتصالات وذلك لعدة أسباب من أهمها سهولة فقدان البطاقة بسبب صغر حجمها والخوف من سوء استخدام البطاقة. ضعف وسائل الإعلام والإعلان فيما يتعلق بوسائل الدفع الإلكترونية. ومن الموصى به في هذا البحث الاهتمام بالتنوع المصرفية والانتمائية في المجالات المختلفة وخاصة التبادلات مع الحكومة وضرورة دعم الحكومة وتوفير البنية التحتية لشبكة الاتصالات بالإضافة إلى وضع القواعد والأنظمة التي تنظم وتضمن العمليات المصرفية الإلكترونية.

15. دراسة رشوان وقاسم 2022 بعنوان:

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

تهدف هذه الدراسة إلى التعرف على أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار المالي والشمول المالي لدى البنوك المدرجة في بورصة فلسطين وتقديم تشخيص لواقع إدارة مخاطر الأمن السيبراني بهدف دعم تطبيق الشمول المالي لزيادة الاستقرار المالي لدى هذه البنوك والإجابة على أسئلة البحث وتم تبني فرضيات البحث. وقد استخدم الباحثون المنهج الوصفي التحليلي واستخدموا الاستبانة كأداة لجمع المعلومات وبعد تقييمها والحكم عليها من قبل عدد من الخبراء تم توزيعها على عينة الدراسة والتي تكونت من أكثر من 90 مديراً عاملاً ومدير فرع ومدير دائرة مالية ومدير إدارة مخاطر في البنوك المدرجة في بورصة فلسطين وقد ثبت أن نتائج المسوحات تشير إلى أن إدارة مخاطر الأمن السيبراني لها أثر على دعم الاستقرار والشمول المالي لدى البنوك المدرجة في بورصة فلسطين. دعم الشمول المالي كما توصي هذه الدراسة البنوك المدرجة في بورصة فلسطين باتخاذ إجراءات الأمن السيبراني لضمان سلامة ومثانة أنظمة المعلومات المالية والإدارية والحفاظ على الاستقرار والشمول المالي من أجل تحقيق أهدافها. وهناك حاجة أيضاً إلى تطوير نماذج فعالة لإدارة المخاطر السيبرانية المتعلقة بتكنولوجيا المعلومات والتي تتطلب مراقبة مستمرة لتحديد هذه المخاطر التي قد تهدد الاستقرار المالي في القطاع المصرفي.

16.دراسة صواق وآخرون 2023 بعنوان

أثر جاهزية الأمن السيبراني على الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر المدركة هدفت هذه الدراسة إلى توضيح أثر جاهزية البيئة المادية والبشرية للأمن السيبراني على استخدام الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر المدركة لدى عينة من العملاء في بنك التنمية المحلي بولاية غرداية وتكونت عينة الدراسة من (127) فرداً أي أن معدل الاستجابة بلغ (97%) وفي هذا البحث تم استخدام نموذج تحليل المسار واختبار التأثير المباشر وغير المباشر ومتغيرات الدراسة واختبار صلاحية وصدق وثبات نموذج الدراسة وتوصل البرنامج الإحصائي (AMOS 25) إلى وجود بعدين لجاهزية البيئة المادية والبشرية لاستخدام الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر وهناك حاجة إلى أن يتبنى بنك التنمية المحلي بولاية غرداية آليات لتقليل المخاطر المتبقية للعملاء لأن العميل يفضل التعامل مع بنك يعالج بنجاح عناصر المخاطر ويقدم خدمات مصرفية إلكترونية موثوقة وآمنة.

17.دراسة (الرحامنة (2023) بعنوان

متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية

أجريت هذه الدراسة بهدف التعرف على متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية المتطلبات الإدارية المتطلبات المالية والفنية بحيث تم توزيع استبانة على العاملين في البنوك الإسلامية وتم تحليل الاستبانة باستخدام برنامج (SPSS) وقد توصلت الدراسة إلى عدم وجود فروق ذات دلالة إحصائية في متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية باختلاف متغير الجنس والمسمى الوظيفي وقد أوصت هذه الدراسة بضرورة إيجاد رؤية مشتركة بضرورة زيادة متطلبات تحقيق الأمن السيبراني وتوفير الدعم المادي والمعنوي لتوفير أفضل التقنيات والبرامج والدورات التدريبية التكنولوجية بهدف تحسين الأداء وتطوير الخدمات المصرفية بأعلى مستوى من الجودة.

دراسات باللغة الإنجليزية

1. دراسة "2019" Maharjan & Chatterjee بعنوان

"Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal"

الهدف من هذه الدراسة هو تطوير إطار عمل للحماية والتخفيف الفعال وفي الوقت المناسب لمشكلة الأمن السيبراني في القطاع المصرفي في نيبال قبل أن تصبح حوادث الأمن السيبراني حقيقة واقعة باستخدام العناصر الأساسية الخمسة للمعهد الوطني للمعايير والتكنولوجيا (NIST) تحديد وحماية

وتحديد والاستجابة والتعافي هو الأساس لتطوير إطار عمل للتخفيف من مشاكل الأمن السيبراني التي ستكون مثمرة في سياق البيئة النيبالية حيث تم استخدام النهج التحليلي الوصفي (28) بنمًا تجاريًا في نيبال والتي كانت عينة الدراسة من موظفي البنوك ومتخصصي تكنولوجيا المعلومات ومخاطر التدقيق ومديري الشبكات وموظفي الأمن السيبراني وعددهم (300) موظفًا وزيارات ميدانية للدراسة تم توزيع الاستبيان على 112 شخصًا وتم استخدام 100 شخص للتحليل الإحصائي الصحيح وتم استخدام برنامج (Excel) لتحليل البيانات. البنوك واسعة جدًا وأمن المعلومات والبنية التحتية قوية أيضًا والتقنيات الموجودة تمنع الهجمات السيبرانية وتحاول التعرف عليها بسرعة في حال حدوثها وأوصت هذه الدراسة بضرورة حفظ أصول البيانات الخاصة بالبنك وضمان حمايتها وعند الاستعداد للتهديد من الضروري تحديد نقاط الضعف والثغرات والتركيز عليها من خلال برامج الأمن السيبراني حتى تتمكن جميع البنوك من حماية أصولها.

2. دراسة "2020" Aldasoro et al بعنوان

"Operational and cyber risks in the financial sector"

تحدثت هذه الدراسة عن قضية المخاطر السيبرانية الناجمة عن العمليات التشغيلية حيث تصف الخسائر السيبرانية بأنها جزء صغير من الخسائر التشغيلية تقدر بنحو ثلثي إجمالي الخسائر في العمليات التشغيلية وتزايد وتصل إلى ذروتها. في عام 2020. وهذا يفسر التكاليف الضخمة لأنظمة الحماية من هذه المخاطر. تظهر هذه الدراسة أن المخاطر السيبرانية للعمليات التشغيلية في فترات ازدهار الائتمان والسياسات النقدية المفرطة في التيسير تلعب دورًا في تقليل نسبة المخاطر السيبرانية في العمليات التشغيلية وبالتالي تجنب أو تقليل الخسائر.

3. دراسة "2020" Al Duhaidahawi بعنوان

"Analyzing the effects of FinTech variables on cyber-Security: Evidence form Iraqi Banks"

وتبين هذه الدراسة أن أمن المعلومات في المؤسسات المالية يتأثر بالمخاطر السيبرانية وكلما زاد حجم المعلومات زاد معها الخطر ونتيجة لذلك هناك حاجة إلى زيادة أمن المعلومات السيبرانية لأن كل وحدة من وحدات أمن المعلومات تزيد من درجة الحماية وبالتالي تقليل المخاطر السيبرانية تجاه أمن المعلومات. ومن ناحية أخرى تبين استنتاجات هذه الدراسة أن هناك علاقة قوية وإيجابية في ثقافة التكنولوجيا لدى العملاء والموظفين لأنه كلما زادت ثقافة التكنولوجيا والوعي بها زادت قدرة الأمن السيبراني. وبالتالي تقل المخاطر السيبرانية تجاه أمن المعلومات.

4. دراسة "2020" Bukht et al بعنوان

Analyzing Cyber - Attacks Targeted On the Banks of Pakistan and Their Solutions"

هدفت هذه الدراسة إلى تحليل الهجمات الإلكترونية التي تستهدف البنوك والحلول والاستراتيجيات للتخفيف من آثارها على الأنشطة المصرفية بالاعتماد على المنهج التحليلي الوصفي. وخلصت الدراسة إلى أن البنوك قيد الدراسة معرضة لهجمات إلكترونية تشمل الحرمان من الخدمة والقوة الغاشمة وبطاقات الائتمان ومتصفحات الويب والحرمان الموزع من الخدمة والروبوتات والتلاعب بالرسائل وتعليق أو انقطاع الاتصالات الداخلية وتدمير البيانات والهجمات على الأجهزة والأدوات وأخطرها هجمات سرقة بطاقات الائتمان وبناءً على ما سبق توصي هذه الدراسة بإنشاء آليات وإجراءات للحد من الهجمات الإلكترونية والتي تنقسم إلى أربعة مكونات: الوقاية والكشف ورد الفعل. وأشارت هذه الدراسة إلى المخاطر الإلكترونية التي تواجه البنوك بشكل عام والبنوك الباكستانية بشكل خاص واقتрحت حلولاً لهذه المخاطر.

5. دراسة "2020" Alahmari & Duncan

"Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence"

تهدف هذه الدراسة إلى تقديم مراجعة منهجية للأدبيات القائمة على الأدلة المتاحة مؤخراً حول إدارة مخاطر الأمن السيبراني في الشركات الصغيرة والمتوسطة وكشف الدور الذي تلعبه إدارة الشركات الصغيرة والمتوسطة في معالجة مخاطر الأمن السيبراني في السنوات الأخيرة كما هو موجود في الأدبيات. واقتراح سبل لمزيد من البحث. اتبعت هذه الدراسة طريقة معروفة لإجراء مراجعة منهجية للأدبيات وتم تحليل 15 من أصل 50 مقالة وفقاً للمعلومات الببليوغرافية وتصميم البحث والنتائج. دور إدارة مخاطر الأمن السيبراني للشركات الصغيرة والمتوسطة والتي هي على التوالي من: التهديدات والسلوكيات وطرق صنع القرار. أوصت هذه الدراسة بإجراء بحث تجريبي حول إدارة مخاطر الأمن السيبراني في الشركات الصغيرة والمتوسطة

6. دراسة "2021" Manoj, بعنوان

"Banks' holistic approach to cyber security: tools to mitigate cyber Risk"

تهدف الدراسة إلى المساعدة في تحديد الآليات والأدوات التي يمكنها مواجهة أو تخفيف المخاطر السيبرانية على البنوك. وتقول الدراسة إن البنوك والمؤسسات المالية تستخدم التكنولوجيا الحديثة وتواكب التطور هدف ثمين للمهاجمين السيبرانيين

7. دراسة "2022" Piotrowski بعنوان

Consumer perceived ethicality of banks in the era of digitalization: The case of Poland"

أجريت هذه الدراسة بهدف تحديد الأنشطة المصرفية التي يعتبرها العملاء أخلاقية ومدى تأثيرها على السلوك الأخلاقي الذي يدركه المستهلكون وكذلك بهدف توضيح آلية استخدام الخدمات المصرفية الإلكترونية واستخدام تقنية الذكاء الاصطناعي لتحسين جودتها. الخدمات المصرفية حيث تم استخدام أسلوب المسح العشوائي والمقابلات بمساعدة الكمبيوتر تكونت عينة الدراسة من (911) مواطن بولندي تتراوح أعمارهم بين (5-1) حيث تم التركيز على المستجيبين الذين لديهم خبرة في استخدام الخدمات المصرفية ولديهم حساب مصرفي (49) لديهم تاريخ وبدون حساب مصرفي وبذلك تكون العينة المدروسة (862). أظهرت النتائج أن العملاء البولنديين يفتقرون إلى المعرفة الكاملة بتطبيقات الذكاء الاصطناعي في الخدمات المصرفية والحسابات وأن هناك أمن للمعلومات والبيانات. تتطلب هذه الدراسة المزيد من الاهتمام بالجوانب الأخلاقية في تنفيذ وتقديم خدمات مالية أكثر تقدماً من خلال القناة. توصي بالخدمات المصرفية.

وعليه توصي هذه الدراسة بضرورة اعتماد البنوك التجارية في الأردن بشكل أكبر على الأنظمة المتقدمة حتى تتمكن البنوك من استخدام الأجهزة والبرامج الحاسوبية الحديثة وبالتالي زيادة اعتماد هذه البنوك على التطبيق الفعال للحوكمة الإلكترونية لمتابعة تطوير الأعمال والمهام وفقاً لاستراتيجياتها.

8. دراسة "2020" Lehenchuk et al بعنوان

Protection of Accounting Information in the Conditions of Cyber Security"

تهدف هذه الدراسة إلى التعرف على الاتجاهات الحديثة في تنظيم حماية المعلومات المحاسبية في مجال الأمن السيبراني ودراسة المخاطر الكامنة في أنظمة المعلومات المحاسبية الإلكترونية والمخاطر المتعلقة بجمع البيانات ودخولها إلى النظام الآلي والمخاطر المتعلقة بمعالجة وتحليل المعلومات والمخاطر المتعلقة بالتخزين في الوسائط الإلكترونية والمخاطر المتعلقة بمرحلة نشر ونقل المعلومات وتحليلها لابتكار الطرق المناسبة للحد منها. ولتحقيق أهداف البحث تم إجراء هذا البحث بالمنهج التحليلي الوصفي وذلك من خلال دراسة ومقارنة وتحليل الدراسات السابقة والبحث في نتائجها. خلصت هذه الدراسة إلى أن التواصل الفعال والاستراتيجيات المشتركة بين الإدارة والمحاسبين والمراجعين مهمة للحد من التهديدات الناشئة وحماية نظام المعلومات المحاسبية ولتقييم المخاطر المحتملة بشكل صحيح يجب أن يكون المحاسبون والمراجعون على دراية كافية بالتقنيات الحالية والجديدة. ليكون التحكم في

الوصول غير المصرح به إلى السجلات المحاسبية عنصرا مهما من عناصر الرقابة الداخلية وتعتبر سياسات الوصول والتشفير والتوقيعات الرقمية أمثلة على عناصر الرقابة التي يجب تحديدها وتسجيلها والإبلاغ عنها عند تقييم فعالية الضوابط. ضرورة إتباع تدابير شاملة وإجراءات مشتركة لتوعية الإدارة والمحاسبين والمراجعين والمؤسسات التعليمية بتدريب المهنيين الحاليين والمستقبليين لضمان حماية المعلومات المحاسبية.

9. دراسة "2023" Despotović et al بعنوان

Cybercrime and Cyber Security in Fintech

أجريت هذه الدراسة بهدف تحليل التهديدات السيبرانية وقضايا الأمن السيبراني في مجال التكنولوجيا المالية بطريقة منهجية من خلال تقديم وتحديد وشرح مفاهيم التهديدات السيبرانية والأمن السيبراني في التقنيات المالية والأساليب الجديدة لحماية الأنظمة المالية منها واتباع هذا البحث المنهج الاستقرائي والمنهج التحليلي الوصفي من خلال مراجعة وتحليل الدراسات والنصوص السابقة وخلصت الدراسة إلى أن أفضل طريقة للوقاية من الهجمات السيبرانية هي تثقيف الموظفين حول كيفية منع الهجمات المحتملة والاختراقات الأمنية العرضية وتوصي هذه الدراسة البنوك وشركات التكنولوجيا المالية والمستخدمين النهائيين بدراسة المخاطر الإلكترونية بعناية والاستجابة المناسبة لكل عنصر من عناصرها وإعداد اللوائح القانونية في مجال العملات الرقمية والجرائم السيبرانية في مجال التقنيات المالية.

المنطلقات النظرية للدراسة:

وفقاً لأهداف هذا البحث، تم تقديم التعاريف الإجرائية والمفاهيمية لجميع متغيرات البحث، والتي جاءت على النحو التالي:

● مخاطر الأمن السيبراني مخاطر الأمن السيبراني

وفقاً للقاموس العربي فإن المخاطر تعني الضرر أو الكارثة أو الدمار ومن الناحية المالية تظهر احتمالات أو توقعات غير عادية تحدث في ظروف استثنائية وغير منتظمة بحيث يصعب التنبؤ بحدوثها ووفقاً لويكيبيديا فإن كلمة cyber كلمة مشتقة من الكلمة اللاتينية "Cyber" وتعني خيالي أو افتراضي وتستخدم عادة للتعبير عن الاختصاص الذي يشمل شبكات الكمبيوتر وشبكات المعلومات والاتصالات وأنظمة التحكم. وهي بعيدة من خلال ثلاث جهات: الأجهزة والبرمجيات الرقمية ومجموعة من المطورين والمبرمجين.

● أما مخاطر الأمن السيبراني بمعناها العام

فهي تعرف بأكثر من معنى وكلها تدور حول معنى عام (2020) ذكر اسم مخاطر الكمبيوتر أو المخاطر الإلكترونية أو المعلوماتية أو مخاطر تكنولوجيا المعلومات أو مخاطر الإنترنت لأن هذه المصطلحات تشير إلى ما يسمى بمخاطر الأمن السيبراني والتي تعني تطور أنماط مختلفة من المخاطر الناتجة عن استخدام تكنولوجيا المعلومات والتأثير الكبير الناتج عن التطور العملي في التقنيات المستخدمة في التداول اليومي.

● مخاطر أمن المعلومات مخاطر أمن المعلومات

تعرف مخاطر أمن المعلومات بأنها أي تهديد أو نشاط من قبل شخص غير مصرح له أو من قبل المطلعين على المعلومات أو أنظمة المعلومات يهدف إلى الوصول إلى المعلومات أو أنظمة المعلومات أو استخدامها أو الكشف عنها أو خرقها أو تغييرها أو تدميرها مما يعتبر تهديدًا لسلامة وخصوصية النظام وجاهزية أنظمة وعمليات المصرف.

● مخاطر تطبيقات الهاتف المحمول مخاطر تطبيقات الهاتف المحمول

مخاطر تطبيقات الهاتف المحمول هي تهديدات أو أنشطة خارجية مثل الاختيال الرقمي والوصول إلى المعلومات السرية واختراق التطبيقات أو إصابة منصات الأجهزة المحمولة بالبرامج الضارة (Android و iOS و Windows) مما يؤدي إلى حدوث استخدام غير سليم للخدمة (تطبيق الخدمات المصرفية). إن إنشاء ثغرات أو نقاط ضعف في البرنامج يسهل على المتسللين الوصول إلى البرنامج أو تخريبه

المنهجية وطرق البحث:

يتبع البحث الحالي المنهج الوصفي التحليلي، حيث تم استخدام الاستبانة كأداة لجمع البيانات من المبحوثين، ومراجعة البحوث والأدبيات الخاصة بالموضوع بهدف بلورة الأسس والمنطلقات التي يقوم عليها الأساس النظري للدراسة. لذلك اعتمد هذا البحث على مصدرين مهمين لجمع المعلومات:

مصادر جمع البيانات

➤ **المصادر الثانوية:** الدراسات السابقة والأدبيات النظرية، وقد تم الاستعانة بهذه المصادر لتغطية الجانب النظري للبحث والتعرف على الأساسيات والأساليب العلمية الصحيحة في كتابة الدراسات، وكذلك تقديم لمحة عامة عن أحدث المواد والتطورات في مجال الدراسة، من خلال

مراجعة واستعراض العديد من النصوص العربية والأجنبية ذات الصلة بموضوع الدراسة، والمتمثلة في الكتب والمجلات والأطروحات العلمية والأبحاث المنشورة، وكذلك المصادر التي تم الحصول عليها من خلال المستودعات الرقمية.

➤ **المصادر الأولية:** من أجل معالجة الجوانب التحليلية لموضوع البحث تم جمع البيانات الأولية من خلال البحث الميداني للبحث من خلال أداة الدراسة وهي الاستبانة التي أعدت لأغراض هذا البحث، ومن ثم تم نسخها وتحليلها باستخدام الأداة المطلوبة وهي الحزمة الإحصائية للعلوم الاجتماعية (SPSS).

أدوات الدراسة :

تعرف أداة البحث بأنها "الوسيلة التي تتم بواسطتها عملية جمع البيانات بهدف الإجابة عن تساؤلاته ، وسيعتمد الباحثين في جمع البيانات على الاستبانة، والتي تُعرف بأنها "صيغة محددة من الفقرات والأسئلة تهدف إلى جمع البيانات من أفراد البحث"

حيث تكونت من قسمين رئيسيين هما:

- **القسم الأول:** وهو الجزء الخاص بالمتغيرات الديمغرافية لأفراد عينة الدراسة ، والمتمثلة ب: النوع ، والعمر، والمؤهل العلمي، والمستوى الوظيفي.
- **القسم الثاني:** اشتمل القسم الثاني على الفقرات والأبعاد التي تقيس متغيرات الدراسة المستقل والتابع.

حدود الدراسة :

- **حدود موضوعية :** اقتصرت الدراسة على التعرف على أثر مخاطر الأمن السيبراني بأبعادها (مخاطر الامن السيبراني، مخاطر امن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية) واستخدام البطاقات المصرفية بأبعادها (البطاقات المصرفية)، دراسة تطبيقية على مصرف الراجحي
- **حدود مكانية:** اقتصرت الدراسة على مصرف الراجحي
- **حدود زمانية :** تم إعداد الدراسة في عام 2024.
- **حدود بشرية :** اقتصرت الدراسة على مصرف الراجحي

المراجع:

1. أبو الخير، محمد حارس محمد طه (2022) أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية، المجلة العلمية للدراسات والبحوث المالية والإدارية، المجلد الخامس عشر العدد الأول
2. أبو الهيجاء، محمد (2021) المخاطر السيبرانية من الناحية الإقتصادية والمالية. مجلة ريادة الأعمال الإسلامية الهيئة العالمية للتسويق الإسلامي، المجلد 6، العدد 1
3. أبو غدة، عبد الستار (2002) بحوث في المعاملات والأساليب المصرفية الإسلامية. ط1، ج 2، مجموعة دلة البركة، جدة، السعودية.
4. اشويقي، يوسف عبد الله وبوحليمة، صالح عبد الرحيم عمر وحسين، أمحمد محمد (2022). معوقات استخدام بطاقات الدفع الإلكتروني في المصارف التجارية مجلة البيان العلمية العدد 12
5. أميرهم جيهان عادل (2022) أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين دراسة ميدانية مجلة البحوث المالية والتجارية، العدد 3.
6. بن مبشر، محمد يسلم مفتاح وعويضة، عدنان عبد الله محمد (2023)، البطاقات الائتمانية في المصارف التشاركية وأثرها على الإقتصاد البنوك التشاركية الترقية أنموذجا، الحلقة 3:1 مجلة الإقتصاد الإسلامي العالمية، العدد 129
7. الخرينج، نواف متعب بنيه متعب البسطويسي، مروة أحمد عبد الرحمن، وداود، ياسر إبراهيم محمد (2022) دور حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي المجلة العلمية للدراسات والبحوث المالية والإدارية، المجلد 13

8. رشوان عبد الرحمن محمد سليمان وقاسم زينب عبد الحفيظ (2022)، أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المؤتمر العلمي الدولي الأول بعنوان أثر الأمن السيبراني على الأمن الوطني، 20-21 ديسمبر
9. السمحان منى عبد الله (2020) متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود. مجلة كلية التربية، جامعة المنصورة، المجلد 1 ، العدد (111)
10. سيد محمد، وبوركايب محمد عبد الماجد (2020) مساهمة تكنولوجيا المعلومات في تحسين جودة المعلومات المالية - دراسة تحليلية مجلة المحاسبة التدقيق والمالية، المجلد 75-62، العدد (2)
11. غزالي، سارة محمد روجي فتحي (2022) الأمن السيبراني ودرجة وعي المؤسسات بأهميتها، المجلة العربية للنشر العلمي، العدد (47).
12. إسماعيل محمد (2019)، الأمن السيبراني في القطاع المصرفي، الدائرة الاقتصادية الفنية، صندوق النقد العربي، أبو ظبي، ع4.
13. بانقا (2019)، مخاطر الهجمات الإلكترونية السيبرانية وآثارها الاقتصادية، المعهد العربي للتخطيط بالكويت، سلسلة دراسات تنموية، الطبعة الأولى
14. الشورة (2020)، الأمن السيبراني في البنوك الإسلامية الأردنية، الجامعة الأردنية، كلية الشريعة، قسم المصارف الإسلامية.
15. الزيود (2020)، إدارة مخاطر الأمن السيبراني في المصرف، جامعة بوسعيد، كلية التجارة، مجلة البحوث المالية والتجارية، مج 23، ع 3.
16. السمحان، (2020)، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، جامعة المنصورة، كلية التربية، مجلة كلية التربية بالمنصورة، مصر، مج 111، ع 1، ص 28.
17. منصور، (2021)، تأثير الأمن السيبراني على الرقابة الداخلية وإنعكاسها على الوحدة الاقتصادية دراسة إستطلاعية لآراء عينة من المدققين والمحاسبين في وزارة التعليم العالي والبحث العلمي، الجامعة المستنصرية - كلية الإدارة والاقتصاد، مجلة الإدارة والاقتصاد، العراق، ع127، ص 223 - 238
18. البغدادي، (2021)، اقتصاديات الأمن السيبراني في القطاع المصرفي، جامعة المنصورة - كلية الحقوق، مجلة البحوث القانونية والاقتصادية، مصر، ع76، 1446 - 1513.
19. محمد عدنان أبو الهيجاء، (2021)، المخاطر السيبرانية من الناحية الاقتصادية والمالية، مجلة ريادة الأعمال الإسلامية، مج. 6، ع1.

20. زوائب وحاج علي، (2021)، تأثير تكنولوجيا المعلومات والاتصال على المخاطر التشغيلية بالبنوك دراسة إستقصائية على عدد من البنوك التجارية الجزائرية، مجلة البحوث و الدراسات التجارية، مج 5، ع 1، ص 207-224
21. أبو الخير، (2022)، أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية، المحاسبة والمراجعة، المعهد العالي للحاسبات والمعلومات وتكنولوجيا الإدارة بطنطا، مج 15، ع 1، ص 1-71
22. أميرهم، (2022)، أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على ترشيد قرارات المستثمرين، جامعة بورسعيد، كلية التجارة، مجلة البحوث المالية والتجارية، مصر، مج 23، ع 3.

ثانياً: المراجع باللغة الإنجليزية

1. Agarwal, Harshit, (2021). Mobile App Security Threats and Ways to Mitigate Them, G2, USA
2. Al Duhaidahawi, H. M. K., Zhang, J., Abdulreza, M. S., Sebai, M., & Harjan, S. A. (2020). Analyzing the effects of FinTech variables on cyber security: Evidence form Iraqi Banks. International Journal of Research in Business and Social Science
3. Alahmari, A., & Duncan, B. (2020, June). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In 2020 international conference on cyber situational awareness, data analytics and assessment
4. Aljniebi, A. (2020). Human Behavior in Cyber Security (Unpublished Doctoral dissertation). The British University in Dubai (BUID)
5. Aziz, A, Ahmed, S. & Khan, F, I, (2019), An Ontology Based Methodology for Hazard Identification and Causation Analysis, Process Safety and Environmental Protection
6. Borky, John and Bradley, Thomas, (2019). Effective Model-Based system Engineering. 1" edition, Switzerland, Springer International

7. Cheng, X Hsu, C Wang, T, D, (2022), Talk too much? The Impact of Cybersecurity Disclosures on investment Decisions, Communications of the Association for Information system
8. Curti F., Gerlach J., Kazinnik S., Lee M. and Mihov A. (2019). Cyber risk definition and classification for financial risk management, Federal Reserve Bank of St Louis, mimeo
9. Curti, F., Gerlach, J., Kazinnik, S., Lee, M. J., & Mihov, A. (2019). Cyber risk definition and classification for financial risk management. Federal Reserve Bank of St Louis, August, mimeo
- 10.Despotović, A., Parmaković, A. & Miljković, M. (2023). Cybercrime and Cyber Security in Fintech. In Digital Transformation of the Financial Industry: Approaches and Applications
- 11.Doerr, S., Gambacorta, L., Leach, T., Legros, B., & Whyte, D. (2022). Cyber risk in central banking, BIS,
- 12.Donalds, Charlette & Kweku, Muata, (2019), toward A Cybercrime Classification Ontology: A Knowledge Human Behavior
- 13.Frank, M. L.. Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance, Journal of information systems
- 14.Hartmann C.C. and J. Carmenate, (2021) Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches Implications for Practice Policy and Research. American Accounting Association
- 15.Hasan, M. F., & Al-Ramadan, N. S. (2021), Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. Social Science and Humanities Journal
- 16.Jones, T. R., Kreisman, D., Rubenstein, R., Searcy, C., & Bhatt, R. (2022). The Effects of Financial Aid Loss on Persistence and Graduation: A

Multi- Dimensional Regression Discontinuity Approach. Education Finance and Policy

17. Lehenchuk, S., Vyhivska, I. & Grigorevska, O. (2022). Protection of accounting information in the conditions of cyber security. Problems of theory and methodology of accounting, control and analysis
-

Mid-Ocean University

College of Management

RISK MANAGEMENT



**The impact of cybersecurity risks on the use of
bank cards: an applied study on Al Rajhi Bank**

Preparatio

NORAH MUTLAQ M ALKHAMISI

233001453

Supervision:

Dr. Al-Faisal Abdul Hamid Mohammed Hassan

1445-2024