DOI: https://doi.org/

http://journal.jadara.edu.jo

# The Efficiency of a Jordanian Version of the Adolescents› Self-Concept Scale on a Sample of Individual With Disabilities in Jordan

**Sahel mohammad soudi albawaneh[*1] - Ghasaan SalimSalih Altaalib [*2]**

The Impact of Cybersecurity Risks on The Use of Bank Cards at Islamic Banks Operating in Jordan

*Correspondence: sahel.albawaneh@safwabank.com

Received : 01 / 04 / 2023

Accepted : 16 / 06 / 2023

## Abstract

The study examined the potential impact of cyber security risks (information security risks, mobile application risks, operational risks, and cyber-attack risks) on the use of bank cards in Islamic banks operating in Jordan, by following a quantitative, descriptive, and analytical approach. The questionnaire was used to collect data from the upper, middle and lower managements in the targeted departments and sections in Islamic banks, which numbered (100) individuals. By using descriptive and inferential statistical strategies, it was concluded that there is a significant impact of cyber security risks and its dimensions in the use of bank cards in Islamic banks operating in Jordan. The study recommended increasing the interest of Islamic bank administrations in developing and implementing the necessary cyber security measures concerned with protecting customer data and preventing any security accidents and disasters from occurring.

**Keywords:** Cyber Security Risks, Information Security Risks, Mobile Application Risks, Operational Risks, Cyber-Attack Risks, Bank Cards, Islamic Banks (7 words).

DOI: https://doi.org/

http://journal.jadara.edu.jo

# أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن

سهل محمد سودي البواعنة*[1] - غسان سالم صالح الطالب [2]*

المحاسبة - كلية المال والأعمال - جامعة العلوم الإسلامية العالمية

*للمراسلة: sahel.albawaneh@safwabank.com

استلام البحث: 01 / 04 / 2023

قبول البحث: 16 / 6 / 2023

## الملخص

تناولت الدراسة الأثر المحتمل لمخاطر الأمن السيبراني (مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية) في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن، وذلك باتباع منهج كمي وصفي تحليلي. واستُخدمت الاستبانة لجمع البيانات من الإدارات العليا والوسطى والدنيا في الإدارات والأقسام المستهدفة في البنوك الإسلامية وعددهم (100) فرد. وباستخدام الاستراتيجيات الإحصائية الوصفية والاستدلالية تم التوصل إلى وجود أثر معنوي لمخاطر الأمن السيبراني وأبعاده في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن. وأوصت الدراسة بزيادة اهتمام إدارات البنوك الإسلامية بتطوير وتنفيذ إجراءات الأمن السيبراني اللازمة والمعنية بحماية بيانات العملاء ومنع وقوع أية حوادث وكوارث أمنية.

**الكلمات المفتاحية:** مخاطر الأمن السيبراني، مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية، البطاقات المصرفية، البنوك الإسلامية (7 كلمات).

## أولاً: الإطار العام

### 1-1 المقدمة

يعد عنصر الأمن والاستقرار من عنصران أساسيان في الحياه، إذ لابد من توافرهما حتى تتمكن الدولة من المحافظة على مواطنيها، لذلك يعد الأمن والخوف مصطلحان متناقضان من حيث المفهوم والمبدأ، وقد ذكرت آيات كثيرة عن أهمية الأمن للناس لقوله تعالى: «وَلَيُبَدِّلَنَّهُمْ مِنْ بَعْدِ خَوْفِهِمْ أَمْنًا» (النور: 55) وقوله: «سِيرُوا فِيهَا لَيَالِيَ وَأَيَّامًا آمِنِينَ» (سبأ: 18) وقول الله تعالى: «وَإِذْ جَعَلْنَا الْبَيْتَ مَثَابَةً لِلنَّاسِ وَأَمْنًا» (البقرة: 125)، ومن أهم مظاهر الأمن في «الشريعة الإسلامية المحافظة على خصوصية الأموال».

ومع الإنفجار المعرفي والتطورات في بيئة الأعمال والاقتصاد، أصبح استخدام الأنظمة الإلكترونية والتكنولوجية عماد الاقتصاد العالمي وخصوصا في القطاع المالي والمصرفي، ومع تزايد هذا التطور زاد حجم التحدي والجرائم الإلكترونية والتي تسمى في الوقت الحالي بالجرائم السيبرانية، والتي هي نتاج التطورات التكنولوجية المُدارة بطريقة غير شرعية كالأختراق والقرصنة وعمليات النصب والاحتيال للمعلومات المصرفية، لذلك عملت البنوك على إعداد برامج تعمل على توفير الحماية لمعلوماتها من «الهجمات السيبرانية التي تهدد النظام المالي بأكملهه، وبالتالي تتكدس خسائر هائلة عند حدوث هذه الهجمات، وهذا أدى إلى ظهور الأمن السيبراني، بحيث تضع كل مؤسسة مالية استراتيجية الأمن السيبراني الخاصة بها وفقًا لممارسات إدارة المخاطر المستندة إلى المبادئ، في حين تقوم الجهات الرقابية بمراجعة هذه الاستراتيجيات كجزء من تقييمها للممارسات الشاملة لإدارة المخاطر في البنوك؛ لذلك عملت هذه الدراسة إلى اقتراح نموذج يمكن استخدامة لتقييم أثر «مخاطر الأمن السيبراني في استخدام البطاقات المصرفية» في البنوك الإسلامية العاملة في الأردن، وتحديد مكان ضعفها.

### 2-1 «مشكلة وأسئلة البحث»

تخضع المؤسسات المصرفية إلى تحديات كبيرة نتيجة التقدم العلمي والتطور الرقمي والتكنولوجي وظهور المخاطر والهجمات السيبرانية؛ وبالتالي فإن إدارة البنوك قد تواجه صعوبة في عمل نظام أمن للهجمات السيبرانية يواكب تلك المخاطر الموجهة إلى هذه البنوك وعملائها، إذ يرى الباحث أن «مشكلة البحث تتجسد في التساؤلات التالية»:

**السؤال الرئيس:** ما أثر مخاطر الأمن السيبراني بأبعادة الأربعة (مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية) في استخدام «البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن»؟

وينبثق من هذا التساؤل التساؤلات التالية:

1. «ما أثر مخاطر أمن المعلومات في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن؟»
2. «ما أثر مخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن؟»
3. «ما أثر المخاطر التشغيلية في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن؟»
4. «ما أثر مخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن؟»

### 3-1 أهمية البحث

**تتضح الأهمية لهذا البحث من جانبين:**

**1-3-1 «الأهمية النظرية:** تنبع الأهمية النظرية للبحث من حداثة الموضوع وأهميته البالغة في البنوك الإسلامية العاملة في الأردن»، حيث يعمل على بيان تأثير مخاطر الأمن السيبراني في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن، وحسب علم الباحث أنه لم يتم دراسه هذا الموضوع بشكل وافٍ، لذلك يأمل أن يشكل هذا البحث إضافة علمية للباحثين لإجراء أبحاث ودراسات ذات صلة بالموضوع.

**2-3-1 «الأهمية العملية:** تنبع الأهمية العملية لهذا البحث من أهمية البنوك الإسلامية العاملة في الأردن بتوفير الأموال لزيادة التنمية الاقتصادية والاجتماعية»، حيث تعمل البنوك بصفة خاصة على تجميع الودائع من خلال المودعين وتوظيف هذه الودائع، وأهمية الأمن السيبراني الذي يمتاز بالحداثة، حيث أصبح مهما في شتى مجالات العمل؛ لما له من دور في «المحافظة على سرية المعلومات في البنوك الإسلامية العاملة في الأردن» والتي بدورها تساعد على تحقيق احتياجات ورغبات العملاء، كما تكمن الأهمية العملية للبحث من زيادة حدة المنافسة في تطبيق الأمن السيبراني في البنوك التي تمتاز بالكفاءة من أجل استقطاب عملاء جدد. لذلك جاءت فكرة هذا البحث لما توفره هذه البنوك من مميزات في شتى المجالات والتي من أهمها المحافظة على الوصول وسرية وأمن البيانات والمعلومات في استخدام البطاقات المصرفية، ويأمل الباحث أن تدعم النتائج والتوصيات صناع القرار «في البنوك الإسلامية العاملة في الأردن».

### 4-1 «أهداف البحث»

يتمثل الهدف العام للبحث في التعرف على أثر مخاطر الأمن السيبراني بأبعادة الأربعة: (مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية) في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن. كما يسعى البحث إلى تحقيق الأهداف التالية:

1. توضيح متغيرات الدراسة والكشف عن مضمونها والعلاقات فيما بينها ضمن إطار نظري مفاهيمي.
2. بيان أثر «مخاطر أمن المعلومات في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن».
3. بيان أثر «مخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن».
4. بيان أثر «المخاطر التشغيلية في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن».
5. بيان أثر «مخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن».

### 5-1 «فرضيات البحث»

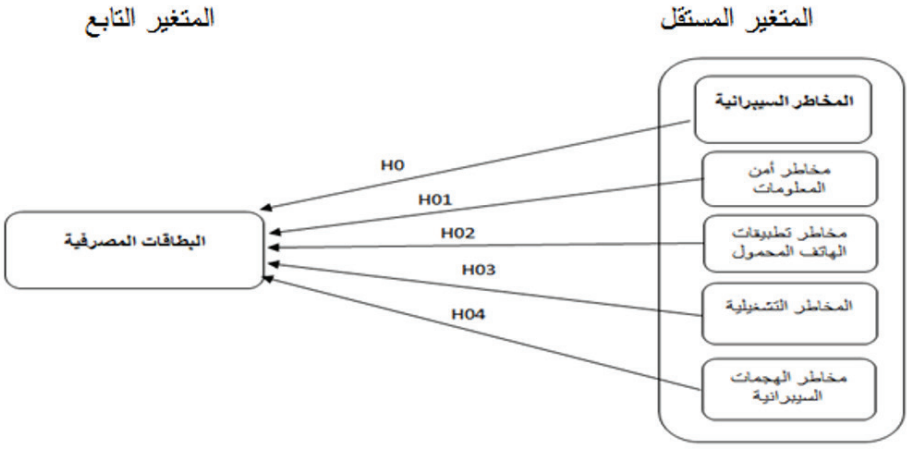
**تسعى الدراسة إلى اختبار الفرضيات الآتية:**

**HO:** «لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤0.05) لمخاطر الأمن السيبراني بأبعادة الأربعة «مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية» في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن».

**«وقد اشتق من هذه الفرضية الفرضيات التالية»:**

- **Ho1:** «لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤0.05) لمخاطر أمن المعلومات في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن».
- **Ho2:** «لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤0.05) لمخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفي في البنوك الإسلامية العاملة في الأردن».
- **Ho3:** «لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤0.05) للمخاطر التشغيلية عبر الانترنت في استخدام البطاقات المصرفي في البنوك الإسلامية العاملة في الأردن».
- **Ho4:** «لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤0.05) لمخاطر الهجمات الإلكترونية في استخدام البطاقات المصرفي في البنوك الإسلامية العاملة في الأردن».

### 6-1 الأنموذج العام للبحث




الشكل (1) أنموذج الدراسة (المصدر: من إعداد الباحث بالاعتماد على manoj, 2021; Al (Duhaidahawi, 2020

### 7-1 حدود البحث

- **الحدود المكانية:** الإدارات الرئيسة للبنوك الإسلامية العاملة في الأردن، وعددها (4) بنوك.
- **الحدود البشرية:** «الأفراد العاملين في المستويات الإدارية العليا والوسطى والدنيا في الإدارات الرئيسة في البنوك الإسلامية العاملة في الأردن».
- **الحدود العلمية:** أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن.

## 2- الاطار النظري والدراسات السابقة

### 2-1 الأمن السيبراني ومخاطره

يعد الأمن الركيزة الأساسية لأي مجتمع، حيث إنه لا يمكن تكوين نشاط ونموه دون وجود الأمن؛ لذلك يعمل الأمن السيبراني على توجيه تصرفات وقرارات الأفراد في المؤسسات والبنوك وإرشادها ومراقبتها وتحسينها لرفع الكفاءة، ويمكن تعريف الأمن السيبراني بأنه: ذلك «النشاط الذي يعمل على تأمين حماية الموارد البشرية والمالية التي ترتبط بتقنيات المعلومات والاتصالات، ويعمل على تقليل الخسائر عند حدوث خطر معين أو تهديدات معينة» (جبور، 2016).

ويرى (Canelón & Leal, 2020) ان الأمن السيبراني هو «مصفوفة من الأدوات التنظيمية والتقنية والإجرائية، والممارسات الهادفة إلى حماية الحواسيب والشبكات وما بداخلها من بيانات من الاختراقات أو التلف أو التغيير أو تعطل الوصول للمعلومات أو الخدمات ويعد توجها عالميا سواء أكان على مستوى الدول أم المنظمات الحكومية أم الشركات، « في حين (Eaton & Grenier, 2019) أوضح ما يتميز الأمن السيبراني من خصائص متمثلة «بالخصوصية والسرية في البيانات والمعلومات ومنع الوصول غير المصرح له مما يجعله قادراً على التصدي للمخاطر والتهديدات السيبرانية السريعة والغامضة».

ويرى الباحث أن الأمن السيبراني عبارة عن آليات منتظمة وتقنيات، يمارسها الموظفون لحماية المعلومات والبيانات في الحواسيب والشبكات من التلف والاختراق أو التعطيل أو التلاعب بها بأي شكل من الأشكال.

إذ تعتمد الأنشطة والخدمات المصرفية على تقديم أفضل خدمة للعملاء، «لذلك أصبح لزاما في ظل التطورات التكنولوجية» أن يتم تقديم الخدمة عبر شبكات الإنترنت، لذلك تواجه البنوك أنواعا من مخاطر الأمن السيبراني الخاصة بممارسة الأعمال والنشاطات داخل البنك، والتي تأخذ ابعادا كثيرة، وقد تم اختيار أربعة من هذه الأبعاد، وهي: مخاطر أمن المعلومات، ومخاطر تطبيقات الهاتف المحمول، والمخاطر التشغيلية، ومخاطر الهجمات السيبرانية (Jin & Fei-Cheng, 2005).

**-1 «مخاطر أمن المعلومات»:** وهي أي تهديد أو نشاط من جهة غير مصرح لها أو عن طريق أفراد داخلين على المعلومات أو أنظمة المعلومات، والذي يهدف فيه للوصول أو الاستخدام المباشر أو غير المباشر أو الإفشاء أو التعديل أو الاخلال أو التدمير للمعلومات أو الأنظمة المعلوماتية؛ لذا فهو تهديد لنظام البنك وعملياته وخصوصيته وجاهزيته (Jin & Fei-Cheng, 2005). ويستوجب على البنوك وضع نظام معلوماتي يحميها ويحمي العميل من الاختراق أو الهجمات السيبرانية، وعلى البنوك توفير سبل وأدوات حماية لأنظمتها، والتي تتجسد في الحماية المادية والأدائية والتقنية (دوادي، 2020)، واتباع استراتيجيات شاملة للحماية الوقائية من هذه المخاطر والتهديدات وذلك من خلال أن تتضمن إدارة أمن المعلومات نظام وأداوت حماية داخلية ضد أنشطة الإساءة الداخلية أو أي جهة يمكن لها الوصول للمعلومات، وبناء استراتيجيات واضحة لحماية أمن المعلومات على مستوى العملاء والعمل على استخدام برامج مضادة للفايروسات والاختراق، وتدريب الموظفين ذي الكفاءات والخبرات لحماية نظام أمن المعلومات (عديسة وآمال، 2018).

**-2 مخاطر تطبيقات الهاتف المحمول:** وهي «التهديدات أو الأنشطة الخارجة، مثل: الاحتيال الرقمي أو الوصول للمعلمات السرية أو الاختراق التطبيق أو البرامج الضارة التي تصيب الأنظمة الأساسية للجهاز المحمول» (Maharjan & Chatterjee, 2019)، ويرى بعض الباحثين أن الخدمات البنكية والمصرفية عن طريق تطبيقات الهاتف المحمول تشهد إقبالاً كبيراً، إذ إن العملاء الذين استخدموا هذه التطبيقات وجدوا نوعا من الابتكار التكنولوجي (مبارك، واخرون، 2022)، لذلك تعمل البنوك جاهدة على ملاحقة التطورات التقنية والابتكار في تقديم الخدمات ومواكبة الحداثة لبناء ميزة تنافسية؛ لإن الثبات على المستوى التقليدي لا يعطي نتائج جيدة في بناء ميزة تنافسية (نابي، 2019)، ويرى بعض من الباحثين أن هذه المخاطر تجعل تبني فكرة تطبيقات الهاتف المحمول للبنوك أمرا سلبيا يضعف من هذه الميزة التكنولوجية، وذلك بسبب مخاوف بعض العملاء من «المخاطر السيبرانية والقرصنة والاختراق» (Al-Jabri & Sohail, 2012)

**-3 «المخاطر التشغيلية»:** «وهي تلك المخاطر التي تنشأ عند ممارسة البنك للأنشطة المختلفة عبر شبكات الإنترنت والتي تنتج عنها مخاطر الخسارة المالية أو تعطل الأعمال أو الأضرار بسمعة البنك من حدث يؤثر على الأصول المعلوماتية أو الحاسوب أو موارد الاتصالات» (Al-Jabri, & Sohail,2012). وتشكل هذه المخاطر والتي تنشأ من مخاطر الأمن السيبراني جزءا صغيرا من اجمالي الخسائر التشغيلية للبنك، وقد تمثل حصة كبيرة من إجمالي القيمة التشغيلية المعرضة للخطر (Aldasoro et al., 2020)، لذلك صنف (العشعوش وغضبان، 2016) أنواع هذه المخاطر إلى:

- **إدارة العمليات:** وتحدث بسبب المعالجات الخاطئة والمغلوطة لعمليات وحسابات العملاء والعمليات اليومية مما ينتج عنها خسائر.
- **العنصر البشري:** وهو ما يتعلق بأخطاء الموظفين بقصد أو بغير قصد، وتشمل أيضا الغش أو إساءة استعمال الأصول والتحايل على القانون والسياسات والاختلاس المالي وإعداد التقارير الخاطئة.

- **الأنظمة الآلية والاتصالات:** تنشا بسبب فشل أو تعطل الأنظمة التكنولوجية والاتصالات بسبب البنية التحتية أو عطل أو خلل ما.
- **أحداث ذات صلة بالأنظمة الخارجية:** والتي ترتبط بالاحتيال الخارجي أو الأخطار السيبرانية أو تغيير القوانين أو الكوارث الطبيعية.

**-4 «مخاطر الهجمات السيبرانية»:** وهي التهديدات التي تمارس على هيئة هجمات إلكترونية ضد أنظمة الكمبيوتر والمعلومات والبرامج والبيانات، وتؤدي إلى إحداث ضرر أو تدمير أو شلل لأنظمة البنك والبيانات والذي ينتج عنها خسائر مالية كبيرة واختلال في عمل البنك ونشاطاته (حجاج، 2013). حيث إن بعض القراصنة يعملون على استغلال متعمد لأنظمة الكمبيوتر والمؤسسات والشبكات المعتمدة على التكنولوجيا، وتَستخدم الهجمات الإلكترونية تعليمات برمجية ضارة لتغيير الرموز أو المنطق أو البيانات، مما يعرضها لخطر الجرائم الإلكترونية. ويُعرف الهجوم السيبراني أيضا باسم هجوم شبكة الكمبيوتر (Kim et al., 2014).

لذلك أصبح لزاما على البنوك أن تدرج في مهامها إدارة «المخاطر السيبرانية» ضمن إدارة المخاطر، وتتضح غاية ذلك في تعريف إدارة مخاطر الأمن السيبراني التي تعرف بأنها عملية مستمر لتحديد وتحليل وتقييم ومعاجلة وردع تهديدات الأمن السيبراني للبنك، حيث إن لكل فرد في البنوك دور يلعبه في هذه العملية، كما وأن هناك ثغرة ضعف في أن قادة إدارة المخاطر يفتقرون إلى المنظور الشامل الضروري للتصدي للمخاطر بطريقة شاملة ومتسقة (Knowles et al., 2015).

وعلى البنوك تحديد ما يلي للتمكن من تقييم مخاطر الأمن السبرانية التي قد تواجهها (تعليمات البنك مركزي، 2018):

أ. الوظائف والعمليات الحرجة.

ب. أصول المعلومات وفهم عملياتها وإجراءاتها ونظمها وما يتعلق بها من موارد ونظم وسبل الوصول إليها.

ج. تصنيف الوظائف والعمليات الحرجة وأصول المعلومات من حيث أهميتها وحساسيتها، ومراجعة وتحديث التصنيفات بشكل مستمر.

### 2-2 البطاقات المصرفية في البنوك

كان أول ظهور للبطاقات المصرفية في «الولايات المتحدة الامريكية عام 1914»، وذلك لتسديد المدفوعات عن الزبائن المميزين لتسهيل معاملاتهم، واختصار الوقت عليهم، إضافة إلى ما فيها من ميزة الالتزام بمهلة معينة لدفع الالتزامات المستحقة، وقد لحق ذلك إصدار بعض المحلات التجارية هذه البطاقة، وبقي العمل بها دارجاً حتى الحرب العالمية الثانية (أبو بكر، 1996).

ويمكن تعريف البطاقات المصرفية بأنها بطاقات بلاستيكية أو من لدائن أخرى ذات أجسام متساوية بمواصفات فنية عالمية محددة ومميزة ، بحيث يصعب تزويرها أو عمل مثلها، وتصدر هذه البطاقات من البنك المعني ضمن آلية معينة وشروط محددة بينها وبين الشركات العالمية لهذه البطاقة مثل شركة فيزا أو ماستر كارد (www.arabnak.com)، وبالتالي تعد هذه البطاقة عبارة عن أداة داخلية مكونة من بطاقة بلاستيكية تحتوي على شريط ممغنط يسجل عليها جميع بيانات الحساب الجاري، بالإضافة إلى رقم سري يستخدم خلال ماكينات آلية معقدة توجد خارج مبنى المصرف، ويتصل الصراف الآلي مباشرة بالحاسب الآلي المركزي للمصرف، ويحصل الصراف الآلي على بيانات العميل المدونة على البطاقة فور إدخال رقم سري خاص (السيسي، 1998) ولهذه البطاقات ميزات خاصة، إذ إنها تُصدر لعملاء البنك والذين يمتلكون رصيد حسابات لدى البنك المُصدر، ويتم الخصم فور استخدامها، وهي محلية الاستخدام وقد يمكن استخدامها دولياً حسب ربط أجهزة الصرف بالدولة الأخرى، وتتيح لحاملها الصرف بها من شبكات البنوك الأخرى المُشاركة في تأمين أجهزة الصرف على الطرقات (ابو زيد، 1999).

**وتنقسم البطاقات إلى ما يلي:**

**- البطاقات الائتمانية:** كان أول ظهور لهذة البطاقات في الدولة عام 1982، حيث تم اصدارها عن طريق بنك البتراء، والذي كان معنياً بإصدارها بترخيص من شركة فيزا العالمية ثم تلاه بنك القاهرة عمان، وعليه فإن بطاقات الائتمان تتيح لحاملها استعمال الائتمان في حدود الاتفاق المبرم بينه وبين مصدر البطاقة (البنك)، فهي تسمح لحاملها بدلا من تسوية حسابه فورا بأن يقوم خلال أجل متفق عليه بتسديد ثمن مشترياته على دفعات، وذلك في حدود مبلغ مكشوف معين مسبقا، فهذه البطاقة أن حاملها مدين، إلا أنه بحاجة إلى الحصول على سلع وخدمات يقوم البنك بتسويتها مع التاجر، ثم يسترد ما دفعه بعد ذلك من حامل البطاقة (Sally, 1999). فالمفهوم الأساس لمعنى الائتمان هو التسليم الفوري للسلع مقابل الوفاء المؤجل، وبالتالي يمكن تعريفها بأنها عن قطعة رقيقة مستطيلة الشكل من البلاستيك أو المعدن صادرة عن مصرف أو شركة خدمات مالية تسمح لحاملها باقتراض الأموال لدفع ثمن السلع والخدمات مع التجار المتعاملين بها، وتفرض بطاقات الائتمان شرطا يقضي بأن يسدد حاملو البطاقات الاموال المقترضة بالاضافة إلى أي فائدة مطبقة، بالإضافة إلى أي رسوم إضافيه متفق عليها، أما بالكامل بحلول تاريخ الفاتورة أو بمرور الوقت (Curti et al., 2019).

**- «البطاقات غير الائتمانية»:** «هي البطاقات التي يستطيع حاملها الحصول على خدمات البنك» المصدر لها ضمن حدود رصيد حسابه دون ترتب أي ذمم على مستخدميها، ويستطيع العميل استعمالها في أي وقت يريد من خلال الصراف الآلي أو نقاط البيع والمشتريات أو تحويل الأرصده ضمن حساباته أو ربما بالشراء من خلال الإنترنت. أي أنها تسمح لحاملها بإجراء أي معاملة المالية ضمن حدود الرصيد المتوفر في البنك، إذ تتميز هذه البطاقات بسهولة الحصول عليها والاستخدام، ولا يسمح هذا النوع من شراء السلع أو الخدمات بالدين أو على الحساب. (www.arabnak.com).

### 3-2 الدراسات السابقة

قام (الذنيبات، 2019) بدراسة التكيف مع «المخاطر السيبرانية» والتعرف على حوكمة الأمن السيبراني لحماية الشركات أعمالها ونشاطها الاقتصادي بما يتوافق مع التطورات والتقنيات والمتطلبات القانونية، الأمر الذي يحتم على الشركات أن تضع أولوياتها ضمن سياق توجه إلى حماية الأمن السيبراني والفضاء السيبراني، وتوصلت الدراسة إلى أن الالتزام بالأمن السيبراني من قبل الشركات المالية والائتمانية والتقنية يساعد على تنظيم عملها، وأوصت الدراسة بتطبيق سياسة الأمن السيبراني وتطبيق برامج الأمن السيبراني بحيث يكون متكاملا مع الإطار العام لإدارة «مخاطر تكنولوجيا المعلومات» والاستمرار بتحديثه وتطويره، وضمان توفير وتحديث سجل خاص بهذا النوع من المخاطر وتحديثه ليكون متوافقا مع ملف الأخطار في تكنولوجيا المعلومات. ووضحت دراسة (إسماعيل، 2019) تقديرات التكلفة للهجمات السيرانية في القطاعات المالية لدى «صندوق النقد الدولي» من واقع الخسائر المحققة جراء هذه الهجمات في 50 دولة على مستوى العالم، حيث تبين أن ارتفاع الهجمات السيبرانية في القطاعات المالية مقارنةً بالقطاعات الأخرى بنسبة (65%) وفق تقديرات البنك الدولي، وأن كلفة هذه الهجمات فيها قدّرت بنحو (270 - 350) مليار دولار سنويا حال تزايد مساحة انتشارها، وأوصت الدراسة بتبني القطاعات المالية استراتيجية «موثوقة ومعززة للأمن السيبراني».

بينما كشفت دراسة (الزيود، 2020) عن «مفهوم المخاطر السيبرانية» من كافة الجوانب وأنواع التهديدات ومجالاتها، وناقش أدوات وأساليب تقييمها وإدارتها في البنوك الأردنية، والتي تهدف للمحافظة على سلامة البنوك وأمن المعلومات، وأظهرت النتائج التزام البنوك الأردنية بالسياسات الخاصة بأمن المعلومات وسياسة الأمن السيبراني وتطبيق جميع تعليمات البنك المركزي الأردني، وقيام «البنك المركزي الأردني بنشر دليل الحاكمية المؤسسة لتكنولوجيا المعلومات ضمن التقارير السنوية».

وبينت دراسة (Al Duhaidahawi, 2020) أن ازدياد حجم المعلومات يؤدي إلى زيادة حجم المخاطر وبالتالي أصبحت الحاجة لزيادة أمن المعلومات السيبرانية أكثر إلحاحا، حيث إن كل زيادة وحدة واحدة في أمن المعلومات يرفع من درجة الحماية، وبالتالي تخفيف الخطر السيبراني تجاة أمن المعلومات. وحاولت دراسة (Manoj(a), 2021) المساعدة في تحديد آليات ووسائل من شأنها مواجهة أو تخفيف أضرار الأخطار السيبرانية على البنوك، وخصوصا بعد تزايد حدتها ونوعها، مما جعل الأمن السيبراني مطلبا مشروعا ورئيسا لدى البنوك بإعتبار معلوماتها تعد من المعلومات الحساسة، وكان أهم النتائج أن أي نظام أمن سيبراني واحد سيكون غير كافٍ للحماية من المخاطر السيبرانية، إذ إنها يجب أن تكون منظومة كاملة تتطور باستمرار وفق تطورات المتسارعة للمخاطر السيبرانية.

وناقشت دراسة (Manoj (B), 2021) دور البنوك في النظام المالي والبناء الاقتصادي لاي دولة، ومقدار التنافس الكبير بينها في تقديم الخدمات المصرفية المتميزة، ومن البديهي

أن للتكنولوجيا دورا فاعلاً في المنافسة بالصناعة المصرفية لما لها من فوائد في تعزيز رضا العملاء، وزيادة الخدمات المصرفية، وبالمقابل فهي معرضة بشكل كبير «للمخاطر السيبرانية»؛ لذلك تعمل البنوك على اتباع سياسات وتشريعات لتقليل هذه المخاطر.

وأفادت دراسة (Qasaimeh & Jaradeh, 2022) أن التطبيق الفعال للأمن السيبراني لا يتم إلا من خلال الخبرات والمعارف لدى موظفي البنوك، ووجود عمليات صيانة دورية للأجهزة المستخدمة لديها، وتوفير الأجهزة والمعدات والبرامج الحديثة، حيث تسهم هذه التقنيات والتطبيقات في تعزيز فاعلية الأمن السيبراني، لذلك بات من الضروري اعتماد البنوك الأردنية بشكل أكبر على الأنظمة المتطورة، بحيث يمكّن البنوك من استخدام أجهزة ومعدات حاسوبية وبرمجيات تمتاز بالحداثة، وبالتالي تزيد اعتمادية هذه البنوك على التطبيق الفعال للأمن السيبراني لمتابعة سير الأعمال والمهام وفقاً لإستراتيجياته، وتجنب «الهجمات والمخاطر السيبرانية».

## ثالثاً: منهجية البحث

### 1-3 منهج البحث

استند البحث على منهجٍ كميٍّ وصفيٍّ تحليليٍّ؛ لوصف وتحليل «مخاطر الأمن السيبراني» وأثرها في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن، حيث تم تحليل البيانات المجمّعة من خلال الإستبانة، «وإيجاد العلاقة بين المتغيرات والعمليات التي تتضمنها والآثار الناتجة عنها».

### 2-3 مجتمع وعينة البحث

«تكوّن المجتمع من البنوك الإسلامية العاملة في الأردن» وعددها (4) بنوك، وهي: (البنك الإسلامي الأردني، بنك صفوة، البنك العربي الإسلامي الدولي، ومصرف الراجحي). وقد اشتملت عينة الدراسة على الإدارات الرئيسة للبنوك الإسلامية العاملة في الأردن، والتي يقع مقرها في العاصمة عمان.

### 3-3 وحدة التحليل

تكونت وحدة التحليل في البحث من «موظفي الإدارات العليا والوسطى والدنيا في الإدارات الرئيسة في البنوك الإسلامية العاملة في الأردن»، والممثلين في -1 الإدارة العليا (المدراء العامين ومساعديهم)، -2 الإدارة الوسطى (مدراء الدوائر)، -3 الإدارة الدنيا (رؤساء أقسام) كل من قسم تكنولوجيا المعلومات وخدمات العملاء والمالية والتسهيلات والمخاطر والأمن السيبراني. ونظراً لصعوبة الحصول على عددهم الحقيقي، قام الباحث بتوزيع (25) استبانة في كل بنك لغايات استهداف أكبر قدر منهم، حيث تم توزيع (100) استبانة. وقد تمكن الباحث من استرداد (89) استبانة صالحة لغايات التحليل.

### 4-3 طرق جمع البيانات

تنوعت المصادر المستخدمة في جمع البيانات اللازمة لتحقيق الأهداف المحددة بين مصادر ثانوية ومصادر أولية، حيث اشتملت «المصادر الثانوية على مقالات ودوريات علمية محكمة، وأبحاث وتقارير ونشرات وأطر نظرية، ارتبطت بالمواضيع والأبعاد والمتغيرات قيد الدراسة.

بينما اشتملت المصادر الأولية على أداة الدراسة والمتمثلة في الاستبانة، والتي تم تصيمها لتحقيق الغرض البحثي، وقد ضمت الاستبانة (36) فقرة تعبر عن الأبعاد والمتغيرات قيد الدراسة، بالإضافة إلى مجموعة من الأسئلة التي تقيس المعلومات العامة لعينة الدراسة، وكما يأتي:

- **الجزء الأول:** المعلومات العامة، والذي تضمن: («مدة الخدمة، المؤهل العلمي، المسمى الوظيفي، وعدد الدورات المتخصصة في مجال الأمن السيبراني»).
- **الجزء الثاني:** «مخاطر الأمن السيبراني»، والذي تضمن: (مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، ومخاطر الهجمات الإلكترونية)، وقد احتوى هذا الجزء على (24) فقرة، تعبر عن الأبعاد الفرعية، وبواقع (6) فقرات للبعد الواحد.
- **الجزء الثالث:** «استخدام البطاقات المصرفية»، وقد احتوى هذا الجزء على (6) فقرات.

### 5-3 الاستراتيجيات الإحصائية

تنوعت الاستراتيجيات الإحصائية المستخدمة بين المقاييس الوصفية والمقاييس التحليلة، والتي تم تطبيقها من خلال البرنامج الإحصائي «SPSS»:

#### أولاً: المقاييس الوصفية

وهي مجموعة من المقاييس التي تم استخدامها لوصف الأبعاد والمتغيرات، والتي اشتملت على:

1. «المتوسطات الحسابية والانحرافات المعيارية والتكرارات والنسب المئوية»: لوصف الأبعاد والمتغيرات والفقرات المخصصة لها، ووصف المعلومات العامة لعينة الدراسة.
2. الأهمية النسبية: وهو مقياس وصفي يقيس مستوى الاهتمام بعنصر محدد، وقد حدد وفق الصيغة الآتية وبالاستناد إلى البدائل المحددة الإجابة عن كل فقرة (الحد الأعلى = 5، الحد الأدنى = 1)، وبالاعتماد على (3) مستويات: أهمية منخفضة، أهمية متوسطة، وأهمية مرتفعة.

$$\text{الأهمية النسبية} = \frac{\text{الحد الأعلى للإجابة – الحد الأدنى للإجابة}}{\text{العدد الكلي للمستويات}} = \frac{5 - 1}{3} = 1.33$$

وتعد الأهمية منخفضة إذا تراوح الوسط الحسابي بين (1.00 - أقل من 2.33)، وتعتبر متوسطة إذا تراوح الوسط الحسابي بين (2.33 - أقل من 3.66)، بينما تعد الأهمية مرتفعة إذا تراوح الوسط الحسابي بين (3.66 - 5.00).

**ثانياً: المقاييس التحليلية**

وهي مجموعة من المقاييس التي تم استخدامها في إجراء المعالجات التحليلية لأداة الدراسة واختبار الفرضيات، والتي اشتملت على:

1. معامل الاتساق الداخلي ألفا كرونباخ: لقياس درجة الثبات والموثوقية في أداة الدراسة.
2. معامل الارتباط الخطي المتعدد: للتحقق من درجة الارتباط بين أبعاد المتغير المستقل.
3. تحليل الانحدار الخطي المتعدد والمتدرج: لاختبار فرضيات الدراسة.

**رابعاً: معالجة البيانات وتحليلها واختبار الفرضيات**

**1-4 اختبار الثبات والموثوقية في أداة الدراسة**

استخدمت الدراسة إختبار ألفا كرونباخ (Alpha Cronbach Test) في تقييم ثبات الأداة المستخدمة في قياس المتغيرات، ويشير كلا من (Sekaran & Bougie 2016) إلى أن أداة القياس تعد مقبولة من الناحية الإحصائية إذا بلغت قيمة المعامل ألفا كرونباخ أكبر من (0.70)، وارتفاع هذه القيمة عن القيمة المقدّرة يدل على ارتفاع الثبات في أداة الدراسة.

**«الجدول (1): قيم معامل ألفا كرونباخ لفقرات أداة الدراسة»**

| الرقم | البعد والمتغير | «قيمة ألفا كرونباخ» |
|---|---|---|
| 1 | مخاطر أمن المعلومات | 0.809 |
| 2 | مخاطر تطبيقات الهاتف المحمول | 0.828 |
| 3 | مخاطر تشغيلية | 0.771 |
| 4 | «مخاطر هجمات سيبرانية» | 0.829 |
| 5 | «مخاطر الأمن السيبراني» | 0.919 |
| 6 | استخدام البطاقات المصرفية | 0.873 |
| | أداة الدراسة | 0.941 |

بالنظر إلى قيم معامل ألفا كرونباخ الواردة في جدول (1)، «يتبيّن أن جميعها كانت أكبر من القيمة (0.70)»، «مما يشير إلى وجود اتساق بين الفقرات في أداة الدراسة، وموثوقية الأداة وإمكانية استخدامها» لإجراء الاختبارات والتحليلات الإحصائية.

### 2-4 ملاءمة «نموذج الدراسة للأساليب الإحصائية المستخدمة»

لاختبار مدى فعالية نموذج الدراسة في تحليل الانحدارات الخطية، تم إجراء اختبار الارتباط الخطي المتعدد بين المتغيرات، «حيث تشير قيم الارتباط الخطي المتعدد إلى نوع الارتباط بين المتغيرات المستقلة»، ويعد «الارتباط الشبه التام بين المتغيرات» من المشاكل التي تسبب عدم ملاءمة النموذج، إذ أنها تؤدي إلى «تزايد قيمة معامل التحديد R2 عن قيمته الفعلية»، ووفقا لـ Guajarati (2004) فإن «هذه المشكلة تظهر عندما تبلغ قيمة معامل الارتباط بين أي متغيرين مستقلين» مختلفين (0.80) أو أكثر.

**الجدول (2): «مصفوفة ارتباط أبعاد متغير مخاطر الأمن السيبرانيج**

| المتغير | «مخاطر أمن المعلومات» | «مخاطر تطبيقات الهاتف المحمول» | «مخاطر تشغيلية» | «مخاطر هجمات سيبرانية» |
|---|---|---|---|---|
| «مخاطر أمن المعلومات» | 1.000 | | | |
| «مخاطر تطبيقات الهاتف المحمول» | **0.604 | 1.000 | | |
| «مخاطر تشغيلية» | **0.508 | **0.568 | 1.000 | |
| «مخاطر هجمات سيبرانية» | **0.476 | **0.577 | **0.739 | 1.000 |

(**) «دال عند مستوى دلالة 0.01»

بالنظر إلى القيم الواردة في الجدول (2)، يتبين أن «جميع القيم بين المتغيرات المستقلة المختلفة» كانت ما دون (0.80)، مما يشير إلى عدم وجود ارتباط شبه تام فيما بينها، وبالتالي فعالية نموذج الدراسة «لإجراء تحليل الانحدارات الخطية».

### 3-4 «وصف المعلومات العامة»

اشتملت البيانات الديموغرافية الخاصة بأفراد عينة الدراسة على (4) متغيرات، وهي: (مدة الخدمة، المؤهل العلمي، المسمى الوظيفي، وعدد الدورات المتخصصة في مجال الأمن السيبراني)، وقد تم تحليل هذه البيانات وذلك باستخدام أساليب الإحصاء الوصفي المتمثلة في التكرار والنسبة المئوية، وعلى النحو الآتي:

**الجدول (3): «وصف المعلومات العامة لأفراد عينة الدراسة»**

| المعلومات العامة | الفئة | التكرار | النسبة المئوية |
|---|---|---|---|
| مدة الخدمة | «أقل من 5 سنوات» | 5 | 5.6 |
| | «-5أقل من 10 سنوات» | 37 | 41.6 |
| | «-10أقل من 15 سنة» | 25 | 28.1 |
| | «15 سنة وأكثر» | 22 | 24.7 |
| | المجموع | 89 | 100 |

| | | | |
|---|---|---|---|
| المؤهل العلمي | «دبلوم» | 3 | 3.4 |
| | «بكالوريوس» | 52 | 58.4 |
| | «دراسات عليا» | 34 | 38.2 |
| | المجموع | 89 | 100 |
| المسمى الوظيفي | مدير | 1 | 1.1 |
| | مساعد مدير | 2 | 2.2 |
| | مدير دائرة | 32 | 36.0 |
| | رئيس قسم | 54 | 60.7 |
| | المجموع | 89 | 100 |
| عدد الدورات المتخصصة في مجال الأمن السيبراني | دورة واحدة | 22 | 24.7 |
| | دورتان | 13 | 14.6 |
| | ثلاث دورات فأكثر | 5 | 5.6 |
| | لا يوجد | 49 | 55.1 |
| | المجموع | 89 | 100 |

«يشير تحليل المعلومات العامة في الجدول» (3) إلى أن:

1. نسبة الموظفين ممن بلغت خدمتهم «(-5أقل من 10 سنوات)» قد شكلوا أكبر نسبة والتي بلغت (41.6%)، وهذا يدل على اهتمام البنوك الإسلامية بالاحتفاظ بموظفيها.

2. نسبة الموظفين الحاصلين على «المؤهل العلمي (بكالوريوس)» قد شكلوا أكبر نسبة والتي بلغت (58.4%)، وهذا يدل على اهتمام البنوك الإسلامية بتوظيف أصحاب الكفاءات والمعرفة العلمية.

3. نسبة الموظفين من «(رؤساء الأقسام) قد شكلوا أكبر نسبة والتي بلغت (60.7%)»، وهذا قد يعود لحجم المهام التي تقوم بها البنوك الإسلامية وبالتالي تعدد أقسامها وإداراتها.

4. نسبة الموظفين «(غير الحاصلين) على الدورات المتخصصة في مجال الأمن السيبراني» قد شكلوا أكبر نسبة والتي بلغت (55.1%)، وهذا قد يعود لتزايد حجم الأعباء والمهام التي يقومون بها وبالتالي عدم توفر الوقت الكافي للحصول على هذه الدورات المتخصصة.

### 4-4 «وصف أبعاد ومتغيرات الدراسة»

«تم استخدام أساليب إحصائية وصفية» لوصف «آراء واتجاهات عينة الدراسة على الأبعاد والمتغيرات»، وقد اشتملت هذه الأساليب على «المتوسطات الحسابية والانحرافات المعيارية، والرتب الأهمية النسبية».

**«الجدول (4): وصف أبعاد ومتغيرات الدراسة»**

| المتغير | «المتوسط الحسابي» | «الانحراف المعياري» | «الرتبة» | «الأهمية النسبية» |
|---|---|---|---|---|
| مخاطر أمن المعلومات | 3.987 | 0.557 | 4 | مرتفعة |
| مخاطر تطبيقات الهاتف المحمول | 4.082 | 0.595 | 3 | مرتفعة |
| مخاطر تشغيلية | 4.103 | 0.494 | 1 | مرتفعة |
| مخاطر هجمات سيبرانية | 4.097 | 0.507 | 2 | مرتفعة |
| مخاطر الأمن السيبراني | 4.067 | 0.425 | --- | مرتفعة |
| استخدام البطاقات المصرفية | 4.182 | 0.587 | --- | مرتفعة |

بالنظر إلى البيانات الواردة في جالجدول (4) يتبين ارتفاع الأهمية النسبية لأبعاد ومتغيرات الدراسة»، «حيث بلغ المتوسط الحسابي» لمخاطر الأمن السيبراني (4.067)، «وبانحراف معياري» (0.425)، كما تبين «ارتفاع الأهمية النسبية لجميع الأبعاد»، حيث «جاءت (المخاطر التشغيلية) في المرتبة الأولى»، «بمتوسط حسابي (4.103)، وبانحراف معياري (0.494)»، «وفي المرتبة الثانية جاءت (مخاطر الهجمات السيبرانية)»، «بمتوسط حسابي (4.097)، وبانحراف معياري (0.507)»، «وفي المرتبة الثالثة جاءت (مخاطر تطبيقات الهاتف المحمول)»، «بمتوسط حسابي (4.082)، وبانحراف معياري (0.595)»، بينما جاءت «(مخاطر أمن المعلومات) في المرتبة الأخيرة»، «بمتوسط حسابي (3.987)، وبانحراف معياري (0.557)». «وبلغ المتوسط الحسابي لاستخدام البطاقات المصرفية (4.182)، وبانحراف معياري (0.587)».

### 5-4 «نتائج اختبار الفرضيات»

#### 1-5-4 «نتائج اختبار الفرضية الرئيسة»

جاء «نص الفرضية الرئيسة للدراسة على أنه»: «لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمخاطر الأمن السيبراني بأبعادة الأربعة (مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية) في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن»

**الجدول (5): * «نتائج اختبار أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية»**

| «المتغير التابع» | «ملخص النموذج» | | «تحليل التباين» | | | | «جدول المعاملات» | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | R | R2 | F | Df | *Sig F | البيان | B | St. Error | T | *Sig t |
| جاستخدام البطاقات المصرفية» | 0.834 | 0.695 | 47.936 | 4 | 0.000 | مخاطر أمن المعلومات | 0.241 | 0.082 | 2.921 | 0.004 |
| | | | | | | مخاطر تطبيقات الهاتف المحمول | 0.211 | 0.083 | 2.538 | 0.013 |
| | | | | | | «مخاطر تشغيلية» | 0.360 | 0.112 | 3.224 | 0.002 |
| | | | | | | مخاطر هجمات سيبرانية | 0.300 | 0.108 | 2.779 | 0.007 |

* «يكون التأثير ذا دلالة إحصائية عند مستوى (α≤0.05)»

بالنظر إلى «القيم الواردة في الجدول رقم (5)» يتبين ارتباط جمخاطر الأمن السيبراني في استخدام البطاقات المصرفية» بعلاقة طردية وقوية، وذلك بالاعتماد على قيمة معامل الارتباط R والتي كانت (0.834)، وأن مخاطر الأمن السيبراني استطاعت تفسير ما نسبته (69.5%) من التغير في استخدام البطاقات المصرفية، وذلك «بالاعتماد على قيمة معامل التحديد R2 والتي كانت» (0.695)، كما يتبين من الجدول معنوية «الأثر لمخاطر الأمن السيبراني في استخدام البطاقات المصرفية»، «حيث كانت قيمة (47.936 F)، وبمستوى الدلالة (Sig=0.000) وهو أقل من 0.05». وبالاستناد لما سبق يتبين أنه: «يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤0.05) لمخاطر الأمن السيبراني بأبعادة الأربعة: (مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية) في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن».

### 2-5-4 «نتائج اختبار الفرضيات الفرعية»

بالنظر إلى جدول المعاملات في الجدول رقم (5) يتبين معنوية الأثر عند (مخاطر أمن المعلومات)، حيث كانت قيمة المعامل B عنده (0.241)، وقيمة (2.921 t)، وبمستوى الدلالة (Sig=0.004)، وبالاستناد لهذا يتبين أنه: «يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤0.05) لمخاطر أمن المعلومات في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن».

ويتبين معنوية الأثر عند (مخاطر تطبيقات الهاتف المحمول)، حيث كانت قيمة المعامل B عنده (0.211)، وقيمة (2.538 t)، وبمستوى الدلالة (Sig=0.013)، وبالاستناد لهذا يتبين أنه: «يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤0.05) لمخاطر تطبيقات الهاتف المحمول في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن».

كما يتبين معنوية الأثر عند «(مخاطر تشغيلية)»، حيث كانت جقيمة المعامل B عنده (0.360)»، وقيمة t (3.224)، وبمستوى دلالة (Sig=0.002)، وبالاستناد لهذا يتبين أنه: «يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤0.05) للمخاطر التشغيلية في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن».

ويتبين كذلك معنوية الأثر عند «(مخاطر هجمات سيبرانية)، حيث كانت قيمة المعامل B عنده (0.300)»، وقيمة t (2.779)، وبمستوى دلالة (Sig=0.007)، وبالاستناد لهذا يتبين أنه: «يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤0.05) لمخاطر الهجمات السيبرانية في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن».

ولترتيب أبعاد «مخاطر الأمن السيبراني» من حيث التأثير في «استخدام البطاقات المصرفية»، تم «إجراء تحليل الانحدار المتدرج»، وكانت النتيجة كما يأتي:

**الجدول (6): «ترتيب مخاطر الأمن السيبراني من حيث تأثيرها في استخدام البطاقات المصرفية»**

| النموذج | «مخاطر الأمن السيبراني» | B | t | *Sig t | R2 | F | *SigF |
|---|---|---|---|---|---|---|---|
| الأول | «مخاطر تشغيلية» | 0.869 | 10.013 | 0.000 | 0.535 | 100.263 | 0.000 |
| الثاني | «مخاطر تشغيلية» | 0.613 | 6.499 | 0.000 | 0.633 | 74.185 | 0.000 |
| | مخاطر تطبييقات الهاتف المحمول | 0.375 | 4.784 | 0.000 | | | |
| الثالث | «مخاطر تشغيلية» | 0.544 | 5.824 | 0.000 | 0.667 | 56.846 | 0.000 |
| | مخاطر تطبييقات الهاتف المحمول | 0.264 | 3.156 | 0.002 | | | |
| | مخاطر أمن المعلومات | 0.253 | 2.961 | 0.004 | | | |
| الرابع | «مخاطر تشغيلية» | 0.360 | 3.224 | 0.002 | 0.695 | 47.936 | 0.000 |
| | مخاطر تطبييقات الهاتف المحمول | 0.211 | 2.538 | 0.013 | | | |
| | مخاطر أمن المعلومات | 0.241 | 2.921 | 0.004 | | | |
| | «مخاطر هجمات سيبرانية» | 0.300 | 2.779 | 0.007 | | | |

* «يكون التأثير ذا دلالة إحصائية عند مستوى (α≤0.05)»

«بالنظر إلى القيم الواردة في الجدول رقم (6)» «يتبين أن (مخاطر تشغيلية)» تعد من أكثر «المخاطر تأثيراً في استخدام البطاقات المصرفية»، «حيث جاءت في المرتبة الأولى، وفسرت ما نسبته (53.5%)ج «من التغير في المتغير التابع»، «وبإضافة (مخاطر تطبيقات الهاتف المحمول) في النموذج الثاني»، «ارتفعت النسبة إلى (63.3%)»، جوبإضافة (مخاطر أمن المعلومات) في النموذج الثالث»، «ارتفعت النسبة إلى» (66.7%)، «وبإضافة (مخاطر هجمات سيبرانية) في النموذج الرابع»، «ارتفعت النسبة إلى» (69.5%).

## 5- «النتائج والتوصيات»

### 5-1 «النتائج»

**«توصلت الدراسة إلى النتائج الآتية»:**

1. «وجود اهتمام مرتفع بمخاطر الأمن السيبراني، بما فيها مخاطر أمن المعلومات، ومخاطر تطبيقات الهاتف المحمول، والمخاطر التشغيلية، ومخاطر الهجمات السيبرانية». وهذا يدل على اهتمام هذه البنوك بتوفير الحماية لعملائها، وتأمين استقرار نظامها المالي، من خلال توفير وتنفيذ وتطوير إجراءات الأمن السيبراني اللازمة لحماية بيانات العملاء والحد من وقوع كوارث وحوادث أمنية. حيث إنها تعد من أكثر القطاعات تعرضاً للمخاطر المتزايدة من هجمات القرصنة الإلكترونية، وسرقة البيانات، والاحتيال الإلكتروني، والتي تؤثر سلباً على سمعتها وتعريض أموال العملاء للخطر.

2. وجود اهتمام مرتفع باستخدام البطاقات المصرفية، وهذا قد يعود للفوائد والمزايا التي تحققها هذه البطاقات المصرفية للعملاء والبنوك الإسلامية، فهي تسهم في «تيسير العمليات المالية وتحويل الأموال بصورة سريعة وآمنة»، كما أنها تساهم في توفير الضبط والرقابة على الإنفاق والمصروفات، مما يساعد العملاء على إدارة أموالهم بشكل فعال وتحديد أولوياتهم وأهدافهم المالية المتعلقة بهم. وفيما يتعلق بالبنوك فهي تعد من الأدوات الأساسية التي تستخدمها البنوك الإسلامية لتوفير الخدمات المصرفية للعملاء، وتساهم في تعزيز وتوطيد «العلاقة بين المصرف والعميل من خلال تقديم خدمات مصرفية سريعة وآمنة، كما تساهم في توفير السيولة المالية للبنوك الإسلامية» من خلال جمع الأموال من العملاء بشكل سريع وفعال، وتساعدها في تقديم خدمات مالية متنوعة.

3. يوجد أثر لمخاطر الأمن السيبراني في استخدام البطاقات المصرفية. ووجود هذا الأثر قد يعود إلى أن «استخدام البطاقات المصرفية يتم عبر الإنترنت، والذي يعد أحد الأساليب الرئيسة التي تستهدفها الهجمات المصرفية لاختراق الحسابات المصرفية»، والاحتيال الإلكتروني، والاستيلاء على الأموال، والهجوم على شبكات الدفع، وبالتالي فإن «توفير الحماية والأمان من المخاطر السيبرانية من شأنه أن ينعكس على حماية المعاملات والتعاملات التي تتم عبر البطاقات المصرفية».

4. «تعد المخاطر التشغيلية من أبرز مخاطر الأمن السيبراني» المؤثرة على البطاقات المصرفية، وهذا قد يعود إلى أن «الهجمات الإلكترونية تعتمد على العديد من التقنيات والمهارات الحديثة لاستهداف شبكات البطاقات المصرفية واختراقها وسرقة البيانات الشخصية والمالية للعملاء»، «ولذا فإن تطبيق حلول تقنية يعد من الوسائل والإجراءات الأمنية التي تضمن الحماية لبيانات العملاء وسلامة العمليات المصرفيةج.

### 2-5 «التوصيات»

**جاءت توصيات الدراسة بما يأتي»:**

1. «زيادة اهتمام إدارات البنوك الإسلامية العاملة في الأردن» بتطوير وتنفيذ إجراءات الأمن السيبراني اللازمة والمعنية بحماية بيانات العملاء ومنع وقوع أية حوادث وكوارث أمنية، من خلال استخدام تقنيات التشفير المتطورة، وتطوير أنظمة وبرامج الحماية ضد الهجمات الإلكترونية، وتنفيذ إجراءات إدارة المخاطر، وتدريب الموظفين على برامج الأمن السيبراني.
2. «توعية البنوك الإسلامية العاملة في الأردن عملائها بمخاطر الأمن السيبراني»، وتشجيعهم على اتخاذ كافة إجراءات الحماية اللازمة لحماية بياناتهم المالية، ومنها تطبيق كلمات مرور قوية، وتحديث برامج مكافحة الفيروسات، وعدم مشاركة المعلومات المصرفية مع الآخرين.
3. «زيادة مستوى اعتماد البنوك الإسلامية العاملة في الأردن على البطاقات المصرفية»، لما لها من أهمية في «تلبية احتياجات ومتطلبات العملاء من الخدمات المصرفية بشكل فوري وآمن، وتعزيز السيولة المالية للبنك وتحسين سمعته وزيادة الثقة بخدماته المصرفية».
4. توجيه مزودي خدمات الدفع الإلكترونية على تطوير «حلول أمنية جديدة وبشكل مستمر للحد من مخاطر الأمن السيبراني المتعلقة بالبطاقات المصرفية».
5. توظيف شركات البطاقات المصرفية أحدث ججالحلول التقنية والبرمجيات الأمنية لحماية بيانات العملاء وضمان السلامة في العمليات المصرفية».
6. «إجراء البنوك الإسلامية العاملة في الأردن عمليات تحديث أمنية مستمرة على أنظمتها»؛ لضمان عدم وجود ثغرات أمنية يمكن استغلالها من قبل المهاجمين.

## المصادر والمراجع

### أولاً: المراجع العربية


- أبو بكر، بكر عبد الله. (1996). بطاقات الائتمان حقيقتها البنكية التجارية وأحكامها الشرعية. (ط1)، مؤسسة الرسالة، بيروت، لبنان.
- أبو زيد، بكر بن عبد الله . (1999). بطاقات الائتمان. مؤسسة الرسالة، بيروت، لبنان.
- اسماعيل، محمد. (2019). الأمن السيبراني في القطاع المصرفي. إصدارات صندوق النقد الدولي، (4)، 1-8.
- جبور، منى الأشقر. (2016). السيبرانية هاجس العصر. مجلة المكتبات والتوثيق في العالم العربي، (5)، 262-263.
- حجاج، أمال. (2013). إدارة المخاطر التشغيلية في البنوك التجارية: دراسة حالة في بنك الفلاحة والتنمية الريفية وكالة 325 - عين البيضاء - ولاية أم البواقي. رسالة ماجستير غير منشورة، جامعة العربي بن مهيدي، أم البواقي، الجزائر.
- دوادي دلندة. (2020). أمن المعلومات المصرفية. رسالة ماجستير غير منشورة، جامعة قاصدي مرباح، ورقلة، الجزائر.
- الذنيبات، محمد عبد المجيد. (2019). التكيف مع المخاطر السيبرانية للشركات المالية والائتمانية والتقنية. جامعة الشرق الأوسط، عمان، الأردن. متاح على الموقع الإلكتروني https://althunibat.com/.
- الزيود، أحمد محمود. (2020) إدارة مخاطر الأمن السيبراني في البنوك الأردنية. مجلة الألفية للعلوم الاقتصادية والإدارية، 1(1)، 4-16.
- السيسي، صلاح الدين حسن. (1998). الحسابات والخدمات المصرفية الحديثة. (ط1)، دار الوسام. بيروت، لبنان.
- عديسة، شهرة وآمال، علي موسى. (2018). إدارة أمن المعلومات من خلال تبني حوكمة تكنولوجيا المعلومات والاتصالات لحماية المعاملات المصرفية الإلكترونية. الملتقى الوطني االثالث حول المستهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية، يومي 23-24 أبريل، المركز الجامعي عبد الحفيظ بوالصوف، ميلة، الجزائر، 1-14.
- العشعوش، أيمن ورضبان، عبادة. (2016). تحليل إدارة المخاطر التشغيلية في المصرف التجاري السوري خلال الفترة 2004-2011. مجلة جامعة تشرين للدراسات والبحوث العلمية: سلسلة العلوم الاقتصادية والقانونية، 38(2)، 409-427.

- مبارك، عبدالقادر، خشان، محمد والسطوحي، محمد. (2022). محددات نية الاستمرار في تبني خدمات الدفع عن طريق الهاتف المحمول، الدور المعدل لابتكار العميل. المجلة المصرية للدراسات التجارية، 46(4)، 1-50.
- نابي، مريم. (2019). الخدمات البنكية الإلكترونية وأثرها في تحسين أداء الإدارة البنكية. رسالة ماجستير غير منشورة، جامعة محمد بومضياف، المسيلة، الجزائر.


**Referances:**


- Al Duhaidahawi, H. M. K., Zhang, J., Abdulreza, M. S., Sebai, M., & Harjan, S. A. (2020). Analyzing the effects of Fin Tech variables on cyber security: Evidence form Iraqi Banks. International Journal of Research in Business and Social Science, 9(6), 123-133.
- Aldasoro, I., Gambacorta, L., Giudici, P. & Leach, T. (2020). Operational and cyber risks in the financial sector. Bank for International Settlements, 1-39.
- Al-Jabri, I. M. & Sohail, M. S. (2012). Mobile banking adoption: Application of diffusion of innovation theory. Journal of electronic commerce research, 13(4), 379-391.
- Canelón, J., Huerta, E.,& Leal, N., Ryan, T. (2020, January). Unstructured Data for Cybersecurity and Internal Control. In Proceedings of the 53rd Hawaii International Conference on System Sciences.
- 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.
- Eaton, T. V., Grenier, J. H. & Layman, D. (2019). Accounting and Cyber Security Risk Management. Current Issues in Auditing, 13(2), C1-C9
- https://www.arabnak.com/%D%8A7
- Jin, N. & Fei-Cheng, M. A. (2005). Network security risks in online banking. In Proceedings. International Conference on Wireless Communications, Networking and Mobile Computing, (Vol. 2, pp. 1229-1234). IEEE.
- Kim, Y., Kim, I. & Park, N. (2014). Analysis of cyber attacks and security intelligence. In Mobile, ubiquitous, and intelligent computing (pp. 489-494). Springer, Berlin, Heidelberg.

- Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P. & Jones, K. (2015). A survey of cyber security management in industrial control systems. International journal of critical infrastructure protection, 9, 52-80.
- Maharjan, R. & Chatterjee, J. M. (2019). Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal. LBEF Research Journal of Science, Technology and Management, 1(1), 82-98.
- Manoj(a), K. S. (2021). Banks' holistic approach to cyber security: tools to mitigate cyber risk. International Journal of Advanced Research in Engineering and Technology, 12(1), 902-910.
- Manoj(B), K. S. (2021), cyber Risk in banking services: the extent of cyber risks prevision and security measures. International Journal of Management, 12(1), 1332-1339.
- Qasaimeh, Ghazi M. & Jaradeh, Hussam Eddin (2022). The Impact of Artificial Intelligence on the Effective Applying of Cyber Governance in Jordanian Commercial Banks. International Journal of Technology, Innovation and Management, 2(1), 68-86.
- Sally, Jones (1999). The Law Relating of Credit Cards. Oxford, London