

جامعة ميد أوشن



كلية الإدارة

تخصص إدارة المخاطر

أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية

دراسة تطبيقية على مصرف الراجحي

إعداد الطالبه/

نوره مطلق الخامسي

233001453

إشراف/

د. الفيصل عبد الحميد محمد حسن

د/ فايز جراد

العام الدراسي: 2024



إهداء

أهدي هذا البحث إلى أحبائي وأسرتي،

الذين كانوا دعماً لا ينضب في رحلتي الأكاديمية.

إلى والدي ووالدتي الذين آمنوا بقدراتي وشجعوني على التفوق والاجتهاد.

إلى أختي وأخي الذين كانوا دائماً بجانبني بالنصيحة والدعم الذي لا يقدر بثمن.

كما أهدي هذا العمل إلى أصدقائي الأعزاء الذين شاركوني لحظات الصعوبة

والفرح خلال هذه السنوات الدراسية.

أتمنى أن يكون هذا البحث قد حقق التوقعات وأن يكون إسهاماً متواضعاً في

المجال الذي اخترته. شكراً لكم جميعاً على دعمكم وتشجيعكم المستمر.

شكر وعتر

الحمد لله، الذي بنعمته تتم الصالحات، وبعد،

أود أن أعبر عن خالص شكري وتقديري لكل من ساهم ودعمني خلال رحلتي في إعداد

وإتمام هذا البحث.

كذلك، أتوجه بالشكر العميق إلى استاذي المشرف على البحث، د/ فايز جراد

و د. الفیصل عبد الحمید محمد حسن

، على إرشاداتهم القيمة وملاحظاتهم البناءة التي ساهمت بشكل كبير في تحسين هذا

البحث. لا يمكنني أن أكون ممتن بما فيه الكفاية لكم.

كما أود أن أعبر عن شكري العميق لزملائي في الدراسة الذين تبادلوا معي الأفكار

والنقاشات الهامة التي ساهمت في تطوير هذا البحث.

أخيراً، أريد أن أشكر كل من دعمني وشجعني سواء بالكلمات أو بالأفعال خلال هذه

الرحلة الأكاديمية. لا يمكنني أن أوصف كم أنا ممتن ومقدره لكل دعمكم.

وفي الختام، أسأل الله العليّ القدير أن يجعل هذا البحث خالصاً لوجهه الكريم وأن يكون

مفيداً للمجتمع وللمستقبل.

المستخلص

هدفت هذه الدراسة إلى التعرف على أثر مخاطر الأمن السيبراني بأبعادها (مخاطر الأمن السيبراني، مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية) في استخدام البطاقات المصرفية بالتطبيق على مصرف الراجحي، ولتحقيق أهداف الدراسة تم استخدام المنهج الوصفي التحليلي، وشمل مجتمع الدراسة جميع العاملين في بنك الراجحي ، وقانم الباحث بتوزيع (237) إستبانة إلكترونية، واسترداد (205) إستبانة وبصورة إلكترونية ، واستخدام الأساليب الإحصائية لتحليل البيانات.

أظهرت نتائج الدراسة وجود تأثير ذو دلالة إحصائية لمخاطر الأمن السيبراني بأبعاده الأربعة مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية في إستخدام البطاقات المصرفية في مصرف الراجحي .

وأوصت الدراسة بضرورة إتخاذ الإحتياطات اللازمة في مصرف الراجحي بالتدريب والتوجيه المستمر للموظفين حول مفاهيم الأمن السيبراني وأفضل الممارسات له، لتعزيز الوعي والحس الأمني لدى الموظفين والعملاء بمخاطر الهجمات السيبرانية ، والأخذ بأراء ومقترحات العملاء في الإجراءات المتبعة في مصرف الراجحي بالسياسات والإجراءات الأمنية الصارمة والواضحة في التعامل مع المخاطر السيبرانية بمختلف أشكالها.

الكلمات المفتاحية: مخاطر الأمن السيبراني ، البطاقات المصرفية ، بنك الراجحي.

قائمة المحتويات

ب.....	بسم الله الرحمن الرحيم
ج.....	إهداء
د.....	شكر وتقدير
ه.....	المستخلص
و.....	قائمة المحتويات
ي.....	قائمة الجداول
ل.....	قائمة الأشكال
1.....	الفصل الأول: الإطار العام للدراسة
1.1.....	1.1 مقدمة
2.....	2.1 مشكلة الدراسة:
3.....	3.1 أهمية الدراسة:
3.....	1.3.1 الأهمية العلمية:
3.....	2.3.1 الأهمية العملية:
4.....	4.1 أهداف الدراسة:
4.....	5.1 تساؤلات الدراسة:
5.....	6.1 فروض الدراسة:
6.....	7.1 نموذج الدراسة:
7.....	8.1 الدراسات السابقة:
7.....	1.8.1 الدراسات العربية:

16.....	2.8.1 دراسات باللغة الإنجليزية.....
21.....	9.1 المنطلقات النظرية للدراسة:.....
22.....	10.1 المنهجية وطرق البحث:.....
23.....	11.1 أدوات الدراسة :.....
23.....	12.1 حدود الدراسة :.....
25.....	الفصل الثاني: الاطار النظري.....
25.....	المبحث الاول: مخاطر الامن السيبراني.....
25.....	1.1.2 مفهوم الامن السيبراني:.....
29.....	2.1.2 اهمية الامن السيبراني.....
30.....	3.1.2 اهداف الامن السيبراني.....
31.....	4.1.2 مفهوم مخاطر الأمن السيبراني.....
34.....	5.1.2 انواع مخاطر الامن السيبراني.....
37.....	المبحث الثاني: البطاقات المصرفية.....
37.....	1.2.2 مفهوم البطاقات المصرفية.....
39.....	2.2.2 مزايا البطاقات المصرفية.....
42.....	3.2.2 عيوب البطاقات المصرفية.....
45.....	4.2.2 خصائص البطاقات المصرفية.....
45.....	5.2.2 اهمية البطاقات المصرفية.....
46.....	6.2.2 انواع البطاقات المصرفية.....
47.....	7.2.2 استخدام البطاقات المصرفية.....

50.....	8.2.2 فائدة البطاقات المصرفية.....
55.....	الفصل الثالث: الطريقة والإجراءات.....
55.....	1.3 تمهيد.....
55.....	2.3 منهجية الدراسة.....
55.....	3.3 مجتمع وعينة الدراسة.....
56.....	4.3 مصادر جمع البيانات والمعلومات.....
56.....	أولاً: المصادر الثانوية.....
56.....	ثانياً: المصادر الأولية.....
57.....	5.3 أداة الدراسة.....
59.....	6.3 اختبار صلاحية أداة الدراسة.....
59.....	1.6.3 اختبار صدق المحتوى الصدق الظاهري (Content Validity Test).....
60.....	2.6.3 اختبار ثبات أداة الدراسة.....
61.....	7.3 اختبار ملاءمة نموذج الدراسة للأساليب الإحصائية المستخدمة.....
63.....	8.3 الأساليب الإحصائية المستخدمة في معالجة البيانات وتحليلها واختبار الفرضيات :.....
63.....	1.8.3 أساليب الإحصاء الوصفي (Descriptive Statistic Methods).....
64.....	2.8.3 أساليب الإحصاء الاستدلالي (Inferential Statistics Methods).....
65.....	الفصل الرابع : تحليل البيانات واختبار الفرضيات.....
65.....	1.4 نتائج تحليل البيانات.....
65.....	2.4 وصف البيانات الديموغرافية.....
65.....	الفرع الأول: وصف متغير الجنس.....

66.....	الفرع الثاني: وصف متغير العمر.....
66.....	الفرع الثالث: وصف متغير المؤهل العلمي.....
67.....	الفرع الرابع: وصف متغير المسمى الوظيفي.....
67.....	الفرع الخامس: وصف مدة الخدمة.....
68.....	الفرع السادس: عدد الدورات المتخصصة في مجال الأمن السيبراني.....
69.....	3.4 وصف متغيرات الدراسة.....
69.....	الفرع الأول: وصف أبعاد متغير المخاطر السيبرانية.....
76.....	الفرع الثاني: وصف متغير استخدام البطاقات المصرفية.....
79.....	4.4 اختبار فرضيات الدراسة.....
91.....	الفصل الخامس : الخاتمة (النتائج والتوصيات).....
91.....	1.5 النتائج.....
91.....	1.1.5 نتائج الإحصاء الوصفي.....
93.....	2.1.5 نتائج اختبار الفرضيات.....
95.....	2.5 التوصيات.....
97.....	Abstract.....
98.....	المراجع:.....
98.....	أولاً : المراجع العربية.....
102.....	ثانياً: المراجع باللغة الإنجليزية.....
I.....	الملاحق.....
II	استمارة استبيان.....

قائمة الجداول

رقم الصفحة	اسم الجدول	م
58	الجدول (1) هيكل أداة الدراسة للمحور الأول (المخاطر السيبرانية)	.1
59	الجدول (2) مقياس ليكرت الخماسي	.2
59	الجدول (3) مستوى الأهمية النسبية لفقرات ومتغيرات الدراسة والأوساط الحسابية التي تقابلها	.3
60	الجدول (4) نتائج اختبارات أداة الدراسة	.4
62	الجدول (5) مصفوفة الارتباط لقيم معامل الارتباط بيرسون	.5
63	الجدول (6) معامل تضخم التباين والتباين المسموح به	.6
65	الجدول (7): وصف أفراد عينة الدراسة حسب متغير الجنس	.7
66	الجدول (8) وصف أفراد عينة الدراسة حسب متغير العمر	.8
66	الجدول (9) وصف أفراد عينة الدراسة حسب متغير المؤهل العلمي	.9
67	الجدول (10) وصف أفراد عينة الدراسة حسب متغير المسمى الوظيفي	.10
67	الجدول (11) وصف أفراد عينة الدراسة حسب متغير مدة الخدمة	.11

68	الجدول (12): وصف أفراد عينة الدراسة حسب عدد الدورات المتخصصة في مجال الأمن	12.
69	الجدول (13) وصف بعدد مخاطر أمن المعلومات	13.
71	الجدول (14) وصف بعدد مخاطر تطبيقات الهاتف المحمول	14.
73	الجدول (15) وصف بعدد المخاطر التشغيلية	15.
74	الجدول (16) وصف بعدد مخاطر الهجمات السيبرانية	16.
76	الجدول (17) وصف متغير المخاطر السيبرانية	17.
77	الجدول (18) وصف متغير استخدام البطاقات المصرفية	18.
80	الجدول (19) ملخص النموذج وتحليل تباين الانحدار للفرضية الرئيسية	19.
81	الجدول (20) معاملات الانحدار للفرضية الرئيسية	20.
83	الجدول (21) ملخص النموذج وتحليل تباين الانحدار للفرضية الفرعية الأولى	21.
84	الجدول (22) معاملات الانحدار للفرضية الفرعية الأولى	22.
85	الجدول (23) ملخص النموذج وتحليل تباين الانحدار للفرضية الفرعية الثانية	23.
86	الجدول (24) معاملات الانحدار للفرضية الفرعية الثانية	24.
87	الجدول (25) ملخص النموذج وتحليل تباين الانحدار للفرضية الفرعية الثالثة	25.

88	الجدول (26) معاملات الإنحدار للفرضية الفرعية الثالثة	.26
89	الجدول (27) ملخص النموذج وتحليل تباين الإنحدار للفرضية الفرعية الرابعة	.27
90	الجدول (28) معاملات الإنحدار للفرضية الفرعية الرابعة	.28

قائمة الأشكال

رقم الصفحة	اسم الشكل	م
6	الشكل رقم (1) متغيرات الدراسة	.1

الفصل الأول: الإطار العام للدراسة

1.1 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

فعلى سبيل المثال، تعرض البيانات الشخصية والمالية لخطر السرقة من قبل قراصنة 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

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 مواجهة الناجحة لمخاطر الأمن السيبراني ستكون حاسمة في الحفاظ على الأمن والاستقرار في عالمنا المتصل رقمياً

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

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 أيضًا البطاقات المسبقة الدفع التي يتم شحنها بمبالغ محددة مسبقًا، وتوفر مرونة في الإنفاق والتحكم بالمصروفات

إن استخدام البطاقات المصرفية يوفر للمستخدمين الراحة والأمان في إجراء المعاملات المالية، سواءً 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.

2.1 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، سواءً 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 ووفقًا 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

ويتفرع منه الأسئلة الفرعية التالية:

1. ما هو تأثير مخاطر أمن المعلومات على استخدام البطاقات المصرفية على مصرف الراجحي؟
2. ما هو تأثير مخاطر تطبيقات الهاتف المحمول على استخدام البطاقات المصرفية على مصرف الراجحي؟
3. ما هو تأثير المخاطر التشغيلية عبر الإنترنت على استخدام البطاقات المصرفية على مصرف الراجحي؟
4. ما هو تأثير مخاطر الهجمات الإلكترونية على استخدام البطاقات المصرفية على مصرف الراجحي؟

3.1 أهمية الدراسة:

تستمد هذه الدراسة أهميتها من جانبين:

1.3.1 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.

2.3.1 الأهمية العملية:

تتعزز 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

4.1 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

5.1 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 الأمن السيبراني على البطاقات المصرفية على مصرف

الراجحي؟

6.1 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 الأمن السيبراني، مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف

المحمول، المخاطر التشغيلية) دراسة تطبيقية على مصرف الراجحي ويتفرع منها الفرضيات الفرعية

التالية:

1. الفرضية الفرعية الأولى H_{01} : 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 H_{02} : لا يوجد تأثير ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$)

لمخاطر أمن المعلومات في استخدام البطاقات المصرفية بالتطبيق على مصرف الراجحي

3. الفرضية الفرعية الثالثة H_{03} : 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 H_{04} : لا يوجد تأثير ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$)

لمخاطر التشغيلية في استخدام البطاقات المصرفية بالتطبيق على مصرف الراجحي

الفرضية الرئيسية الثانية: لا يوجد تأثير ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لاستخدام

البطاقات المصرفية بأبعادها (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

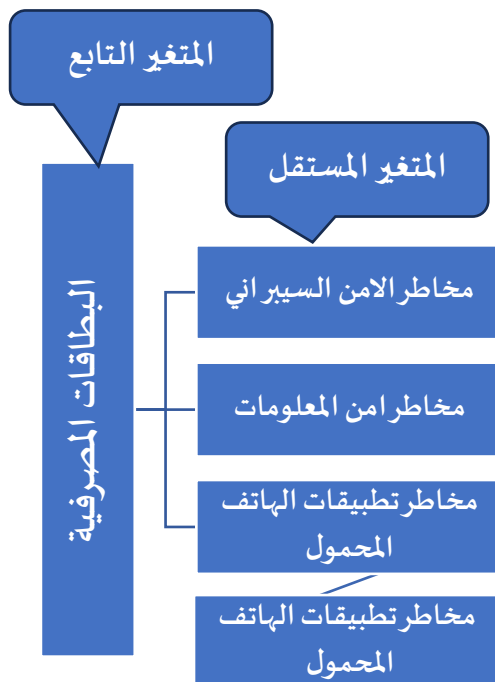
السيبراني في البطاقات المصرفية بالتطبيق على مصرف الراجحي

7.1 نموذج الدراسة

يوضح الشكل (1) النموذج المدروس مع متغيراته مخاطر التطبيق والمخاطر التشغيلية والمخاطر

السيبرانية ومتغير تابع يتمثل في البطاقات المصرفية في مصرف الراجحي.

الشكل رقم (1) متغيرات الدراسة



المصدر: إعداد الباحث

8.1 الدراسات السابقة:

1.8.1 الدراسات العربية

1. دراسة إسماعيل 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 بقاءها 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 بتثبيت 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 و آثارها 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 والتثقيف 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 بنوك المملكة العربية السعودية 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 إستطلاعية لأراء 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 الزبود (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 بالتكرارات 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 الإقتصادية والمالية

ويهدف 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 والتنبؤ 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 مسئولي إدارة الخدمات ومسئولي تكنولوجيا المعلومات ومسئولي 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 قرزیز وزیدان (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 الإلكتروني في السوق الليبي والمصارف التجارية بالإضافة إلى معرفة وعي المصرف باستخدام بطاقات الدفع الإلكتروني 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 بالتوعية المصرفية والائتمانية في المجالات المختلفة وخاصة التبادلات مع الحكومة وضرورة دعم الحكومة وتوفير البنية التحتية شبكة 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 ومتانة 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 وأمنة.

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.

2.8.1 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"

تتحدث 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 أثارها 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 واقترحت 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 (1-5) 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.

"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. وخلصت 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.

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 واتبع 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.

9.1 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 الاحتيال 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

10.1 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).

11.1 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.

12.1 حدود الدراسة :

- **حدود موضوعية:** اقتصرَت 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: اقتصرَت الدراسة على مصرف الراجحي.
- حدود زمانية: تم إعداد الدراسة في عام 2024.
- حدود بشرية: اقتصرَت الدراسة على مصرف الراجحي.

الفصل الثاني: الاطار النظري

المبحث الاول: مخاطر الامن السيبراني

1.1.2 مفهوم الامن السيبراني:

بحسب التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات إصلاحات الاتصالات للأعوام 2018-2019 هو مجموعة من المهام مثل جمع الأساليب والسياسات والإجراءات الأمنية والمبادئ التوجيهية وأساليب إدارة المخاطر والتدريب والممارسات والتدابير الأمنية ويمكن استخدامه لحماية البيئة السيبرانية وأصول المنظمات والمستخدمين ويمكن تعريف الأمن السيبراني وفقاً لما ورد في دراسة بناءً على أهدافه فهو يؤمن الموارد البشرية والمالية المتعلقة بتكنولوجيا الاتصالات والمعلومات وإمكانية تقليل الخسائر والأضرار الناجمة عن المخاطر والتهديدات كما يتيح إمكانية عودة الوضع إلى حالته السابقة في أسرع وقت ممكن ولا يتوقف حتى تصبح الأضرار دائمة. (البغدادي، 2021)

ويرى أن نشاط الأمن السيبراني يظهر جانبا حيويا في ضمان أمن الموارد البشرية والمالية المتعلقة بتقنيات الاتصالات والمعلومات لأن هدفه هو حماية هذه الموارد بشكل شامل من خلال تحديد المخاطر والتهديدات المحتملة واتخاذ التدابير اللازمة للحد من الخسائر المحتملة بالإضافة إلى ذلك، يسعى هذا النشاط إلى تمكين استعادة الوضع الطبيعي في أسرع وقت ممكن في حالة وقوع حوادث أو هجمات مما يساعد على ضمان استمرارية الإنتاج ومنع الضرر من أن يصبح خسائر لا يمكن إصلاحها ويعرف هذا النشاط بأنه نشاط يهدف إلى الحد من تأثير الهجمات وتقليل الأضرار الناجمة عنها بالإضافة إلى تصحيح المشكلات وإصلاح ما تسببه الهجمات ويساعد هذا النشاط على ضمان استقرار العمليات التجارية ومنع الأضرار من أن تصبح غير قابلة للإصلاح. (هوازي، 2019)

ويعرف بأنه هو التدابير المتخذة لحماية الأنظمة وشبكات المعلومات والبنية التحتية الحيوية من حوادث الأمن السيبراني والقدرة على استعادة العمليات والاستمرارية بغض النظر عما إذا تم الوصول إليها

دون تصريح أو نتيجة اختلاس أو عدم المتابعة الإجراءات الأمنية أو التعرض للخداع الذي يؤدي إليها" (قانون الأمن السيبراني (2019) يعرف بأنه العملية التي توفر الحماية لمبادئ المعلومات التي يتم إدخالها وتخزينها ونقلها عبر الإنترنت وهذا يتم استخدام الحماية للحد من المخاطر السيبرانية والتعامل مع الآثار المترتبة على البنك. (صالح، 2022)

بين Borky and Bradley بأن الأمن السيبراني هو عملية متوازنة لتوفير مستوى مناسب من الحماية يعالج ويستجيب للتهديدات السيبرانية المعروفة أو المشتبه فيها مما يمكن البنك من تشغيل أنظمتها والمستخدمين من أداء واجباتهم لتحقيق أهداف ومهام العمل. مواصلة عملها واعتبر كشيئري الأمن السيبراني بأنه علم الحاسوب الذي يشمل تقنيات وآليات وممارسات مستمدة من المفاهيم والسياسات والأطر التي تحكم وتنظم الأمن السيبراني وتستخدم لحماية أجهزة الكمبيوتر والبنية التحتية والتطبيقات والخدمات والاتصالات وشبكات المعلومات والبيئة السيبرانية من أي تهديدات قد تحدث وكذلك الوصول غير المصرح به وتعرف أيضاً بالإجراءات والأدوات التي تحمي سرية وسلامة وإتاحة أصول تكنولوجيا المعلومات التي يتم إدخالها وتخزينها ونقلها في أنظمة البنك وشبكات الاتصال. (البسام، 2020)

وضح European Union Agency for Network and Information Security ان الأمن السيبراني هو نشاط متعدد الأوجه يشمل الوقاية والتوقع والكشف والتخفيف من التهديدات والحوادث السيبرانية وإزالة وتحليل والتحقيق في تأثيرها والذي يستهدف بشكل أساسي البنية التحتية لتكنولوجيا المعلومات والاتصالات التي توفرها شبكة الإنترنت وأجهزة وأنظمة الكمبيوتر والمعالجات وأجهزة التحكم المتكاملة وشبكات الاتصالات السلكية واللاسلكية بالإضافة إلى جميع الأصول التي تقوم بتخزينها ومعالجتها ونقل المعلومات إلكترونياً وعرف National initiative for cybersecurity careers and studies الأمن السيبراني بأنه يشير إلى النشاط أو العملية أو القدرة التي يجب على البنك الاستفادة منها من المعلومات الواردة والمخزنة في أنظمتها والمرسلة عبر شبكات الاتصال. (العتيبي، 2020)

يتم تعريفه على أنه عملية تنظيمية تتضمن عملية تجميع الموارد والهياكل والعمليات التي تستخدم الحماية للفضاء السيبراني والأنظمة التي تدعم الفضاء السيبراني، بينما يتم تعريف الأمن

السيبراني على أنه عملية يكون غرضها محدودًا وضارًا لمنع المخاطر والهجمات وتعرفها هيئة الاتصالات وتقنية المعلومات بأنها حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنية التشغيلية ومكوناتها المادية والبرمجية والخدمات التي تقدمها والبيانات التي تحتويها من أي اقتحام أو تعطيل أو تغيير أو وصول أو استخدام أو الاستغلال غير القانوني يشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الرقمي (صبري، 2021)

يُعرّف الأمن السيبراني بأنه نشاط أو قدرة أو عملية أو قدرة أو حالة تهدف إلى حماية اتصالات وأنظمة المعلومات والدفاع عنها ضد التلف أو التغيير أو الاستخدام غير المصرح به أو أي استغلال غير قانوني أو غير قانوني، حيث تهدف هذه العملية إلى ضمان السلامة والأمن للبيانات والمعلومات والبنية التحتية السيبرانية في مواجهة التهديدات والهجمات السيبرانية المتزايدة وتتبع هذه المجموعة مجموعة من العمليات الشاملة لدعم قدرات البنك في إدارة المخاطر السيبرانية بهدف حماية أنظمة معلومات البنك وشبكات الاتصالات والبنية التحتية الحيوية لمنع ومكافحة التهديدات السيبرانية والحد من آثارها ويوفر الإمكانيات والأدوات التي تعمل على استعادة كفاءة أداء المهام والحفاظ على استمراريته (خليل، 2022)

وفي حين أنه من الواضح أنه يمثل عملية حماية المعلومات من خلال معالجة التهديدات التي تتعرض لها هذه المعلومات ومعالجتها وتخزينها ونقلها عبر شبكات متداخلة من أنظمة المعلومات، فإن الأمن السيبراني يمتد أيضًا إلى جميع المجالات وتتوسع اقتصاديا واجتماعيا وسياسيا وقانونيا فهو بالنسبة لجميع المجتمعات المعاصرة ويحمي أيضاً أمن موارد الثروة: "والتقدم في الحاضر والذي يشمل القدرة على الاتصال والتواصل والبيانات والمعلومات التي يقوم عليها الإنتاج والإبداع والقدرة على المنافسة يعتقد مجموعة من الباحثين أن الأمن السيبراني هو جزء من أمن تكنولوجيا المعلومات ويسعون إلى اتخاذ الاحتياطات اللازمة لحماية أنظمة الكمبيوتر والمعلومات المتصلة بالإنترنت من الجرائم السيبرانية. (عصام، 2019)

وعرفاه Eling & Wirfs مجموعة من المهام المتعلقة بالأمن السيبراني من خلال تطوير الأساليب والسياسات والإجراءات والمبادئ التوجيهية بالإضافة إلى الأساليب اللازمة لإدارة المخاطر وتطوير التدريب والممارسات الجيدة بالإضافة إلى توفير التقنيات الفعالة التي يمكن استخدامها لحماية استخدام البيئة

السيبرانية وأصول البنوك والمستخدمين باستخدام هذه المهام والممارسات الشاملة يمكن للبنوك والمستخدمين حماية البيئة السيبرانية وضمان سلامة أصولهم ضد التهديدات السيبرانية وتضمن هذه المهام: (زكريا، 2022)

- أساليب وسياسات التجميع يجب جمع معلومات ومصادر متعددة وتحليلها لوضع سياسات وإجراءات فعالة للحماية السيبرانية.
- إدارة المخاطر ينبغي وضع نهج شامل لإدارة المخاطر، يهدف إلى تحليل وتقييم التهديدات السيبرانية المحتملة وتحديد مستوى المخاطر المحتملة، ويشمل ذلك وضع إجراءات لمنع هذه المخاطر والتعامل معها في حالة حدوثها.
- التدريب والممارسات الجيدة: ينبغي تنظيم دورات تدريبية دورية للفرق ذات الصلة بالأمن السيبراني لتحسين مهاراتهم وتطوير قدراتهم على التعامل مع التهديدات السيبرانية. وينبغي أيضًا توفير المبادئ التوجيهية والممارسات الجيدة للموظفين والمستخدمين للمساهمة في ضمان سلامة البيئة السيبرانية.
- تقنيات الحماية لحماية البيئة السيبرانية، ينبغي استخدام تقنيات متقدمة، مثل أنظمة كشف التسلل، وجدران الحماية، وتقنيات التشفير، وإدارة الوصول، وما إلى ذلك.
- ويرى أن نشاط الأمن السيبراني يظهر جانبًا حيويًا في ضمان أمن الموارد البشرية والمالية المتعلقة بتقنيات الاتصالات والمعلومات، لأن هدفه هو حماية هذه الموارد بشكل شامل من خلال تحديد المخاطر والتهديدات المحتملة واتخاذ التدابير اللازمة للحد من الخسائر المحتملة. بالإضافة إلى ذلك، يسعى هذا النشاط إلى خلق القدرة على استعادة الوضع الطبيعي في أسرع وقت ممكن في حالة وقوع حوادث أو هجمات، مما يساعد على ضمان استمرارية الإنتاج ومنع الضرر من أن يصبح خسائر لا يمكن إصلاحها.
- ويعرف أيضًا بأنه نشاط يهدف إلى الحد من تأثير الهجمات وتقليل الأضرار الناجمة عنها، وبالإضافة إلى تصحيح المشكلات وإصلاح ما تسببت فيه الهجمات، يساعد هذا النشاط على

ضمان استقرار العمليات التجارية ومنع حدوثها. الأضرار الناجمة عن أن تصبح خسائر لا يمكن إصلاحها.

وبحسب التعريفات السابقة يرى الباحث أن الأمن السيبراني هو مجموعة من العمليات الشاملة والكاملة التي تدعم قدرات البنك في إدارة المخاطر السيبرانية بهدف حماية أنظمة معلومات البنك وشبكات الاتصالات والبنية التحتية الحيوية لتجنبها والتعامل معها والتهديدات والتخفيف من أثارها والتي توفر هذه الإمكانيات والوسائل التي تعمل على استعادة كفاءة أداء المهام والحفاظ على الاستمرارية.

2.1.2 أهمية الامن السيبراني

وتكمن أهمية الأمن السيبراني في فهم المخاطر المستقبلية ومحاولة إدارتها والسيطرة عليها بشكل فعال عند فهم المخاطر السيبرانية وتأثيرها المحتمل على الأنظمة والبيانات يمكن للبنوك اتخاذ الإجراءات والإجراءات اللازمة لمواجهةها والتخفيف من أثارها وتكمن أيضا في عدة جوانب أهمها ما يلي: - (ناصر، 2020)

- يشمل كافة الأمور المتعلقة بحماية البيانات ضد المهاجمين المتخصصين في سرقة المعلومات وإحداث الضرر لأن هذه البيانات من الممكن أن تكون معلومات حساسة حكومية وتكون صناعية معلومات شخصية أو بيانات تعريف شخصية أو حقوق ملكية فكرية
- إن وجود برامج الأمن السيبراني وآليات الدفاع الإلكتروني هي أدوات متقدمة لها أهمية كبيرة في حماية البيانات وخدمة مصالح الجميع لأن جميع أعضاء المجتمع يعتمد على الأشياء الحيوية والبنية التحتية مثل المستشفيات ومؤسسات الرعاية الصحية التي تحتاج إلى صيانة.
- إن تحقيق الاستقرار والاستمرارية في البنوك من خلال التحكم والسيطرة على المخاطر السيبرانية ومنع انقطاع أو توقف الخدمات في الإنتاج والتشغيل يساعد على تحقيق استقرار الأنظمة والبنى التحتية وضمان استمرارية العمليات والخدمات الأساسية.

- حماية البيانات الحساسة تعد البيانات الحساسة للأفراد والشركات والمؤسسات من الأصول القيمة ويجب حمايتها من الوصول غير المصرح به والاستخدام غير القانوني.
 - الحفاظ على سمعة وثقة العملاء يمكن أن يكون تأثير الهجمات السيبرانية على سمعة البنوك والمؤسسات كارثيًا، من خلال تطبيق تدابير الأمن السيبراني المناسبة، يتم الحفاظ على سمعة المؤسسات وثقة العملاء والشركاء.
 - الالتزام بالقوانين واللوائح تتطلب العديد من القطاعات الاقتصادية والحكومية الالتزام بالقوانين واللوائح المتعلقة بالأمن السيبراني.
 - الحماية من التهديدات الناشئة تتطور التهديدات السيبرانية بشكل سريع ومستمر، مما يسلط الضوء على الدور الحاسم للأمن السيبراني في تحديد التهديدات الناشئة والاستجابة لها بشكل فعال، وبالتالي تقليل التأثير السلبي على الأنظمة والمستخدمين.
- وترى الدراسة أن أهمية الأمن السيبراني تظهر في توفير حماية فائقة للبيانات والمعلومات والأجهزة والشبكات وزيادة الثقة والأمان في استخدام التكنولوجيا الرقمية وتحقيق جاهزية البيانات عند الحاجة إليها كما تؤمن بضرورة فهم البنوك والمؤسسات للمخاطر السيبرانية واتخاذ التدابير الوقائية والتعامل بشكل استباقي مع التهديدات السيبرانية لضمان سلامة الأنظمة والبيانات والحفاظ على استقرار العمليات والثقة في عالم رقمي متصل.

3.1.2 اهداف الامن السيبراني

- ينبغي تحديد أذونات الوصول للأشخاص والمستخدمين على أساس مستوى الحاجة والكفاءة، بحيث يجب منح الوصول فقط للأشخاص المصرح لهم ويجب منع الوصول غير المصرح به.
- تنفيذ التدابير الأمنية: يجب تنفيذ تدابير أمنية فعالة لمنع الأشخاص غير المصرح لهم من الوصول إلى المعلومات الحساسة، مثل استخدام أساليب التشفير، وتنفيذ جدران الحماية وأنظمة كشف التسلل.

- توعية وتدريب الموظفين والمستخدمين يجب أن يكونوا على دراية بأهمية السرية والحفاظ على سرية المعلومات، ويجب توفير التدريب المناسب لهم لفهم وتنفيذ أفضل الممارسات الأمنية. (سنة، 2019)
- المراقبة والتحكم في الوصول: يجب مراقبة ومراقبة الوصول إلى المعلومات الحساسة وتسجيل الأنشطة والتدقيق عليها لاكتشاف أي أنشطة غير مصرح بها أو مشبوهة.
- الحفاظ على سلامة البيانات: يجب اتخاذ تدابير وإجراءات لحماية سلامة البيانات ومنع تغييرها أو تلفها أثناء النقل أو التخزين، مثل استخدام طرق التشفير والنسخ الاحتياطي المناسبة.

4.1.2 مفهوم مخاطر الأمن السيبراني

يشهد العالم زيادة كبيرة في حجم وتعقيد مخاطر الأمن السيبراني التي تستهدف مختلف البلدان وخاصة المنطقة العربية ويعد القطاع المالي الأكثر عرضة لهذه المخاطر لأن المؤسسات المالية والبنوك تعتبر هدفا جذابا يتم أخذها كجزء حيوي في الوساطة والمعاملات المالية ولا تزال بعض هذه البنوك تستخدم أنظمة قديمة ولا تستطيع توفير الحماية اللازمة ضد هذه المخاطر التي تتطور كل يوم ويزداد حجم المخاطر والتهديدات والتي قد تكون عواقبها وخيمة وتسبب في خسائر مالية وأضرار كبيرة في البيانات والمعلومات بالإضافة إلى الأضرار التي تلحق بالتعاملات اليومية في البنوك بل يشمل المؤسسات بشكل عام والحكومة حيث يشمل التأمين ضد مخاطر أمن المعلومات والتأمين ضد مخاطر الهاتف المحمول والتأمين ضد المخاطر التشغيلية والتأمين ضد مخاطر الهجمات السيبرانية بالإضافة إلى استخدام البروتوكولات الآمنة في عملية الاتصال تدريب وتأهيل الموظفين على كيفية التصرف في حالة الاشتباه بشيء وبوسائل أخرى. (سامي، 2021)

وذكر أن عملية متابعة الحد من خسائر البنوك في منطقة الخليج العربي بسبب مخاطر الأمن السيبراني تجاوزت مليار دولار في السنوات الماضية وقال إن هذا الرقم من المتوقع أن يصل إلى ثلاثة تريليونات دولار في عام 2025 مع تزايد حجم الخسائر في الاقتصاد العالمي وهذا فعليا أرجع عدد كبير من الآثار السلبية لتطور تكنولوجيا المعلومات وأشار المطورون إلى أنه لا يزال هناك وقت للبنوك لاتخاذ

الاحتياطات اللازمة للتعامل مع مخاطر الأمن السيبراني لأنهم يمتلكون الخبرة والقدرات التي تسمح لهم بحماية تطبيقاتهم وبياناتهم وكذلك زيادة قدرتهم التنافسية. (فيصل، 2021)

تعتبر الشركات المالية بشكل عام هدفًا مهمًا للتعرض لمخاطر الأمن السيبراني حيث تمثل هذه المخاطر تهديد الهجوم الخبيث الذي يستهدف عمليات البنك أو الأصول والقدرات المملوكة للبنك يقومون بتدمير أو تغيير المعلومات المصرفية في البنية التحتية لتكنولوجيا المعلومات تعتبر مخاطر الأمن السيبراني هي المخاطر التي تؤثر على سرية المعلومات وأصول أنظمة المعلومات مما يؤدي إلى تعطيل الأنظمة والمعلومات. (محمد، 2023)

يتم تعريف سوء الاستخدام على أنه ضعف كلي أو جزئي في الضوابط الأمنية أو ضعف أو عدم وجود برامج مكافحة الفيروسات في البنك مما يؤثر على البنية التحتية لتكنولوجيا المعلومات ويؤدي إلى سرقة الأصول أو الفساد والإضرار بها وهذا يؤدي إلى مخاطر في البنك ونتيجة لذلك خسائر كبيرة غياب الأمن السيبراني الذي يؤدي إلى قدرة المتسللين على الوصول غير المصرح به إلى المعلومات أو إساءة استخدامها أو تعطيلها أو تدمير البيانات والمعلومات. (البغدادي، 2021)

وفي حين عرفه عدد من الباحثين على أنه فرصة للقراصنة أو منظمات القرصنة لكشف ممتلكات البنك والتلاعب بها مما يؤدي إلى خسائر فهو بالتالي تهديد متوقع حدوثه أو حدث بالفعل من ضعف قدرات البنك التي يتم استغلالها وتعرف قدراتهم في تحقيق الأمن السيبراني على أنه أي حدث يشكل تهديدًا للأنظمة المعلومات أو المعلومات التي يعالجها النظام أو عملية نقل المعلومات فضلًا عن خطر توقف أو فقدان أو فشل تشغيل المعلومات الخاصة بالبنك. أنظمة التكنولوجيا ومن المعروف أن ذلك يؤدي إلى خسائر مالية في سمعة البنك ونتيجة لذلك تعطيل وتضرر الائتمان الضعيف للبنك. (هواري، 2019)

وقد عرفه معهد المدققين الداخليين بأنه الوصول غير المصرح به لمجموعة من الأشخاص أو الجهات من خارج أو داخل البنك إلى أجهزة أو أنظمة البنك للاطلاع على أصوله وممتلكاته ومعلوماته ونقلها وتخزينها في أجهزة خارج البنك أو تعديلها في حين تم تعريفه على أنه حدث أو مجموعة أحداث تهدد سرية وسلامة المعلومات بسبب انتهاكها من قبل شخص أو جهة غير مصرح لها والفيروسات الخبيثة التي

تهاجم البنية التحتية المالية للبنك وتؤثر على أعماله وتسرقها أو التلاعب ببياناتها وهويتها فيما يعرف مفهوم مخاطر الأمن السيبراني بأنها تقنية حديثة تؤثر على سرية أو توفر أو سلامة المعلومات أو المعلومات التشغيلية للأنظمة تعتبر البنوك من المخاطر التشغيلية التي تهدد الأصول المعلوماتية داخل البنك أو خارجه ونتيجة لذلك تتراكم خسائر فادحة عند حدوث هذه الهجمات وترى هذه الدراسة أنه يمكن تعريف مخاطر الأمن السيبراني بأنها المخاطر التي تسبب خسائر مادية ومعنوية لسمعة البنوك في المملكة العربية السعودية ويتم تنفيذها من خلال مجموعة هاكلر أو منظمات متخصصة في التسلل وتكون هذه المخاطر من خارج البنك والتي تعمل من خلال معرفة نقاط الضعف في أمن المعلومات أو البرامج المضادة لإيقاف التكنولوجيا وتعطيل أنظمة المعلومات أو تدميرها. (صالح، 2022)

أكدت إحدى الدراسات أن المخاطر السيبرانية تعني المخاطر التشغيلية لأصول المعلومات والتكنولوجيا والتي لها آثار على السرية والنزاهة وأنظمة المعلومات مخاطر الملكية والمسؤولية فضلاً عن المخاطر الكارثية والتشغيلية وتؤكد بلا شك أن تكنولوجيا المعلومات والاتصالات توفر إمكانات هائلة وغير مسبوقة لتحسين الإنتاجية في جميع القطاعات والاتصالات عبر القارات وتمثل هذه التقنيات حلقة وصل بين مصالح متعددة وخدمات مختلفة والعديد من البلدان مما يجعل المخاطر في المجال السيبراني عالمية لذلك ما دام أمن الآخرين في خطر فلن يتمكن أي طرف من البقاء. (أبو الخير، 2022)

يتم تعريف المخاطر السيبرانية على أنها القيمة التي تحسب احتمالية حدوث حالة أو حدث قد يستغل عن قصد أو عن غير قصد نقطة ضعف واحدة أو أكثر في بيئة تكنولوجيا المعلومات والاتصالات في البنك وتأثير ذلك الحدث على البنك المركزي وفي واقع الأمر قام أفراد أو كيانات سواء خارج البنك أو داخله بالوصول غير المصرح به إلى أجهزته أو شبكاته أو أنظمتها للاطلاع على أصوله المعلوماتية حيث يتم إدخالها ومعالجتها وتخزينها وإرسالها من خلالها وتعديلها. (محمد، 2021)

أضاف International Organization of Securities Commission's بأن المخاطر السيبرانية تعتبر موقفاً أو حدثاً يمكن استغلاله للتأثير سلباً أو عن غير قصد على واحدة أو أكثر من نقاط الضعف الأمنية في أصول المعلومات الخاصة بالبنك وبيئة تكنولوجيا المعلومات والتي تتكون من الأشخاص

والعمليات وتعرف البيانات والأنظمة والشبكات المرتبطة والمتفاعلة مع بعضها البعض بأنها حادث أو أحداث ضارة تؤدي إلى تعطيل أو تعطيل مكونات وجوانب الأمن السيبراني للبنك. (اشويقي، 2022)

قام National Institute of Standards and Technology بتعريف المخاطر السيبرانية على أنها مقياس لمستوى التهديد والتأثير الذي حدث بالفعل أو من المحتمل أن يحدث، أو كليهما ويستهدف واحدًا أو أكثر من معلومات البنك أو عملياته أو قدراته أو سمعته وتعرف بأنها فرصة لتكبد خسائر ناتجة عن تعرض البنك أو موظفيه أو عملائه أو الجهات التي يتعامل معها لتهديد حدث أو محتمل الحدوث ويستغل ضعف قدراته وبين كل من Borky and Bradley مفهوم المخاطر السيبرانية هو استغلال غياب أو ضعف الضوابط الأمنية أو التدابير المضادة في أصول المعلومات في البنية التحتية الحيوية لتكنولوجيا المعلومات لسرقة أحد الأصول أو إفسادها أو إزالتها أو إتلافها مما يؤدي إلى تأثير سلبي يؤدي إلى ذهابها إلى البنك. (أميرهم، 2022)

المخاطر السيبرانية هي مزيج من توقعات التعرض لحادث سيبراني يستهدف نطاق الأصول المعلوماتية للبنك وموارده ومكونات تكنولوجيا المعلومات ويتم تحديد عواقب هذا الحادث على البنك بمخاطر تعطل أنظمة تكنولوجيا المعلومات في البنك أو فشل أو تدمير عملياته مما يترتب عليه خسارة مالية أو تعطل أو ضرر يؤثر على سمعة البنك أو مركزه المالي أو استمرارية أعماله. (عدنان، 2023)

وفي ضوء ما سبق يرى الباحث أن المخاطر السيبرانية هي عبارة عن أنشطة هجومية خبيثة وتأثيرها يستهدف وظائف البنك بكافة أشكالها وجوانبها أو القدرات التي يمتلكها أو من خلال استغلال الثغرات الأمنية وفي قاعدة البيانات يتم تدميرها أو اعتراضها أو تعديل مكونات البنية التحتية لتكنولوجيا المعلومات.

5.1.2 انواع مخاطر الامن السيبراني

الغرض الرئيسي من اختراق الأفراد أو المؤسسات أو العاملين فيها هو إيجاد فرصة أو ثغرة في البنوك من أجل سرقة بياناتها أو معلوماتها أو نقل البيانات المالية أو تعديلها أو الاحتيال المالي أو الوصول إلى بيانات مالية أو غير مالية المعلومات المالية أو تعطيل النظام المصرفي وتعطيل البنية التحتية (البسام،

(2020)

هناك أنواع مختلفة من مخاطر الأمن السيبراني وأهمها ما يلي:

- المخاطر التقنية للأمن السيبراني، والتي تتزامن مع تطور التكنولوجيا والاتصالات، مع المخاطر الخاصة المرتبطة مباشرة بهندسته المحددة والبيئة التي تعمل فيها.
- وتتجلى المخاطر القانونية في عدم وجود هيكل قانوني وتنظيمي مناسب، وبالتالي تزداد المخاطر القانونية مع انعدام الأمن القانوني، وتناقض بعض الأنظمة والقوانين، وتعارض النظم القانونية واتساع الإمكانيات.

هناك من يعتقد أن هناك أنواعًا أخرى من مخاطر الأمن السيبراني على النحو التالي

- مخاطر الأمن والمرونة وهي عملية التسلل إلى أصول البنك من خلال الاستخدام غير المصرح به والذي يؤدي إلى خسارة البنك أو إتلافه أو تعديله أو إضافة أو حذف للأصول والبيانات المالية من قبل مجموعة من الأفراد والجهات.
- مخاطر تكنولوجيا المعلومات، وهي مخاطر ضياع الفرص لاستغلال التكنولوجيا لتحسين أداء البنك.
- المخاطر التشغيلية هي تدمير العمليات الداخلية للبنك، وتؤدي هذه المخاطر إلى تعطيل أو تأخير إنجاز المهام والأهداف المرجوة.
- مخاطر السمعة: هذا النوع من المخاطر له أهمية خاصة في البنوك.
- تتمثل مخاطر الإمتثال في عدم الإلتزام باللوائح والقوانين الحالية في البنك، وذلك بسبب عدم معرفة الموظفين وعدم الإهتمام بتنفيذ القوانين.
- المخاطر الاستراتيجية تعني المخاطر الناجمة عن عدم التنفيذ الدقيق والصحيح للبرنامج، وهذا يؤدي إلى ضعف أو خلل في خلق الأمن السيبراني.

بينما اتفق عدد من الباحثين على أن مخاطر الأمن السيبراني تتكون من ثلاثة أنواع:

- مخاطر الأمن السيبراني تتعلق بالسرية، وهي الكشف عن المعلومات المملوكة للبنك لطرف آخر، مثل اختراق البيانات.
- مخاطر الأمن السيبراني المتعلقة بالنزاهة، وهي إساءة استخدام الأنظمة المصرفية مثل الاحتيال.
- مخاطر الأمن السيبراني المتعلقة بالأداء، وهي مخاطر الانقطاع أو الفساد أو تعطيل الأنشطة التجارية للبنك.

المبحث الثاني: البطاقات المصرفية

1.2.2 مفهوم البطاقات المصرفية

أولاً: البطاقة المصرفية لغة:

الورقة والبطاقة: هي ورقة صغيرة تسجل مقدار ما تضعه عليها، إذا كانت سلعة فوزنها أو عددها، وإذا كانت سلعة فمقدارها. (ياسر، 2022)

ثانياً: البطاقة المصرفية اصطلاحاً:

وهي بطاقة خاصة يصدرها البنك لعميله ليتمكن عند تقديم هذه البطاقة من استلام البضائع والخدمات من المتاجر والأماكن الخاصة على أن يتم السداد على فترات زمنية حيث يحق للعميل دفع جزء من المبلغ في نهاية الشهر والباقي على أقساط في الأشهر اللاحقة بزيادات من 17 أو 19 بالمائة بناءً على ما يتم الاتفاق عليه في العقد بين عميل الحامل والجهة المصدرة. (رشوان، 2022)

ويشير هذا التعريف إلى أن نظام البطاقة المصرفية نظام ربوي ويتضمن غرامات في حالة التأخر في السداد أو فوائد القرض الممنوحة أثناء استخدام البطاقة وهذا مخالف للأحكام الشرعية مما يحرم الربا بأي شكل من الأشكال ولهذا السبب قامت البنوك بإزالة التعديلات مثل تعديل بيت التمويل السعودي فيما يتعلق بالربا المتعلق ببطاقات المصرف وربط البطاقات بحسابات العملاء وهو ما يكفي لجميع مشترياته من السلع والخدمات سواء مقدماً أو عند وصول الفواتير ويشمل أيضاً وكالة المال، والسند الحر، والقرض العرضي. (السمحان، 2020)

كما ظهرت تجربة بنك الراجحي والتي تم فيها التعديل من خلال حذف الفوائد المتأخرة وربط الدفعات النقدية بالحساب الجاري للعميل بالإضافة إلى توفير التأمين النقدي في حالة وجود مشتريات زائدة على حسابه ويلتزم العميل أن يدفع مبلغ التأمين الذي يتم دفعه على الفور. (راضية، 2021)

هناك عدة تعريفات للبطاقات المصرفية جميعها تتناسب مع نفس الشكل حتى لو اختلفت خصائصها بسبب العلاقة المتشابكة الناتجة عن نظام البطاقة تستقبل هذه البطاقة السلع والخدمات من

متاجر وأماكن معينة ثم يقوم بائع السلع والخدمات بتقديم فاتورة موقعة من العميل إلى البنك مصدر الائتمان ويقوم بالدفع قيمتها ويقوم البنك بإرسال كشف شهري للعميل بإجمالي القيمة المقرر سدادها أو خصمها من حسابه الجاري. (سيد، 2020)

ويبدو أن هذا التعريف يركز على طبيعة عمل نظام البطاقة وإجراءاته من الاستخدام إلى الدفع والبعض الآخر يعرفه على أنه عملية شراء فقط: عقد يتعهد بموجبه مصدر البطاقة بفتح عملية اعتماد بمبلغ مخصص في لصالح شخص آخر وهو حامل البطاقة حيث يستطيع من خلالها إجراء عمليات شراء شخصية في المحلات التجارية المتعاقدة مع الجهة المصدرة للبطاقة حيث تتعهد بقبول المشتريات الصادرة عن حامل البطاقة الطرف الأول، على أن تتم التسوية النهائية بعد أي فترة محددة. (نبيل آيت، 2019)

يوضح هذا التعريف موقف البنك بناءً على الالتزام السابق كضامن لقيمة مشتريات العميل بالبطاقة وهذا الالتزام القانوني يساعد على فهم طبيعة موقف البنك تجاه العملاء لتتمكن فيما بعد من إنشاء موقف مناسب الامتثال القانوني الذي يغطي جميع جوانب البطاقة وتغطية خطواته ومن الناحية الاقتصادية هناك تعريف آخر وهو الأداة البلاستيكية التي من خلالها يقوم مصدر مثل البنك أو الاتحاد الائتماني أو مؤسسة الادخار أو أي مؤسسة مالية أخرى بمنح خط ائتمان متجدد. قرض يمكن للمستهلك استخدامه لشراء أجهزته وإذا لم يرغب في سداد جميع ما اقترضه في وقت لاحق من كل شهر فيسمح له بتحويل جزء أو كل المبلغ المقترض إلى شهر آخر وفي هذه الحالة يجب عليه دفع الفائدة على رصيد الدين الحالي. (Hossain, 2021)

ويركز هذا التعريف على نوع من أنواع البطاقات وهي بطاقة المصرف ذات قروض دوارة تستخدم على نطاق واسع في الأسواق العالمية وعندما نقول بطاقة مصرفية فإننا نعني نوع البطاقة التي عرفها الفقهاء المسلمون على هذا النحو: الوثيقة التي يعطى مصدرها لشخص طبيعي أو معنوي بموجب عقد بينهما، يستطيع بموجبها شراء بضائع أو خدمات من مظهري الوثيقة دون سداد ثمنها فوراً. وتتضمن التزام المصدر بالدفع وهي أحد أنواع هذه الوثيقة التي تسمح بسحب الأموال من البنوك على حساب المصدر فيما يتعلق بالاستخدامات الرئيسية للبطاقة: السحب والشراء. (غزالي، 2022)

يتضح من التعريفات السابقة أن فكرة بطاقة مصرفية تقوم على الالتزام بالدفع لاحقاً مقابل التمتع بمصاريف أنية، أي أنها جسر بينهما وبالتالي ليست أموالاً تحدث الحاجة إلى المال عندما يأتي البيان التفصيلي للمعاملات التي تمت على البطاقة ومن ثم يتم الدفع الفعلي نقداً، ولكن ليس نقداً حتى السداد (التسوية). (اسماعيل، 2019)

ولذلك فإن جميع التعريفات السابقة تركز حقاً على فكرة أساسية واحدة وهي الائتمان الممنوح للعميل وهو جوهر البطاقة، وتفترض هذه الفكرة: أن هناك فاصل زمني بين منح الاعتماد وهو ما يوفر تعني ببطء إجراء المعاملة واسترجاع تلك الوسائل، لذلك يمكن القول أن بطاقة مصرفية هي بطاقة تحتوي على معلومات معينة، بما في ذلك اسم ورقم حساب صاحبها، صادرة عن جهة ما عادة ما تكون بنكاً أو مؤسسة مالية ويلتزم الحائز بدفع قيمة مشترياته من خلالها، بحيث تقوم الجهة المصدرة بتعجيل سداد قيمة المشتريات للتاجر، على أن يستردها لاحقاً من الحائز على دفعات أو دفعة واحدة وفقاً لأحكام محددة تم الاتفاق على الشروط. (بانقا، 2019)

2.2.2 مزايا البطاقات المصرفية

إن استخدام البطاقات المصرفية له فوائد عديدة لكلا الطرفين وتختلف هذه الفوائد من طرف إلى آخر، لذا سأحدث عن فوائد كل منها على حدة. (Ndhine, 2020)

- سرعة السحب والفعالية التي جعلت العملاء يستخدمونه.
- توفر بطاقة المصرف الأمان من خلال عدم حمل النقود وتعريضها للسرقة أو الخسارة أو التلف.
- منح حامل البطاقة القدرة على الاقتراض بما يزيد عن دخله
- تداول مع الآخرين بأي عملة دون الحاجة إلى حمل عملات متعددة خاصة عند السفر.
- وهي تمكن حاملها من شراء ما يريد وقتما يشاء، حتى لو تعرض لموقف مفاجئ لم يكن مستعداً له بحمل النقود ذات الصلة.
- يحصل الحائز على مكافآت وهدايا من مصدره أو من الطرف الآخر (التاجر).

- الاحتفاظ بحسابات منتظمة، حيث تعتبر البطاقة وسيلة للمحاسبة وضبط النفقات وتوثيق متطلبات الدفع.
- أنها تمكن الناقل من تلبية احتياجاته من السلع والخدمات قبل دفع الثمن
- إمكانية التسوق عبر الإنترنت
- القدرة على سحب النقود من أجهزة الصراف الآلي
- توفر البطاقة لحاملها ميزة ضمان العيوب الخفية، حيث يرفض حاملها دفع قيمة البضاعة المعيبة لجهة الإصدار.
- غالباً ما يستفيد حامل البطاقة من الدفع بالتقسيط لأن البنك لا يطلب منه دفع الفواتير دفعة واحدة.
- يمكن لحامل البطاقة إعطاء حق استخدام البطاقة المصرفية لأي شخص يريده في حساب ائتماني مثل زوجته وابنه، وهذه الميزة مهمة في بعض الحالات مثل الرحلات الطارئة، كما أنه من السهل إنشاءها وإلغاءها في نفس الوقت وقت.
- وتتيح لحاملها شراء بعض السلع والخدمات بأسعار مخفضة، بالإضافة إلى أن وجود صورة شخصية على البطاقة المصرفية يسمح باستخدامها كبطاقة تعريف شخصية، خاصة عند السفر.
- يعمل على تقليل الفواتير والإيصالات الورقية المختلفة في جميع الشؤون الشخصية والعائلية
- ومن خلال قبول البطاقة يستطيع التاجر جذب عملاء جدد وبالتالي زيادة مبيعاته
- ويجب على التاجر أن يكون واثقاً من حصوله على السعر مع ضمان المصدر، لأنه بمجرد تقديم الفواتير والمستندات المطلوبة يكون البنك هو الضامن لهذه المبالغ.
- استخدام البطاقة يوفر الأمان، إذ قضى التجار على الكثير من السرقات التي يرتكبها المحاسبون
- الاستفادة من الحملات الإعلانية التي ينظمها البنك لتحفيز عملية إصدار البطاقات، خاصة عند ذكر أسماء المؤسسات والمتاجر التي تقبل هذه البطاقات.
- زيادة التسهيلات التي يحصل عليها حامل البطاقة ستشجعه على زيادة مشترياته وهذا سيفيد التجار.

- التاجر الذي يقبل البطاقة يميز نفسه عن أقرانه الذين لا يقبلونها وهذه ميزة تنافسية.
- تساعد بطاقة المصرف على تحقيق السرعة في إجراء المعاملات التجارية
- ويمثل إصدار البطاقة مصدراً جديداً للإيرادات يتمثل في الرسوم التي يتم تحصيلها من حاملي البطاقات والعمولات التي يتم تحصيلها من التجار
- استقطاب عملاء جدد للبنك الذين يقومون بفتح حساب في البنك لتسجيل حقوقهم، وكذلك حاملي البطاقة الذين يلجأون إلى فتح حساب لدى البنك وإيداع مبالغ الضمانات لديهم.
- الحصول على عمولة مقابل استخدام خدمة تحويل الأموال عبر الصراف الآلي
- ويحصل البنك على فرق العملة عند تحويله إلى عملته الوطنية.
- تحصيل نسبة من ثمن البضاعة التي يتسلمها البنك من البائع التاجر، هذا التحصيل المشترك هو المصدر الرئيسي وأكثر الدخل الذي يبحث عنه البنك، وهي المشكلة الأهم التي تتناول مشروعية التعامل مع بطاقة الائتمان.
- تلقي الأموال لدفع الفواتير الأجنبية.
- توفر تجمع للسيولة لدى البنك المصدر بسبب التدفق النقدي الموضح في الفترة ما بين استلام الدفعات من حاملي البطاقة وصرف المبالغ للتجار.
- إن استخدام البطاقة يقلل من كتابة الشيكات الشخصية، الأمر الذي يؤدي نتيجة متابعة الأمور المصرفية المختلفة إلى تكاليف باهظة.
- تحقيق الرخاء الاقتصادي من خلال الائتمان الممنوح لهذه البطاقة من خلال زيادة الطلب على السلع والخدمات وكل ذلك يؤدي إلى النهوض بالاقتصاد.
- تقليل مخاطر المعاملات النقدية، بما في ذلك التزيف والسرقه والتلف والخسارة، وبالتالي إنقاذ الحكومة من طباعة النقود الجديدة بشكل مستمر.
- تعتبر الضرائب المفروضة على الشركات الكبيرة المصدرة للبطاقات مورداً هاماً للحكومة، وهو ما ينعكس على القدرة الإنفاقية للدولة.

3.2.2 عيوب البطاقات المصرفية

يتم انتقاد البطاقات المصرفية في بعض الأحيان لأنها تغري الناس بشراء أكثر مما يستطيعون تحمله أو بعبارة أخرى "نشر الطلب الكاذب والإفراط في الشراء لأن المشتريات لا تعتمد على دخل الشخص أو رصيده البنكي بل على مستوى الدخل المتوقع". (عمر، 2020)

فضلاً عن خفض معدل الادخار للفرد وكلما كان التأخير في سداد الدين على مسؤوليته زاد لأن غرامات التأخير تضاعف الفوائد الربوية للبنك المصدر للبطاقة ويترتب على ذلك أن المسلم يخالف ما حرم الله في البنوك الربوية اهتمام وفي حالة البنوك التي تصدر البطاقات المصرفية وفق الضوابط فلا مكان للغرامات المتأخرة وحتى تراكم الديون لأن البنك يشترط على العميل أن يكون له حساب في البنك يستحق الشراء منه البطاقة متوفرة لكن في حال عدم وفاء العميل بالتزامه بدفع قيمة المصاريف الناجمة عن استخدام البطاقة أو الكشف عن رصيده بشكل متكرر يكتفي البنك بإلغاء البطاقة أو عدم التعامل معها. كما أن من أكبر المخاطر هي سرقة البطاقة أو ضياعها واستخدامها من قبل اللصوص أو من يستنكرها وهو أمر نادراً ما يحدث لكنه يؤثر بسرعة على سمعة النظام وتتخذ البنوك إجراءات احترازية في مثل هذه الحالات لأنها تطلب من حاملي البطاقات الإبلاغ عن سرقة حالة بطاقتهم في أسرع وقت والاتصال بهاتف البنك كما أن التكاليف مرتفعة مقارنة بالتكاليف والمنافسة على العمولة المعدلات التي يتقاضاها البنك من التاجر الذي يقوم به بالإضافة إلى تكاليف توزيع البطاقات التي لا يستخدمها أصحابها أو الخسائر بسبب عدم الأمانة في استخدام البطاقات والقروض المجانية لمدة قد تصل إليها ونظراً لارتفاع حجم المعاملات فإن يوم التعامل بالبطاقة أيضاً يخلق خطراً على سيولة البنك كما أن ارتفاع حجم القروض التي يتم الحصول عليها من حاملي هذه البطاقات يتطلب من البنك تقليل الاستثمار في مجالات أخرى. التصور العام للبنك قد يزداد الأمر سوءاً إذا اعتقد عامة الناس أن استخدام البطاقة هو أحد أسباب ارتفاع التكلفة. التاجر هو الرسم الذي يتقاضاه البنك من المستهلك عن طريق زيادة سعر البضائع المشتراة منه. ومن السلبيات الأخرى المرتبطة بنظام البطاقة أن الشركات المصدرة تتأخر في إرسال الفاتورة لحامل البطاقة مما يستغرق الوقت المسموح له بالدفع بدون فوائد ثم تسارع الشركة في السداد بعد 25 يوماً. تطبيق الفائدة على الرصيد غير المدفوع. 30 يوماً من تاريخ الفاتورة التي لم يستلمها إلا قبل أيام قليلة من نهاية المدة المسموح بها ولا يتم

تسجيل الدفعات التي يقوم بها مباشرة في حسابه بل يتم تسجيلها مع تأخير مما يفرض فائدة إضافية عليه وربما في رأي أن هذا الأمر مقصود في بعض الأحيان من جانب البنوك من أجل تقليل حجم القروض المجانية الممنوحة للعملاء بالإضافة إلى ذلك لأنه على سبيل المثال يتم إرجاع البضائع المشتراة من قبل العميل بسبب عيوب. وقد يرفضها التاجر لأنه استلم قيمتها من البنك. (راضية، 2021)

وهنا لا بد من ذكر نقطة مهمة وهي أن المؤسسات التي تتحكم في روابط الاتصال عن بعد تدخل في سلسلة التوريد وتصر أو تؤكد أن العميل النهائي هو في الواقع عميلها والبنك ببساطة صاحب المصنع أو المصنع كتاجر تجزئة يمكن اعتبار البنك بنكاً وبالتالي ستصبح هذه المنظمات مالكة للمستهلك في المستقبل ويريد المستهلك التعامل مع البنك وليس مع الشخص الذي يتحكم في التوزيع لذلك يجب على البنوك أن تتحمل مبالغ كبيرة من الإعلانات وتطوير العلامة التجارية لتعزيز ولاء المستهلك في المستقبل. (الشورة، 2020)

وبحسب ما سبق فمن الواضح أن على البنوك أن توازن سياساتها في منح القروض الاستهلاكية على شكل بطاقات مصرفية حتى لا تؤثر على الاستثمار في مجالات أخرى بحيث تتجاهل البنوك مجالات أخرى بسبب الأرباح التي تحصل عليها. ولأن حجم التعاملات الكبيرة بالبطاقة يؤثر على سيولة البنك فهذه سلسلة من النقاط السلبية التي لا يمكن تجاهلها خاصة في مجتمعاتنا لأنها مشاكل تعيق تقدم النظام وتحد منه إلا إذا تم السيطرة عليها والتغلب عليها ووضع الحلول المناسبة للتغلب عليها. (نبيل آيت، 2019)

وعلى الرغم من المزايا العديدة التي تتمتع بها البطاقات المصرفية إلا أنها لا تخلو من العيوب وتختلف هذه العيوب باختلاف الجهة.

- الإساءة لحاملي البطاقة بتجاوز الحد الائتماني المحدد لها وعدم سداد الدين بسببها.
- إذا لم يحم حامل البطاقة بسداد التزاماته المالية في الوقت المحدد فسيتم وضع اسمه في القائمة السوداء للبنوك ذات الائتمان غير المقبول، مما يسبب الكثير من الإرباك لحامل البطاقة.
- الإفراط في الاستهلاك بسبب سهولة الشراء وتأخير الدفع، ينفق بعض الأشخاص الكثير دون حساب أو تنظيم.

- ارتفاع نسبة الفوائد الممنوحة من خلال البطاقة، خاصة في حالة التأخير، وهذا الخلل مخالف للمعايير الشرعية، لذا يجب أن يتخلص نظام البطاقة من الفوائد الربوية وغرامة التأخير للالتزام بها أحكام الشريعة وحتى لا يقع المسلم في الربا.
- إمكانية سرقة البطاقة أو تزويرها، وفي هذه الحالة يلتزم صاحب البطاقة بدفع قيمة ما اشتراه بها.
- عدم قيام التاجر بالتحقق والتأكد من صلاحية البطاقة والالتزام بتوقيعه أو عدم الحصول على موافقة البنك في حالة تجاوز العميل الحد الأقصى مما يتسبب في خسارة التاجر المالية.
- وعدم قدرة البنوك على سداد ديون مستخدمي البطاقة ولو لفترة قصيرة يعرض التجار للخسائر وربما للإفلاس.
- وجود مشاكل وخلافات بين حامل البطاقة والبنك المصدر لها بسبب عدم اهتمام حامل البطاقة باستلام الفواتير أو عدم سداد الديون مما يخلق أزمة ثقة بين البنك والعميل.
- التكاليف المالية للبنك تتعلق بتوزيع وطباعة البطاقات، وتكاليف فقدان البطاقة والسرقة والاحتيال والتزوير هي مسؤولية البنك.
- عدم سداد الديون من قبل حاملي البطاقات ونتيجة لذلك ترتفع نسبة الديون المستحقة بسبب زيادة نسبة بطاقات الائتمان ووجود حوافز استهلاكية لدى مستخدمي البطاقات.
- عدم توفر رأس المال الكافي للتعامل مع عمليات السحب النقدي والاقتراض بالبطاقات المصرفية، مما يهدد سيولة البنوك.
- يتطلب العمل بالبطاقة المصرفية توفير شبكة اتصالات عالية الجودة لتسهيل عملية استخدامها لحاملها والتجار وحمايتها من مخاطر الاستخدام غير القانوني.
- خفض معدل الادخار، لأنه يستنزف أموال الناس.
- يمكن أن يؤدي الاستخدام إلى ارتفاع الأسعار لأن التجار يقدمون ائتمناً للمستهلكين بنسبة مماثلة أو أكبر مما يفرضه عليهم مصدرو البطاقات.

4.2.2 خصائص البطاقات المصرفية

هي أداة ولاء وانتماء لأن صاحبها يستطيع الوفاء بالتزاماته تجاه التاجر أو صاحب الخدمة دون الحاجة لحمل النقود وذلك من خلال إبراز البطاقة. أن يقوم التاجر بتسليم الفاتورة للبنك. (الزبيد، 2020)،

ومن مميزات البطاقة المصرفية البنكية أنها تعتبر بطاقة مصرفية شخصية ولا تعود لصاحبها، ولكل مالك رقم تسلسلي خاص به، فلا يمكن تسليمها إلى شخص آخر، لأن هذا يعتبر بمثابة خرق العقد وستكون الالتزامات التي تؤدي إلى مسؤولية حامل البطاقة والاستخدام غير القانوني للبطاقة من قبل الآخرين تؤدي أيضاً إلى المسؤولية الجنائية والمدنية (CB). 2021).

علاقة ثلاثية حيث تقوم البطاقة المصرفية على علاقة ثلاثية من حيث جهة إصدار البطاقة (البنك، حامل البطاقة، التاجر) ولكل من هذه الأطراف حقوق والتزامات وترتبط بالآخرين بشكل منفصل من خلال عقود مستقلة ينتج عنها كيان واحد مع علاقات ثلاثية ومن مميزات بطاقة الائتمان أنه لا يمكن استخدامها إلا عن طريق الأجهزة التقنية حيث أنه يوجد العديد من طرق استخدام البطاقات المصرفية في الماضي هي أن تقوم جهة ما وهي عادة بنك بإصدار هذه البطاقات من الورق أو البلاستيك أو أي مادة أخرى يصعب التلاعب أو تزوير المعلومات ويكتب عليها رقم وعندما يقوم العميل يريد شراء سلع أو خدمات، يقوم بتقديم البطاقة إلى صاحب السلعة أو مقدم الخدمة الذي يقوم بكتابة معلومات حامل البطاقة على الفاتورة ثم يقوم العميل بالتوقيع. ومن ثم تقوم بإرسال الفاتورة إلى جهة إصدار البطاقة، حيث تقوم بدفع قيمة الفاتورة بشكل فوري، وتقوم جهة إصدار البطاقة بإرسال الفاتورة إلى العميل في نهاية كل شهر أو كل فترة متفق عليها والتي يتوجب عليه سدادها. (عمر، 2020)

5.2.2 أهمية البطاقات المصرفية

وقد تميزت البطاقة المصرفية بتحقيق نجاحات ملموسة في العديد من الجوانب السلبية والإيجابية في التعاملات المصرفية، وفي الواقع اكتسبت الأمان لحاملها من السرقة أو السرقة أو فقدان

الأموال كما أنها تتمتع برقم رمزي لحاملها ومن الحقوق أنه بعد التأكد بواسطة جهاز إلكتروني (كمبيوتر) يضمن سداد مبلغ دين حامل البطاقة وهي مقبولة عالميًا لأنها أداة مفضلة على المال نفسه في الأعمال التجارية والمطاعم والفنادق وما إلى ذلك. وقد كانت سببًا في زيادة المبيعات في المتاجر التجارية وحقت أرباحًا ملموسة وهادفة ونشطة لمصدري البطاقات. آلية سريعة في العمل وضمان الحقوق. (راضية، 2021)

6.2.2 أنواع البطاقات المصرفية

بطاقات الائتمان المتداولة في الأسواق العالمية والمستخدم في شراء الخدمات وتلقها هي على ثلاثة أنواع:

❖ النوع الأول: بطاقة الخصم الفوري

ويتم تعريف ذلك بأن المالك لديه رصيد في البنك، فيقوم مباشرة بتحصيل قيمة الشراء ومقابل الخدمات المقدمة له بناءً على السند الموقع.

وتعرف بأنها يكون لدى حامل البطاقة رصيد بنكي ومن ثم يفوض البنك مصدر البطاقة بالسحب مباشرة من رصيد حامل البطاقة قيمة مشترياته ورسوم الخدمات المستلمة باستخدام البطاقة من السندات الموقعة منه.

يتم إصدار مثال على هذا النوع من بطاقات الخصم التلقائية للعملاء الذين لديهم حسابات جارية أو حسابات توفير لدى البنك الذي أصدر البطاقة.

❖ النوع الثاني: بطاقات المصرف القروض غير القابلة للتجديد

وهو بنك يقوم فيه البنك المصدر للبطاقة بإعطاء قرض لحامل البطاقة ضمن حدود معينة حسب درجة البطاقة الفضية أو الذهبية ولمدة معينة يجب سدادها بالكامل في وقت معين يتم الاتفاق عليه في ذلك الوقت لقضية عندما يتأخر السداد يتحمل حامل البطاقة الفائدة وهي الشكل الأساسي للبطاقة المصرفية.

وهي بطاقة تمكن حاملها من استخدامها لشراء واستلام الخدمات بالإضافة إلى السحب النقدي من خلال الأجهزة التابعة للبنوك المصدرة حول العالم.

وأهم ما يميز هذه البطاقات هو أن العميل لا يحتاج إلى حساب لإصدارها كما أنه مطالب بدفع سحوباته كاملة خلال فترة معينة، والتي عادة لا تتجاوز الثلاثين يوماً وفي حالة تأخر حامل البطاقة خلال هذه الفترة يلزمه دفع غرامة تأخيره وتم استرداد البطاقة منه واتخاذ الإجراء ضد حاملها كما يلزمه دفع رسوم الاشتراك ورسوم التجديد و فائدة القرض.

❖ النوع الثالث: البطاقات المصرفية الدوارة

وهو ما تمنحه البنوك المفتوحة لعملائها بشرط أن يكون لهم الحق في الشراء والسحب النقدي حتى مبلغ معين ولديهم التسهيلات في سداد القرض المتأخر على أقساط وممتدة قرض يمكن تمديده على فترات بنسبة فائدة معينة وهي الزيادة في سعر الفائدة للبطاقة الأكثر شيوعاً في العالم وأشهرها: بطاقة الفيزا.

يحق للمالك الاختيار بين سداد السحوبات كاملة في الموعد المحدد أو دفع جزء منها وتأجيل الباقي إلى الفاتورة التالية في حالة التأخير سيتم محاسبته غرامة التأخير في السداد وغير ذلك غرامة غير مدفوعة غرامة ولكن إذا تم سداد جزء منها في الموعد المحدد ما دام المالك مستمراً في دفع جزء من الدين والفوائد فلا يلزمه إلا تأجيل الفوائد وأهم ما يميز هذه البطاقة أنها لا تحتاج إلى حساب مستخدم لإصدارها بل يقوم البنك المصدر بإقراض العميل مبلغاً بحد أقصى يسمى "حد الائتمان" ومن ثم يقوم العميل بدفعه بالتقسيط ولا يقتصر على شهر واحد ويلتزم حامل البطاقة بسداد أربع دفعات رسوم العضوية ورسوم التجديد وفوائد القرض والفائدة المتأخرة.

7.2.2 استخدام البطاقات المصرفية

ومن خلال المقدمة السابقة يتضح ما هي أهم استخدامات البطاقة لأن جميعها تتناول شراء السلع والخدمات التي تلبي الاحتياجات اليومية للشخص يستطيع العميل الذي يحمل البطاقة شراء سلع متنوعة

والاستفادة من المزايا والخدمات في أكثر من (13,000,000) منشأة ومحل تجاري بما في ذلك الفنادق ومكاتب السفر والسياحة وشركات الطيران المنتشرة في معظم دول العالم كما يمكن السحب النقدي أو من خلال ماكينات الصراف الآلي التي تحمل العلامة التجارية (Cyrus) لبطاقة الماستر كارد العالمية والعلامة التجارية (Visa) لبطاقة الفيزا الدولية والتي تتوفر في معظم دول العالم ويبلغ عدد أجهزة الصراف الآلي يتوفر أكثر من (280,000) جهاز صراف آلي في (87) دولة منها 38,000 جهاز صراف آلي في الشرق الأوسط وأفريقيا أو من خلال الفروع التابعة لأكثر من (25,000) مؤسسة مالية أو بنك أعضاء في ماستركارد. كما أن خدمة إجراء المكالمات الهاتفية بتكلفة أقل من الرسوم المعتمدة للمكالمات الدولية مع بطاقات الخدمة الهاتفية الأخرى وذلك لأن البنك الإسلامي يقدم خدمات متقدمة نسبياً لحاملي بطاقة ماستركارد وهي خدمة Masterphone لإجراء مكالمات هاتفية دولية من أكثر من 70 دولة. بسبع عشرة لغة من بينها اللغة العربية يتم تقديم خدمة Masterphone مجاناً لحاملي بطاقة MasterCard داخل الدولة وفي هذه الحالة سيتمتع العميل بالمزايا التالية: (CB, 2021)

- وفر حتى 80% على المكالمات الدولية التي تتم عبر بطاقات الخدمة الهاتفية أو مباشرة عبر الفنادق.
- تجنب الرسوم والضرائب الإضافية التي تفرضها معظم الفنادق على المكالمات الدولية حيث يجب استخدام رقم التعريف الشخصي لخدمة MasterPhone لهذه الخدمة فقط وليس المقصود منه أن يحل محل رقم التعريف الشخصي للبطاقة المستخدم في السحب النقدي.

وهناك استخدامات أخرى للبطاقات المصرفية في دول العالم المتقدمة، منها:

- الشراء عن طريق البريد أو الهاتف: تقوم بعض المؤسسات والمتاجر بالإعلان عن خدماتها وبضائعها في الصحف والمجلات، ويمكن لحامل البطاقة تعبئة قسيمة الإعلان لشراء السلع أو الخدمات وإدخال رقم بطاقته.
- بطاقات الدفع: يستخدمها العميل لدفع ثمن السلع والخدمات، وفي هذه الحالة لا يكون للعميل أي رصيد لدى البنك مصدر البطاقة، من فواتيره، جميع الخدمات التي تقدمها البطاقة غير ملزمة

به فلا يدفع إلا في آخر الشهر أو في نهاية المدة المتفق عليها وحتى حلول الأجل ففيه اعتماد قصير وغير مرغوب فيه.

تستخدم البطاقات المصرفية الحقيقية للدفع كما في الصورة السابقة ولكنها تضيف الحقوق الائتمانية المتفق عليها للعميل وتمكنه من دفع قيمة فواتيره ومعظم البطاقات. واليوم هم من هذا النوع، وفي الحقيقة هذه البطاقة عبارة عن قرض، يجوز تحويل جزء أو كل المبلغ المقترض إلى الشهر التالي، وفي هذه الحالة يشترط دفع الفائدة على المبلغ المتبقي الديون (بنجاح).

- **بطاقة الحساب أو البطاقة المصرفية العادية (بطاقة الشحن) أو بطاقة الدفع المؤجل، والتي** يتم فيها خصم المبلغ الإجمالي في نهاية كل شهر، بغض النظر عن تاريخ شراء السلع أو الخدمات، ودون تسجيل فوائد على الدين في حسابك عند استخدام البنك، يحصل تلقائياً على قرض يساوي قيمة السلع أو الخدمات، ويلتزم المالك حسب شروط الإصدار دفع مبلغ الفاتورة كاملاً خلال فترة لا تتجاوز عادة ثلاثين (30) يوماً من تاريخ الاستلام. ولسداد ديونه، ومن أشهرها البطاقة الخضراء الأمريكية

- **بطاقة الخصم أو بطاقة الخصم المباشر أو بطاقة الخصم الفوري، تعني أنه في حالة إجراء** عملية شراء عبر البطاقة، يتم خصم قيمة الشراء من حساب العميل فوراً أو خلال أيام قليلة، دون دفع المبلغ بالتقسيط على فترات زمنية دون حملها من شهر إلى آخر فمعنى الخصم الفوري هو أن يتم تسجيل المبلغ لدى البنك مباشرة بعد استلام الحساب أو الفاتورة والتي في حالة استخدام البطاقة تكون مرتبطة بالحساب الجاري للعميل الذي تمت المشتريات منه يتم خصمها. هو الرصيد المتوفر تحت تصرف العميل (الوديعة). وهذا الحساب يشبه الضمان النقدي، وكما تم استخدام البطاقة يقوم مصدر البطاقة بالسحب مباشرة من حسابه لدفع قيمة الفاتورة الواردة من التاجر. ويتواجد هذا النوع من البطاقات في العديد من الدول النامية بهدف التحكم بكمية الأموال الموجودة في الاقتصاد، وذلك لعدم وجود أسواق نقد متطورة يمكن من خلالها تنفيذ سياسة نقدية لتحقيق ذلك الهدف. الدول حريصة على الادخار وهو هدف من خلال التوسع في استخدام البطاقات المصرفية، وتقوم العديد من البنوك الإسلامية بإصدار هذه

البطاقات اعتماداً على موافقة نموذج العقد من قبل كياناتها القانونية مثل مصرف الراجحي وبيت التمويل الكويتي أن هذه البطاقة لا تعتبر بطاقة انتمائية ولا تؤخذ في الاعتبار عندما يتعلق الأمر بالبطاقات الانتمائية.

- بطاقة ذكية. وهي بطاقة مصرفية تفاعلية تحمل رؤية مستقبل البطاقات البلاستيكية، إلا أنه على الرغم من توفر التكنولوجيا اللازمة لإصدارها واستخدامها، إلا أن هذه البطاقة لم تصل بعد إلى شريحة رقيقة وشريط كهرومغناطيسي يمكن قراءته إلكترونياً (الشريط المغناطيسي) يمكن أن يتفاعل مع أجهزة الصراف الآلي أو أي آلية أخرى، لذلك ليست هناك حاجة للحصول على موافقة مسبقة من الجهة المصدرة للبطاقة.

8.2.2 فائدة البطاقات المصرفية

- فائدة البطاقات المصرفية على حاملها

بالنسبة للمستهلك لم تعد البطاقة تقتصر على خدمات السفر والترفيه فحسب بل تجاوزت ما هو مرئي ولملموس لتمكنه من شراء كافة احتياجاته المتنوعة بالإضافة إلى الخدمات الأخرى الضرورية لتقديم حياتك وحياتك. وسائل الراحة مثل دخول المطاعم والإقامة في الفنادق والحصول على تذاكر السفر التي قد تكون مصحوبة بالتأمين ضد الحوادث. ليست هناك حاجة لحمل النقود أو كتابة الشيكات بل أصبحت البطاقة ضماناً للشيكات التي تصدرها وبذلك تؤدي البطاقة بل وتؤدي جميع وظائف النقود واستخداماتها. وبالإضافة إلى كل هذا فإن المستهلك يشعر بالهبة وراحة البال عندما يشعر أنه يستطيع الدخول إلى أكثر من نصف مليون محل تجاري وشراء ما يريد منها دون أن يكون معه ريال واحد. (Hossain, 2021)

والأكثر من ذلك أن البطاقة ساعدت المستهلك على اقتراض الأموال وخاصة البطاقات المصرفية لأن بطاقة ماستركارد توفر للمستهلك سلفة نقدية بقيمة 500 دولار دون طرح أي أسئلة. لذا فهو يجمع بين فوائد ائتمان التجزئة العادي وقروض التقسيط والقروض الشخصية.

وأصبحت هذه الأداة بديلاً للنقود والشيكات مما يترتب عليه تجنب مخاطر السرقة والخسارة كما سبق أن ذكرنا إمكانية السحب النقدي من أي فرع من فروع البنوك العالمية الكبرى. كما أن المصدر عند الرغبة هو رصيد مناسب إذا أراد حامله مبلغاً في حدود معينة فعندما يدفع المستهلك شهرياً مبلغاً ثابتاً حسب شروطه فهو مساعد. تعتبر بطاقة الائتمان مسؤولة قانوناً عن التضخم في كل عملية شراء تتم باستخدام البطاقة تماماً كما أنت الآن قبل ارتفاع الأسعار.

وهناك فوائد أخرى يحصل عليها المستهلك حيث يسهل هذا النظام المعاملات التجارية والمشتريات والمشتريات حيث أن استخدام البطاقة في إجراء عمليات الشراء يبسط عملية الشراء من حيث عد الأموال والتحويل من عملة أخرى أثناء السفر. علمياً يجعلها سلسلة ومريحة. فضلاً عن تجنب العملات المعدنية التي تضر وتضر بالشخص فإنه في هذه الأيام يصعب أيضاً على الأشخاص أخذها من الآخرين بشكل مستمر وهنا تظهر أهمية البطاقات من خلال إجبار الناس على الاقتراض من الجهات المختصة. دون الشعور بالحرج والشك وعادة بعد الحصول على البطاقة واستخدامها يعد ذلك عاملاً مهماً لأنه يخلق سجلاً ائتمانياً لكل حامل بطاقة لديه بطاقة صالحة وقابلة للاستخدام مقارنة بمن لا يملكونها. لا يحملها أصحاب الفنادق ولا تأجير السيارات فهي لا تزال معروفة. - عمليات الدفع للمشتريات التي تزيد من نشاط التسوق والازدهار الاقتصادي وهذا ينعكس إيجاباً على حركة السوق التجاري كما توفر البطاقة الحماية اللازمة في أوقات الحاجة وعند الحاجة للعلاج أو الدواء. على سبيل المثال ليس من الممكن الحصول على الخدمات المصرفية. (Ndhine, 2020)

الفوائد هائلة ولا يمكن للناس أن يصدقوا مدى التقدم الذي تم إحرازه في هذا المجال لأنهم في بعض الأحيان يعتقدون أن الأمر ضرب من الخيال (توفير الوقت والجهد والمال عندما يستخدم العميل بطاقته في الخارج ويستخدم البلد ويدفع سحوباته بالدينار الأردني ويتجنب تكلفة التحويل إلى العملات الأجنبية كما يتمتع العميل بتغطية تأمينية تصل إلى 150 ألف دولار أمريكي وهي على سبيل المثال بطاقة فيزا الذهبية وهذه البطاقة بمثابة جواز السفر أو وثيقة توضيح القدرة لحاملها ويستفيد حامل البطاقة من رصيد مجاني وهي الفترة الزمنية بين إتمام المعاملة التجارية وتقديم الفاتورة للدفع من قبل حاملها على غرار فترة دين حاملها بدون فوائد لمدة 20 إلى 30 يوماً لأن الفواتير يتم تقديمها

شهرًا بالإضافة إلى ذلك يمكن لحامل البطاقة سحب الأموال من أي فرع من فروع البنك (ومن أجهزة الصراف الآلي الموزعة في حوالي 75 ألف موقع حول العالم) للسحب النقدي. (CB, 2021)

وكذلك دعم البنك هو أن السلعة المشتراة مطابقة للمواصفات المطلوبة في بعض الأحيان يتم تخفيض قيمة الشراء كبطاقة خصم من التاجر - أكثر من سعر السوق من 5% إلى 30% حسب السلعة ومؤسسة العمل - كما تضمن عدم خسارة حاملها أكثر من مبلغ معين في حالة الضياع أو السرقة أو الاستخدام غير القانوني من قبل شخص آخر ولا يمكن للتاجر الرجوع إليها إذا لم يتمكن من استلام حقه من الجهة المصدرة للبطاقة. التي تطلب من المصدر ومصدرها يطلب من حاملها (Quazzani, 2022)

وكذلك دعم البنك هو أن البضائع المشتراة مطابقة للمواصفات المطلوبة. وفي بعض الأحيان يكون تخفيض قيمة الشراء كبطاقة الخصم من التاجر - أكثر من سعر السوق من 5% إلى 30% حسب السلعة ومؤسسة العمل - كما يضمن عدم معاناة حاملها أكثر من مبلغ معين في حالة فقدانها أو سرقتها أو استخدامها من قبل شخص آخر مخالف للقانون وإذا لم يتمكن التاجر من الرجوع إلى مصدر البطاقة ضد حاملها باعتباره المصدر فإنه يطالب بها ومصدرها يطالب بها صاحبها

• فائدة البطاقات المصرفية على التجار

أرباح كثيرة تعود على التجار الذين يتعاملون بنظام البطاقة مع تكبدتهم تكاليف مالية لأن البنك المصدر للبطاقة يأخذ نسبة من كل فاتورة في حساب التاجر تسمى رسوم الخدمة يتم تحميلها على البنك ونسبة للسلع والخدمات ذات القيمة العالية وتصل إلى 5% للسلع ذات القيمة المنخفضة إلا أن التاجر يستفيد من ضمان البنك لسداد قيمة الفواتير من قبل العميل لصالح التاجر لأن هذا الشيك قد يكون له رصيد في البنك الذي صدرت عليه ولم يتم ذلك فيتعرض التاجر لعدم استيفاء حقوقه بينما يستطيع الوصول إلى حقوقه بطريقة أسهل. من خلال البطاقة الائتمانية والتسهيلات التي يحصل عليها العميل من خلال البطاقة تشجعه على زيادة الشراء وهذا يصب في مصلحة التجار. (عمر، 2020)

بالإضافة إلى ذلك يمكن للمحلات التجارية الحصول على فوائد المبيعات الائتمانية مع تلقي النقد مقابل قيمة مبيعاتها ويمكن للزوار الأجانب شراء المزيد بمجرد تقديم إثبات البيع إلى أقرب فرع من فروع البنك بحيث يمكن لمتاجر التجزئة الآن فتحه تساعد الاكتشافات ومعاملات البطاقة أيضاً في المحاسبة وزيادة التدفق النقدي تقلل من احتمالية الديون المعدومة على المستهلك كما يستفيد التاجر من إدراج اسمه في قائمة التجار الذين يرحبون بالمعاملات بالبطاقة وتقديم حوافز وهدايا مجانية من جهة إصدار البطاقة لعدد العملاء ليزيد مبيعاته وبالتالي ربحه.

تعتبر البطاقة وسيلة دفع آمنة أو مضمونة فحتى الدفع نقداً له مخاطره خاصة وجود دولارات مزيفة فمثلاً انتشار هذه الظاهرة واستخدام البطاقة يحفظ التجار في مأمن من تراكم الأموال في حوزته والمخاطر التي قد يتعرض لها من سرقة وخسارة واستهلاك قيمة الشراء ففي الدول المتقدمة يتم شراء جميع السلع المعمرة تقريباً ولا توجد وسيلة للشراء نقداً إلا في حالات نادرة فقد وجدنا أن عائلة في تدفع الولايات المتحدة حوالي 5% من دخلها كفوائد على الديون وبالتالي فإن التجار الذين ليس لديهم حلول مبيعات ائتمانية لن يحصلوا على العديد من العملاء. ومن حيث ضمان الدفع من قبل الشركة المصدرة للبطاقة فهو أفضل من التقسيط المباشر من التاجر. (راضية، 2021)

• فائدة البطاقات المصرفية للشركة أو المؤسسة المالية المصدرة للبطاقة (البنك)

هناك العديد من الفوائد التي يمكن جنمها من التعامل مع هذا النظام بما في ذلك "زيادة استخدام الجهة المصدرة لأموالها إلى حد كبير كلما سمحت موارد البنك بذلك أو تأمين جزء كبير من مستخدمي البطاقات المصرفية أصبحوا كعملاء منتظمين للبنك وفي أغلب الأحيان يجبرون المحلات التجارية ومحلات الخدمات على فتح حساب وديعة لدى البنك لتسهيل عملهم وأيضاً في كثير من الأحيان يتوجهون إلى البنك للاستفادة من خدمات البنك الأخرى وكذلك ارتفاع حجم البنك. عودة هذا النظام مقارنة بعصره يعتبر نجاح هذا النظام بحد ذاته أداة جديدة للإعلان عن البنك لأنه يعلن على المداخل عن قبول بطاقات الائتمان على أبواب المتاجر

عادة يتقاضى البنك الافتتاحي رسوم إصدار وتجديد وتغيير البطاقة ونسبة من ثمن السلع أو الخدمات التي يحصل عليها من التاجر وربما من حاملها ويحصل على فرق العملة. يدفع فيها وقد يأخذ أجرة سداد الدين الخارجي ورسم تأخير ومقابل استخدام نظام التحويل الإلكتروني وربما يحصل على عمولة من سداده يحصل أيضا على نسبة من الثمن على سبيل المثال تحويل الأموال إلى بطاقة ائتمان صادرة عن شركة الخدمات الائتمانية "فيزا" ومن الممكن أن نتصور تجمعا للسيولة لديه بسبب تدفق المدفوعات قبل الدفع مثل العمولة الاحتياطية وما إلى ذلك. (نبيل آيت، 2019)

وتشمل الفوائد الأخرى كما أوضح المصرفيون "تخفيف عبء المعاملات النقدية والتحويلات والمدفوعات والمشاكل التي قد تنشأ عن تزيف الأموال وتلفها وضياعها وسوء حسابها فضلا عن تقليل المشاكل الناجمة عن مواجهتها وأشار من سوء استخدام الشيكات والعمل المعتاد الناتج عنها وكذلك حفظ الأموال بين البنوك ونتيجة لذلك الاستفادة منها قدر الإمكان كما يمكن للبنك الحصول على ضمانات تفيد حامل البطاقة وهو ينطبق الآن خاصة إذا كانت هذه الضمانات عبارة عن أموال مخزنة في حساباتهم.

● فائدة البطاقات المصرفية للمنظمة الوسيطة بين المصدر والبنك

وتتلخص هذه المزايا باختصار فيما يلي: الرسوم التي يدفعها البنك مصدر البطاقة للمنظمة الوسيطة الراعية للبطاقة (رسوم الاشتراك) وأيضا الرسوم التي يدفعها البنك للمنظمة مقابل عمليات التسوية والتفويض وغيرها من الخدمات. دعم البطاقة وتطوير نظامها. (Hossain, 2021)

ولذلك فإن الفوائد التي يعود بها استخدام البطاقة المصرفية على طرفي العلاقة، من خلال تحقيق سلسلة من الفوائد للاقتصاد العام وتحقيق الرخاء الاقتصادي من خلال الإقراض من خلال البطاقات المصرفية، كطلب على السلع والخدمات، لصالح للمجتمع وعلى الرغم من توفر السيولة ونتيجة لذلك يزداد الازدهار في السوق.

الفصل الثالث: الطريقة والإجراءات

1.3 تمهيد

يقدم هذا الفصل عرضاً مفصلاً لمنهجية الدراسة التي تم اتباعها في الكشف عن أثر المخاطر السيبرانية في استخدام البطاقات المصرفية في مصرف الراجحي، حيث يوضح منهج الدراسة ومجتمعها وعينتها ووحدة التحليل المستهدفة، ومصادر الحصول على المعلومات، كما يبين هيكل أداة الدراسة المستخدمة في جمع البيانات من مجتمع الدراسة، ونتائج التحقق من ثباتها وصدقها وملائمة البيانات للتحليل الإحصائي، والمعالجات الإحصائية المستخدمة في تحليل البيانات واختبار الفرضيات.

2.3 منهجية الدراسة

يهدف موضوع الدراسة الى بيان أثر المخاطر السيبرانية في استخدام البطاقات المصرفية مصرف الراجحي . ولهذا فقد تم إستخدام المنهج الاستقرائي من خلال إستقراء الدراسات السابقة والبحوث ذات الصلة بالمخاطر السيبرانية واستخدام البطاقات المصرفية، وتم استخدام المنهج الاستنباطي الذي يعتمد على التفكير المنطقي لمحاولة إيجاد ربط منطقي للعلاقة بين المتغيرات. بالإضافة إلى إستخدام المنهج الوصفي التحليلي في إجراء الدراسة الميدانية بهدف إختبار أثر المخاطر السيبرانية في إستخدام البطاقات المصرفية لدى مصرف الراجحي.

3.3 مجتمع وعينة الدراسة

تكون مجتمع الدراسة من جميع العاملين في مصرف الراجحي، ونظراً إلى أن حجم مجتمع الدراسة يعد صغيراً، فقد إتبع الباحث إستراتيجية المسح الشامل لتحديد عينة الدراسة، لتشتمل عينة الدراسة على كافة مصرف الراجحي الممثلة لمجتمع الدراسة إستهدفت الدراسة جميع موظفي الإدارات العليا والوسطى والدنيا في مصرف الراجحي ن، والبالغ عددهم (237) فرداً، والذين تم تحديدهم من خلال

التواصل المباشر مع مصرف الراجحي، وتم توزيع (237) إستبانة إلكترونية، واسترداد (205) إستبانة وبصورة إلكترونية، وبعد تدقيق الاستبانات ومراجعتها تم التأكد من ملاءمة جميع الاستبانات المستردة للتحليل الاحصائي، وأنه لا وجود لفقرات غير مكتملة الإجابة عليها، وبهذا يتوفر (205) إستبانة صالحة للتحليل، ونسبة بلغت (86.5) من إجمالي الإستبانات الموزعة، وهي نسبة مقبولة احصائياً.

4.3 مصادر جمع البيانات والمعلومات

اعتمد الباحث على عين من المصادر للحصول على البيانات والمعلومات اللازمة لإعداد الجانب النظري والعملي للدراسة الحالية وتحقيق أهدافها، وقد تمثلت هذه المصادر في المصادر الثانوية، والمصادر الأولية.

أولاً: المصادر الثانوية

تمثل المصادر الثانوية الأدبيات العلمية والبحثية التي تناولت مواضيع الدراسة ومتغيراتها، حيث تم الإطلاع على العديد من الكتب الاجنبية والعربية، ومواقع الانترنت والمجلات، وذلك لإعداد ومعالجة الجانب النظري للدراسة الحالية والإلمام بكافة المجالات والجوانب التي تناولتها والمرتبطة بمواضيع ومتغيرات الدراسة، ومعرفة أحدث المستجدات وآخر التطورات التي حصلت عليها، والاستفادة من أدواتها، بالإضافة إلى التعرف على القواعد والأسس العلمية التي يُستند عليها في إعداد الرسائل والأطاريح العلمية، مما يساهم في تحقيق الأهداف النظرية للدراسة الحالية.

ثانياً: المصادر الأولية

تُمثل المصادر الأولية الوسائل والأدوات التي اعتمد عليها الباحث في تحقيق أهداف الدراسة ومعالجة الجانب العملي، وقد تمثلت هذه المصادر في الاستبانة التي تم إعدادها بالرجوع إلى المصادر الثانوية، بالإضافة إلى الأخذ بآراء أصحاب الاختصاص والخبرة، حيث تم توزيع الإستبانة على أفراد عينة

الدراسة للحصول على البيانات التي تعبر عن آرائهم وإتجاهاتهم حول القضايا المتعلقة بالمخاطر السيبرانية واستخدام البطاقات المصرفية لدى مصرف الراجحي

وقد تم الأخذ بعين الاعتبار عند إعداد الاستبانة ملائمة الفقرات ودقتها وتسلسلها وترابطها وعدم وجود معيقات أثناء الإجابة عليها والملحق رقم (1) يبين الصورة النهائية لأداة الدراسة.

5.3 أداة الدراسة

تُمثل الاستبانة الأداة الرئيسية التي تم الإعتماد عليها في جمع البيانات من الأفراد والجهات المستهدفة في الدراسة والتي تعبر عن آرائهم حول أبعاد ومتغيرات الدراسة، وذلك لفهم طبيعة وشكل العلاقة بين المتغيرات، على ضوء مشكلة الدراسة وأهدافها.

وتضمنت أداة الدراسة (الإستبانة) مجموعة من الأسئلة والفقرات ذات إختيارات متعددة، موزعة على جزأين، وهما:

♦ الجزء الأول: المتغيرات الديموغرافية

يهدف هذا الجزء من الإستبانة إلى التعرف على السمات والخصائص الوظيفية والشخصية السائدة لدى مصرف الراجحي، وذلك من خلال الإجابة عن (6) أسئلة متمثلة في الجنس، العمر مدة الخدمة المؤهل العلمي، المسمى الوظيفي وعدد الدورات المتخصصة في مجال الأمن السيبراني.

♦ الجزء الثاني: متغيرات الدراسة

يهدف هذا الجزء من الإستبانة إلى التعرف على إتجاهات وآراء أفراد عينة الدراسة حول المخاطر السيبرانية واستخدام البطاقات المصرفية في مصرف الراجحي، وتحديد مدى مستوى الاهتمام بها ودرجة ممارستها من قبل الأطراف المعنية، وذلك من خلال مجموع من الفقرات التي تعبر عنها، والتي تم توزيعها على

محورين يعبر كل محور منها عن المتغيرات الرئيسية الدراسة، ويندرج ضمنها الأبعاد الفرعية المستخدمة لقياسها. وذلك كما يأتي:

المحور الأول : المتغير المستقل،

والمتمثل في المخاطر السيبرانية، وقد اشتمل هذا المحور على (29) فقرة موزعة على (4) أبعاد فرعية، وهي مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، ومخاطر الهجمات السيبرانية، والجدول رقم (1) يوضح بشكل مفصل حدود وعدد عبارات أداة الدراسة التي تعبر عن المحور الأول (المخاطر السيبرانية).

الجدول (1) هيكل أداة الدراسة للمحور الأول (المخاطر السيبرانية)

المتغير	البعد	حدود الفقرات	عدد الفقرات
المخاطر السيبرانية	مخاطر أمن المعلومات	8 – 1	8
	مخاطر تطبيقات الهاتف المحمول	15 – 9	7
	المخاطر التشغيلية	22 – 16	7
	مخاطر الهجمات السيبرانية	29 – 23	7

المحور الثاني: المتغير التابع،

والمتمثل في استخدام البطاقات المصرفية وقد اشتمل هذا المحور على (16) فقرة.

ولقياس اتجاهات أفراد عينة الدراسة حول أبعاد ومتغيرات الدراسة، فقد استخدمت الإستبانة مقياس ليكرت الخماسي (cale)، والذي يتكون من (5) درجات تمثل أوزان الإجابات على الفقرات المخصصة لقياس كل بعد، وكما هو موضح في الجدول رقم (2).

الجدول (2) مقياس ليكرت الخماسي(1)

الاتجاه	مو افق بشدة	مو افق	محايد	غير مو افق	غير مو افق بشدة
الوزن	5	4	3	2	1

ولتحديد مستوى الاهتمام ودرجة ممارسة وتطبيق أبعاد ومتغيرات الدراسة، تم تطبيق الصيغة الآتية:

الحد الأعلى للبديل - الحد الأدنى للبديل

$$1.33 = \frac{1-5}{3} = \frac{\text{الحد الأعلى للبديل} - \text{الحد الأدنى للبديل}}{\text{عدد المستويات}} = \text{طول الفترة}$$

حيث تم تحديد مستوى الأهمية النسبية بالاعتماد على قيمة الوسط الحسابي لأوزان الإجابات على فقرات أداة الدراسة ومتغيرات أنموذجها ، ووفقاً لثلاثة مستويات، وكما هو موضح في الجدول رقم (3-4).

الجدول (3) مستوى الأهمية النسبية لفقرات ومتغيرات الدراسة والأوساط الحسابية التي تقابلها

مستوى الأهمية النسبية	منخفض	متوسط	مرتفع
الوسط الحسابي	1 - أقل من 2.33	2.33 – أقل من 3.66	3.66 - 5.00

6.3 اختبار صلاحية أداة الدراسة

يهدف اختبار صلاحية أداة الدراسة إلى التحقق من قدرة الإستبانة على تحقيق الأهداف التي صممت من أجلها، وإمكانية استخدامها في جمع البيانات المتعلقة بموضوع الدراسة، من خلال إجراء عدة اختبارات تمثلت بما يأتي:

1.6.3 اختبار صدق المحتوى الظاهري (Content Validity Test)

يهدف اختبار صدق المحتوى إلى التحقق من صحة الصياغة اللغوية لأداة الدراسة، ووضوح معانيها، ومدى ترابط فقراتها وموضوعيتها وإنتمائها للأبعاد التي تعبر عنها، بما يضمن تحقيق أهداف

الدراسة ويعتبر المحكمون من أصحاب الاختصاص والخبرة الأقدر والأجدر في الحكم على صدق محتوى أداة الدراسة، ولهذا فقد قام الباحث بعرض الاستبانة على مجموعة من أعضاء هيئة التدريس المتخصصين في مجالات الدراسة في الجامعات السعودية الحكومية والخاصة، والبالغ عددهم (8) محكمين والمدرجة أسماؤهم في الملحق رقم (2).

وقد تم الأخذ بعين الاعتبار ملاحظات واقتراحات المحكمين، وإجراء التعديلات المشار إليها من قبلهم من حيث الإضافة أو الحذف أو إعادة صياغة الفقرات لتظهر الاستبانة بصورتها النهائية، وكما هو مدرج في الملحق رقم (1). وبناءً على ذلك، فإن أداة الدراسة تعتبر صالحة لقياس ما صممت له.

2.6.3 اختبار ثبات أداة الدراسة

يهدف اختبار ثبات أداة الدراسة إلى التحقق من مدى التماسك والترابط بين الفقرات، بتطبيق اختبار معامل الاتساق الداخلي كرونباخ ألفا (Cronbach Alpha Coefficient). حيث يشير هذا المقياس إلى اتصاف أداة الدراسة بدرجات عالية من الثبات إذا بلغت قيمة معامل كرونباخ ألفا 70% فما فوق، وكلما زادت القيمة عن ذلك دلّ على ارتفاع ثبات واتساق أداة الدراسة (1). والجدول الآتي يبين نتائج اختبار ثبات أداة الدراسة:

الجدول (4) نتائج اختبار ثبات أداة الدراسة

المتغير	رقم البعد	البعد	قيمة ألفا
المتغير المستقل	1	مخاطر أمن المعلومات	0.757
	2	مخاطر تطبيقات الهاتف المحمول	0.859
	3	المخاطر التشغيلية	0.910
	4	مخاطر الهجمات السيبرانية	0.852
المتغير التابع		استخدام البطاقات المصرفية	0.852
		أداة الدراسة	0.944

يبين الجدول (4) أن قيم معامل كرونباخ ألفا تراوحت بين (0.757 – 0.910)، في حين بلغت قيمة معامل كرونباخ ألفا لأداة الدراسة ككل، (0.944)، وكلاهما أعلى من القيمة (0.70)، وهذا يشير إلى تمتع أداة الدراسة بدرجة عالية من الثبات، وبقدرتها على تحقيق أهداف وغايات الدراسة، وبالتالي إمكانية الإعتماد عليها لإجراء التحليل الإحصائي.

7.3 اختبار ملاءمة نموذج الدراسة للأساليب الإحصائية المستخدمة

يهدف اختبار ملاءمة نموذج الدراسة للأساليب الإحصائية إلى التحقق من ملاءمة البيانات المستخدمة في إجراء الاختبارات الإحصائية وتحليل الانحدار وللتحقق من ذلك تم إجراء اختبار الارتباط الخطي المتعدد Multicollinearity إذ تمثل استقلالية المتغيرات شرطاً أساسياً لتطبيق النموذج الخطي العام (General Linear Model (GM)، وتتحدد استقلالية المتغيرات بخلو البيانات من مشكلة الارتباط الخطي المتعدد، حيث تشير هذه المشكلة إلى وجود ارتباط خطي عالي (تام أو شبه تام بين متغيرين أو أكثر من المتغيرات المستقلة، مما يؤثر سلباً على دقة القياسات، إذ يعمل على تضخيم قيمة معامل التحديد R^2 بحيث تتجاوز قيمتها القيمة الفعلية (1).

وللتحقق من هذه المشكلة تم تطبيق طريقتين، تمثلت الأولى في حساب معامل الارتباط بيرسون، والثانية في حساب معامل تضخم والتباين المسموح به عند كل بعد من أبعاد المتغير المستقل.

يشير معامل الارتباط بيرسون إلى خلو البيانات من مشكلة الارتباط الخطي المتعدد إذا لم تتجاوز قيمة المعامل بين متغيرين أو أكثر القيمة (0.80) () ، وفيما يأتي نتائج معامل الارتباط بيرسون به لأبعاد المتغير المستقل.

الجدول (5) مصفوفة الارتباط لقيم معامل الارتباط بيرسون

الابعاد	مخاطر أمن المعلومات	مخاطر تطبيقات الهاتف المحمول	المخاطر التشغيلية	مخاطر الهجمات السيبرانية
مخاطر أمن المعلومات	1.000			
مخاطر تطبيقات الهاتف المحمول	0.558**	1.000		
المخاطر التشغيلية	**0.495	0.715**	1.000**	
مخاطر الهجمات السيبرانية	**0.507	0.683**	0.767**	1.000**

(**) عند مستوى دلالة 0.01

يوضح الجدول (5) أن أعلى قيمة لمعامل الارتباط بلغت (0.767)، وهي بين المتغيرين المخاطر (التشغيلية) و (مخاطر الهجمات السيبرانية)، وهذا يدل على عدم وجود مشكلة الارتباط الخطي المتعدد بين المتغيرات، حيث لم تظهر أي من القيم بقيمة أكبر من (0.80).

وللتحقق من النتيجة السابقة، تم إيجاد معامل تضخم التباين (Variance Inflation Factor (VIE))، حيث يشير هذا المعامل إلى خلو البيانات من مشكلة الارتباط الخطي المتعدد إذا تراوحت قيم المعامل بين (1.0 – 10.0)، وتراوحت قيم معامل التباين المسموح به (Tolerance) بين

(0.1 - 1.0) وفيما يأتي نتائج اختبار معامل تضخم التباين والتباين المسموح به لأبعاد المتغير

المستقل:

الجدول (6) معامل تضخم التباين والتباين المسموح به

الابعاد	معامل تضخم التباين VIF	التباين المسموح به Tolerance
مخاطر أمن المعلومات	1.524	0.656
مخاطر تطبيقات الهاتف المحمول	2.453	0.408
المخاطر التشغيلية	2.927	0.342
مخاطر الهجمات السيبرانية	2.723	0.367

يُبين الجدول (6) خلو البيانات من مشكلة الارتباط الخطي المتعدد، حيث تراوحت قيم معامل تضخم التباين (IF) ما بين (1.524 - 2.927) وهي بين (1.0 - 10.0)، وتراوحت قيم التباين المسموح به (Tolerance) بين (0.342 - 0.656) وهي بين (0.1 - 1.0).

8.3 الأساليب الإحصائية المستخدمة في معالجة البيانات وتحليلها واختبار

الفرضيات :

تم استخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية الإصدار 20 (Statistical Package 20 for Social Sciences- SPSS v)، وذلك في تحليل بيانات الدراسة واختبار الفرضيات، حيث تم استخدام الأساليب الإحصائية الآتية:

1.8.3 أساليب الإحصاء الوصفي (Descriptive Statistic Methods)

تم استخدام هذه الأساليب من أجل وصف البيانات الديموغرافية لأفراد عينة الدراسة، وتحليل إجابات أفراد العينة على فقراتها المختلفة، ووصف أبعاد ومتغيرات أنموذج الدراسة. وقد تمثلت هذه الأساليب فيما يأتي:

1- التكرار والنسبة المئوية لوصف البيانات الديموغرافية الخاصة بأفراد عينة الدراسة من المستجيبين.

2- الوسط الحسابي والانحراف المعياري لتحليل إجابات أفراد عينة الدراسة، ووصف متغيرات أنموذج الدراسة وأبعادها الفرعية.

2.8.3 أساليب الاحصاء الاستدلالي (Inferential Statistics Methods)

تم استخدام هذه الأساليب للتحقق من ثبات أداة الدراسة وملاءمة نموذج الدراسة، بالإضافة إلى اختبار الفرضيات. وقد تمثلت هذه الأساليب فيما يأتي:

1) الأساليب المستخدمة للتحقق من ثبات أداة الدراسة وملاءمة نموذج الدراسة

- تم التحقق من ثبات أداة الدراسة من خلال استخدام اختبار الإتساق الداخلي (كرونباخ ألفا).
- تم التحقق من ملاءمة نموذج الدراسة من خلال اختبار الارتباط الخطي المتعدد (Multicollinearity) باستخدام معامل الارتباط بيرسون ومعامل تضخم التباين والتباين المسموح به، للتحقق من إستقلالية أبعاد المتغير المستقل.

2) الأساليب المستخدمة في اختبار الفرضيات

تم اختبار فرضيات الدراسة باستخدام الاختبارات الآتية:

- تحليل الإنحدار الخطي المتعدد (Multiple Linear Regression Analysis) لاختبار أثر المخاطر السيرانية بأبعادها مجتمعة في استخدام البطاقات المصرفية لدى مصرف الراجحي
- تحليل الإنحدار الخطي البسيط (Simple Linear Regression Analysis) لاختبار أثر المخاطر السيرانية بأبعادها منفردة في استخدام البطاقات المصرفية لدى مصرف الراجحي

الفصل الرابع : تحليل البيانات واختبار الفرضيات

1.4 نتائج تحليل البيانات

يهدف هذا الفصل إلى عرض نتائج تحليل البيانات، حيث يقدم وصفاً مفصلاً للمتغيرات الديموغرافية المتعلقة بأفراد عينة الدراسة من المستجيبين، وتحليلاً لإجاباتهم على فقرات أداة الدراسة، ووصفاً لمتغيرات أنموذج الدراسة وأبعاده الفرعية.

2.4 وصف البيانات الديموغرافية

يبين هذا الجزء من الدراسة عرضاً مفصلاً للبيانات الديموغرافية الخاصة بأفراد عينة الدراسة. وقد شملت هذه المتغيرات على العمر، الجنس، المؤهل العلمي، الخبرة والمستوى الإداري. ولتحقيق ذلك تم استخدام أساليب الإحصاء الوصفي والمتمثلة في التكرارات والنسب المئوية، وفيما يأتي وصفاً لخصائص أفراد عينة الدراسة تبعاً للبيانات الديموغرافية.

الفرع الأول: وصف متغير الجنس

الجدول (7): وصف أفراد عينة الدراسة حسب متغير الجنس

المتغير	الفئة	التكرار	النسبة المئوية
الجنس	ذكر	168	82.0
	أنثى	37	18.0
	المجموع	205	100.0

يوضح الجدول (7) أن غالبية أفراد عينة الدراسة هم من الذكور، حيث بلغت النسبة (82.0%)، في حين بلغت نسبة الاناث (18.0%)، وهذا قد يرتبط بطبيعة العاملين في الإدارات العليا في البنوك الإسلامية، حيث يزداد عدد الذكور فيها نظراً لسبق الرجل للمرأة في سوق العمل.

الفرع الثاني: وصف متغير العمر

الجدول (8) وصف أفراد عينة الدراسة حسب متغير العمر

المتغير	الفئة	التكرار	النسبة المئوية
العمر	أقل من 30 سنة	51	24.9
	من 30- أقل من 40 سنة	103	50.2
	من 40- أقل من 50 سنة	41	20.0
	50 سنة فأكثر	10	4.9
	المجموع	205	100.0

يوضح الجدول (8) أن أفراد العينة قد توزعوا على جميع الفئات العمرية، وقد تبين أن الفئة العمرية من 30 إلى أقل من 40 سنة هي الفئة الكبرى، والتي بلغت (50.2%)، وهذا يشير إلى أن مصرف الراجحي تهدف إلى إستقطاب فئة الشباب المؤهلين لتولي المناصب الإدارية.

الفرع الثالث: وصف متغير المؤهل العلمي

الجدول (9) وصف أفراد عينة الدراسة حسب متغير المؤهل العلمي

المتغير	الفئة	التكرار	النسبة المئوية
المؤهل العلمي	دبلوم	9	4.4
	بكالوريوس	162	79.0
	دراسات عليا	34	16.6
	المجموع	205	100.0

يوضح الجدول (9) أنه غالبية أفراد عينة الدراسة حاصلين على المؤهل العلمي (بكالوريوس)، حيث بلغ عددهم (162) فرداً، وشكلوا ما نسبته (79.0%) من إجمالي أفراد عينة الدراسة، ويرى الباحث

أن إرتفاع هذه النسبة يتوافق مع الاتجاه العام في القطاعين العام والخاص لإستقطاب حملة البكالوريوس كحد أدنى.

الفرع الرابع: وصف متغيرالمسمى الوظيفي

الجدول (10) وصف أفراد عينة الدراسة حسب متغيرالمسمى الوظيفي

المتغير	الفئة	التكرار	النسبة المئوية
المسمى الوظيفي	موظف	84	41.0
	رئيس قسم	24	11.7
	مساعد مدير	31	15.1
	مدير	66	32.2
	المجموع	205	100.0

يوضح الجدول (10) أن أفراد عينة الدراسة قد توزعوا على جميع المستويات الوظيفية، كما نلاحظ وجود زيادة لفئة (مدير) والتي بلغت (32.2%) ، ثم فئة (موظف) والتي بلغت (41.0%) تلاها فئة (مساعد مدير) والتي بلغت (15.1%) ، ثم جاء أخيراً، فئة (رئيس قسم) والبالغة (11.7%).

الفرع الخامس: وصف مدة الخدمة

الجدول (11) وصف أفراد عينة الدراسة حسب متغيرمدة الخدمة

المتغير	الفئة	التكرار	النسبة المئوية
مدة الخدمة	أقل من 5 سنوات	36	17.6
	من 5 سنوات إلى أقل من 10 سنوات	61	29.8
	من 10 سنوات إلى أقل من 15 سنة	47	22.9
	15 سنة فأكثر	61	29.8

100.0	205	المجموع	
-------	-----	---------	--

يوضح الجدول (11) أن افراد عينة الدراسة يتوزعون على جميع فئات الخبرة، كما تبين أن النسبة الصغرى ظهرت عند الفئة أقل من 5 سنوات، والتي بلغت (17.6%)، وهذا يشير إلى أن العاملين في الإدارات الرئيسة للبنوك الإسلامية يمتلكون الخبرات العالية في العمل المصرفي الإسلامي، وأن مدة خدمتهم طويلة وكافية في هذا المجال.

الفرع السادس: عدد الدورات المتخصصة في مجال الأمن السيبراني

الجدول (12): وصف أفراد عينة الدراسة حسب عدد الدورات المتخصصة في مجال الأمن

المتغير	الفئة	التكرار	النسبة المئوية
عدد الدورات المتخصصة في مجال الأمن السيبراني	دورة واحدة فقط	54	26.3
	دورتان	39	19.0
	ثلاث دورات فأكثر	52	25.4
	لا يوجد	60	29.3
	المجموع	205	100.0

يوضح الجدول (12) أن جميع أفراد عينة الدراسة حاصلين على دورات متخصصة في مجال الأمن السيبراني، كما أنهم يتفاوتون في عدد هذه الدورات، فقد كان ما نسبته (26.3%) منهم حاصلين على دورة واحدة فقط، و ما نسبته (19.0%) حاصلين على (دورتين)، بالإضافة إلى أن ما نسبته (25.4%) حاصلين على ثلاث دورات. ومن جهة أخرى فقط تبين أن ما نسبته (29.3%) منهم غير حاصلين على أي دورة وهذه النسب تشير إلى اهتمام مصرف الراجحي على توفير الكفاءة والمعرفة اللازمة للعاملين فيما يتعلق بالأمن السيبراني ومخاطره.

3.4 وصف متغيرات الدراسة

يهدف هذا الجزء من الدراسة إلى وصف أبعاد ومتغيرات أنموذج الدراسة، وذلك من خلال تحليل إجابات أفراد عينة الدراسة على الفقرات التي تقيس هذه الأبعاد والمتغيرات. ولتحقيق ذلك تم استخدام أساليب الإحصاء الوصفي والمتمثلة في المتوسطات الحسابية والانحرافات المعيارية، بالإضافة إلى الرتبة والأهمية النسبية.

الفرع الأول: وصف أبعاد متغير المخاطر السيبرانية

يمثل متغير المخاطر السيبرانية المتغير المستقل في الدراسة، وقد تم قياس هذا المتغير من خلال (4) أبعاد، وهي مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، ومخاطر الهجمات السيبرانية. وفيما يأتي تحليلاً لإجابات أفراد عينة الدراسة على الفقرات التي تقيس هذه الأبعاد، ووصفاً لها وللمتغير المستقل ككل.

البعد الأول: مخاطر أمن المعلومات

يقدم هذا الجدول عرضاً مفصلاً لتحليل آراء وإتجاهات أفراد عينة الدراسة على الفقرات التي تقيس بعد مخاطر أمن المعلومات ومدى أهميتها من وجهة نظرهم، وذلك من خلال إيجاد المتوسطات الحسابية والانحرافات المعيارية والرتبة وتحديد مستوى الأهمية النسبية للفقرات، وقد ظهرت النتائج كما يأتي:

الجدول (13) وصف بعد مخاطر أمن المعلومات

الرقم	الفقرة	الوسط الحسابي	الانحراف المعياري	الرتبة	الأهمية النسبية
1	تلتزم إدارة البنك بتعليمات امن المعلومات الصادرة عن البنك المركزي السعودي	0.450	0.450	1	مرتفعة

2	تدرك إدارة البنك الأهمية القصوى لأمن بيانات العملاء والبنك ووضعها ضمن مستويات وظيفية متعددة	4.74	0.481	2	مرتفعة
3	تعمل إدارة البنك على بيان المسؤوليات المتبعة في سياسة أمن المعلومات والمتمثلة في (السرية، النزاهة، التوافر)	4.66	0.523	3	مرتفعة
4	تقوم إدارة البنك بتحديد الجهة أو الموظفين المخول لهم بالاطلاع أو استخدام البيانات والمعلومات	4.56	0.659	4	مرتفعة
5	تعرض بعض عملاء البنك إلى استيلاء على بياناتهم الشخصية	3.20	1.31	8	متوسطة
6	تقدم إدارة البنك تقارير منتظمة تشمل الحوادث التقنية التي وقعت على أصوله من المعلومات مع النتائج والتوصيات	4.13	0.850	7	مرتفعة
7	تتبنى إدارة البنك سياسات إدارية وقانونية للتعامل مع الحالات التي يكون موظف البنك طرفاً في وقوع حادثة تخص أمن المعلومات للبنك أو العملاء	4.40	0.677	5	مرتفعة
8	يتم تخزين بيانات العملاء في أكثر من جهة وبشكل متزامن	4.27	0.836	6	مرتفعة
	مخاطر أمن المعلومات	4.334	0.417		مرتفعة

يُبين الجدول (13) إرتفاع الأهمية النسبية لبعء مخاطر أمن المعلومات في مصرف

الراجحي، حيث بلغ الوسط الحسابي العام (4.334) والانحراف المعياري (0.417). وقد جاءت

الفقرة رقم (1) والتي تنص على تلتزم إدارة البنك بتعليمات امن المعلومات الصادرة عن البنك المركزي السعودي " في المرتبة الأولى بوسط حسابي (4.74) وبأهمية نسبية مرتفعة، في حين جاءت الفقرة رقم (5) والتي تنص على "تعرض بعض عملاء البنك إلى إستيلاء على بياناتهم الشخصية" في المرتبة الأخيرة بوسط حسابي (3.20) وبأهمية نسبية متوسطة.

البعد الثاني: مخاطر تطبيقات الهاتف المحمول

يقدم هذا الجدول عرضاً مفصلاً لتحليل آراء واتجاهات أفراد عينة الدراسة على الفقرات التي تقيس بعد مخاطر تطبيقات الهاتف المحمول، ومدى أهميتها من وجهة نظرهم، وذلك من خلال إيجاد المتوسطات الحسابية والانحرافات المعيارية والرتبة وتحديد مستوى الأهمية النسبية للفقرات، وقد ظهرت النتائج كما يأتي:

الجدول (14) وصف بعد مخاطر تطبيقات الهاتف المحمول

الرقم	الفقرة	الوسط الحسابي	الانحراف المعياري	الرتبة	الأهمية النسبية
9	تتولى إدارة البنك تطبيق برامج الأمن السيبراني وتحديثها وبيان توافقها مع مخاطر تطبيقات الهاتف المحمول لدى العملاء	4.41	0.699	1	مرتفعة
10	تقوم إدارة البنك بتأمين الحماية الكاملة على تطبيقات الهاتف المحمول ضد أي نوع من التهديدات السيبرانية والإختراقات الخارجية	4.37	0.685	2	مرتفعة
11	تُقاس ميزة وكفاءة تطبيقات الهاتف المحمول الخاصة بالبنك بمستوى الحماية والأمان أكثر من ميزة الخدمات المستفادة من خلالها	4.15	0.753	6	مرتفعة

12	تقوم إدارة البنك بتقييم قدرة وكفاءة برامج الأمان والحماية المطبقة في تطبيقات الهاتف المحمول الخاصة بالبنك	4.32	0.715	5	مرتفعة
13	تحدد إدارة البنك صلاحيات العملاء في استخدام الخدمات الإلكترونية عبر تطبيقات الهاتف المحمول الخاصة بالبنك	4.35	0.637	4	مرتفعة
14	يحدد البنك خدمات معيارية ثابتة للتطبيقات الهاتف المحمول الخاصة بالبنك	4.36	0.622	3	مرتفعة
15	يدرك عملاء البنك المخاطر السيبرانية في حال استخدام التطبيقات الهاتفية	3.80	1.007	7	مرتفعة
		4.251	0.545		مرتفعة

يُبين الجدول (14) إرتفاع الأهمية النسبية لبعء مخاطر تطبيقات الهاتف المحمول) في مصرف الراجحي، حيث بلغ الوسط الحسابي العام (4.251) والانحراف المعياري (0.545). وقد جاءت الفقرة رقم (9) والتي تنص على "تتولى إدارة البنك تطبيق برامج الأمن السيبراني وتحديثها وبيان توافقها مع مخاطر تطبيقات الهاتف المحمول لدى العملاء" في المرتبة الأولى بوسط حسابي (4.41) وبأهمية نسبية مرتفعة. في حين جاءت الفقرة رقم (15) والتي تنص على "يدرك عملاء البنك المخاطر السيبرانية في حال إستخدام التطبيقات الهاتفية" في المرتبة الأخيرة بوسط حسابي (3.80) وبأهمية نسبية مرتفعة.

البعد الثالث: المخاطر التشغيلية

يقدم هذا الجدول عرضاً مفصلاً لتحليل آراء واتجاهات أفراد عينة الدراسة على الفقرات التي تقيس بعدد المخاطر التشغيلية، ومدى أهميتها من وجهة نظرهم، وذلك من خلال إيجاد المتوسطات الحسابية والانحرافات المعيارية والرتبة وتحديد مستوى الأهمية النسبية للفقرات، وقد ظهرت النتائج كما يأتي:

الجدول (15) وصف بعد المخاطر التشغيلية

الرقم	الفقرة	الوسط الحسابي	الانحراف المعياري	الرتبه	الأهمية النبيه
16	يملك البنك البرمجيات والمعدات اللازمة التي لديها القدرة على منع أي اختراق سربراني يمس عمليات التشغيل	4.37	0.649	2	مرتفعة
17	التطبيق البنكي الخاص بالعملاء سواء على الهاتف او الحاسوب لديها القدرة على مواجهة الاختراق السبراني	4.10	0.813	7	مرتفعة
18	يقوم البنك بتدريب الموظفين وتوعيتهم بالمخاطر التشغيلية المحتملة	4.34	0.735	3	مرتفعة
19	برامج الحماية المطبقة في البنك تحدد أهم التهديدات الإلكترونية المحتملة داخل البنك وخارجه	4.32	0.682	4	مرتفعة
20	يتم تحديث التطبيقات الهاتفية والحاسوبية والآلية الخاصة بالعملاء والبنك التي تهدف لتجنب الثغرات التطبيقات والعمليات التشغيلية	4.40	0.697	1	مرتفعة
21	العمليات التشغيلية في البنك محمية من المخاطر التقنية	4.24	0.753	5	مرتفعة
22	البنك لتبني خدمات التكنولوجيا المالية وشركاء يسعى خارجين لإتمام عملياته التشغيلية	4.23	0.805	6	مرتفعة

مرتفعة		0.582	4.287	المخاطر التشغيلية	
--------	--	-------	-------	-------------------	--

يُبين الجدول (15) إرتفاع الأهمية النسبية لبعء المخاطر التشغيلية) في مصرف الراجحي، حيث بلغ الوسط الحسابي العام (4.287) والانحراف المعياري (0.582). وقد جاءت الفقرة رقم (20) والتي تنص على "يتم تحديث التطبيقات الهاتفية والحاسوبية والآلية الخاصة بالعملاء والبنك التي تهدف لتجنب الثغرات في التطبيقات والعمليات التشغيلية" في المرتبة الأولى بوسط حسابي (4.40) وبأهمية نسبية مرتفعة، في حين جاءت الفقرة رقم (17) والتي تنص على "التطبيق البنكي الخاص بالعملاء سواء على الهاتف أو الحاسوب لديها القدرة على مواجهة الإختراق "السيراني في المرتبة الأخيرة بوسط حسابي (4.10) وبأهمية نسبية مرتفعة.

البعد الرابع: مخاطر الهجمات السيبرانية

يقدم هذا الجدول عرضاً مفصلاً لتحليل آراء وإتجاهات أفراد عينة الدراسة على الفقرات التي تقيس بعدد مخاطر الهجمات السيبرانية، ومدى أهميتها من وجهة نظرهم، وذلك من خلال إيجاد المتوسطات الحسابية والانحرافات المعيارية والرتبة وتحديد مستوى الأهمية النسبية للفقرات، وقد ظهرت النتائج كما يأتي:

الجدول (16) وصف بعدد مخاطر الهجمات السيبرانية

الرقم	الفقرة	الوسط الحسابي	الانحراف المعياري	الرتبة	الأهمية النسبية
23	في حال وقوع اعتداء أو اختراق إلكتروني، فإن البنك يتبع استراتيجية عمل للتعافي من خلالها من الأضرار التي نتجت حين وقوعه	4.32	0.652	2	مرتفعة
24	إذا وقع اعتداء إلكتروني على البنك يقوم البنك جهات مع مختصة وموثوقة للاستجابة بسرعة كبيرة للتصدي للاعتداء الإلكتروني	4.12	0.771	5	مرتفعة

مرتفعة	1	0.653	4.36	إذا حدث أي اعتداء إلكتروني يتابع البنك الهجوم بعمل تحقيق لبيان مدى الضرر وطبيعته	25
مرتفعة	3	0.739	4.20	تتخذ إدارة البنك سياسة السرية والتكتم إزاء الإعتداءات الإلكترونية التي تحدث على البنك	26
مرتفعة	7	0.997	3.73	ينشر البنك تقارير مفصلة بخصوص الإعتداءات الإلكترونية	27
مرتفعة	4	0.827	4.13	تتبنى إدارة البنك اتفاقيات تعاون مشترك مع شركات عالمية مزودة لخدمات وبرامج وأجهزة حماية إلكترونية ضد الإعتداءات الإلكترونية	28
مرتفعة	5	0.889	4.12	تعيّن إدارة البنك مديرا للأمن السيبراني ويتمتع بصلاحيات ونفوذ للتصدي واتخاذ القرارات عند حدوث اعتداءات إلكترونية	29
مرتفعة		0.581	4.139	مخاطر الهجمات السيبرانية	

يُبين الجدول (16) ارتفاع الأهمية النسبية لبعد مخاطر الهجمات السيبرانية في مصرف الراجحي، حيث بلغ الوسط الحسابي العام (4.139) والانحراف المعياري (0.581). وقد جاءت الفقرة رقم (25) والتي تنص على "إذا حدث أي اعتداء إلكتروني يتابع البنك الهجوم بعمل تحقيق لبيان مدى الضرر وطبيعته في المرتبة الأولى بوسط حسابي (4.36) وبأهمية نسبية مرتفعة. في حين جاءت الفقرة رقم (27) والتي تنص على " ينشر البنك تقارير مفصلة بخصوص الاعتداءات الإلكترونية" في المرتبة الأخيرة بوسط حسابي (3.73) وبأهمية نسبية مرتفعة.

وصف متغير المخاطر السيبرانية

يعرض الجدول الآتي وصفاً لمتغير المخاطر السيبرانية، وتحديد مستوى أهميته في مصرف الراجحي، وذلك من خلال إيجاد المتوسطات الحسابية والانحرافات المعيارية والرتبة وتحديد مستوى الأهمية النسبية للتطبيقات وللمتغير ككل، وقد ظهرت النتائج كما يأتي:

الجدول (17): وصف متغير المخاطر السيبرانية

الرقم	الفقرة	الوسط الحسابي	الانحراف المعياري	الرتبة	الأهمية النسبية
1	مخاطر أمن المعلومات	4.443	0.417	1	مرتفعة
2	مخاطر تطبيقات الهاتف المحمول	4.251	0.545	3	مرتفعة
3	المخاطر التشغيلية	4.287	0.582	2	مرتفعة
4	مخاطر الهجمات السيبرانية	4.139	0.581	4	مرتفعة
	المخاطر السيبرانية	4.253	0.454		مرتفعة

يُبين الجدول (17) إرتفاع مستوى الأهمية النسبية لمتغير المخاطر السيبرانية في مصرف الراجحي، حيث بلغ الوسط الحسابي العام (4.253) والانحراف المعياري (0.454). وقد جاء بعد مخاطر أمن المعلومات في المرتبة الأولى بوسط حسابي (4.334) وانحراف معياري (0.417) وبأهمية نسبية مرتفعة، في حين جاء بعد مخاطر الهجمات السيبرانية في المرتبة الأخيرة بوسط حسابي (4.139) وانحراف معياري (0.581) وبأهمية نسبية مرتفعة.

الفرع الثاني: وصف متغير استخدام البطاقات المصرفية

يمثل متغير استخدام البطاقات المصرفية المتغير التابع في الدراسة، والجدول الآتي يقدم عرضاً مفصلاً لتحليل آراء واتجاهات أفراد عينة الدراسة على الفقرات التي تقيس هذا المتغير، ومدى الإهتمام به في مصرف الراجحي، وذلك من خلال إيجاد المتوسطات الحسابية والانحرافات المعيارية والرتبة وتحديد مستوى الأهمية النسبية للفقرات، وقد ظهرت النتائج كما يأتي:

الجدول (18) وصف متغير استخدام البطاقات المصرفية

الرقم	الفقرة	الوسط الحسابي	الانحراف المعياري	الرتبه	الأهمية النبيه
30	يوفر البنك ضمانات أو تعويضات ضد اي خسائر تحصل للعملاء نتيجة للحوادث الإلكترونية الواقعة على البطاقات المصرفية	3.91	1.044	13	مرتفعة
31	الانتشار الواسع لأجهزة الصراف الآلي التابع للبنك يزيد استخدام البطاقات المصرفية من مستوى الأمن والثقة في بالنسبة للعميل	4.21	0.775	4	مرتفعة
32	تقدم عملاء بشكاوى واستفسارات بخصوص حوا وادث أو أحداث مريبة وقعت على بطاقتهم المصرفية في الأونة الأخيرة	3.89	0.954	14	مرتفعة
33	تنوع البطاقات المصرفية واستعمالها يقلل من حجم الحوادث الواقع عليها	3.92	0.931	12	مرتفعة
34	يقوم البنك دائما بتطوير آليات زيادة حماية استخدام البطاقات المصرفية	4.40	0.661	1	مرتفعة
35	إن حدوث خلل في شبكة الإنترنت أو تعطل النظام يزيد من عدد حوادث البطاقات المصرفية	3.96	0.917	10	مرتفعة
36	تتبنى إدارة البنك خطة طوارئ للتعامل مع أي حدث تقني قد يصيب خدمات البطاقات المصرفية	4.28	0.738	3	مرتفعة

مرتفعة	9	0.939	4.00	يتردد بعض العملاء من استخراج بطاقات مصرفية بسبب القلق أو التخوف من وقوع حوادث تقنية أو إلكترونية عليها	37
مرتفعة	15	1.038	3.78	يطرح العملاء أفكاراً ومتطلبات لزيادة مستوى الأمان والحماية لبطاقاتهم المصرفية	38
مرتفعة	7	0.968	4.07	يفعل البنك أسلوب الاتصال الفوري مع العملاء (من خلال مركز اتصال العملاء عند تلقي إشارة مشتريات إلكترونية بمبلغ يفوق ال حسب سياسات البنك) دينار مثلاً	39
مرتفعة	6	1.008	4.09	يطبق البنك سياسة الإيقاف الفوري للبطاقة المصرفية اذا وقع عليها استخدام خارج الوطن لحين التحقق من العميل	40
مرتفعة	11	0.964	3.95	استلام العميل للبطاقة المصرفية من خلال شركة نقل يُفقد العميل فرصة التدريب والارشاد من قبل موظف البنك للتعامل الآمن مع البطاقات المصرفية	41
مرتفعة	16	1.077	3.77	إن توجهات وسياسات البنك في حث العملاء على استخدام البطاقات المصرفية لخفض عدد المراجعين يزيد من احتمال وقوع حوادث إلكترونية على البطاقات المصرفية	42
مرتفعة	8	0.934	4.03	إن إضافة خدمات وميزات في استخدام البطاقات المصرفية كربطها بالهاتف المحمول أو إتمام عملية الدفع بمجرد	43

				اقترباها من جهاز الخصم المباشر يزيد من خطر الحوادث الإلكترونية عليها	
مرتفعة	4	0.686	4.21	يؤخذ بعين الاعتبار وضمن سياسات إصدار البطاقات المصرفية الحوادث المحتملة	44
مرتفعة	2	0.698	4.30	يمكن ويشجع البنك العملاء من استخدام البطاقات المصرفية للدفع مقابل خصم من خلال نقاط البيع	45
مرتفعة		0.548	4.049	استخدام البطاقات المصرفية	

يُبين الجدول (18) ارتفاع الأهمية النسبية لمتغير استخدام البطاقات المصرفية) في مصرف الراجحي، حيث بلغ الوسط الحسابي العام (4.049) والانحراف المعياري (0.548). وقد جاءت الفقرة رقم (34) والتي تنص على "يقوم البنك دائما بتطوير آليات زيادة حماية استخدام البطاقات المصرفية" في المرتبة الأولى بوسط حسابي (4.40) وبأهمية نسبية مرتفعة، في حين جاءت الفقرة رقم (42) والتي تنص على "إن توجهات وسياسات البنك في حث العملاء على استخدام البطاقات المصرفية لخفض عدد المراجعين يزيد من احتمال وقوع حوادث الإلكترونية على البطاقات المصرفية" في المرتبة الأخيرة بوسط حسابي (3.77) وبأهمية نسبية مرتفعة.

4.4 اختبار فرضيات الدراسة

يعرض هذا الجزء من الدراسة نتائج اختبار فرضيات الدراسة، والتي تم التوصل إليها من خلال تطبيق أساليب الإحصاء الاستدلالي المناسبة، حيث تم إخضاع الفرضيات الرئيسة لتحليل الانحدار الخطي المتعدد Multiple Linear Regression في حين تم إخضاع الفرضيات المتفرعة عنها لتحليل الانحدار الخطي البسيط Simple Linear Regression. وفيما يأتي نتائج اختبار فرضيات الدراسة.

نتائج اختبار الفرضية الرئيسية

تهدف الفرضية الرئيسية الأولى التعرف على أثر المخاطر السيبرانية بأبعادها مجتمعه في استخدام البطاقات المصرفية مصرف الراجحي حيث تنص هذه الفرضية على أنه: "لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (as0.05) لمخاطر الأمن السيبراني بأبعاده الأربعة مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية في مصرف الراجحي"

ولإختبار هذه الفرضية كم استخدام تحليل الانحدار المتعدد Multiple Linear Regression ، وظهرت النتائج كما يأتي:

الجدول (19) ملخص النموذج وتحليل تباين الانحدار للفرضية الرئيسية

تحليل التباين ANOVA			ملخص النموذج				
Sig F*	قيمة F المحسوبة	درجات الحرية	الخطأ المعياري للنموذج	Adjusted R ² معامل التحديد المعدل	R ² معامل لتحديد	R معامل الارتباط	المتغير التابع
0.000	40.865	4	0.411	0.439	0.450	0.671	استخدام البطاقات المصرفية

* التأثير دال إحصائياً عند مستوى الدلالة (050.05)

يبين الجدول (19) وجود علاقة ارتباط بين المخاطر السيبرانية واستخدام البطاقات المصرفية، حيث بلغت قيمة معامل الارتباط (R=0.671)، وبلغت قيمة معامل التحديد (R²=0.450)، وهذا يشير إلى

أن متغير المخاطر السيبرانية أصر ما نسبته (45.0%) من التغير الحاصل في استخدام البطاقات المصرفية. أما قيمة معامل التحديد المعدل Adj.R2 فقد بلغت (0.439)، وبلغ الفرق بينها وبين معامل التحديد (0.011)، وهي قيمة ضئيلة جداً، مما يشير إلى قدرة النموذج على التنبؤ بقيمة متغير استخدام البطاقات المصرفية.

كما يتبين من الجدول معنوية النموذج، حيث بلغت قيمة F المحسوبة (40.865) وبمستوى الدلالة (SigF=0.000) وهي أقل من 0.05 مما يشير إلى وجود أثر دال إحصائياً لمتغير المخاطر السيبرانية في استخدام البطاقات المصرفية عند مستوى الدلالة (as0.05).

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الرئيسية، وقبول الفرضية البديلة، التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمخاطر الأمن السيبراني بأبعاده الأربعة مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية في مصرف الراجحي"

الجدول (20) معاملات الانحدار للفرضية الرئيسية

معاملات الانحدار					
المخاطر السيبرانية	B المعاملات	الخطأ المعياري	قيمة Beta	قيمة T المحسوبة	Sig T* مستوي الدلالة
مخاطر أمن المعلومات	0.167	0.085	0.127	1.969	0.050
مخاطر تطبيقات الهاتف المحمول	0.316	0.083	0.314	3.826	0.000
المخاطر التشغيلية	-0.153	0.084	-0.163	-1.816	0.071
مخاطر الهجمات السيبرانية	0.437	0.082	0.463	5.349	0.000

* التأثير دال إحصائياً عند مستوى الدلالة ($\alpha \leq 0.05$)

يوضح الجدول (20) قيم معاملات الانحدار لأبعاد المخاطر السيبرانية، حيث يتبين أن قيمة B عند بعد مخاطر أمن المعلومات قد بلغت (0.167)، وبلغت قيمة T المحسوبة عند هذا البعد (1.969) وبمستوى الدلالة ($\text{SigT}=0.050$)، وهي أقل أو يساوي من 0.05، مما يشير إلى وجود أثر معنوي إيجابي لمخاطر أمن المعلومات في استخدام البطاقات المصرفية. ويتبين من الجدول أن قيمة B عند بعد مخاطر تطبيقات الهاتف المحمول قد بلغت (0.316)، وبلغت قيمة T المحسوبة عند هذا البعد (3.826) وبمستوى الدلالة ($\text{SigT}=0.000$)، وهي أقل من 0.05، مما يشير إلى وجود أثر معنوي إيجابي لمخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية. ويتبين من الجدول أن قيمة B عند بعد (المخاطر التشغيلية) قد بلغت (-0.153)، وبلغت قيمة T المحسوبة عند هذا البعد (-1.816) وبمستوى الدلالة ($\text{SigT}=0.071$)، وهي أكبر من 0.05 مما يشير إلى عدم وجود أثر معنوي للمخاطر التشغيلية في استخدام البطاقات المصرفية. ويتبين من الجدول أن قيمة B عند بعد مخاطر الهجمات السيبرانية قد بلغت (0.437)، وبلغت قيمة T المحسوبة عند هذا البعد (5.349) وبمستوى الدلالة ($\text{SigT}=0.000$)، وهي أقل من 0.05 مما يشير إلى وجود أثر معنوي إيجابي لمخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية.

وتشير نتائج اختبار الفرضية الرئيسة إلى الأثر الإيجابي لمخاطر الأمن السيبراني على استخدام البطاقات المصرفية، وحيث أن الباحث قام بصياغة فقرات الاستبانة حتى تقيس مدى قيام مصرف الراجحي بإدارة هذه المخاطر والحد من احتمالية حدوثها وأثرها على أعمال المصرف، ولهذا يعتبر ظهور الأثر الإيجابي مؤشرا على المساهمة التي تؤديها عملية إدارة المخاطر السيبرانية في تشجيع العملاء على استخدام البطاقات المصرفية.

🔍 نتائج اختبار الفرضيات المتفرعة من الفرضية الرئيسة

للتحقق من تأثير المخاطر السيبرانية في استخدام البطاقات المصرفية، تم تجزئة الفرضية الرئيسة إلى أربع فرضيات فرعية، وقد تم استخدام تحليل الانحدار الخطي البسيط Simple Linear Regression لإختبار هذه الفرضيات، وفيما يأتي نتائج اختبار الفرضيات المتفرعة من الفرضية الرئيسة.

⇐ نتائج اختبار الفرضية الفرعية الأولى

تهدف الفرضية الفرعية الأولى إلى التعرف على أثر مخاطر أمن المعلومات في استخدام البطاقات المصرفية. حيث تنص هذه الفرضية على أنه: "لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة (0.05) لمخاطر أمن المعلومات في استخدام البطاقات المصرفية في مصرف الراجحي". وقد ظهرت نتائج اختبار هذه الفرضية كما يأتي:

الجدول (21) ملخص النموذج وتحليل تباين الانحدار للفرضية الفرعية الأولى

تحليل التباين ANOVA			ملخص النموذج				
Sig F*	قيمة F المحسوبة	درجات الحرية	الخطأ المعياري للنموذج	Adjusted R ² معامل التحديد المعدل	R ² معامل التحديد	R معامل الارتباط	المتغير التابع
0.000	53.550	1	0.489	0.205	0.209	0.457	استخدام البطاقات المصرفية

* التأثير دال إحصائياً عند مستوى الدلالة ($\alpha \leq 0.05$)

يتضح من الجدول (21) وجود علاقة إرتباط بين بُعد مخاطر أمن المعلومات ومتغير استخدام البطاقات المصرفية، حيث بلغت قيمة معامل الإرتباط ($R=0.457$)، وبلغت قيمة معامل التحديد ($R^2=0.209$)، وهذا يشير إلى أن بعد مخاطر أمن المعلومات فسر ما نسبته (20.9%) من التغير الحاصل في متغير استخدام البطاقات المصرفية. أما قيمة معامل التحديد المعدل Adj.R² فقد بلغت (0.205)، وبلغ الفرق بينها وبين معامل التحديد (0.004)، وهي قيمة ضئيلة جداً، مما يشير إلى قدرة النموذج على التنبؤ بقيم متغير استخدام البطاقات المصرفية.

كما يتبين من الجدول معنوية النموذج، حيث بلغت قيمة F المحسوبة (53.550) وبمستوى الدلالة (SigF=0.000) وهي أقل من 0.05، مما يشير إلى وجود أثر إيجابي دال إحصائياً لبعد مخاطر أمن المعلومات في متغير استخدام البطاقات المصرفية عند مستوى الدلالة ($\alpha \leq 0.05$).

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الأولى، وقبول الفرضية البديلة التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمخاطر أمن المعلومات في استخدام البطاقات المصرفية في مصرف الراجحي".

الجدول (22) معاملات الانحدار للفرضية الفرعية الأولى

معاملات الانحدار					
Sig T*	قيمة T	قيمة Beta	الخطأ المعياري	B	البعد
مستوى الدلالة	المحسوبة			المعاملات	
0.000	7.318	0.457	0.082	0.600	مخاطر أمن المعلومات

* التأثير دال إحصائياً عند مستوى الدلالة ($\alpha \leq 0.05$)

يوضح الجدول (22) قيم معاملات الانحدار لبعد مخاطر أمن المعلومات، حيث يتبين أن قيمة B عند بعد مخاطر أمن المعلومات قد بلغت (0.600)، وبلغت قيمة T المحسوبة عند هذا البعد (7.318) وبمستوى الدلالة (SigT=0.000)، وهي أقل من 0.05، مما يشير إلى وجود أثر إيجابي ومعنوي لبعد مخاطر أمن المعلومات في استخدام البطاقات المصرفية. الفرع الثاني: نتائج اختبار الفرضية الفرعية الثانية

تهدف الفرضية الفرعية الثانية إلى التعرف على أثر مخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية. حيث تنص هذه الفرضية على أنه: "لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية في مصرف الراجحي". وقد ظهرت نتائج اختبار هذه الفرضية كما يأتي:

الجدول (23) ملخص النموذج وتحليل تباين الإنحدار للفرضية الفرعية الثانية

ANOVA تحليل التباين			ملخص النموذج				
Sig F*	قيمة F المحسوبة	درجات الحرية	الخطأ المعياري للنموذج	Adjusted R ² معامل التحديد المعدل	R ² معامل لتحديد	R معامل الارتباط	المتغير التابع
0.000	105.681	1	0.445	0.339	0.342	0.585	استخدام البطاقات المصرفية

* عند مستوى الدلالة ($\alpha \leq 0.05$)

يتضح من الجدول (23) وجود علاقة ارتباط بين بُعد مخاطر تطبيقات الهاتف ومتغير استخدام البطاقات المحمول المصرفية، حيث بلغت قيمة معامل الارتباط ($R=0.585$)، وبلغت قيمة معامل التحديد ($R^2=0.342$)، وهذا يشير إلى أن بعد مخاطر تطبيقات الهاتف المحمول فسر ما نسبته (34.2%) من التغير الحاصل في متغير استخدام البطاقات المصرفية. أما قيمة معامل التحديد المعدل Adj.R2 فقد بلغت (0.339)، وبلغ الفرق بينها وبين معامل التحديد (0.003)، وهي قيمة ضئيلة جداً، مما يشير إلى قدرة النموذج على التنبؤ بقيم متغير استخدام البطاقات المصرفية.

كما يتبين من الجدول معنوية النموذج، حيث بلغت قيمة F المحسوبة (105.681) وبمستوى الدلالة ($SigF=0.000$) وهي أقل من 0.05 مما يشير إلى وجود أثر ايجابي دال إحصائياً لبعد مخاطر تطبيقات الهاتف المحمول في متغير استخدام البطاقات المصرفية عند مستوى الدلالة ($\alpha \leq 0.05$).

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الثانية، وقبول الفرضية البديلة التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية في مصرف الراجحي".

الجدول (24) معاملات الانحدار للفرضية الفرعية الثانية

معاملات الانحدار					
البعد	B المعاملات	الخطأ المعياري	قيمة Beta	قيمة T المحسوبة	Sig T* مستوى الدلالة
مخاطر تطبيقات الهاتف المحمول	0.588	0.057	0.585	10.280	0.000

* التأثير دال إحصائياً عند مستوى الدلالة ($\alpha \leq 0.05$)

يوضح الجدول (24) قيم معاملات الانحدار لبعد مخاطر تطبيقات الهاتف المحمول، حيث يتبين أن قيمة B عند بعد مخاطر تطبيقات الهاتف المحمول قد بلغت (0.588)، وبلغت قيمة T المحسوبة عند هذا البعد (10.280) وبمستوى الدلالة (SigT=0.000)، وهي أقل من 0.05، مما يشير إلى وجود أثر إيجابي ومعنوي لبعد مخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية.

⇐ مناقشة اختبار الفرضية الفرعية الثالثة

تهدف الفرضية الفرعية الثالثة إلى التعرف على أثر المخاطر التشغيلية في استخدام البطاقات المصرفية. حيث تنص هذه الفرضية على أنه: "لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للمخاطر التشغيلية في استخدام البطاقات المصرفية في مصرف الراجحي". وقد ظهرت نتائج اختبار هذه الفرضية كما يأتي:

الجدول (25) ملخص النموذج وتحليل تباين الإنحدار للفرضية الفرعية الثالثة

ANOVA تحليل التباين			ملخص النموذج				
Sig F*	قيمة F المحسوبة	درجات الحرية	الخطأ المعياري للنموذج	Adjusted R ² معامل التحديد المعدل	R ² معامل لتحديد	R معامل الارتباط	المتغير التابع
0.000	60.817	1	0.482	0.227	0.231	0.480	استخدام البطاقات المصرفية

* التأثير دال إحصائياً عند مستوى الدلالة ($\alpha \leq 0.05$)

يتضح من الجدول (25) وجود علاقة ارتباط بين بُعد المخاطر التشغيلية ومتغير استخدام البطاقات المصرفية، حيث بلغت قيمة معامل الارتباط ($R=0.480$)، وبلغت قيمة معامل التحديد ($R^2=0.231$)، وهذا يشير إلى أن بعد مخاطر تطبيقات الهاتف المحمول فسر ما نسبته (23.1%) من التغير الحاصل في متغير استخدام البطاقات المصرفية. أما قيمة معامل التحديد المعدل Adj.R2 فقد بلغت (22.7)، وبلغ الفرق بينها وبين معامل التحديد (0.004)، وهي قيمة ضئيلة جداً، مما يشير إلى قدرة النموذج على التنبؤ بقيم متغير استخدام البطاقات المصرفية.

كما يتبين من الجدول معنوية النموذج، حيث بلغت قيمة F المحسوبة (60.817) وبمستوى الدلالة ($SigF=0.000$) وهي أقل من 0.05 مما يشير إلى وجود أثر إيجابي دال إحصائياً لبعد المخاطر التشغيلية في متغير استخدام البطاقات المصرفية عند مستوى الدلالة ($\alpha \leq 0.05$)

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الثالثة، وقبول الفرضية البديلة التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للمخاطر التشغيلية في استخدام البطاقات المصرفية في مصرف الراجحي".

الجدول (26) معاملات الانحدار للفرضية الفرعية الثالثة

معاملات الانحدار					
Sig T*	قيمة T	قيمة Beta	الخطأ المعياري	B	البعد
مستوى الدلالة	المحسوبة			المعاملات	
0.000	7.799	0.480	0.058	0.452	المخاطر التشغيلية

* التأثير دال إحصائياً عند مستوى الدلالة ($\alpha \leq 0.05$)

يوضح الجدول (26) قيم معاملات الانحدار لبعد المخاطر التشغيلية، حيث يتبين أن قيمة B عند بعد (المخاطر التشغيلية) قد بلغت (0.452)، وبلغت قيمة T المحسوبة عند هذا البعد (7.799) وبمستوى الدلالة (SigT=0.000)، وهي أقل من 0.05، مما يشير إلى وجود أثر إيجابي ومعنوي لبعد المخاطر التشغيلية في استخدام البطاقات المصرفية.

⇐ نتائج اختبار الفرضية الفرعية الرابعة

تهدف الفرضية الفرعية الرابعة إلى التعرف على أثر مخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية. حيث تنص هذه الفرضية على أنه: "لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية في مصرف الراجحي". وقد ظهرت نتائج اختبار هذه الفرضية كما يأتي:

الجدول (27) ملخص النموذج وتحليل تباين الإنحدار للفرضية الفرعية الرابعة

ANOVA تحليل التباين			ملخص النموذج				
Sig F*	قيمة F المحسوبة	درجات الحرية	الخطأ المعياري للنموذج	Adjusted R ² معامل التحديد المعدل	R ² معامل لتحديد	R معامل الارتباط	المتغير التابع
0.000	125.014	1	0.432	0.378	0.381	0.617	استخدام البطاقات المصرفية

* التأثير دال إحصائياً عند مستوى الدلالة ($\alpha \leq 0.05$)

يتضح من الجدول (27) وجود علاقة ارتباط بين بُعد مخاطر الهجمات السيبرانية ومتغير استخدام البطاقات المصرفية، حيث بلغت قيمة معامل الارتباط ($R=0.617$)، وبلغت قيمة معامل التحديد ($R^2=0.381$)، وهذا يشير إلى أن بعد مخاطر الهجمات السيبرانية فسر ما نسبته (38.1%) من التغير الحاصل في متغير استخدام البطاقات المصرفية. أما قيمة معامل التحديد المعدل $Adj.R^2$ فقد بلغت (0.378)، وبلغ الفرق بينها وبين معامل التحديد (0.003)، وهي قيمة ضئيلة جداً، مما يشير إلى قدرة النموذج على التنبؤ بقيم متغير استخدام البطاقات المصرفية

كما يتبين من الجدول معنوية النموذج، حيث بلغت قيمة F المحسوبة (125.014) وبمستوى الدلالة ($SigF=0.000$) وهي أقل من 0.05، مما يشير إلى وجود أثر ايجابي دال إحصائياً لبعد مخاطر الهجمات السيبرانية في متغير استخدام البطاقات المصرفية عند مستوى الدلالة ($\alpha \leq 0.05$)

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الرابعة، وقبول الفرضية البديلة التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية في مصرف الراجحي".

الجدول (28) معاملات الانحدار للفرضية الفرعية الرابعة

معاملات الانحدار					
البعد	B المعاملات	الخطأ المعياري	قيمة Beta	قيمة T المحسوبة	Sig T* مستوى الدلالة
مخاطر الهجمات السيبرانية	0.583	0.052	0.617	11.181	0.000

* التأثير دال إحصائياً عند مستوى الدلالة ($\alpha \leq 0.05$)

يوضح الجدول (28) قيم معاملات الانحدار لبعد مخاطر الهجمات السيبرانية، حيث يتبين أن قيمة B عند بعد (مخاطر الهجمات السيبرانية) قد بلغت (0.583)، وبلغت قيمة T المحسوبة عند هذا البعد (11.181) وبمستوى الدلالة (SigT=0.000)، وهي اقل من 0.05، مما يشير إلى وجود أثر ايجابي ومعنوي لبعد مخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية.

الفصل الخامس : الخاتمة (النتائج والتوصيات)

1.5 النتائج

بالإعتماد على المخرجات الوصفية والتحليلية لأداة الدراسة واختبار الفرضيات، تم التوصل إلى

النتائج الآتية:

1.1.5 نتائج الإحصاء الوصفي

[1] إرتفاع مستوى الأهمية النسبية للمخاطر السيبرانية في مصرف الراجحي، حيث بلغ الوسط الحسابي (4.253)، وقد ظهرت جميع الأبعاد بأهمية نسبية مرتفعة وعلى التوالي: مخاطر أمن المعلومات، المخاطر التشغيلية، مخاطر تطبيقات الهاتف المحمول، وأخيراً مخاطر الهجمات السيبرانية. وهذا يدل على الإهتمام الذي توليه مصرف الراجحي لمكافحة ومنع المخاطر والتهديدات السيبرانية، حفاظاً على سلامة العملاء (أموالهم ومعلوماتهم الشخصية الحساسة)، وسمعة البنك، والتأكيد على الإلتزام بمتطلبات وقواعد الشريعة الإسلامية فيما يتعلق بالأمن والحفاظ على سرية المعلومات والإمتثال للتشريعات والقوانين المالية المتعلقة بالأمان السيبراني والحماية الإلكترونية في القطاع المالي ومواكبتها للتقنيات الجديدة وتبني الحلول الأمنية المتطورة للوقاية من المخاطر والتهديدات الإلكترونية وحماية أنظمتها ومعلوماتها.

وقد توافقت هذه النتيجة مع نتيجة دراسة (الزيود، 2020)، والتي توصلت إلى أن البنوك السعودية تلتزم بالسياسات الخاصة بأمن المعلومات وسياسة الأمن السيبراني بالإضافة إلى تطبيق ومتابعة جميع التعليمات الصادرة عن البنك المركزي السعودي، كما تقوم البنوك بنشر دليل الحاكمية المؤسسية لتكنولوجيا المعلومات ضمن التقارير السنوية وتوافقت مع نتيجة دراسة (البغدادى، 2021)، والتي توصلت إلى أن القضايا الخاصة بالأنترنت (cyber issues) يمكن معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنيات وتوافقت مع نتيجة دراسة

(أبو الهيجاء، 2021، والتي توصلت إلى أن القطاعات الإقتصادية أكثر تعرضاً للجريمة الإلكترونية (السيبرانية) وفي مقدمتها القطاع المصرفي، ووفق البنك الدولي فإن قطاع الخدمات المالية يشهد هجمات سيبرانية تفوق القطاعات الأخرى بنسبة (65%).

كما توافقت مع نتيجة دراسة (Kopp et al., 2017)، والتي توصلت إلى إزدياد وعي البنوك تجاه المخاطر من خلال الإستثمار الجاد في تبني سياسات واجراءات بما يخص الأمن السيبراني. وتوافقت مع نتيجة دراسة Li & Wang, 2018 والتي توصلت إلى أن هناك إفصاحات عن مخاطر الأمن السيبراني، وأن هذه الإفصاحات حدثت من المخاطر السيبرانية، لأن الشركات عملت على مبدأ الحيطة والحذر في توفير الأمن للبيانات. وتوافقت مع نتيجة دراسة (Marjan & Chatterjee, 2019)، والتي توصلت إلى أن حماية الأصول المعمول بها في البنوك واسع جداً، وأن أمان المعلومات قوية والبنية التحتية، أيضاً، وأن التقنيات المعمول بها تمنع الهجمات السيبرانية وتعمل على كشفها بسرعة عند حدوثها.

[2] إرتفاع مستوى الأهمية النسبية لإستخدام البطاقات المصرفية في مصرف الراجحي، حيث بلغ الوسط الحسابي (4.049)، وهذا يدل على الاهتمام الذي توليه مصرف الراجحي بإعتبارها أداة مالية فعالة تعمل على تلبية إحتياجات العملاء وتتوافق مع مبادئ وقوانين الشريعة الإسلامية، حيث توفر للعملاء السهولة والمرونة في إجراء المعاملات المالية، وتمنحهم المزيد من الأمان والحماية من التعرض للإحتيال، كما أنها تتيح للمصرف تتبع وتحليل المعاملات التي تتم بإستخدام البطاقات المصرفية، مما يزود الإدارة بالمعلومات الهامة حول الأنماط المالية للعملاء وإستخدامها في تحسين الخدمات المصرفية وتقديم الإقتراحات والتوصيات المالية المناسبة للعملاء.

وقد توافقت هذه النتيجة مع نتيجة دراسة شاشو) والحموي، 2011، والتي توصلت أن بطاقة الإئتمان أصبحت أداة وفاء شائعة للإلتزامات النقدية في البيوع وتقديم الخدمات، ووفرت لحاملها الأمان من السطو والسرقة، ووفرت عليهم الجهد والتعب بالحصول على ما يحتاجونه دون الحاجة إلى دفع النقود أو صرفها.

2.1.5 نتائج اختبار الفرضيات

[1] أشارت نتائج اختبار الفرضية الرئيسة إلى وجود أثر دال إحصائياً لمخاطر الأمن السيبراني بأبعاده الأربعة مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية في مصرف الراجحي. وهذا يشير إلى أن اهتمام مصرف الراجحي بالمخاطر السيبرانية يؤثر إيجاباً على استخدام البطاقات المصرفية من خلال تعزيز الثقة والأمان في استخدامها، وتبني تقنيات وحلول أمنية متقدمة لحمايتها وحماية معلومات العملاء، وتوعية العملاء وتثقيفهم وزيادة معرفتهم بالمخاطر السيبرانية، بالإضافة إلى إسقاط المزيد من العملاء الباحثين والمهتمين بالأمان المصرفي.

وقد توافقت هذه النتيجة مع نتيجة دراسة السمحان 2020، والتي توصلت إلى أن متطلبات تحقيق الأمن السيبراني ضرورية بدرجة أكبر لحماية أنظمة المعلومات بالجامعة تحت مظلة المتطلبات المالية.

كما توافقت هذه النتيجة مع نتيجة دراسة Kuju & Shah, 2015، والتي توصلت إلى أن مستوى المخاطر السيبرانية يؤخذ على كل خدمة على حدى وذلك تبعاً لمستوى التعقيد في كل خدمة ونوع التكنولوجيا الداعمة لتلك الخدمة وتوافقت مع نتيجة دراسة (Aldasoro et al 2020)، والتي توصلت إلى أن المخاطر السيبرانية على العمليات التشغيلية تكون مرتفعة في فترات الإزدهار الإقتصادي والسياسات النقدية التيسيرية المفرطة، وأن الجودة العالية للتنظيم المالي والإشراف الجيد والإجراءات الوقائية تلعب الدور الأكبر في تخفيض نسبة المخاطر السيبرانية على العمليات التشغيلية وبالتالي تجنب أو تخفيض الخسائر.

[2] أشارت نتائج اختبار الفرضية الفرعية الأولى إلى وجود أثر دال إحصائياً لمخاطر أمن المعلومات في استخدام البطاقات المصرفية في مصرف الراجحي وهذا يشير إلى أن اهتمام مصرف الراجحي بمخاطر أمن المعلومات يؤثر إيجاباً على استخدام البطاقات المصرفية من خلال تعزيز الثقة وحماية البيانات الشخصية، والوقاية من الاحتيال، وتوفير المعرفة والإرشادات بمخاطر أمن المعلومات والتعامل مع

التحديات السيبرانية، والتشجيع على تطوير الحلول والإبتكارات التقنية لحماية البطاقات المصرفية وتعزيز أمان المعاملات المالية عبر الإنترنت.

وقد توافقت هذه النتيجة مع نتيجة دراسة قرزیز وزیدان (2022)، والتي توصلت إلى وجود أثر ذو دلالة احصائية بين أمن المعلومات وجودة الخدمات المصرفية.

[3] أشارت نتائج إختبار الفرضية الفرعية الثانية إلى وجود أثر دال إحصائياً لمخاطر تطبيقات الهاتف المحمول في إستخدام البطاقات المصرفية في مصرف الراجحي وهذا يشير إلى أن اهتمام مصرف الراجحي بمخاطر تطبيقات الهاتف المحمول يؤثر إيجاباً على استخدام البطاقات المصرفية، من خلال تحسين سهولة وملاءمة الاستخدام، وتعزيز الأمان في البطاقات المصرفية بتطبيق تقنيات التشفير والمصادقة المتعددة والرصد المستمر للأنشطة المشبوهة مما يحد من فرص الإختراق والإحتيال السيبراني، وزيادة قدرة العملاء على إدارة وضبط بطاقاتهم المصرفية وإستخدام حساباتهم المصرفية وإجراء المعاملات في أي وقت وأي مكان التحكم والوصول العالمي للعملاء.

[4] أشارت نتائج إختبار الفرضية الفرعية الثالثة إلى وجود أثر دال إحصائياً للمخاطر التشغيلية في استخدام البطاقات المصرفية في مصرف الراجحي وهذا يشير إلى أن إهتمام مصرف الراجحي بالمخاطر التشغيلية يؤثر إيجاباً على استخدام البطاقات المصرفية، من خلال ضمان إستمرارية الخدمات المصرفية والإعتماد على البطاقات المصرفية لإجراء المعاملات بصورة مستمرة، وتحسين البنية التحتية والعمليات التشغيلية لتقليل فرص حدوث الأعطال التي تؤثر على الوصول إلى البطاقات المصرفية وتنفيذ المعاملات، وزيادة الكفاءة والجودة في تقديم خدمات البطاقات المصرفية، وتطوير الإجراءات والسياسات لإدارة ومراقبة المخاطر التشغيلية المتعلقة بالبطاقات المصرفية، بالإضافة إلى توفير الدعم الفني المتخصص لعملاء البطاقات المصرفية في حال وجود مشاكل تشغيلية او تقنية تؤثر على استخدام البطاقات المصرفية.

وقد توافقت هذه النتيجة مع نتيجة دراسة عبد الهادي 2015، والتي توصلت إلى أن الإفتقار إلى الرقابة الداخلية وضعف سيطرة الإدارة على مجريات الأمور في البنوك من أهم مخاطر التشغيل،

وقد يترتب عليه خسائر غير متوقعة تقود إلى مخاطر تشغيلية تتمثل في مخاطر السمعة، التزوير، السرقة والسطو، الجرائم الإلكترونية وأخطار أخرى تتعلق بأخلاقيات العمل والمهنية.(1) وتوافقت مع نتيجة دراسة (زوانب) وحاج علي 2021، والتي توصلت إلى وجود علاقة ارتباطية بين استخدام تكنولوجيا المعلومات والاتصال في البنوك التجارية والمخاطر التشغيلية، أي أنه كلما كان البنك يعمل وفق تكنولوجيا عالية كلما تم التحكم بالمخاطر التشغيلية والتنبؤ بها وضمان التسيير الجيد لها.

[5] أشارت نتائج اختبار الفرضية الفرعية الرابعة إلى وجود أثر دال إحصائياً لمخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية في مصرف الراجحي وهذا يشير إلى أن إهتمام مصرف الراجحي بمخاطر الهجمات السيبرانية يؤثر إيجاباً على استخدام البطاقات المصرفية، من خلال زيادة الثقة والأمان في استخدام البطاقات المصرفية، وتوفير الحماية للعملاء ضد التهديدات السيبرانية المحتملة، حيث أن الإهتمام بهذه المخاطر وإدارتها يساعد في توفير الحماية لبيانات العملاء الشخصية المرتبطة ببطاقاتهم المصرفية، والكشف المبكر عن الهجمات السيبرانية المحتملة والإستجابة الفاعلة لها، وتوجيه العملاء للحفاظ على سلامة معلوماتهم المالية وأخذ الإحتياطات الأمنية عند استخدام البطاقات المصرفية، بالإضافة إلى تحسين التقنية والبنية التحتية للتصدي للهجمات السيبرانية لحماية البطاقات المصرفية.

وقد توافقت هذه النتيجة مع نتيجة دراسة (Bukht et al., 2020) والتي توصلت إلى تعرض البنوك محل الدراسة للهجمات السيبرانية أخطرها هو هجمات سرقة بطاقات الإئتمان.

2.5 التوصيات

بناءً على النتائج التي تم التوصل إليها، فإن الدراسة توصي بما يأتي:

1. ضرورة اتخاذ الاحتياطات اللازمة في مصرف الراجحي بالتدريب والتوجيه المستمر للموظفين حول مفاهيم الأمن السيبراني وأفضل الممارسات له، لتعزيز الوعي والحس الأمني لدى الموظفين والعملاء بمخاطر الهجمات السيبرانية.

2. ضرورة الأخذ بآراء ومقترحات العملاء في الإجراءات المتبعة في مصرف الراجحي بالسياسات والإجراءات الأمنية الصارمة والواضحة في التعامل مع المخاطر السيبرانية بمختلف أشكالها، لزيادة مستوى الأمان والحماية في بطاقتهم المصرفية، والأخذ بها بما يتناسب مع سياسات وتعليمات البنك.
3. تعزيز عملية إصدار بطاقات مصرفية متنوعة في مصرف الراجحي، مما يسهم في التقليل من حجم الحوادث المرتبطة بها.
4. زيادة مستوى إهتمام مصرف الراجحي في الاستفادة من سياسات البنوك الاخرى الوطنية أو العالمية في التعامل مع حوادث الأمن السيبراني.
5. إجراء مصرف الراجحي عمليات مراجعة وتحديث مستمرة ومنظمة لأنظمتها وتطبيقاتها الأمنية، وإجراء اختبارات أمان للتأكد من سلامة الأنظمة.

Abstract

This study aimed to identify the impact of cyber security risks in its dimensions (cyber security risks, information security risks, mobile application risks, operational risks) on the use of banking cards, with a specific application to Al Rajhi Bank. To achieve the objectives of the study, the descriptive-analytical method was used. The study population included all employees of Al Rajhi Bank. The researcher distributed 237 electronic questionnaires and retrieved 205 of them electronically. Statistical methods were used to analyze the data.

The results of the study showed a statistically significant impact of cyber security risks in its four dimensions: information security risks, mobile application risks, operational risks, and cyber-attacks risks on the use of banking cards at Al Rajhi Bank.

The study recommended that Al Rajhi Bank take necessary precautions, including continuous training and guidance for employees on cyber security concepts and best practices to enhance awareness and security sensitivity among employees and customers about cyber-attacks risks. Additionally, the study suggested considering customer opinions and proposals in the bank's security policies and procedures to effectively handle various forms of cyber risks.

Keywords: Cyber Security Risks, Banking Cards, Al Rajhi Bank.

المراجع:

أولاً: المراجع العربية

1. 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
2. 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
3. أبو الهيجاء، محمد (2021) المخاطر السيبرانية من الناحية الإقتصادية والمالية. مجلة ريادة الأعمال الإسلامية الهيئة العالمية للتسويق الإسلامي، المجلد 6، العدد ١
4. أحمد ، سناء (2019) ، " مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة ، مجلة البحث العلمي في 493-534 ، التربية
5. إسماعيل محمد (2019)، الأمن السيبراني في القطاع المصرفي، الدائرة الاقتصادية الفنية، صندوق النقد العربي، أبو ظبي، ع4.
6. 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
7. أعمر بن موسى (2020) الخدمات المصرفية الالكترونية ومتطلبات تطويرها في الجزائر - دراسة ميدانية (أطروحة دكتوراه). كلية العلوم الاقتصادية والتسيير والعلوم التجارية غرداية جامعة غرداية
8. أميرهم جهمان 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.

9. 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.

10. بانقا (2019)، مخاطر الهجمات الإلكترونية السيبرانية وأثارها الاقتصادية، المعهد العربي للتخطيط بالكويت، سلسلة دراسات تنموية، الطبعة الأولى

11. البسام، سارة عبد الرحمن (2020) ، التحقيق في العوامل المتعلقة بالتوعية بالأمن السيبراني في القطاع المصرفي البحريني ، رسالة ماجستير غير منشورة، البحرين: جامعة الخليج العربي ، ص 129

12. البغدادي ، مروة فتحي السيد ، (2021) ، اقتصاديات الأمن السيبراني في القطاع المصرفي ، مجلة البحوث القانونية والاقتصادية كلية الحقوق - جامعة المنصورة ، ع76 ، ص ص 1513 - 1446

البنك الدولي ، (2021) ، تعليمات ومؤشرات البنك الدولي بشأن المخاطر السيبرانية المصرفية
13. البغدادي، (2021)، اقتصاديات الأمن السيبراني في القطاع المصرفي، جامعة المنصورة - كلية الحقوق، مجلة البحوث القانونية والاقتصادية، مصر، ع76، 1513 – 1446.

14. بن مبشر، محمد يسلم مفتاح وعويضة، عدنان عبد الله محمد (2023)، البطاقات الائتمانية في المصارف التشاركية وأثرها على الإقتصاد البنوك التشاركية التركية أنموذجا، الحلقة 3:1 مجلة الإقتصاد الإسلامي العالمية، العدد 129

15. حسين ، رحيم ، ومعراج ، هوارى (2019) ، الصيرفة الإلكترونية كمدخل لعصرنة المصارف الجزائرية ، ملتقى المنظومة المصرفية الجزائرية والتحوللات الاقتصادية واقع وتحديات ، ص 18

16. الخرينج، نواف متعب بنيه متعب البسطويسى، 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

17. خليل ، تيسير ، (2022) ، " أثر الاستثمار في الأمن السيبراني علي الإداء المصرفي " ، رسالة ماجستير ، كلية تجارة ، جامعة عين شمس ، ص 86

18. راضية مصداق، وزهرة بود بودة (2021) التحول نحو الصيرفة الالكترونية كالية لتفعيل التجارة الالكترونية في الجزائر مجلة المنهل الاقتصادي 251-270

19. رشوان عبد الرحمن محمد سليمان وقاسم زينب عبد الحفيظ (2022)، أثر إدارة مخاطر الأمن السيبراني على دعم الإستقرار والشمول المالي في البنوك المؤتمر العلمي الدولي الأول بعنوان أثر الأمن السيبراني على الأمن الوطني، 20-21 ديسمبر
20. زكريا محمد . (2022) ، " دور المعهد المصرفي في نشر الثقافة المالية كمحور أساسي في منظمة البنوك التجارية . ، الإكاديمية العربية للعلوم الإدارية والمصرفية ، المجلد 19 - العدد الأول - السنة 19 يناير 2019 .
21. زوايب وحاج علي، (2021)، تأثير تكنولوجيا المعلومات والإتصال على المخاطر التشغيلية بالبنوك دراسة إستقصائية على عدد من البنوك التجارية الجزائرية، مجلة البحوث و الدراسات التجارية، مج 5، ع 1، ص 207-224
22. الزيود (2020)، إدارة مخاطر الأمن السيبراني في المصرف، جامعة بوسعيد، كلية التجارة، مجلة البحوث المالية والتجارية، مج 23، ع 3.
23. السمحان منى عبد الله (2020) متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود. مجلة كلية التربية، جامعة المنصورة، المجلد 1 ، العدد (111)
24. 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.
25. 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)
26. شغللال نبيل آيت (2019). البطاقات البنكية وعوائق استخدامها في الجزائر محلة الدراسات القانونية والاقتصادية، 2(2) الصفحات 8-16
27. الشورة (2020)، الأمن السيبراني في البنوك الإسلامية الأردنية، الجامعة الأردنية، كلية الشريعة، قسم المصارف الإسلامية.
28. صالح ، نرمين محمد شاكر إبراهيم ، (2022) ، محددات فعالية المراجع الداخلي للأمن السيبراني، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة بعنوان تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين ، كلية التجارة - جامعة الإسكندرية ، ص ص 1-24 .

29. صندوق النقد العربي ، (2019) ، سلسلة موجز سياسات حول أمن الفضاء السيبراني في القطاع

المصرفي ، العدد الرابع.

30. العتيبي، عبد الرحمن بن بجاد ، (2020) ، " دور الأمن السيبراني في تعزيز الأمن الإنساني " ، رسالة

ماجستير منشورة، السعودية جامعة نايف العربية للعلوم الأمنية.

31. عسيري، فيصل محمد ، (2021) - الأمن السيبراني وحماية أمن المعلومات " ، مجلة الدراسات

المالية والمصرفية ، كلية تجارة ، جامعة أسيوط ، 78 .

32. عصام المحاولي البكري ، (2019) ، " تطوير وتنشيط العمل المصرفي ودوره في تحقيق الوعي

المصرفي بالاحتيايل البنكي ، المجلة العلمية للاقتصاد والتجارة جامعة عين شمس، العدد الرابع ،

23 - 40 الصحفي، وعسكول،

33. غزالي، سارة محمد روي فتحي (2022) الأمن السيبراني ودرجة وعي المؤسسات بأهميتها، المجلة

العربية للنشر العلمي، العدد (47).

34. محمد صابر ، (2023) - فاعلية توظيف العلاقات العامة لتكنولوجيا المعلومات عبر المواقع

الإلكترونية في التوعية بالأمن السيبراني ، المجلة العربية للبحوث الأعلام والاتصال ، جامعة الأهرام

الكندية ، مصر ، المجلد 2 ، العدد 33 ، ص 33

35. محمد عدنان أبو الهيجاء، (2021)، المخاطر السيبرانية من الناحية الاقتصادية والمالية، مجلة

ريادة الأعمال الإسلامية، مج.6، ع1.

36. مشتهى ، وصبرى حمدان ، (2022) ، مدى موثوقية نظم المعلومات البنكية وأثرها في تحسين

مؤشرات الأداء المصرفي دراسة مقارنة علي المصارف الأردنية والفلسطينية المدرجة ببيروت عمان

ونابلس"، دراسات العلوم الإدارية ، ص 258

37. 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

38. ناصر سليمان ، (2020) ، " مدى مساهمة البنوك التجارية في نشر الوعي المصرفي لدى العملاء ،

المجلة العلمية للاقتصاد والتجارة ، كلية التجارة ، جامعة القاهرة ، العدد الأول ، 44 - 66 .

39. الوكيل سامي (2021)، " الأمن السيبراني.. حماية وطنية لأمن الفرد والمجتمع في المملكة " ، وكالة

الأخبار السعودية، مجلد البحوث العلمية ، ص 152 - 160 .

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 from 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. 1st edition, Switzerland, Springer International
7. CB en chiffres. (2021). Nombre de cartes CB. Consulté le 30, 2022, sur <https://observatoirech.cartes-bancaires.com/https://observatoirecb.cartes-bancaires.com/>
8. Chelangat, M. N., Kiprop, S., & Mutai, J. K. (2022, 1). Effects of Payment Cards on Financial Performance of Commercial Banks in Kenya. *Journal of Finance and Accounting*, 6(1), pp. 46-56.
9. 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*

10. 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
11. 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
12. Despotović, A., Parmaković, A. & Miljković, M. (2023). Cybercrime and Cyber Security in Fintech. In Digital Transformation of the Financial Industry: Approaches and Applications
13. Doerr, S., Gambacorta, L., Leach, T., Legros, B., & Whyte, D. (2022). Cyber risk in central banking, BIS,
14. Donalds, Charlette & Kweku, Muata, (2019), toward A Cybercrime Classification Ontology: A Knowledge Human Behavior
15. 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
16. 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
17. Hasan, M. F., & Al-Ramadan, N. S. (2021), Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. Social Science and Humanities Journal
18. Hossain, I. (2021). Effects of E-Banking Adoption the Financial Performance of State-Owned Commercial Banks in Bangladesh, Information Resources Management journal, 34(4), pp. 93-112

19. 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*
20. 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*
21. Ndhine, T. O. Kibati, P., & Jeptepkeny, B. (2020, 11), Effect of Debit Cards on Financial Performance of Listed Commercial Banks in Kenya, *World Journal of Innovative Research*, 9(5), pp. 23-28
22. Quazzani, M. (2022, 7.25). <https://www.challenge.ma/>. Consulté le 3 31, 2023, sur 17,9 millions de cartes bancaires en circulation en 2021: <https://www.challenge.ma/179-millions-de-cartes-bancaires-en-circulation-en-2021-242978/>
23. Tunisie, M. (2021). <https://www.monetiquetunisie.com/>. Consulté le 230, 2023, sur Statistiques: <https://www.monetiquetunisie.com/statistiques/>

الملاحق

استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

يقوم الباحثين بإجراء دراسة حول قياس أثر مخاطر الأمن السيبراني في استخدام البطاقات

المصرفية دراسة تطبيقية على مصرف الراجحي

ونظراً لما لديكم من المعرفة العلمية والخبرة العملية ذات الصلة بموضوع البحث، نأمل الحصول منكم على العون والمساعدة في توفير المعلومات المناسبة لأغراض البحث، من خلال التكرم بإبداء رأيكم بالتأشير على الإجابة المناسبة من وجهة نظركم.

وأثقدم لحضراتكم بجزيل الشكر والتقدير للمساهمة في جهدكم في تعبئة هذا الاستبيان علماً أن جميع البيانات التي سيتم الحصول عليها منكم ستعامل بسرية تامة، ولن تستخدم لغير أغراض هذا البحث، وسوف أزودكم بنتائج هذه الدراسة حال اكتمالها إن شاء الله.

وتفضلوا بقبول فائق التقدير والاحترام

أولاً: البيانات الشخصية

- 1- النوع الاجتماعي ☐ ذكر ☐ أنثى
- 2- الفئة العمرية ☐ أقل من 30 سنة ☐ من 30 – أقل من 40 سنة ☐ من 40 – أقل من 50 سنة ☐ 50 سنة فأكثر
- 3- المؤهل العلمي ☐ دبلوم ☐ بكالوريوس ☐ دراسات عليا
- 4- مدة الخدمة ☐ أقل من 5 سنوات ☐ من 5 – أقل من 10 سنوات ☐ من 10 – أقل من 15 سنة ☐ 15 سنة فأكثر
- 5- المسمى الوظيفي ☐ موظف ☐ رئيس قسم ☐ مدير ☐ مساعد مدير
- 6- عدد الدورات المتخصصة في مجال الأمن السيبراني ☐ دورة واحدة فقط ☐ دورتان ☐ ثلاث دورات فأكثر ☐ لا يوجد

ثانياً محاور الاستبيان

المحور الأول: مخاطر الأمن السيبراني ، ضع إشارة (√) في المربع المناسب لاختيارك:

معارض بشدة	معارض	محايد	أو افق أو افق	أو افق بشدة	البعد
مخاطر أمن المعلومات					
					تلتزم إدارة البنك بتعليمات امن المعلومات الصادرة عن البنك المركزي السعودي
					تدرك إدارة البنك الأهمية القصوى لأمن بيانات العملاء والبنك ووضعتها ضمن مستويات وظيفية متعددة
					تعمل إدارة البنك على بيان المسؤوليات المتبعة في سياسة أمن المعلومات والمتمثلة في (السرية، النزاهة، التوافق)
					تقوم إدارة البنك بتحديد الجهة أو الموظفين المخول لهم بالاطلاع أو إستخدام البيانات والمعلومات
					تعرض بعض عملاء البنك الى استيلاء على بياناتهم الشخصية
					تقدم إدارة البنك تقارير منتظمة تشمل الحوادث التقنية التي وقعت على أصوله من المعلومات مع النتائج والتوصيات
					تتبنى إدارة البنك سياسات إدارية وقانونية للتعامل مع الحالات التي يكون موظف البنك

					طرفاً في وقوع حادثة تخص أمن المعلومات للبنك أو العملاء
					يتم تخزين بيانات العملاء في أكثر من جهة وبشكل متزامن
مخاطر تطبيقات الهاتف المحمول					
					تتولى إدارة البنك تطبيق برامج الأمن السيبراني وتحديثها وبيان توافقها مع مخاطر تطبيقات الهاتف المحمول لدى العملاء
					تقوم إدارة البنك بتأمين الحماية الكاملة على تطبيقات الهاتف المحمول ضد أي نوع من التهديدات السيبرانية والإخترافات الخارجية
					تُقاس ميزة وكفاءة تطبيقات الهاتف المحمول الخاصة بالبنك بمستوى الحماية والأمان أكثر من ميزة الخدمات المستفادة من خلالها
					تقوم إدارة البنك بتقييم قدرة وكفاءة برامج الأمان والحماية المطبقة في تطبيقات الهاتف المحمول الخاصة بالبنك
					تحدد إدارة البنك صلاحيات العملاء في استخدام الخدمات الإلكترونية عبر تطبيقات الهاتف المحمول الخاصة بالبنك
					يحدد البنك خدمات معيارية ثابتة للتطبيقات الهاتف المحمول الخاصة بالبنك

					يدرك عملاء البنك المخاطر السبرانية في حال استخدام التطبيقات الهاتفية
المخاطر التشغيلية					
					يملك البنك البرمجيات والمعدات اللازمة التي لديها القدرة على منع أي اختراق سبراني يمس عمليات التشغيل
					التطبيق البنكي الخاص بالعملاء سواء على الهاتف أو الحاسوب لديها القدرة على مواجهة الاختراق السبراني
					يقوم البنك بتدريب الموظفين وتوعيتهم بالمخاطر التشغيلية المحتملة
					برامج الحماية المطبقة في البنك تحدد أهم التهديدات الإلكترونية المحتملة داخل البنك وخارجه
					يتم تحديث التطبيقات الهاتفية والحاسوبية والآلية الخاصة بالعملاء والبنك التي تهدف لتجنب الثغرات التطبيقات والعمليات التشغيلية
					العمليات التشغيلية في البنك محمية من المخاطر التقنية
					البنك لتبني خدمات التكنولوجيا المالية وشركاء يسعى خارجين لإتمام عملياته التشغيلية

مخاطر الهجمات السيبرانية					
					في حال وقوع اعتداء أو اختراق إلكتروني، فإن البنك يتبع استراتيجية عمل للتعافي من خلالها من الأضرار التي نتجت حين وقوعه
					إذا وقع اعتداء إلكتروني على البنك يقوم البنك جهات مع مختصة وموثوقة للاستجابة بسرعة كبيرة للتصدي للاعتداء الإلكتروني
					إذا حدث أي اعتداء إلكتروني يتابع البنك الهجوم بعمل تحقيق لبيان مدى الضرر وطبيعته
					تتخذ إدارة البنك سياسة السرية والتكتم إزاء الإعتداءات الإلكترونية التي تحدث على البنك
					ينشر البنك تقارير مفصلة بخصوص الإعتداءات الإلكترونية
					تتبنى إدارة البنك اتفاقيات تعاون مشترك مع شركات عالمية مزودة لخدمات وبرامج وأجهزة حماية إلكترونية ضد الاعتداءات الإلكترونية
					تعيّن إدارة البنك مديراً للأمن السيبراني ويتمتع بصلاحيات ونفوذ للتصدي واتخاذ القرارات عند حدوث اعتداءات إلكترونية

المحور الثاني: استخدام البطاقات المصرفية، ضع إشارة (√) في المربع المناسب لاختيارك:

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
					يوفر البنك ضمانات أو تعويضات ضد أي خسائر تحصل للعملاء نتيجة للحوادث الإلكترونية الواقعة على البطاقات المصرفية
					الانتشار الواسع لأجهزة الصراف الآلي التابع للبنك يزيد استخدام البطاقات المصرفية من مستوى الأمن والثقة في بالنسبة للعميل
					تقدم عملاء بشكاوى واستفسارات بخصوص حواادث أو أحداث مريبة وقعت على بطاقتهم المصرفية في الأونة الأخيرة
					تنوع البطاقات المصرفية واستعمالها يقلل من حجم الحوادث الواقعة عليها
					يقوم البنك دائما بتطوير آليات زيادة حماية استخدام البطاقات المصرفية
					إن حدوث خلل في شبكة الإنترنت أو تعطل النظام يزيد من عدد حوادث البطاقات المصرفية

				تتبنى إدارة البنك خطة طوارئ للتعامل مع أي حدث تقني قد يصيب خدمات البطاقات المصرفية
				يتردد بعض العملاء من استخراج بطاقات مصرفية بسبب القلق أو التخوف من وقوع حوادث تقنية أو إلكترونية عليها
				يطرح العملاء افكاراً ومتطلبات لزيادة مستوى الأمان والحماية لبطاقاتهم المصرفية
				يفعل البنك اسلوب الاتصال الفوري مع العملاء (من خلال مركز اتصال العملاء عند تلقي اشارة مشتريات إلكترونية بمبلغ يفوق ال حسب سياسات البنك) دينار مثلاً
				يطبق البنك سياسة الايقاف الفوري للبطاقة المصرفية اذا وقع عليها استخدام خارج الوطن لحين التحقق من العميل
				استلام العميل للبطاقة المصرفية من خلال شركة نقل يُفقد العميل فرصة التدريب والارشاد من قبل موظف البنك للتعامل الآمن مع البطاقات المصرفية

					إن توجهات وسياسات البنك في حث العملاء على استخدام البطاقات المصرفية لخفض عدد المراجعين يزيد من احتمال وقوع حوادث إلكترونية على البطاقات المصرفية
					إن إضافة خدمات وميزات في استخدام البطاقات المصرفية كربطها بالهاتف المحمول أو إتمام عملية الدفع بمجرد اقترابها من جهاز الخصم المباشر يزيد من خطر الحوادث الإلكترونية عليها
					يؤخذ بعين الاعتبار وضمن سياسات إصدار البطاقات المصرفية الحوادث المحتملة
					يمكن ويشجع البنك العملاء من استخدام البطاقات المصرفية للدفع مقابل خصم من خلال نقاط البيع

مع خالص التقدير والاحترام

Mid-Ocean University

College of Management

Department of Risk Management



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

Preparation:

Noura Mutlaq Alkhamsi

233001453

Supervision:

Dr. Al-Faisal Abdul Hamid Mohammed Hassan

Dr. Fayez Jarad

1445-2024