Sada Al-Jamiah Journal for Humanities (مجلة صدى الجامعة للعلوم الإنسانية)
Volume 4 - Issue 4 - 2026 - Pages 149-159
Website: https://oujournals.ly/index.php/sajh/index

The Role of Cybersecurity in Mitigating Cyber Risks in Commercial Banks: A Field Study on Libyan Commercial Banks

Nasir Mukhtar Murad [1]*, Nasser Saleh Alsoul [2]
[1,2] Finance and Banking Department,Faculty Of Economics & Commerce ,Elgarabulli , Elmergib University - Libya
*Email (for reference researcher): nmmorad@elmergib.edu.ly

دور الأمن السيبراني في الحد من المخاطر الالكترونية في المصارف التجارية دراسة ميدانية على المصارف التجارية الليبية

ناصر مختار مراد[1]*، ناصر صالح الصول [2]
[1،2] قسم التمويل والمصارف، كلية الاقتصاد والتجارة، القره بوللي، جامعة المرقب – ليبيا

تاريخ الاستلام: 20-09-2026، تاريخ القبول: 05-11-2026، تاريخ النشر08-11-2026

Abstract
This study aimed to highlight the role of cybersecurity in mitigating cyber risks for Libya commercial banks. operating in the city of Tripoli. To achieve the objectives of the study, the descriptive-analytical approach was adopted, whereby A questionnaire was used as a tool to collect data and information, ensuring its validity and reliability. The data was also analysed using software (SPSS). The study's findings revealed that cybersecurity plays a significant role in mitigating cyber risks by protecting customer data and funds, fostering trust and credibility, ensuring the continuity of banking services, and mitigating risks. It also provided The study presents a set of recommendations, the most important of which is to modernise the technological infrastructure and communication networks to ensure swift service delivery.
Banking services, achieving higher levels of customer satisfaction, and training and developing bank employees to enhance their skills. Technical and administrative skills, enabling them to efficiently handle recent developments in the field of digital banking.

Keywords: Cybersecurity, Cyber Risks, Libyan Commercial Banks.

الملخص
هدفت هذه الدراسة إلى تسليط الضوء على دور الأمن السيبراني في الحد من المخاطر الإلكترونية للمصارف التجارية الليبية العاملة في مدينة طرابلس ، ولتحقيق أهداف الدراسة تم الاعتماد على المنهج الوصفي التحليلي ، حيث تم تصميم استمارة استبيان كأداة لجمع البيانات والمعلومات ، مع التأكد من صدقها وثباتها ، كما تم تحليل البيانات باستخدام برنامج (SPSS) واظهرت نتائج الدراسة إلى وجود دور كبير للأمن السيبراني في الحد من المخاطر الإلكترونية من خلال حماية البيانات للعملاء وأموالهم ،وتعزيز الثقة والمصداقية ، وضمان استمرارية الخدمات المصرفية ، والحد من المخاطر ، وقدمت الدراسة مجموعة من التوصيات أهمها العمل على تحديث البنية التكنولوجية وشبكات الاتصال لضمان سرعة تقديم الخدمات المصرفية ، وتحقيق مستويات أعلى من رضا العملاء ، وتدريب وتطوير العاملين بالمصرف لتنمية مهاراتهم التقنية والادارية وتمكينهم من التعامل بكفاءة مع التطورات الحديثة في مجال الخدمات المصرفية الرقمية .

الكلمات المفتاحية: الامن السيبراني ، المخاطر الالكترونية ، المصارف التجارية الليبية.

المقدمة

في ظل التطور التكنولوجي المتسارع الذي شهدته مختلف القطاعات الاقتصادية أصبح الامن السيبراني ركيزة أساسية في الحفاظ على استقرار المؤسسات المالية وحمايتها من المخاطر التي تهدد سرية وموثوقية المعلومات , ومع تزايد استخدام المصارف التجارية للتقنيات الرقمية في تقديم خدماتها المصرفية أصبح من الضروري حماية هذه البيانات والأنظمة من المخاطر الالكترونية أمرا غاية في الاهمية لضمان استقرار العمل المصرفي وحماية أموال العملاء , ومن هنا برز دور الأمن السيبراني في التقليل من المخاطر الالكترونية من خلال توفير حماية قوية للأنظمة المصرفية مما يقلل من فرص الاحتيال المالي والهجمات الالكترونية .

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

يعد القطاع المصرفي الأكثر عرضة للاختراقات السيبرانية والهجمات الالكترونية نظرا لاحتوائه على كميات هائلة من البيانات الحساسة ، مثل البيانات الشخصية للعملاء ، وتفاصيل الحسابات ، وكلمات المرور ، وغيرها من البيانات ذات القيمة العالية التي تجعلها هدفا رئيسيا لمجرمي الانترنت .

وكذلك مع ظهور الخدمات المصرفية الرقمية واعتماد المصارف بشكل متزايد على التكنولوجيا لادارة معلوماتها المالية تزايدت المخاطر المرتبطة بالتهديدات والاختراقات ، يمكن أن تؤدي هذه الاختراقات إلى عواقب مدمرة بما في ذلك الخسائر المالية وسرقة البيانات والأضرار بسمعة المؤسسة فضلا عن المسؤولية القانونية .

كما أصبحت البيانات المالية في المصارف التجارية هدفا رئيسيا لمجرمي الانترنت مما يتطلب تعزيز التدابير الأمنية لحماية معلومات العملاء والمعاملات المالية ، لذا يجب على المتخصصين في مجال الأعمال المصرفية إدراك الأهمية الحيوية لتطبيق تدابير أمنية قوية لحماية المعلومات الحساسة والحفاظ على سلامة البيانات المالية .

مشكلة الدراسة

تتمثل مشكلة الدراسة في أن المصارف التجارية رغم التقدم التكنولوجي والتطور الذي شهدته في السنوات الأخيرة واعتمادها على الحلول الرقمية لتحسين خدماتها, تواجه تحديات كبيرة في مجال الأمن السيبراني هذه التحديات تتعلق بحماية البيانات والمعاملات المالية للعملاء من الاختراقات الالكترونية مما يعرض هذه المصارف لمخاطر تهدد استقرارها المالي , ومدى تأثير هذه المخاطر على الحسابات المالية للعملاء في المصارف التجارية , وعليه تكمن مشكلة الدراسة في الإجابة على التساؤل الاتي :-

ما هو دور الأمن السيبراني في الحد من المخاطر الالكترونية في المصارف التجارية؟

أهداف الدراسة:

1 - التعرف على مفهوم الأمن السيبراني.
2 - بيان أهمية الأمن السيبراني في المصارف التجارية.
3 - دراسة دور الأمن السيبراني في الحد من مخاطر الإلكترونية التي قد تهدد استقرا القطاع المصرفي. .
4 - بيان أهمية الأمن السيبراني في حماية بيانات العملاء من السرقة والتلاعب والاحتيال المالي.

أهمية الدراسة:

1- تسهم هذه الدراسة في اثراء الادبيات المتعلقة بتقديم نظرية متكاملة تجمع بين الأمن السيبراني والمخاطر الالكترونية.
2- توضح الدراسة المفاهيم الأساسية لكل من مفهوم الأمن السيبراني والمخاطر الالكترونية، وتقدم تحليلا لأهمية الأمن السيبراني كضرورة حتمية في البيئة الرقمية.
3- تسلط الدراسة الضوء على كيفية مساهمة الأمن السيبراني في تعزيز الثقة للعملاء عبر الانترنت وهو عامل حيوي لزيادة اعتماد الخدمات المالية الرقمية على نطاق واسع.
4- تبرز أهمية الأمن السيبراني في حماية البيانات الحساسة للمؤسسات المالية ومنع الخسائر المالية الكبيرة الناتجة عن المخاطر الالكترونية وسرقة المعلومات.
5- توفر الدراسة إطارا لفهم كيفية مساهمة الأمن السيبراني في ضمان استمرارية الأعمال والخدمات الأساسية دون انقطاع مما يحقق الاستقرار المالي للقطاع المصرفي.

فرضيات الدراسة:

فرضية رئيسية:

H0: لا يوجد اثر ذو دلالة إحصائية لدور الأمن السيبراني من خلال حماية بيانات العملاء وأموالهم , ضمان استمرارية الخدمات المصرفية , تعزيز الثقة والمصداقية) على الحد من المخاطر الالكترونية بالمصارف التجارية .

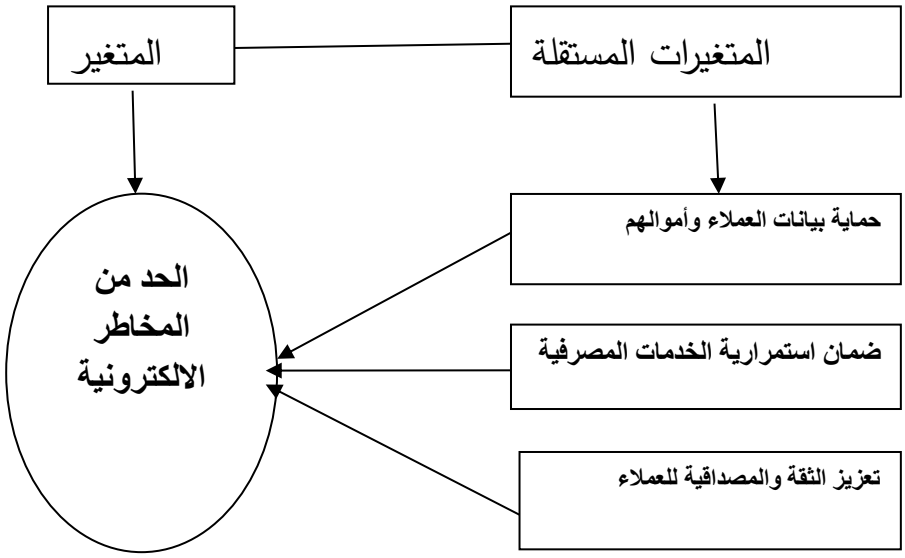
فرضيات فرعية:

H01: لا يوجد أثر ذو دلالة إحصائية لدور الأمن السيبراني من خلال حماية بيانات العملاء وأموالهم على الحد من مخاطر الالكترونية .
H02: لا يوجد أثر ذو دلالة إحصائية لدور الأمن السيبراني من خلال ضمان استمرارية الخدمات المصرفية على الحد من مخاطر الالكترونية .
H03: لا يوجد اثر ذو دلالة احصائية لدور الأمن السيبراني من خلال تعزيز الثقة والمصداقية على الحد من مخاطر الالكترونية .

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Sada Al-Jamiah Journal for Humanities (مجلة صدى الجامعة للعلوم الإنسانية)
Volume 4 - Issue 4 - 2026 - Pages 149-159
Website: https://oujournals.ly/index.php/sajh/index

النموذج العام للدراسة :



المصدر : من إعداد الباحثان

منهجية الدراسة:

من أجل تحقيق أهداف الدراسة واختبار الفرضيات ثم الاعتماد في هذه الدراسة على المنهج الوصفي التحليلي , حيث تم تغطية الجانب النظري من خلال مراجعة الكتب والدوريات العربية والاجنبية , بالإضافة الى الدراسات السابقة ذات الصلة بموضوع الدراسة , أما بالنسبة للجانب العملي من الدراسة فقد تم الاعتماد على تصميم استمارة استبيان بشكل يتوافق مع متطلبات الدراسة , وذلك بهدف جمع البيانات اللازمة وتحليلها باستخدام الأساليب الإحصائية المناسبة ,مما يسهم في تحقيق أهداف الدراسة بشكل فعال.

مجتمع وعينة الدراسة:

يتكون مجتمع الدراسة من المصارف التجارية العامة والخاصة في مدينة طرابلس والتي تضم مصرف الجمهورية، التجاري الوطني، مصرف الوحدة، مصرف شمال إفريقيا، مصرف التجارة والتنمية ، مصرف الصحاري ، وقد بلغ حجم العينة (183) استمارة تم اختيارها وفق الطرق الإحصائية المتعارف عليها، حيث تم توزيع استمارات الاستبيان على جميع المصارف ، وبعد عمليات التوزيع والفحص تم استبعاد (44) استمارة ، لتبقى إجمالي الاستبانات الصحيحة القابلة للتحليل الإحصائي (139) استمارة بنسبة استجابة (75.95) والجدول رقم (1) يوضح عدد استمارات الاستبيان التي تم توزيعها على عينات الدراسة.

جدول رقم (1) يوضح توزيع الاستبيان

ت	المصرف	الاستمارات الموزعة	الاستمارات المستلمة	النسبة
1	الجمهورية	40	30	%75
2	الصحاري	27	20	%74.07
3	الوحدة	30	21	%70
4	شمال أفريقيا	23	19	%82.60
5	التجارة والتنمية	28	24	%85.71
6	التجاري الوطني	35	25	%71.42
		183	139	%75.95

مصادر جمع البيانات والمعلومات:

1- المصادر الأولية: تم الاعتماد على تصميم استمارة استبيان تتضمن اسئلة مغلقة تعتمد على مقياس ليكرت الخماسي إلى جانب بعض الأسئلة المفتوحة ، وتم توزيعه على عينة الدراسة لجمع البيانات المطلوبة لخدمة أهداف الدراسة .

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

2- المصادر الثانوية: تم الاعتماد على المراجع العربية والأجنبية والدوريات والمجلات العلمية والدراسات السابقة التي تناولت موضوع الدراسة .

الأساليب الإحصائية المستخدمة : سيتم الاعتماد على البرنامج الإحصائي SPSS لتحليل بيانات الدراسة مع استخدام الاساليب الاحصائية التالية :

1- الإحصاء الوصفي :سيتم استخدام الانحراف المعياري والمتوسط الحسابي لوصف البيانات وتحليلها.
2- معيار الصدق والثبات ألفاكرونباخ .
3-معامل الانحدار والارتباط لمعرفة الأثر بين متغيرات الدراسة.

حدود الدراسة :

1 _ الحدود المكانية :انحصرت هذه الحدود في المصارف التجارية الواقع بمدينة طرابلس .
2 _ الحدود البشرية : موظفي المصارف التجارية .
3 _ الحدود الزمنية : خلال الفترة من 2026/7/15 إلى 2026/9/15 .الفترة الزمنية التي تم فيها توزيع الاستبيان على عينة الدراسة .

الدراسات السابقة :

1-دراسة (التائب والسائح ،2025) بعنوان " أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية ".
هدفت هذه الدراسة إلى التعرف على مفهوم الأمن السيبراني المحاسبي وتوضيح أهمية الأمن السيبراني المحاسبي في المصارف ، وتحديد الصعوبات والعراقيل التي تواجه تطبيق الأمن السيبراني المحاسبي ، تناول أهم المنافع التي يمكن تحقيقها أثناء تنفيذ الأمن السيبراني المحاسبي في المصارف ، واعتمدت الدراسة على المنهج الوصفي التحليلي ، وتتكون عينة الدراسة من 189 عاملا وعاملة ، وتوصلت الدراسة إلى أن هناك اهتماما فائق بالأمن السيبراني المحاسبي من أجل ضمان حماية المصارف والعملاء من المخاطر المتوقعة ، وأوصت الدراسة بضرورة القيام بعقد دورات وورش عمل منتظمة للعاملين في المصارف من أجل توعيتهم بأحدث المخاطر السيبرانية ، وضرورة القيام بالتعاون مع المصرف المركزي والهيئات الحكومية الأخرى لتبادل المعلومات والخبرات في مجال الأمن السيبراني .

2- دراسة (يوسف ،2024) بعنوان " تقييم تأثير المخاطر السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية ، هدفت هذه الدراسة على التعرف على المخاطر السيبرانية المستهدفة لأنظمة المعلومات المحاسبية في المؤسسات المالية الليبية ، وتقييم مدى تأثير تلك المخاطر على موثوقية وسلامة سرية تلك الأنظمة والبيانات المالية المخزنة فيها ، إضافة إلى مدى مساهمتها في تحديد نقاط الضعف والفجوات الأمنية التي يمكن إستغلالها من خلال الهيئات الخبيثة ، واعتمدت الدراسة على المنهج الوصفي ، وتوصلت هذه الدراسة إلى أن المخاطر السيبرانية تؤثر تأثير عظيما على اقتصاد المنظمات المالية الليبية ، وأن المنظمات المالية تواجه مخاطر سيبرانية متزايدة ومتباينة ، وأوصت الدراسة إلى ضرورة تعزيز الوعي والتدريب وتحديث السياسات والإجراءات وتعزيز التعاون والشراكات ، وتطوير التكنولوجيا والبنية التحتية والتشجيع والتوعية للعملاء .

3- دراسة (Hassan, L , Hossain , M.H .johora ,2024) بعنوان "الأهمية الحاسمة للأمن السيبراني في حماية البيانات المالية في مهنة المحاسبة في سياق التهديدات السيبرانية المتزايدة ".
هدفت هذه الدراسة إلى اختيار الأهمية الحاسمة للأمن السيبراني في حناية البيانات المالية في ظل التهديدات السيبرانية ، واعتمدت الدراسة على تحليل نوعي يشمل دراسات الحالة , والمقابلات مع الخبراء , لفحص دمج تقنيات الأمن السيبراني المتقدمة مثل الذكاء الاصطناعي والبلوك تشين من قبل شركات كبرى مثل Deloitte . PWC , EY . وأظهرت النتائج فعالية استراتيجيات الامن السيبراني في تعزيز حماية البيانات ومكافحة الاحتيال , على الرغم من وجود تحديات مستمرة مثل التكاليف المرتفعة والتطور السريع للتهديدات , واوصت الدراسة بضرورة الابتكار المستمر في مجال الامن السيبراني لضمان حماية البيانات المالية في العصر الرقمي .

4- دراسة (أبونصار ، 2022) بعنوان " دور الأمن السيبراني في تعزيز المرونة التنظيمية والمالية في المصارف الإسلامية الأردنية " . هدفت هذه الدراسة إلى قياس مساهمة إجراءات الحماية في تمكين المصارف من استعادة نشاطها المالي بعد الهجمات الرقمية ، حيث اشتمل مجتمع الدراسة موظفي أقسام المخاطر والتدقيق الداخلي وتكنولوجيا المعلومات , وتكونت العينة من (145 موظفا) واظهرت النتائج أن الالتزام بمعايير الأمن السيبراني يسهم بشكل فعال في تعزيز المرونة المالية ويقلل من احتمالات نزوح الودائع الناتج عن فقدان العملاء ، واوصت الدراسة بتبني إطار عمل متكامل لإدارة المخاطر السيبرانية كجزء من الاستراتيجية المالية الكلية للمصرف .

5- دراسة (سمرة واخرون ,2022) بعنوان " تاثير دور ادارة مخاطر الصيرفة الالكترونية في ضوء مقررات بازل بالبنوك " . هدفت هذه الدراسة إلى تحديد دور إدارة مخاطر الصيرفة الالكترونية في المصارف التجارية الخاصة في ضوء مقررات بازل , وقد تم اعتماد المنهج الوصفي التحليلي و استخدمت الاستبانة كأداة لجمع البيانات وتالف مجتمع الدراسة من 17 مصرفا , وتوصلت الدراسة إلى أن البنوك تمتلك أنظمة فعالة لإدارة العمليات الالكترونية وقد اهتمت بالإجراءات اللازمة لضمان فاعلية انظمة التشغيل مثل وضع خطط للطوارئ , أليات لمنع الاختراق , وسائل تخزين البيانات , إلا أنها أهملت متابعة وفحص أنظمة التشغيل , واوصت الدراسة بتطوير اداء العاملين بالتدريب , والتعاون بين الادارات بهدف

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

ضبط ومراقبة والابلاغ عن المخاطر وإخضاع معاملات إدارة المخاطر للتدقيق الداخلي وفحص سلامة أنظمة التشغيل واتباثها في تقارير دورية .

6- دراسة (Shulha , Yanenko ,Kuzub , Muda, Nazarenko , 2022) بعنوان "نمدجة نظام الأمن السيبراني لمعلومات البنكية " . هدفت هذه الدراسة على تطوير نماذج معرفية غامضة (Fuzzy Cognitive Maps) لتقييم مستوى الحماية الأمنية في المؤسسات المصرفية في ظل تزايد التهديدات السيبرانية ، استخدمت الدراسة أسلوب النمدجة المعرفية الغامضة كأداة تحليلية لقياس تأثير التهديدات السيبرانية مثل الهجمات الشبكية ، البرمجيات الخبيثة ، أخطاء المستخدمين ، التأثيرات الفيزيائية ، وهجمات حجب الخدمة (Dos) على البنية التحتية للمصارف ، وذلك من خلال تطوير نموذج معرفي باستخدام برنامج Mental Modeler وتوصلت نتائج الدراسة إلى أن أكثر العوامل تأثيرا على أمن الشبكات البنكية تمثلت في البرمجيات الخبيثة ، والأخطاء غير المقصودة من قبل المستخدمين ، والتأثيرات الفيزيائية على البنية التحتية ، كما بينت النمادج أن اتخاد تدابير أمنية مناسبة يمكن أن يؤدي إلى رفع مستوى أمن الشبكة بنسبة تصل إلى 65% ،وركزت الدراسة على أهمية الجمع بين الابتكار المفتوح وتطوير نظم أمنية متقدمة في مواجهة التهديدات المعاصرة

7-دراسة (العنزي ، 2021) بعنوان " أثر مخاطر الأمن السيبراني على جودة التقارير المالية في البنوك التجارية الكويتية " . هدفت هذه الدراسة إلى معرفة تأثير التهديدات السيبرانية على دقة وموثوقية البيانات المالية ، استهدفت الدراسة الموظفين في الإدارات العليا والوسطى وتقنية المعلومات بمجتمع البنوك التجارية ، وبلغ حجم العينة (120 فردا) ، وكشفت النتائج عن وجود تأثير سلبي ذو دلالة إحصائية للمخاطر السيبرانية على جودة التقارير المالية وكذلك إلى تحمل المصارف تكاليف تشغيلية طارئة تؤدي إلى تآكل الربحية ، وأوصت الدراسة بضرورة تحديث سياسات الحوكمة الإلكترونية والإستثمار في تقنيات التشفير المتقدم لحماية سلامة البيانات المالية .

ثانياً : الجانب النظري

مفهوم الأمن السيبراني وأهميته :

هو مجموعة الإجراءات الاحترازية التي يتعين اتخاذها من قبل الأجهزة الأمنية والمؤسسات الأخرى للمحافظة على سرية المعلومات الإلكترونية ومنع الاختراقات الفيروسية وتهدف تلك الإجراءات إلى ضمان وصول المعلومات الحاسوبية إلى الجهات المختصة المعنية بحفظها ، وفي الوقت ذاته منع وقوعها في أيدي الأعداء أو الأصدقاء على حد سواء (جيجان ، 2021) .

أهمية الأمن السيبراني :

إن للأمن السيبراني العديد من الأثار والمزايا التي تعد مؤثرة بشكل فعال على النظام العالمي في مجال الأمن والحماية وله أهمية بالغة نظرا للدور الذي يلعبه في جميع المجالات ، وتكمن اهميته بتقديمه الحماية وبكونه اداة فعالة وقوية لحفظ البيانات ولديه عدة آليات وأنظمة وسبل واستراتيجيات يقوم من خلالها بأداء دوره ،ولكن بالرغم من ضرورة التوسع المعرفي الحاصل في المنطقة فيما يتعلق بمفهوم الأمن السيبراني ومع ضرورة الالتفات إلى اهمية الدور الفاعل الذي يقوم به (الفضل وأخرون ، 2024).

أصبحت البينات المالية في عصر التحول الرقمي عرضة بشكل متزايد للمخاطر الالكترونية مما يجعل تطبيق الأمن السيبراني أمرا حيويا لحماية المؤسسات والشركات من المخاطر ، وتتجلى أهمية الأمن السيبراني للحد من المخاطر الالكترونية في عدة ابعاد رئيسية وهي :

1- حماية البيانات المالية للعملاء :

تحتوي الأنظمة المالية على معلومات حساسة للغاية ، مثل البيانات المالية للمؤسسة ، وسجلات العملاء ، وكشوف الحسابات ، والتقارير المالية ، أي إختراق قد يؤدي إلى سرقة هذه البيانات والتلاعب بها مما قد يتسبب في خسائر مالية كبيرة ، وفقدان الميزة التنافسية (Abrahams etal , 2024) .

2- استمرار الخدمات المصرفية :

يقصد به ضمان استمرارية الأعمال المصرفية في بيئة رقمية تتسم بارتفاع المخاطر ، ومدى قدرة هذه المصارف على حماية أنظمتها المعلوماتية من المخاطر الالكترونية التي تعطل الخدمات المصرفية ، مما يؤدي إلى توقف هذه الخدمات ، فالأمن السيبراني يساعد في ضمان استمرارية الأعمال من خلال حماية الأنظمة الحيوية .

3- تعزيز الثقة والمصداقية :

يساهم الأمن السيبراني في بناء الثقة عندما يعلم أصحاب المصلحة أن المصرف يولي اهتماما كبيرا لحماية أصوله وبيانات عملاءه ، فان ذلك ينعكس إيجابا على تعزيز الثقة والمصداقة .

ثانياً : مفهوم المخاطر الالكترونية وانواعها :

مفهوم المخاطر الالكترونية :

هي تلك المخاطر التي ترتبط باستخدام تقنيات الانظمة الالكترونية ويعد هذا النوع من المخاطر أكثر أهمية بالنسبة للخدمات المصرفية الالكترونية نظرا للاعتماد الكبير على تقنيات في أوجه تقديم هذه الخدمات كافة ، وتنتج عن خلل في كفاءة البنية التحتية القائمة أو عن ملائمة تصميم الانظمة أو الاجراءات الموضوعة أو عن عدم توفير المتطلبات الامنية اللازمة او عدم المام وظفي المصارف بالاستخدام الامثل للتكنولوجيا الحديثة يؤدي إلى القصور في اداء العمليات

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

الالكترونية بشكل صحيح وبروز قضايا انتهاك الخصوصية بشكل متزايد في العمليات المالية والمصرفية ، بحيث يمكن اختراق نظم حاسبات المصرف بهدف التعرف على المعلومات الخاصة بالعملاء واستغلالها سواء تم ذلك من خارج المصرف أو من العاملين فيه ، بما يستلزم توافر إجراءات كافية لكشف واعاقة ذلك الاختراق (جلايله , 2019) .

أنواع المخاطر الالكترونية التي يواجهها القطاع المصرفي:

يواجه القطاع المصرفي في ظل التحول الرقمي تحديات جسيمة ناتجة عن تزايد المخاطر الالكترونية ، التي لا تقتصر تأثيراتها على اختراق البيانات الحساسة فحسب بل تمتد إلى تعريض أمن الأنظمة المالية للخطر ، ومع تطور هذه التهديدات بشكل مستمر أصبح من الضروري أن تواكب البنوك أحدث أساليب الهجمات الالكترونية وأن تعزز إجراءاتها الوقائية لضمان حماية فعالة لبنيتها التحتية وبيانات عملاءها فيما يلي أبرز أنواع المخاطر الالكترونية (Haxhosaj , 2022) .

مخاطر التشغيل :تنشأ مخاطر عمليات الاحتيال أو أخطاء المعالجة أو تعطل النظام أو غيرها من الأحداث غير المتوقعة التي تؤدي إلى عدم قدرة المؤسسة على تقديم المنتجات أو الخدمات, ترتبط المخاطر التشغيلية جزئيا بمخاطر التكنولوجيا مما يجعلها ذات أهمية بالنسبة لخدمات الصيرفة الالكترونية . من بينها :

أ- مخاطر أمن وسلامة نظام المعلومات في البنك, وتحدث بسبب عدم التامين الكافي للنظم وامكانية اختراقها , أي القصور في سلامة وامن نظام الملومات وموثوقيته .

ب- مخاطر عدم ملائمة تصميم وصيانة نظام المعلومات في البنك بشكل احترافي , حيث يؤدي ذلك إلى اخفاقه في تلبية طلبات العملاء وعدم السرعة في معالجة المشاكل الأمنية والبطء في الاداء , أو الفشل في مواجهة التهديدات السيبرانية وتسرب المعلومات .

بينما يرتبط الجزء الاخر بآداء الموظفين وسلوكياتهم , مثل : الاحتيال والتزوير والاخطاء الناتجة عن سوء الاستخدام التي يرتكبها الموظفون عند ادائهم وظائفهم .

مخاطر السمعة : تنشأ هذه المخاطر عندما تتشكل صورة سلبية لدى العملاء اتجاه المصرف الأمر الذي قد يتسبب في انخفاض عدد العملاء وتدفق الأموال والايرادات . يمكن أن يحدث نتيجة ضعف في شبكة الاتصال التفاعلية بين البنك وعملائه أي عدم مقدرة البنك على إدارة أنظمته بكفاءة , أو عندما يكون عدد كبي من العملاء غير راضيين عن سياسات البنك , يمكن أيضا أن تتعرض مخاطر السمعة للتهديد نتيجة لسوء الاستخدام والاحتيال أو حدوث اختراق خارجي من قبل أطراف ثالثة أو بسبب نشر معلومات كاذبة عن المصرف , مما يسبب الشكوك وانعدام الأمان في نظام أعمال المصرف , تأثير هذا الخطر لا يقتصر على مصرف واحد فقط , ولكن من الممكن أن يمتد إلى جميع البنوك , أو النظام المصرفي بأكمله في بلد ما .

المخاطر القانونية أو مخاطر عدم الامتثال : وتنشأ عندما لا يمتثل البنك للقواعد والمعايير واللوائح المنظمة للمعاملات المصرفية الالكترونية أو في حالة عدم تحديد القواعد القانونية واللوائح والاجراءات بشكل واضح وصريح , قد يتعرض البنك لمستوى عالي من مخاطر الامتثال بسبب التغيرات القانونية والتنظيمية المتطورة نتيجة الوتيرة السريعة للتغيرات التكنولوجية , غالبا ما يؤدي عدم الامتثال لهذه التغيرات الى عواقب وخيمة تشمل خفض التصنيف , والغرامات المالية , وتعليق العمليات , والاضرار بالسمعة وحتى سحب ترخيص التشغيل كذلك غالبا ما تتفاقم مخاطر الامتثال في المواقف عبر الحدود نظرا لان القوانين المتعارضة والاجراءات الضريبية ومتطلبات الابلاغ تزيد من حجم هذه المخاطر .

ثالثاً: الاطار العملي :

ثبات الاستبيان :

يقصد بثبات الاستبيان أن يعطي هذا الاستبيان نفس النتيجة حتي ولو تم إعادة توزيعه أكثر من مرة تحت نفس الظروف والشروط، أو بعبارة أخرى أن ثبات الاستبيان يعني الاستقرار في نتائجه وعدم تغييرها بشكل كبير فيما لو تم إعادة توزيعها على أفراد العينة عدة مرات خلال فترات زمنية معينة. وقد تحقق الباحثان من ثبات استبيان الدراسة من خلال طريقة معامل ألفا كرونباخ

وذلك كما يلي:

معامل كرونباخ ألفا Cronbach's Alpha Coefficient:

عند حساب قيمة معامل الثبات (ألفا كرونباخ) كانت النتائج كما هي مبينة بالجدول التالي:

جدول رقم (2) يوضح نتائج اختبار ألفا كرونباخ لقياس ثبات الاستبانة

ت	المحاور	معامل ألفاكرونباخ	الثبات
-1	حماية بيانات العملاء واموالهم	**0.917**	**0.958**
-2	ضمان استمرارية الخدمات المصرفية	**0.868**	**0.932**
-3	تعزيز الثقة والمصداقية	**0.954**	**0.977**
-4	الحد من المخاطر	**0.905**	**0.951**
	جميع عبارات الاستبيان	**0.976**	**0.988**

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Sada Al-Jamiah Journal for Humanities (مجلة صدى الجامعة للعلوم الإنسانية)
Volume 4 - Issue 4 - 2026 - Pages 149-159
Website: https://oujournals.ly/index.php/sajh/index

واضح من النتائج الموضحة في جدول (2) أن قيمة معامل ألفا كرونباخ كانت مرتفعة لكل المحاور وتتراوح بين(0868 , 0.954) لكل محور من محاور الاستبيان .كذلك كانت قيمة معامل ألفا لجميع فقرات الاستبيان (0.976). وكانت قيمة الثبات مرتفعة لكل المحاور وتتروح بين (0.932, 0.977)لكل محور من محاور الاستبيان. كذلك كانت قيمة الثبات لجميع فقرات الاستبيان مساوية لي (0.988) وهذا يعني انه معامل الثبات مرتفع جدا
وبذلك يكون الباحثان قد تأكد من صدق وثبات استبيان الدراسة مما يجعله على مقدار من الثقة بصحة الاستبيان وصلاحيته لتحليل النتائج والإجابة على أسئلة الدراسة واختبار فرضياتها.

الأساليب الإحصائية المستخدمة في البحث:

تمت المعالجة الإحصائية للبيانات باستخراج الأعداد، النسب المئوية، المتوسطات الحسابية، الانحرافات المعيارية، وفحص فرضيات الدراسة عند مستوى (α<=0.05) باستخدام الاختبارات الإحصائية التالي: تحليل الانحدار و لارتباط بين المتغيرات ومعادلة الثبات كرونباخ ألفا، وذلك باستخدام برنامج الرزم الاحصائية (SPSS).

عرض وتحليل نتائج الدراسة

1- ابعاد العبارات المتعلقة بالأمن السيبراني؟

أ- المتغيرات الخاصة بحماية بيانات العملاء واموالهم.

الجدول رقم (3) تقييم أفراد العينة بحماية بيانات العملاء واموالهم من خلال العبارات

ت	العبارات	المتوسط	الانحراف المعياري	الأهمية النسبية	درجة القبول
-1	يمتلك المصرف اجراءات أمن سيبرانى كافية لحماية البيانات والمعلومات	4.18	0.431	4	موافق تماما
-2	بضمن الامن السيبرانى سرية وسلامة التعامل وتوافر البيانات المصرفية	4.40	0.503	1	موافق تماما
-3	توجد انظمة تشفير حديثة داخل المصرف لحماية المعلومات المصرفية	4.25	0.444	3	موافق تماما
-4	يعمل المصرف بشكل دورى على تحديث انظمة الامن السيبرانى	4.35	0.499	2	موافق تماما
-5	يلتزم المصرف بالمعايير الدولية في امن المعلومات مثل ios	4.06	0.422	5	موافق تماما
-6	يعتمد المصرف على انظمة حماية متقدمة مثل الجدران النارية وانظمة كشف التسلل	4.01	0.401	6	موافق تماما
	معدل النسب	4.21	0.450		موافق تماما

يوضح الجدول المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات حماية بيانات العملاء وموالهم حيث جاءت الفقرة (بضمن الامن السيبراني سرية وسلامة التعامل وتوافر البيانات المصرفية) هي الأولي بدرجة كبيرة حيث كان متوسطها الحسابي(4.40) تلاها الفقرة (يعمل المصرف بشكل دوري على تحديث انظمة الامن السيبراني) بمتوسط حسابي (4.35) في حين كان أقل الفقرات تقديراً هي الفقرة (يعتمد المصرف على انظمة حماية متقدمة مثل الجدران النارية وانظمة كشف التسلل) بمتوسط (4.01) . ومن هذا يتبين أن الآراء حول فقرات هذا المحور جاءت بالموافقة تماما كما تشير المعطيات الإحصائية في الجدول السابق أن المتوسط العام للإجابات جاء بدرجة كبيرة وتقدر بـــ: 4.21 هذا يدل علي أن إجابات افراد العينة تتفق تماما بحماية بيانات العملاء واموالهم.\

ب- ضمان استمرارية الخدمات المصرفية ؟

الجدول رقم (4) تقييم أفراد العينة بضمان استمرارية الخدمات المصرفية من خلال العبارات التالية

ت	العبارات	المتوسط	الانحراف المعياري	الأهمية النسبية	درجة القبول
-1	**يساعد الامن السيبرانى على حماية الانظمة المصرفية من هجمات التحول الرقمى مما يضمن تقديم الخدمات دون انقطاع**	4.40	0.503	4	موافق تماما
-2	**يوجد بالمصرف ضوابط وقائية تقلل من احتمالية تعطل الخدمات المصرفية نتيجة الهجمات والاختراقات**	4.35	0.489	5	موافق تماما
-3	**يقوم المصرف باحتواء الهجمات الالكترونية قبل تاثيرها على الخدمات المصرفية**	4.50	0.513	1	موافق تماما
-4	**يستطيع المصرف استعادة عملياته بسرعة بعد اى حادث امنى**	4.45	0510.	2	موافق
-5	**يتم اجراء نسخ احتياطى دورى للبيانات المصرفية**	4.40	0.503	3	موفق تماما

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Sada Al-Jamiah Journal for Humanities (مجلة صدى الجامعة للعلوم الإنسانية)
Volume 4 - Issue 4 - 2026 - Pages 149-159
Website: https://oujournals.ly/index.php/sajh/index

-6	يمتلك المصرف خطة فعالة لاستمرارية الخدمات في حال وقوع هجوم الكتروني	4.15	0.875	6	موافق تماما
	معدل النسب	4.38	0.565		موافق تماما

يوضح الجدول المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات ضمان اسمراريه الخدمات المصرفية حيث جاءت الفقرة (يقوم المصرف باحتواء الهجمات الالكترونية قبل تأثيرها على الخدمات المصرفية) هي الأولي بدرجة كبيرة حيث كان متوسطها الحسابي(4.50) تلاها الفقرة (يستطيع المصرف استعادة عملياته بسرعة بعد أي حادث امنى) بمتوسط حسابي (4.45) في حين كان أقل الفقرات تقديراً هي الفقرة (يمتلك المصرف خطة فعالة لاستمرارية الخدمات في حال وقوع هجوم الكتر ونى) بمتوسط (4.15) . ومن هذا يتبين أن الآراء حول فقرات هذا المحور جاءت بالموافقة تماما. كما تشير المعطيات الإحصائية في الجدول السابق أن المتوسط العام للإجابات جاء بدرجة كبيرة وتقدر بـــ: 4.38 هذا يدل علي أن إجابات افراد العينة تتفق تماما بضمان استمرارية الخدمات المصرفية .

ج- تعزيز الثقة والمصداقية؟

الجدول رقم (5) تقييم أفراد العينة لتعزيز الثقة والمصداقية من خلال العبارات التالية:

ت	العبارات	المتوسط	الانحراف المعياري	الأهمية النسبية	درجة القبول
-1	يساعد تطبيق الامن السيبرانى على الحفاظ على ثقة العملاء في المصرف	4.35	0.489	4	موافق تماما
-2	تساعد الانظمة الامنية الفعالة من تقليل احتمالية الاختراقات والهجمات الالكترونية مما يحافظ على سمعة المصرف	4.30	0.470	6	موافق تماما
-3	تطبيق الحوكمة الامنية والاقصاح على اجراءات الحماية يعزز الثقة لدى العملاء بالمصرف	4.35	0.489	5	موافق تماما
-4	يحمى الامن السيبرانى انظمة الدفع من الهجمات المتقدمة مما يحافظ على كفاءة الاداء وتعزيز الثقة	4.35	0.489	3	موافق تماما
-5	يعزز الامن السيبراني ثقة العملاء في الخدمات الرقمية المقدمة	4.60	0.503	1	موافق تماما
-6	يلتزم المصرف بالشفافية والافصاح عند حدوث مشكلات امنية	4.50	0.513	2	موافق تماما
	معدل النسب	4.40	0.492		موافق تماما

يوضح الجدول المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات تعزيز الثقة والمصداقية حيث جاءت الفقرة (يعزز الامن السيبراني ثقة العملاء في الخدمات الرقمية المقدمة) هي الأولي بدرجة كبيرة حيث كان متوسطها الحسابي(4.60) تلاها الفقرة (يلتزم المصرف بالشفافية والافصاح عند حدوث مشكلات امنية) بمتوسط حسابي (4.50) في حين كان أقل الفقرات تقديراً هي الفقرة (تساعد الانظمة الامنية الفعالة من تقليل احتمالية الاختراقات والهجمات الالكترونية مما يحافظ على سمعة المصرف) بمتوسط (4.30) . ومن هذا يتبين أن الآراء حول فقرات هذا المحور جاءت بالموافقة .تماما كما تشير المعطيات الإحصائية في الجدول السابق أن المتوسط العام للإجابات جاء بدرجة كبيرة وتقدر بـــــ 4.40 هذا يدل علي أن إجابات افراد العينة تتفق تماما بتعزيز الثقة والمصدقية .

2 . المتغيرات الخاصة بالحد من المخاطر الالكترونية.

الجدول رقم (6) تقييم أفراد العينة بالحد من المخاطر الالكترونية من خلال العبارات

ت	العبارات	المتوسط	الانحراف المعياري	الأهمية النسبية	درجة القبول
-1	يسعى المصرف الى تقليل المخاطر الالكترونية عن طريق تطبيق الامن السيبرانى	4.25	0.444	5	موافق تماما
-2	يساعد تطبيق السيبرانى على الحد من احتمالية التعرض لهجمات الكترونية مثل الاختراقات وسرقة البيانات	4.60	0.940	1	موافق تماما
-3	ادراك المصرف بأهمية الامن السيبرانى يساعده على استعداد بشكل افضل لمواجهة التهديدات الالكترونية والحد منها	4.50	0.513	2	موافق تماما
-4	يساهم الامن السيبرانى في تقليل الخسائر المالية الناتجة عن الهجمات الرقمية	4.35	0.489	4	موافق تماما
-5	يمتلك المصرف خطة للتعافى من الكوارث الرقمية	4.10	0.308	6	موافق تماما

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Sada Al-Jamiah Journal for Humanities (مجلة صدى الجامعة للعلوم الإنسانية)
Volume 4 - Issue 4 - 2026 - Pages 149-159
Website: https://oujournals.ly/index.php/sajh/index

-6	انخفت الحوادث والهجمات الالكترونية بعد تطبيق ممارسات الامن السيبراني .	4.40	0.503	3	موافق
	معدل النسب	4.37	0.532		موافق تماما

يوضح الجدول المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات الحد من المخاطر الالكترونية حيث جاءت الفقرة (يساعد تطبيق السيبراني على الحد من احتمالية التعرض لهجمات الكترونية مثل الاختراقات وسرقة البيانات) هي الأولي بدرجة كبيرة حيث كان متوسطها الحسابي(4.60) تلاها الفقرة (ادراك المصرف بأهمية الامن السيبراني يساعده على استعداد بشكل افضل لمواجهة التهديدات الالكترونية والحد منها) بمتوسط حسابي (4.50) في حين كان أقل الفقرات تقديراً هي الفقرة (يمتلك المصرف خطة للتعافى من الكوارث الرقمية) بمتوسط (4.10) . ومن هذا يتبين أن الآراء حول فقرات هذا المحور جاءت بالموافق تماما . كما تشير المعطيات الإحصائية في الجدول الجدول السابق أن المتوسط العام للإجابات جاء بدرجة كبيرة وتقدر بـــــ 4.37 هذا يدل علي أن إجابات افراد العينة تتفق تماما بالحد من المخاطر الالكترونية .

تقييم الفرضيات

الفرضية الفرعية الأولي :-

الفرض الصفري : لا يوجد أثر ذو دلالة إحصائية بين حماية بيانات العملاء واموالهم والحد من المخاطر الالكترونية .

الفرض البديل : يوجد أثر ذو دلالة إحصائية بين حماية بيانات العملاء واموالهم والحد من المخاطر الالكترونية .

الجدول رقم (7): يوضح لنا نتائج تحليل الانحدار لبيان اثر حماية بيانات والعملاء واموالهم في الحد من المخاطر الالكترونية .

المتغيرات المستقلة	معامل الارتباط (r)	معامل التحديد R^2	اختبار التأثير T-test	معامل الانحدار β	Sig
حماية بيانات والعملاء واموالهم	0.931	0.866	17.233	1.196	0.000

تشير النتائج بالجدول السابق وفقا لآراء أفراد عينة الدراسة بوجود أثر ذي دلالة إحصائية لحماية بيانات العملاء واموالهم في الحد من المخاطر الالكترونية عند مستوي معنوية (α=0.05). حيث يلغ معامل الارتباط (R =0.607) وهذ يدل علي وجود ارتباط قوي. أما معامل التحديد R^2 فقد بلغ (0.866) ، أي أن ما نسبته 86.6% من التغير في الحد من المخاطر الالكترونية ناتج عن التغير من حماية بيانات العملاء واموالهم كما بلغت قيمة درجة التأثير (β=1.196)وهذا يعني أن الزيادة بدرجة واحدة في حماية بيانات العملاء واموالهم يؤدي إلي الحد من المخاطر الالكترونية بقيمة (1.196). وقد بلغت قيمة (T =17.233) بمستوي دلالة (0.000) وهي أصغر من مستوي الدلالة (0.05) وعليه فإننا نرفض الفرضية الصفرية ونقبل الفرضية البديلة والتي تدل علي وجود أثر ذو دلالة إحصائية لحماية بيانات العملاء واموالهم في الحد من المخاطر الالكترونية عند مستوي معنوية (α=0.05).

الفرضية الفرعية الثانية:

الفرض الصفري: لا يوجد أثر ذو دلالة إحصائية لضمان استمرارية الخدمات المصرفية في الحد من المخاطر الالكترونية.

الفرض البديل: يوجد أثر ذو دلالة إحصائية لضمان استمرارية الخدمات المصرفية في الحد من المخاطر الالكترونية .

الجدول رقم (8) يوضح لنا نتائج تحليل الانحدار لبيان اثر ضمان استمرارية الخدمات المصرفية في الحد من المخاطر الالكترونية .

المتغيرات المستقلة	معامل الارتباط (r)	معامل التحديد R^2	اختبار التأثير T-test	معامل الانحدار β	Sig
ضمان استمرارية الخدمات المصرفية	0.899	0.808	7.190	0.887	0.000

تشير النتائج بالجدول السابق وفقا لآراء أفراد عينة الدراسة بوجود أثر **دو دلالة احصائية لضمان استمرارية** الخدمات المصرفية في الحد من المخاطر الالكترونية. عند مستوي معنوية (α=0.05). حيث يلغ معامل الارتباط (R =0.899) وهذ يدل علي وجود ارتباط قوي أما معامل التحديد R^2 فقد بلغ (0.808) ، أي أن ما نسبته 80.8 % من التغير في الحد من المخاطر الالكترونية ناتج عن التغير في ضمان استمرارية الخدمات المصرفية كما بلغت قيمة درجة التأثير (β=0.887)وهذا يعني أن الزيادة بدرجة واحدة في الاهتمام بضمان استمرارية الخدمات المصرفية يؤدي إلي الحد من المخاطر الالكترونية بقيمة (0.887). وقد بلغت قيمة (T =7.190) بمستوي دلالة (0.000) وهي أصغر من مستوي الدلالة (0.05) وعليه فإننا نرفض الفرضية الصفرية ونقبل الفرضية البديلة والتي تدل علي وجود أثر ذو دلالة إحصائية لضمان استمرارية الخدمات المصرفية في الحد من المخاطر الالكترونتية عند مستوي معنوية (α=0.05).

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Sada Al-Jamiah Journal for Humanities (مجلة صدى الجامعة للعلوم الإنسانية)
Volume 4 - Issue 4 - 2026 - Pages 149-159
Website: https://oujournals.ly/index.php/sajh/index

الفرضية الفرعية الثالثة:

الفرض الصفري: لا يوجد أثر ذو دلالة إحصائية بين تعزيز الثقة والمصداقية في الحد من المخاطر الالكترونية.

الفرض البديل: يوجد أثر ذو دلالة إحصائية بين تعزيز الثقة والمصداقية في الحد من المخاطر الالكترونية.

الجدول رقم (10) يوضح لنا نتائج تحليل الانحدار لبيان اثر تعزيز الثقة والمصداقية في الحد من المخاطر الالكترونية

المتغيرات المستقلة	معامل الارتباط (r)	معامل التحديد R^2	اختبار التأثير T-test	معامل الانحدار β	Sig
تعزيز الثقة والمصداقية	0.940	0.883	16.071	1.016	0.000

تشير النتائج بالجدول السابق وفقا لآراء أفراد عينة الدراسة بوجود أثر ذو دلالة إحصائية ء لتعزيز الثقة والمصداقية في الحد المخاطر الالكترونية عند مستوي معنوية (α=0.05). حيث يلغ معامل الارتباط (R =0.940) وهذ يدل علي وجود علاقة ارتباط قوي أما معامل التحديد R^2 فقد بلغ (0.883) ، أي أن ما نسبته 88.3 % من التغير في الحد من المخاطر الالكترونية ناتج عن التغير في تعزيز الثقة والمصداقية كما بلغت قيمة درجة التأثير (β=1.016)وهذا يعني أن الزيادة بدرجة واحدة في الاهتمام بتعزيز الثقة والمصداقية يؤدي إلي زيادة في الحد من المخاطر الالكترونية رضاء العملاء بقيمة (1.016). كما بلغت قيمة (T =16.071) بمستوي دلالة (0.000) وهي أصغر من مستوي الدلالة (0.05) وعليه فإننا نرفض الفرضية الصفرية ونقبل الفرضية البديلة والتي تدل علي وجود أثر ذو دلالة إحصائية لتعزيز الثقة والمصداقية في الحد مخاطر الالكترونية عند مستوي معنوية (α=0.05).

الفرضية الرئيسية:

الفرض الصفري: لا يوجد أثر ذو دلالة إحصائية لدور الامن السيبراني في الحد من المخاطر الالكترونية .

الفرض البديل: يوجد أثر ذو دلالة إحصائية لدور الامن السيبراني في الحد من المخاطر الالكترونية.

الجدول رقم (9): يوضح لنا نتائج تحليل الانحدار لبيان أثر الامن السيبراني في الحد من المخاطر الالكترونية.

المتغيرات المستقلة	معامل الارتباط (r)	معامل التحديد R^2	اختبار التأثير T-test	معامل الانحدار β	Sig
دور الامن السيبراني	0.951	0.904	14.074	0. 355	0.000

تشير النتائج بالجدول السابق وفقا لآراء أفراد عينة الدراسة بوجود أثر ذو دلالة إحصائية **لدور الامن** السيبراني في الحد من المخاطر الالكترونية عند مستوي معنوية (α=0.05). حيث يلغ معامل الارتباط (R =0.951) وهذا يدل على وجود ارتباط قوي، كما تشير قيمة معامل التحديد (R^2=0.904) إي أن المتغير المستقل المتمثل في دور الامن السيبراني يفسر التغير في الحد من المخاطر الالكترونية بنسبة 90.4 % والنسبة المتبقية تفسرها عوامل أخري بالإضافة إلي الأخطاء العشوائية الناتجة عن دقة اختيار العينة وغيرها ونلاحظ أن قيمة sig = 0.000 وهي اقل من مستوي المعنوية (0.05)عليه يمكننا رفض الفرضية الصفرية وقبول الفرضية البديلة والتي تدل علي وجود أثر ذو دلالة إحصائية لدور الامن السيبراني في الحد من المخاطر الالكترونية عند مستوي معنوية (α=0.05).

النتائج:

1- يوجد تأثير ايجابي معنوي ايجابي لحماية بيانات العملاء واموالهم في الحد من المخاطر الالكترونية.
2- يوجد تأثير ايجابي معنوي لضمان استمرارية الخدمات في الحد من المخاطر الالكترونية.
3- وجود أثر ايجابي معنوي في تعزيز الثقة والمصداقية في الحد من المخاطر الالكترونية.
4- وجود أثر ايجابي قوى ذو دلالة احصائية لدور الامن السيبراني في الحد من المخاطر الالكترونية.
5- تعزيز الامن السيبراني ثقة العملاء في الخدمات الرقمية ويساعد من الحد من التعرض للهجمات الالكترونية.

التوصيات:

1- تعزيز اجراءات الامن السيبراني وحماية المعلومات المصرفية لزيادة ثقة العملاء في استخدام الخدمات المالية الرقمية وتشجيعهم على الاعتماد بشكل أكبر.
2- العمل على تحديث البنية التكنولوجية وشبكات الاتصال بصورة مستمرة لضمان سرعة وكفاءة تقديم الخدمات المصرفية الالكترونية وتحقيق مستويات اعلي من رضا العملاء.

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

3- التوسع في نشر اجهزة ونقاط البيع والخدمات المصرفية الرقمية في مختلف المناطق، بما يسهم في زيادة حجم التعاملات المصرفية.
4- تنفيذ برامج تدريبية مستمرة للعاملين بالمصرف لتنمية مهاراتهم التقنية والادارية وتمكينهم من التعامل بكفاءة مع التطورات الحديثة في مجال الخدمات المصرفية الرقمية.

قائمة المراجع:

أولاً: المراجع العربية:

1_ أبو نصار، محمد (2022). إدارة مخاطر الأمن السيبراني في تعزيز المرونة التنظيمية والمالية في المصارف الإسلامية الأردنية. المجلة الأردنية في إدارة الأعمال، (2018) , 244 _ 266.
2_ العنزي، مشعل. (2021). أثر مخاطر الأمن السيبراني على جودة تقارير المالية في البنوك التجارية الكويتية. مجلة الدراسات التجارية المعاصرة , 7(12) , 101_134.
3_ يوسف، عبد السلام عطية عبد السلام. (2024). تقييم تأثير المخاطر السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية. المجلة العلمية للدراسات التجارية والبيئية. المجلد 15 , العدد 1.
4_ جيجان , إسراء شريف ,(2021) . الأمن السيبراني الصيني، دراسة في الدوافع والتحديات، جامعة بغداد، كلية العلوم السياسية , مجلة قضايا سياسية , 65.
5_ الفضل , علي عبدالحسين , والعرداوي , أمير عقيد كاظم , ومعله , قيصر علي هادي , (2024) . تكنولوجيا المعلومات وقواعد البيانات للتخصصات الإدارية والمالية والاقتصادية والدراسات الأولية والعليا , مطبعة جامعة الكوفا , الطبعة الأولى , العراق , النجف الأشرف .
6_ التائب , علي مفتاح , والسائح , جبريل عمر (2025) :أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية , دراسة تطبيقية على المصارف التجارية العاملة في مدينة سرت , مجلة الدراسات الاقتصادية ,المجلد 8 , العدد 1.
7_ جلايله ,عبدالجليل (2019) : الصيرفة الالكترونية , خدماتها , مخاطرها , بحث منشور في مجلة الاصلاحات الاقتصادية والاندماج في الاقتصاد العالمي , مجلد 13 , العدد 1 , الجزائر , 255 .
8_ سمرة , ياسر محمد , وعزازي ,محمد فتحي , ودرويش , حسين مصطفى , (2022) . تأثير دور إدارة مخاطر الصيرفة الالكترونية في ضوء مقررات بازل بالبنوك , مجلة البحوث للدراسات البيئية معهد الدراسات والبحوث البيئية , جامعة مدينة السادات , مصر , المجلد 12 , العدد 1 .

ثانياً: المراجع الأجنبية:

1. Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking information resource cybersecurity system modeling. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(2), Article 80.
2. Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Mastering compliance: A comprehensive review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal, 5*(1), 120–132.
3. Hasan, L., Hossain, M. Z., Johora, F. T., & Hasan, M. H. (2024). Cybersecurity in accounting: Protecting financial data in the digital age. *European Journal of Applied Science, Engineering and Technology, 2*(6), 63–79.
4. Haxhosaj , A. (2022) The Risks of Electronic Banking , International Journal of Science and Research (IJSR) , Volume 11 Issue 8, Haxhi Zeka University_Kosova .

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of **SAJH** and/or the editor(s). **SAJH** and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).