

تقييم المخاطر السيبرانية وأثرها على استقرار الخدمات المصرفية
الإلكترونية في البنوك السعودية

إعداد الطالبة/ ابرار دعيج الراجح

الرقم الجامعي/ 253000930

إشراف/ د. الفيصل عبد الحميد محمد حسن

د. فايز جراد

العام الدراسي/ 2026

حقوق الطباعة

حقوق الطباعة تمتلكها جامعة ميدأوشن. حيث إن جميع المواد والمحتويات الواردة في هذا البحث هي ملك للجامعة، ولا يجوز استخدامها أو إعادة نشرها أو توزيعها بدون إذن مسبق من جامعة ميدأوشن.

الباحث

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الشكر والتقدير

الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، سيدنا محمد وعلى آله وصحبه أجمعين.

في البداية، أ حمد الله سبحانه وتعالى وأشكره على نعمه الكثيرة وفضله وتوفيقه لي لإتمام هذا البحث، فلولا عونته وتيسيره لما تمكنت من إنجاز هذا العمل.

كما أتقدم بخالص الشكر والتقدير إلى سعادة الدكتور (د. فايز الجراد - د. الفيصل عبد الحميد) على توجيهاته القيمة، وملاحظاته البناءة، ودعمه المستمر خلال مراحل إعداد هذا البحث، فقد كان لإرشاداته العلمية ومتابعته أثر كبير في تطوير محتوى هذا العمل وإتمامه بالصورة المطلوبة.

كما أعبر عن بالغ امتناني وتقديري لكل من أسهم في دعمي ومساندتي خلال فترة إعداد هذا البحث، من أساتذة وزملاء، ممن قدموا لي النصيحة أو المعلومة أو الدعم الذي ساعدني في إنجاز هذا العمل وتطويره.

أتقدم بجزيل الشكر والتقدير لكل من ساهم في توفير البيئة المناسبة لإتمام هذا البحث.

وفي الختام، أهدي هذا الجهد المتواضع إلى والدتي الغالية، التي كانت ولا تزال مصدر الدعم والعطاء في حياتي، وإلى والدي رحمه الله وأسكنه فسيح جناته، وإلى إخوتي وأخواتي على دعمهم وتشجيعهم المستمر، فقد كان لمساندتهم ومحبتهم أثر كبير في منحي الدافع لمواصلة التقدم والنجاح.

أسأل الله تعالى أن يجزي الجميع خير الجزاء، وأن يجعل هذا العمل خالصاً لوجهه الكريم، وأن ينفع به.

المستخلص

يهدف هذا البحث إلى دراسة أثر المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، وذلك في ظل التوسع المتسارع في استخدام التقنيات الرقمية والتحول نحو الخدمات المصرفية الإلكترونية. وقد أدى هذا التطور إلى زيادة تعرض البنوك لمجموعة من المخاطر السيبرانية، مثل الهجمات الإلكترونية، وسرقة البيانات، والاحتيال الإلكتروني، والتي قد تؤثر على استمرارية الخدمات المصرفية وثقة العملاء.

اعتمد البحث على المنهج الوصفي التحليلي باستخدام المنهج الكمي، حيث تم جمع البيانات الأولية من خلال استبانة وزعت على عينة من موظفي البنوك السعودية العاملين في المجالات المرتبطة بالخدمات المصرفية الإلكترونية وتقنية المعلومات والأمن السيبراني وإدارة المخاطر، ثم تحليل البيانات باستخدام الأساليب الإحصائية المناسبة.

أظهرت نتائج الدراسة وجود تأثير للمخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية، حيث تؤدي زيادة المخاطر السيبرانية إلى ارتفاع احتمالية تعطل الخدمات والتأثير على كفاءة الأنظمة ومستوى ثقة العملاء. كما أشارت النتائج إلى أهمية دور إجراءات الأمن السيبراني والاستراتيجيات الوقائية في تعزيز استقرار الخدمات المصرفية الإلكترونية والحد من آثار المخاطر السيبرانية.

وبناءً على نتائج الدراسة، يقدم البحث مجموعة من التوصيات التي تسهم في تطوير ممارسات إدارة المخاطر السيبرانية وتعزيز أنظمة الحماية الرقمية في البنوك السعودية، بما يدعم استمرارية الخدمات المصرفية الإلكترونية ورفع مستوى موثوقيتها.

الكلمات المفتاحية: المخاطر السيبرانية، الخدمات المصرفية الإلكترونية، البنوك السعودية، استقرار الخدمات المصرفية، الأمن السيبراني، إدارة المخاطر.

فهرس المحتويات

المحتويات

الشكر والتقدير	ت
المستخلص.....	ث
فهرس المحتويات.....	ح
قائمة الجداول	ذ
قائمة الاشكال.....	ر
مصطلحات البحث	ز
الفصل الأول.....	١
الإطار العام للدراسة.....	١
١.١ المقدمة:	٢
٢.١ مشكلة الدراسة:	٣
٣.١ أهمية الدراسة:	٥
٤.١ أهداف الدراسة:	٦
٥.١ تساؤلات الدراسة:	٧
٦.١ فرضيات الدراسة:	٨
٧.١ النظرية العلمية المتبعة لإعداد البحث:	٩
٨.١ المتغيرات في النموذج:	١٠
٩.١ النموذج النظري للعلاقة بين المتغيرات.....	١١
الفصل الثاني:.....	١٣
الإطار النظري والدراسات السابقة.....	١٣
٢.١ المقدمة الفصل:.....	١٤

٢٠٢	الإطار النظري للدراسة.....	١٥
٢٠٣	الدراسات السابقة:.....	٢١
٢٠٤	مناقشة نتائج الدراسات السابقة والفجوة البحثية:.....	٢٧
٢٠٥	الفجوة البحثية.....	٢٨
٢٠٦	النموذج النظري للدراسة.....	٢٩
٢٠٧	خاتمة الفصل.....	٣١
	الفصل الثالث:.....	٣٢
	منهجية الدراسة.....	٣٢
٣٠١	مقدمة:.....	٣٣
٣٠٢	منهج البحث:.....	٣٣
٣٠٣	تصميم البحث:.....	٣٤
٣٠٤	مجتمع البحث:.....	٣٦
٣٠٥	عينة الدراسة:.....	٣٦
٣٠٦	أداة الدراسة:.....	٣٧
٣٠٧	قياس متغيرات الدراسة.....	٤٠
٣٠٨	فرضيات الدراسة.....	٤١
٣٠٩	صدق وثبات أداة الدراسة.....	٤١
٣٠١٠	أساليب التحليل الإحصائي.....	٤٢
٣٠١١	حدود الدراسة.....	٤٢
٣٠١٢	خاتمة الفصل.....	٤٣
	الفصل الرابع:.....	٤٤
	النتائج ومناقشتها.....	٤٤
٤٠١	مقدمة:.....	٤٥

٥٠	٤.٣ التحليل الوصفي لمحاوَر الدراسة
٥١	٤.٤ اختبار فرضيات الدراسة
٥٥	٤.٥ ملخص نتائج الفصل الرابع
٥٧	الفصل الخامس:
٥٧	التوصيات والمقترحات الملاحق
٥٨	١,٥ مقدمة:
٥٨	٥.٢ مناقشة نتائج الدراسة
٦٢	٥.٣ استنتاجات الدراسة
٦٣	٥.٤ توصيات الدراسة
٦٤	٥.٥ مقترحات الدراسات المستقبلية
٦٥	المراجع:
٦٥	أولاً: المراجع العربية
٦٦	ثانياً: المراجع الإنجليزية
٦٩	الملاحق

قائمة الجداول

جدول ١ (١-١): متغيرات الدراسة.....	١٢
جدول ٢ (١-٣): قياس متغيرات الدراسة.....	٤٠
جدول ٣ (٣-٢): توزيع فقرات الاستبانة على متغيرات الدراسة.....	٤٠
جدول ٤ (١-٤): توزيع أفراد عينة الدراسة حسب الجنس.....	٤٦
جدول ٥ (٢-٤): توزيع افراد عينة الدراسة حسب العمر.....	٤٧
جدول ٦ (٣-٤): توضيح أفراد عينة الدراسة حسب المؤهل العلمي.....	٤٧
جدول 7 (4-4): توزيع أفراد عينة الدراسة حسب سنوات الخبرة.....	٤٨
جدول 8 (٥-٤): توزيع أفراد عينة الدراسة حسب المجال الوظيفي.....	٤٩
جدول 9 (٤-٦): المتوسطات الحسابية لمحاور الدراسة.....	٥٠
جدول 10 (٧-٤): العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الالكترونية.....	٥٢
جدول 11 (٨-٤): العلاقة بين استراتيجيات الأمن السبراني واستقرار الخدمات المصرفية.....	٥٣
جدول ١٢ (٩-٤): اختبار العلاقة بين المخاطر السيبرانية والإجراءات الأمنية و الاستراتيجيات الوقائي.....	٥٤
جدول 13 (١٠-٤): اختبار العلاقة بين الوعي الأمني لدى الموظفين واستقرار الخدمات	
الخدمات المصرفية الإلكتروني.....	٥٥

قائمة الاشكال

رسم توضيحي ٢ شكل (٢-١) النموذج النظري للدراسة.....	٣٠
رسم توضيحي ٣ (1-4) التوزيع النسبي لأفراد العينة حسب الجنس.....	٤٦
رسم توضيحي ٤ (٢-٤).....	٤٩

مصطلحات البحث

تضمن الدراسة الحالية مجموعة من المصطلحات الأساسية المرتبطة بموضوع البحث، وهي كما يلي:

١ - المخاطر السيبرانية:

تُعرف المخاطر السيبرانية بأنها مجموعة التهديدات والهجمات الإلكترونية التي تستهدف الأنظمة المعلوماتية والشبكات والبنية التحتية الرقمية للمؤسسات، والتي قد تؤدي إلى اختراق الأنظمة، أو سرقة البيانات، أو الاحتيال الإلكتروني، أو تعطيل الخدمات المصرفية الإلكترونية.

٢ - الخدمات المصرفية الإلكترونية:

تشير الخدمات المصرفية الإلكترونية إلى الخدمات المالية التي تقدمها البنوك للعملاء باستخدام القنوات الرقمية، مثل المواقع الإلكترونية والتطبيقات المصرفية والوسائل التقنية الأخرى، بهدف تسهيل تنفيذ المعاملات المصرفية بسرعة وكفاءة.

٣ - الإجراءات الأمنية والاستراتيجيات الوقائية:

يقصد بها مجموعة السياسات والإجراءات والتقنيات الأمنية التي تطبقها البنوك بهدف حماية الأنظمة والبيانات الرقمية، والحد من تأثير المخاطر السيبرانية، وتعزيز قدرة المؤسسة على مواجهة التهديدات الإلكترونية.

٤ - استقرار الخدمات المصرفية الإلكترونية:

يقصد به قدرة البنوك على تقديم خدماتها المصرفية الإلكترونية بصورة مستمرة وآمنة وفعالة دون انقطاع، مع ضمان حماية بيانات العملاء والمحافظة على جودة الخدمة وثقة المستخدمين

الفصل الأول

الإطار العام للدراسة

١.١ المقدمة:

شهد القطاع المصرفي في السنوات الأخيرة تطوراً ملحوظاً نتيجة التقدم التكنولوجي المتسارع والتحول الرقمي، الأمر الذي انعكس بشكل مباشر على طبيعة الخدمات المصرفية وأساليب تقديمها للعملاء. وقد أصبح الاعتماد على الخدمات المصرفية الإلكترونية أحد أهم مخرجات هذا التحول، حيث تعتمد البنوك على القنوات الرقمية مثل الإنترنت وتطبيقات الهواتف الذكية لتقديم خدماتها المالية بسرعة وكفاءة عالية، بما يسهم في تحسين جودة الأداء وتسهيل تنفيذ المعاملات في أي وقت ومن أي مكان (الدرعي، ٢٠٢٢).

وفي المقابل، أدى هذا التوسع في الاعتماد على الأنظمة الرقمية إلى زيادة مستوى التعرض للمخاطر السيبرانية، والتي تشمل الهجمات الإلكترونية مثل الاختراقات، وسرقة البيانات، والاحتيال المالي، وهي مخاطر قد تؤثر بشكل مباشر على استقرار الخدمات المصرفية الإلكترونية وثقة العملاء. وتشير تقارير البنك المركزي السعودي (SAMA) إلى أن القطاع المالي يُعد من أكثر القطاعات استهدافاً للهجمات السيبرانية، نظراً لحساسية البيانات المالية واعتماده الكبير على الأنظمة الرقمية (SAMA, 2023).

كما تؤكد الهيئة الوطنية للأمن السيبراني (NCA) أن التحول الرقمي المتسارع في المملكة العربية السعودية، رغم ما يحققه من كفاءة وابتكار، إلا أنه يرفع من مستوى المخاطر السيبرانية، مما يستدعي تبني استراتيجيات متقدمة لإدارة هذه المخاطر وتعزيز أمن المعلومات في القطاع المالي (NCA, 2024). وفي السياق ذاته، تشير تقارير دولية مثل صندوق النقد الدولي (IMF) وبنك التسويات الدولية (BIS) إلى أن المخاطر السيبرانية أصبحت أحد أبرز التحديات التي تواجه الاستقرار المالي للمؤسسات المصرفية عالمياً.

وقد تناولت بعض الدراسات الحديثة موضوع الأمن السيبراني في القطاع المصرفي، حيث أشارت إلى أن ارتفاع مستوى المخاطر السيبرانية يؤدي إلى زيادة الاضطرابات التشغيلية وتقليل كفاءة

الخدمات المصرفية الإلكترونية، بينما تسهم الاستراتيجيات الوقائية الفعالة في الحد من هذه التأثيرات وتعزيز استقرار الأنظمة المصرفية الرقمية (Bensaid & Mezrag, 2023). كما تؤكد دراسات أخرى أن فعالية إدارة المخاطر السيبرانية تُعد عاملاً رئيسياً في الحفاظ على استمرارية وجودة الخدمات المصرفية.

وفي المملكة العربية السعودية، تسعى البنوك إلى مواكبة متطلبات التحول الرقمي بما يتماشى مع رؤية المملكة ٢٠٣٠، التي تؤكد أهمية تطوير الاقتصاد الرقمي وتعزيز التحول التقني في مختلف القطاعات، بما في ذلك القطاع المالي (رؤية المملكة العربية السعودية ٢٠٣٠). إلا أن هذا التوسع في الخدمات الرقمية يصاحبه ارتفاع في احتمالية التعرض للمخاطر السيبرانية، مما يجعل من الضروري دراسة هذه المخاطر وتحليل أثرها على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

وعلى الرغم من اهتمام الدراسات السابقة بموضوع الأمن السيبراني في القطاع المصرفي، إلا أن معظمها ركز على الجوانب التقنية أو أثر التحول الرقمي بشكل عام، في حين ما تزال الدراسات التي تتناول العلاقة المباشرة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية محدودة نسبياً. ومن هنا تتبّع الفجوة البحثية التي تسعى هذه الدراسة إلى معالجتها من خلال تحليل أثر المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية، ودراسة دور الإجراءات الأمنية والاستراتيجيات الوقائية في الحد من هذا التأثير.

٢.١ مشكلة الدراسة:

تواجه البنوك في الوقت الحاضر تحديات متزايدة في مجال الأمن السيبراني نتيجة الاعتماد المتسارع على الأنظمة الرقمية والتقنيات الحديثة في تقديم الخدمات المصرفية الإلكترونية، مما جعل القطاع المصرفي من أكثر القطاعات استهدافاً للهجمات السيبرانية عالمياً (SAMA, 2023؛ NCA, 2024). ومع التوسع الكبير في استخدام الخدمات المصرفية الإلكترونية،

أصبحت المؤسسات المالية عرضة لأنواع متعددة من التهديدات مثل الاختراقات الإلكترونية، وسرقة البيانات، والاحتيال المالي، وهجمات تعطيل الخدمات.

وتكمن مشكلة الدراسة في أن هذه المخاطر السيبرانية قد تؤثر بشكل مباشر على استقرار الخدمات المصرفية الإلكترونية، حيث يمكن أن تؤدي إلى توقف الأنظمة المصرفية أو تسريب البيانات الحساسة أو التأثير على مستوى ثقة العملاء في الخدمات الرقمية المقدمة من البنوك. وعلى الرغم من الجهود الكبيرة التي تبذلها البنوك السعودية في تطوير أنظمة الأمن السيبراني وتطبيق تقنيات الحماية الرقمية، إلا أن التطور المستمر في أساليب الهجمات السيبرانية يجعل من الصعب الحد من هذه المخاطر بشكل كامل.

وقد أشارت بعض الدراسات السابقة إلى أن المخاطر السيبرانية في القطاع المصرفي ترتبط بزيادة المخاطر التشغيلية وانخفاض كفاءة الخدمات الإلكترونية، كما أوضحت دراسات أخرى أن وجود استراتيجيات فعالة لإدارة الأمن السيبراني يساهم في تقليل آثار هذه المخاطر وتحسين استقرار الأنظمة المصرفية (Bensaid & Mezrag, 2023). إلا أن معظم هذه الدراسات ركزت على السياق العالمي أو على الجوانب التقنية العامة، بينما ما تزال الدراسات التي تتناول العلاقة المباشرة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية محدودة نسبيًا، خصوصًا في ظل التوسع الكبير في التحول الرقمي داخل القطاع المصرفي السعودي.

ومن جهة أخرى، تشير التقارير الصادرة عن البنك المركزي السعودي (SAMA) والهيئة الوطنية للأمن السيبراني (NCA) إلى ارتفاع معدل التهديدات السيبرانية الموجهة للقطاع المالي، مما يعزز الحاجة إلى دراسات تحليلية أكثر عمقًا لفهم طبيعة هذه المخاطر وأثرها الفعلي على استقرار الخدمات المصرفية الإلكترونية، خاصة في بيئة البنوك السعودية التي تعتمد بشكل متزايد على الخدمات الرقمية.

وبناءً على ذلك، تتمثل مشكلة الدراسة في الحاجة إلى تحليل طبيعة المخاطر السيبرانية التي تواجه البنوك السعودية، وقياس مدى تأثيرها على استقرار الخدمات المصرفية الإلكترونية، بالإضافة إلى دراسة دور الإجراءات الأمنية والاستراتيجيات الوقائية في الحد من هذا التأثير. كما تسعى الدراسة إلى سد الفجوة البحثية من خلال تقديم تحليل ميداني يركز على البيئة المصرفية السعودية، بما يسهم في تعزيز المعرفة العلمية وتقديم نتائج يمكن الاستفادة منها في تطوير سياسات الأمن السيبراني داخل البنوك

٣.١ أهمية الدراسة:

تتبع أهمية هذه الدراسة من كونها تتناول أحد الموضوعات الحيوية في القطاع المصرفي، والمتمثل في المخاطر السيبرانية وأثرها على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، في ظل التوسع المتسارع في الاعتماد على الأنظمة الرقمية. وتكمن أهمية الدراسة في مساهمتها العلمية والتطبيقية في تحليل هذه العلاقة وتقديم فهم أعمق لطبيعة تأثير المخاطر السيبرانية على استقرار الخدمات المصرفية.

كما تسعى هذه الدراسة إلى تقديم إضافة علمية من خلال تحليل العلاقة بين المتغيرات محل الدراسة (المخاطر السيبرانية، استقرار الخدمات المصرفية الإلكترونية، والإجراءات الوقائية)، بما يسهم في تطوير المعرفة في مجال الأمن السيبراني المصرفي، خاصة في السعودية التي تشهد تحولاً رقمياً متسارعاً.

❖ أولاً: الأهمية العلمية:

- يسهم هذا البحث في إثراء الأدبيات العلمية المتعلقة بالمخاطر السيبرانية في القطاع المصرفي، من خلال دراسة تأثيرها المباشر على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

- يساعد هذا البحث في سد فجوة بحثية تتمثل في محدودية الدراسات التي تناولت العلاقة المباشرة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البيئة المصرفية السعودية.
- يسهم هذا البحث في تقديم إطار تحليلي يمكن الاستفادة منه في الدراسات المستقبلية المتعلقة بالأمن السيبراني وإدارة المخاطر في المؤسسات المالية، وخاصة في ظل التحول الرقمي المتسارع.

❖ ثانيًا: الأهمية العملية:

- تساعد نتائج الدراسة إدارات البنوك السعودية على فهم طبيعة المخاطر السيبرانية ومدى تأثيرها على استقرار الخدمات المصرفية الإلكترونية.
- يمكن ان تسهم في دعم تطوير استراتيجيات وإجراءات الأمن السيبراني داخل البنوك بما يعزز القدرة على مواجهة التهديدات الإلكترونية.
- تقدم الدراسة توصيات تطبيقية يمكن أن تساعد في رفع كفاءة أنظمة الحماية الرقمية، وتقليل أثر الهجمات السيبرانية، وتعزيز ثقة العملاء في الخدمات المصرفية الإلكترونية.
- كذلك يمكن أن تدعم نتائج الدراسة الجهات التنظيمية مثل البنك المركزي السعودي في تطوير سياسات أكثر فاعلية لإدارة المخاطر السيبرانية في القطاع المالي.

٤.١ أهداف الدراسة:

تهدف هذه الدراسة إلى تحليل أثر المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية،

وذلك من خلال تحقيق هدف رئيسي يتفرع منه مجموعة من الأهداف الفرعية التي تتمثل في:

أولاً: الهدف الرئيسي

تحليل أثر المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية

ثانياً: الأهداف الفرعية

- التعرف على مفهوم المخاطر السيبرانية وأهميتها في القطاع المصرفي.
- تحديد أنواع المخاطر السيبرانية التي تواجه البنوك السعودية في مجال الخدمات المصرفية الإلكترونية.
- قياس وتحليل تأثير المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية.
- التعرف على دور الإجراءات الأمنية والاستراتيجيات الوقائية في الحد من تأثير المخاطر السيبرانية.
- تقديم تصور علمي حول العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، بما يساعد في فهم التحديات التي تواجه البنوك السعودية.

٥.١ تساؤلات الدراسة:

تنطلق هذه الدراسة من مشكلة بحثية تتمثل في تحليل أثر المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، وتتمثل مشكلة الدراسة في الإجابة عن التساؤلات التالية:

١. ما مفهوم المخاطر السيبرانية في القطاع المصرفي السعودي؟
٢. ما أهم أنواع المخاطر السيبرانية التي تواجه البنوك السعودية في مجال الخدمات المصرفية الإلكترونية؟

٣. ما مدى تأثير المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية؟

٤. ما الإجراءات والاستراتيجيات التي تعتمد عليها البنوك السعودية للحد من تأثير المخاطر السيبرانية؟

٥. كيف يمكن تعزيز استقرار الخدمات المصرفية الإلكترونية من خلال إدارة فعالة للمخاطر السيبرانية في البنوك السعودية؟

٦.١ فرضيات الدراسة:

استناد المشكلة الدارسة وأهدافها والإطار النظري والدراسات السابقة، تم صياغة فرضيات الدراسة كما يلي:

❖ H1 الفرضية الرئيسية:

توجد علاقة ذات دلالة إحصائية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية

❖ H1-1 الفرضية الأولى:

توجد علاقة ذات دلالة إحصائية بين الهجمات الإلكترونية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

❖ H1-2 الفرضية الثانية:

توجد علاقة ذات دلالة إحصائية بين سرقة البيانات والاحتيال الإلكتروني واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية

❖ H1-3 الفرضية الثالثة:

توجد علاقة ذات دلالة إحصائية بين انقطاع الخدمات الناتج عن المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

❖ 4-1 H1 الفرضية الرابعة:

توجد علاقة ذات دلالة إحصائية بين إجراءات الأمن السيبراني والاستراتيجيات الوقائية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

٧.١ النظرية العلمية المتبعة لإعداد البحث:

يعتمد هذا البحث على نظرية إدارة المخاطر كإطار علمي لتفسير العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية. وتفترض هذه النظرية أن المؤسسات تواجه مجموعة من المخاطر التي قد تؤثر على تحقيق أهدافها التشغيلية والاستراتيجية، مما يتطلب تحديد هذه المخاطر وتحليلها وتقييمها ووضع الإجراءات المناسبة للحد من أثارها.

وفي إطار الدراسة الحالية، يتم توظيف نظرية إدارة المخاطر لتفسير أثر المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية، حيث تفترض الدراسة أن ارتفاع مستوى المخاطر السيبرانية قد يؤدي إلى انخفاض مستوى استقرار الخدمات الإلكترونية، بينما تسهم الإجراءات الأمنية والاستراتيجيات الوقائية الفعالة في تعزيز قدرة البنوك على مواجهة هذه المخاطر والحفاظ على استمرارية الخدمات المصرفية الإلكترونية.

٨.١ المتغيرات في النموذج:

❖ المتغير المستقل:

المخاطر السيبرانية.

وتشير إلى التهديدات والهجمات الإلكترونية التي قد تواجه البنوك وتؤثر على أنظمتها وخدماتها المصرفية الإلكترونية، وتشمل: التي تواجه البنوك، مثل:

- الهجمات الإلكترونية
- سرقة البيانات
- الاحتيال المالي الإلكتروني
- انقطاع الخدمة أو الأعطال الناتجة عن الهجمات السيبرانية

❖ المتغير التابع:

استقرار الخدمات المصرفية الإلكترونية

ويقصد به قدرة البنوك على تقديم خدماتها الإلكترونية بصورة مستمرة وأمنة وفعالة دون انقطاع، ويقاس من خلال:

- استمرارية الخدمات الإلكترونية
- حماية بيانات العملاء والمعاملات المالية
- ثقة العملاء بالخدمات المصرفية الإلكترونية
- سرعة الاستجابة للحوادث والأعطال

❖ العامل المفسر:

إجراءات الأمن السيبراني والاستراتيجيات الوقائية

وتشير إلى سياسات والإجراءات والتقنيات التي تطبقها البنوك للحد من المخاطر السيبرانية وتعزيز حماية الأنظمة والخدمات الإلكترونية وتشمل:

- أنظمة الحماية الأمنية
- تحديث الأنظمة الأمنية
- سياسات إدارة المخاطر السيبرانية
- التدريب والتوعية الأمنية للموظفين
- تقنيات التشفير والمراقبة المستمرة

٩.١ النموذج النظري للعلاقة بين المتغيرات

يوضح النموذج النظري العلاقة بين المتغيرات، حيث تؤثر العلاقة بين المتغيرات، حيث تؤثر المخاطر السيبرانية بشكل مباشر على استقرار الخدمات المصرفية الإلكترونية، بينما تعمل إجراءات الأمن السيبراني كعامل معدل يخفف من هذا التأثير السلبي.

شكل رقم (١-١) متغيرات الدراسة

جدول ١ (١-١) متغيرات الدراسة

نوع المتغير	اسم المتغير	التعريف المختصر	مؤشرات القياس
المتغير المستقل	المخاطر السيبرانية	هي التهديدات والهجمات التي تواجه البنوك عبر الأنظمة والخدمات الرقمية	الهجمات الإلكترونية، سرقة البيانات، الاختيال الإلكتروني، انقطاع الخدمات
المتغير التابع	استقرار الخدمات المصرفية الإلكترونية	قدرة البنوك على تقديم خدمات إلكترونية مستمرة وأمنه وفعالة	استمرارية الخدمات حماية البيانات، ثقة العملاء، سرعة الاستجابة للحوادث
المتغير المفسر	إجراءات الأمن السيبراني والاستراتيجيات الوقائية	السياسات والتقنيات والإجراءات المستخدمة للحد من المخاطر السيبرانية	أنظمة الحماية، التدريب الأمني، سياسات الأمن، أنظمة المراقبة

الفصل الثاني:

الإطار النظري والدراسات السابقة

٢.١ المقدمة الفصل:

تُعد الدراسات السابقة والإطار النظري من الركائز الأساسية في البحث العلمي، حيث يساعد الباحث فهم المعرفة العلمية المتراكمة حول موضوع الدراسة، وتحديد المفاهيم الأساسية، وتحليل الاتجاهات البحثية السابقة بالإضافة إلى تحديد الفجوة البحثية التي تسعى الدراسة الحالية إلى معالجتها.

يتناول هذا الفصل الإطار النظري والدراسات السابقة المتعلقة بالمخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، وذلك من خلال استعراض مفهوم المخاطر السيبرانية وأنواعها، ومصادرها، وطرق إدارتها، إضافة إلى توضيح مفهوم استقرار الخدمات المصرفية الإلكترونية ودور الإجراءات الأمنية والاستراتيجيات الوقائية في الحد من تأثير المخاطر السيبرانية.

كما يناقش هذا الفصل الدراسات السابقة المرتبطة بمتغيرات الدراسة، حيث تمثل المخاطر السيبرانية المتغير المستقل الأول، بينما يمثل استقرار الخدمات المصرفية الإلكترونية المتغير التابع، وتمثل الإجراءات الأمنية والاستراتيجيات الوقائية متغيراً مستقلاً مفسراً يسهم في تعزيز استقرار الخدمات المصرفية الإلكترونية وتقليل آثار المخاطر السيبرانية.

ويختتم هذا الفصل بتحديد الفجوة البحثية التي تستهدف الدراسة الحالية معالجتها من خلال دراسة العلاقة بين هذه المتغيرات في البيئة المصرفية السعودية.

٢.٢ الإطار النظري للدراسة

أولاً: مفهوم المخاطر السيبرانية

أصبحت المخاطر السيبرانية من أبرز التحديات التي تواجه المؤسسات المالية نتيجة الاعتماد المتزايد على الأنظمة الرقمية والخدمات الإلكترونية.

وتشير المخاطر السيبرانية إلى احتمالية تعرض الأنظمة والشبكات والبيانات لهجمات إلكترونية أو اختراقات قد تؤثر على سرية المعلومات وسلامتها واستمرارية الخدمات.

تُعرف المخاطر السيبرانية بأنها مجموعة من التهديدات الرقمية التي تستهدف الأصول المعلوماتية للمؤسسات، وقد تؤدي إلى فقدان البيانات أو تعطيل العمليات التشغيلية أو التأثير على قدرة المؤسسة على تقديم خدماتها بكفاءة (Kopp et al., 2017).

وفي القطاع المصرفي، تزداد أهمية إدارة المخاطر السيبرانية بسبب حساسية البيانات المالية واعتماد العملاء بشكل كبير على الخدمات المصرفية الإلكترونية، مما يجعل أي اختراق أو تعطل تقني ذا تأثير مباشر على استمرارية العمليات وثقة العملاء.

ثانياً: أنواع المخاطر السيبرانية في القطاع المصرفي

تتعدد أنواع المخاطر السيبرانية التي تواجه البنوك، ومن أبرزها:

١. الهجمات الإلكترونية:

تتمثل في الوصول غير المشروع إلى المعلومات الحساسة الخاصة بالعملاء أو العمليات المالية، مما قد يؤدي إلى خسائر مالية وانخفاض ثقة العملاء.

٢. سرقة البيانات:

تمثل في الوصول غير المشروع إلى المعلومات الحساسة الخاصة بالعملاء أو العمليات المالية، مما قد يؤدي إلى خسائر مالية وانخفاض ثقة العملاء.

٣. الاحتيال الإلكتروني:

يشير إلى استخدام الوسائل الرقمية لتنفيذ عمليات احتيالية مثل سرقة الحسابات أو الحصول على معلومات العملاء بطرق غير قانونية.

٤. انقطاع الخدمات الإلكترونية:

ينتج عن الهجمات السيبرانية أو الأعطال التقنية التي تؤدي إلى توقف أو انخفاض كفاءة الخدمات المصرفية الإلكترونية

وتؤكد الدراسات أن تنوع هذه المخاطر يجعل من الضروري تطوير أنظمة أمنية متقدمة واستراتيجيات فعالة لإدارة المخاطر داخل المؤسسات المصرفية (Alrawad,2024)

ثالثاً: مصادر المخاطر السيبرانية

يمكن تصنيف مصادر المخاطر السيبرانية إلى ثلاثة مصادر رئيسية:

١. مصادر داخلية:

وتشمل أخطاء الموظفين، ضعف الوعي الأمني، أو سوء استخدام الأنظمة الداخلية.

٢. مصادر خارجية:

مثل الهجمات الإلكترونية المنظمة البرمجيات خبيثة، ومحاولا الاحتيال الخبيثة.

٣. مصادر تقنية:

وتتمثل في الثغرات الأمنية تحديث الأنظمة، وعدم كفاءة البنية التحتية الرقمية.

رابعاً: خطوات إدارة المخاطر السيبرانية

تعد إدارة المخاطر السيبرانية من العمليات الأساسية التي تساعد المؤسسات المصرفية على التعرف على التهديدات المحتملة وتحليل آثارها ووضع الإجراءات المناسبة للحد منها. وتعتمد

إدارة المخاطر على منهجية منظمة تهدف إلى تقليل احتمالية حدوث المخاطر وتقليل تأثيرها على استمرارية الأعمال.

وفقاً لمعيار ISO 31000 (٢٠١٨)، تمر عملية إدارة المخاطر بعدة مراحل رئيسية تشمل:

تمر عملية إدارة المخاطر السيبرانية بعدة مراحل أساسية تهدف إلى الحد من تأثيرها على المؤسسات المصرفية، وتشمل:

١. تحديد المخاطر:

تمثل هذه المرحلة في التعرف على مصادر التهديدات المحتملة التي قد تؤثر على الأنظمة المصرفية الإلكترونية، مثل الهجمات الإلكترونية أو تسريب البيانات أو الأعطال التقنية.

٢. تحليل المخاطر:

يتم خلالها دراسة احتمالية حدوث الخطر وحجم تأثيره على العمليات والخدمات المصرفية، بهدف فهم مستوى التهديدات بشكل دقيق.

٣. تقييم المخاطر:

تهدف هذه المرحلة إلى تحديد أولويات المخاطر وتصنيفها وفقاً لدرجة تأثيرها واحتمالية حدوثها، مما يساعد الإدارة على توجيه الموارد المناسبة لمعالجتها.

٤. معالجة المخاطر:

تشمل وضع الإجراءات والاستراتيجيات المناسبة للتعامل مع المخاطر، مثل تقوية الأنظمة الأمنية، وتطوير سياسات الحماية، وتنفيذ برامج التدريب والتوعية.

٥. المراقبة والمراجعة المستمرة:

تتطلب المخاطر السيبرانية المتغيرة متابعة مستمرة وتحديث الإجراءات الأمنية لمواكبة التهديدات الحديثة.

وتؤكد أطر إدارة المخاطر الحديثة أن الإدارة الفعالة للمخاطر السيبرانية تسهم في تعزيز قدرة المؤسسات المالية على المحافظة على استمرارية عملياتها وتقليل الآثار الناتجة عن الحوادث الأمنية (COSO, 2017).

• الإجراءات الأمنية والاستراتيجيات الوقائية (المتغير المستقل المفسر)

تمثل الإجراءات الأمنية والاستراتيجيات الوقائية أحد العوامل الأساسية التي تساعد البنوك على مواجهة المخاطر السيبرانية وتعزيز استقرار الخدمات المصرفية الإلكترونية.

ويقصد بالإجراءات الأمنية مجموعة السياسات والضوابط والتقنيات التي تطبقها المؤسسات لحماية الأنظمة والشبكات والبيانات من التهديدات الإلكترونية. وتشمل الإجراءات الأمنية في القطاع المصرفي عدة أبعاد رئيسية:

أولاً: سياسات وإدارة الأمن السيبراني

تشمل وضع سياسات واضحة لإدارة المخاطر السيبرانية وتحديد المسؤوليات والإجراءات اللازمة لحماية المعلومات.

ثانياً: أنظمة الحماية والمراقبة المستمرة

تساعد أنظمة المراقبة الأمنية على اكتشاف التهديدات ومحاولات الاختراق بشكل مبكر، مما يقلل من تأثير الحوادث السيبرانية.

ثالثاً: التشفير وحماية البيانات

يعد استخدام تقنيات التشفير من أهم وسائل حماية البيانات والمعاملات الإلكترونية وضمان سريتها.

رابعاً: التدريب والتوعية الأمنية

يُعد الموظفون أحد العناصر المهمة في منظومة الأمن السيبراني، لذلك فإن تدريبهم ورفع مستوى وعيهم يقلل من المخاطر الناتجة عن الأخطاء البشرية.

وتشير أطر الأمن السيبراني الدولية إلى أن بناء منظومة أمنية فعالة يتطلب الجمع بين الجوانب التقنية والبشرية والتنظيمية لتحقيق مستوى أعلى من الحماية (NIST, 2024).

كما أكد البنك المركزي السعودي أهمية تطبيق ضوابط الأمن السيبراني في المؤسسات المالية بهدف تعزيز الحماية ورفع مستوى جاهزية القطاع المصرفي لمواجهة التهديدات الرقمية (SAMA, 2022).

• استقرار الخدمات المصرفية الإلكترونية (المتغير التابع)

يمثل استقرار الخدمات المصرفية الإلكترونية قدرة البنوك على تقديم خدماتها الرقمية بصورة مستمرة وآمنة وفعالة دون حدوث انقطاع أو تأثير جوهري نتيجة المخاطر التقنية أو السيبرانية.

ويعد استقرار الخدمات المصرفية الإلكترونية عنصراً أساسياً في نجاح التحول الرقمي للقطاع المصرفي، حيث يعتمد العملاء بشكل متزايد على الخدمات الإلكترونية في تنفيذ العمليات المالية المختلفة.

ويتضمن استقرار الخدمات المصرفية الإلكترونية عدة أبعاد رئيسية:

أولاً: استمرارية الخدمات الإلكترونية

ويقصد بها قدرة البنك على المحافظة على توفر الخدمات المصرفية الإلكترونية وعدم توقفها أثناء الظروف الطارئة أو الحوادث الأمنية.

ثانياً: حماية بيانات العملاء والمعاملات المالية

تشير إلى قدرة البنك على المحافظة على سرية وسلامة المعلومات المالية ومنع الوصول غير المصرح به.

ثالثاً: سرعة الاستجابة للحوادث السيبرانية

تعكس قدرة البنك على اكتشاف الحوادث الأمنية والتعامل معها بسرعة للحد من آثارها.

رابعاً: ثقة العملاء بالخدمات الإلكترونية

تعد ثقة العملاء مؤشراً مهماً على نجاح الخدمات المصرفية الإلكترونية، حيث ترتبط بمدى شعور العملاء بالأمان والاعتمادية.

وقد أوضحت الدراسات أن المخاطر السيبرانية يمكن أن تؤثر بشكل مباشر على استمرارية العمليات المصرفية، بينما تسهم الإدارة الفعالة للمخاطر والإجراءات الوقائية في تعزيز استقرار الخدمات المصرفية (Kopp et al., 2023; Basel Committee, 2023)

٢.٣ الدراسات السابقة:

تناولت العديد من الدراسات موضوع المخاطر السيبرانية وتأثيرها على القطاع المصرفي والخدمات المالية الإلكترونية، كما ركزت بعض الدراسات على دور الإجراءات الأمنية والاستراتيجيات الوقائية في تعزيز استقرار الأنظمة المصرفية وتقليل آثار التهديدات الرقمية. وفيما يلي عرض لأبرز الدراسات ذات العلاقة بموضوع الدراسة الحالية:

▪ الدراسات المتعلقة بالمخاطر السيبرانية في القطاع المصرفي

دراسة Al Mohayya & Makeen (٢٠٢٥)

هدفت الدراسة إلى تحليل تأثير الهندسة الاجتماعية باعتبارها أحد أساليب الهجمات السيبرانية على مستوى المخاطر في البنوك بمدينة الرياض.

اعتمدت الدراسة على المنهج الوصفي التحليلي، باستخدام الاستبيان كأداة لجمع البيانات وتحليلها إحصائياً. وتمثل مجتمع الدراسة في موظفي البنوك بمدينة الرياض، وخاصة العاملين في الأقسام المرتبطة بالأمن السيبراني وتقنية المعلومات.

أظهرت النتائج أن الهندسة الاجتماعية تعد من أكثر أساليب الهجوم السيبراني تأثيراً على البنوك، وأن ارتفاع مستوى الوعي الأمني لدى الموظفين لا يمنع بشكل كامل التعرض للمخاطر السيبرانية.

وأوصت الدراسة بضرورة تعزيز برامج التدريب الأمني، ورفع مستوى الوعي لدى الموظفين، وتطوير السياسات الداخلية للأمن السيبراني.

أوجه الاستفادة من الدراسة الحالية:

تدعم هذه الدراسة أهمية العنصر البشري والوعي الأمني باعتباره أحد مصادر المخاطر السيبرانية في القطاع المصرفي.

دراسة Alrawad (٢٠٢٤)

هدفت الدراسة إلى دراسة التهديدات السيبرانية التي تواجه المؤسسات المالية في ظل التحول الرقمي.

اعتمدت الدراسة على المنهج النوعي من خلال تحليل الأدبيات والتقارير السابقة المتعلقة بالأمن السيبراني في القطاع المالي.

أوضحت النتائج أن التوسع في التحول الرقمي يؤدي إلى زيادة احتمالية التعرض للهجمات السيبرانية، مما قد يسبب خسائر مالية وانخفاض مستوى ثقة العملاء.

وأوصت الدراسة بضرورة تعزيز البنية التحتية للأمن السيبراني وتطوير استراتيجيات الحماية الرقمية.

أوجه الاستفادة من الدراسة الحالية:

توضح العلاقة بين التحول الرقمي وارتفاع مستوى المخاطر السيبرانية، وهو ما يرتبط بدراسة تأثير المخاطر السيبرانية على الخدمات المصرفية الإلكترونية.

■ الدراسات المتعلقة بالخدمات المصرفية الإلكترونية

دراسة Sayari (٢٠٢٤)

هدفت الدراسة إلى تحليل أثر الخدمات المصرفية الإلكترونية على أداء البنوك في المملكة العربية السعودية.

استخدمت الدراسة المنهج الكمي من خلال تحليل البيانات المالية الفعلية لعينة مكونة من ١٠ بنوك سعودية خلال الفترة (٢٠١٣-٢٠٢٢).

توصلت النتائج إلى أن الخدمات المصرفية الإلكترونية تؤثر بشكل إيجابي على الأداء المالي للبنوك، كما أكدت أهمية الاستثمار في الخدمات الرقمية لتعزيز الكفاءة التشغيلية.

أوجه الاستفادة من الدراسة الحالية:

توضح أهمية الخدمات المصرفية الإلكترونية وارتباطها بأداء واستقرار القطاع المصرفي.

■ الدراسات المتعلقة بالأمن السيبراني والحوكمة

دراسة Elsayed et al (٢٠٢٤)

هدفت الدراسة إلى دراسة تأثير الإفصاح عن الأمن السيبراني والحوكمة على الأداء المؤسسي للبنوك.

اعتمدت الدراسة على المنهج الكمي باستخدام الاستبيانات والتحليل الإحصائي، وشملت عينة من العاملين في المؤسسات المالية والمصرفية.

أظهرت النتائج أن الإفصاح عن ممارسات الأمن السيبراني وتطبيق الحوكمة يسهمان في تعزيز الأداء المؤسسي وزيادة مستوى الثقة.

وأوصت الدراسة بزيادة الشفافية وتطوير أنظمة الحوكمة في القطاع المصرفي.

أوجه الاستفادة من الدراسة الحالية:

تدعم أهمية الإجراءات الأمنية والسياسات التنظيمية في تحسين قدرة البنوك على مواجهة المخاطر السيبرانية.

■ الدراسات المتعلقة باستمرارية الأعمال والمرونة التشغيلية

دراسة Kopp et al. (٢٠٢٣)

هدفت الدراسة إلى تحليل تأثير المخاطر السيبرانية على استمرارية الأعمال في القطاع المصرفي.

اعتمدت الدراسة على المنهج الوصفي التحليلي من خلال دراسة تقارير وممارسات المؤسسات المالية الدولية.

أظهرت النتائج أن المخاطر السيبرانية تؤثر بشكل مباشر على استمرارية العمليات التشغيلية، وأن ضعف الاستعداد الأمني يزيد من تأثير الحوادث السيبرانية.

وأوصت الدراسة بتطوير استراتيجيات متقدمة لإدارة المخاطر السيبرانية وتعزيز المرونة التشغيلية.

أوجه الاستفادة من الدراسة الحالية:

تدعم العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية.

■ الدراسات التنظيمية والتقارير الدولية

دراسة Basel Committee (٢٠٢٣)

هدفت إلى تقديم إطار تنظيمي لإدارة المخاطر السيبرانية والمرونة التشغيلية في القطاع المصرفي.

اعتمدت على منهج تحليلي للتقارير والمعايير الدولية المتعلقة بإدارة المخاطر.

أكدت النتائج أن تطبيق أطر فعالة لإدارة المخاطر يساهم في تقليل الأعطال وتعزيز الاستقرار التشغيلي للمؤسسات المصرفية.

وأوصت بضرورة تطبيق ضوابط تنظيمية قوية للأمن السيبراني.

دراسة World Bank (٢٠٢٤)

هدفت إلى دراسة تأثير التحول الرقمي على زيادة المخاطر في القطاع المالي.

اعتمدت على تحليل التقارير والمؤشرات المالية العالمية.

أوضحت النتائج أن التحول الرقمي رغم فوائده الكبيرة يزيد من الحاجة إلى تعزيز الأمن السيبراني بسبب ارتفاع احتمالية التعرض للهجمات الإلكترونية.

وأوصت بضرورة تحقيق التوازن بين التحول الرقمي وتطوير أنظمة الحماية السيبرانية

٢.٤ مناقشة نتائج الدراسات السابقة والفجوة البحثية:

مناقشة الدراسات السابقة

من خلال استعراض الدراسات السابقة، يتضح وجود اهتمام متزايد بدراسة المخاطر السيبرانية وتأثيرها على القطاع المصرفي، خاصة مع التوسع الكبير في استخدام الخدمات المصرفية الإلكترونية والتحول الرقمي.

اتفقت معظم الدراسات السابقة على أن المخاطر السيبرانية أصبحت من أبرز التحديات التي تواجه البنوك والمؤسسات المالية، لما لها من تأثير مباشر على استمرارية العمليات، وحماية البيانات، وثقة العملاء. فقد أوضحت دراسة Kopp et al (٢٠٢٣) أن المخاطر السيبرانية تؤثر بشكل مباشر على استمرارية الأعمال والعمليات التشغيلية في القطاع المصرفي، بينما أشارت دراسة Alrawad (٢٠٢٤) إلى أن التحول الرقمي يزيد من احتمالية التعرض للتهديدات السيبرانية.

كما أكدت الدراسات أهمية الإجراءات الأمنية والاستراتيجيات الوقائية في تقليل تأثير المخاطر السيبرانية، حيث أوضحت دراسة Elsayed et al (٢٠٢٤) أن تطبيق ممارسات الأمن السيبراني والحوكمة يساهم في تعزيز الأداء المؤسسي وزيادة ثقة أصحاب المصلحة. كذلك أكدت تقارير Basel Committee (٢٠٢٣) أهمية وجود أطر تنظيمية فعالة لإدارة المخاطر وتعزيز المرونة التشغيلية للمؤسسات المصرفية.

ومن جانب آخر، ركزت بعض الدراسات على الخدمات المصرفية الإلكترونية وأثرها على أداء البنوك، مثل دراسة Sayari (٢٠٢٤) التي أوضحت أن الخدمات المصرفية الإلكترونية تساهم في تحسين الكفاءة والأداء المالي للبنوك السعودية، إلا أن هذه الدراسات لم تركز بشكل كافٍ على تأثير المخاطر السيبرانية على استقرار هذه الخدمات.

كما أظهرت دراسة Al Mohayya & Makeen (٢٠٢٥) أهمية العامل البشري في منظومة الأمن السيبراني، حيث بينت أن ضعف الوعي الأمني قد يؤدي إلى زيادة احتمالية التعرض للهجمات السيبرانية، مما يؤكد أهمية التدريب والتوعية الأمنية داخل المؤسسات المصرفية.

وبشكل عام، تشير الدراسات السابقة إلى وجود علاقة بين مستوى المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، كما تؤكد أهمية الإجراءات الأمنية في الحد من تأثير هذه المخاطر.

٢.٥ الفجوة البحثية

على الرغم من تعدد الدراسات التي تناولت موضوع الأمن السيبراني والمخاطر الرقمية في القطاع المالي، إلا أن هناك عددًا من الفجوات البحثية التي ما زالت بحاجة إلى مزيد من الدراسة.

أولاً: ركزت بعض الدراسات السابقة على نوع محدد من المخاطر السيبرانية، مثل الهندسة الاجتماعية أو التحول الرقمي، دون تناول المخاطر السيبرانية بصورة شاملة تشمل الهجمات الإلكترونية، وسرقة البيانات، والاحتياز الإلكتروني، وانقطاع الخدمات.

ثانيًا: اهتمت بعض الدراسات بدراسة الأمن السيبراني أو الأداء المالي للبنوك، بينما لم تتناول بشكل مباشر العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية.

ثالثًا: ركزت العديد من الدراسات على بيانات دولية مختلفة، مع محدودية الدراسات التطبيقية التي تناولت البيئة المصرفية السعودية والعاملين في البنوك السعودية.

رابعاً: توجد حاجة إلى دراسة دور الإجراءات الأمنية والاستراتيجيات الوقائية باعتبارها متغيراً مستقلاً مفسراً يمكن أن يسهم في تعزيز استقرار الخدمات المصرفية الإلكترونية وتقليل آثار المخاطر السيبرانية.

وبناءً على ذلك، تسعى الدراسة الحالية إلى سد هذه الفجوة من خلال دراسة العلاقة بين:

- المخاطر السيبرانية.
- الإجراءات الأمنية والاستراتيجيات الوقائية.
- استقرار الخدمات المصرفية الإلكترونية.

وذلك بالتطبيق على البنوك السعودية.

٢.٦ النموذج النظري للدراسة

تعتمد الدراسة الحالية على إطار نظري يوضح العلاقة بين متغيرات الدراسة الثلاثة، حيث تمثل المخاطر السيبرانية أحد أهم التحديات التي قد تؤثر على استقرار الخدمات المصرفية الإلكترونية، بينما تمثل الإجراءات الأمنية والاستراتيجيات الوقائية عوامل تساعد على تعزيز قدرة البنوك على مواجهة هذه المخاطر.

ويتكون النموذج النظري من المتغيرات التالية

شكل رقم (٢-١) النموذج النظري للدراسة

نوع المتغير	المتغير	الابعاد
المتغير المستقل الأول	المخاطر السيبرانية	الهجمات الإلكترونية، سرقة البيانات، الاحتيال الإلكتروني، انقطاع الخدمات
المتغير المستقل الثاني/ المفسر	الإجراءات الأمنية الاستراتيجيات الوقائية	سياسات الأمن السيبراني، التدريب الأمني، أنظمة الحماية، التشغيل
المتغير التابع	استقرار الخدمات المصرفية الإلكترونية	استمرارية الخدمات، حماية البيانات، ثقة العملاء، سرعة الاستجابة للحوادث

رسم توضيحي ١ شكل (٢-١) النموذج النظري للدراسة

بناءً على الإطار النظري والدراسات السابقة، تم صياغة فرضيات الدراسة كما يلي:

الفرضية الأولى:

توجد علاقة ذات دلالة إحصائية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

الفرضية الثانية:

توجد علاقة ذات دلالة إحصائية بين الإجراءات الأمنية والاستراتيجيات الوقائية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

الفرضية الثالثة:

توجد علاقة ذات دلالة إحصائية بين المخاطر السيبرانية والإجراءات الأمنية والاستراتيجيات الوقائية في البنوك السعودية.

٢.٧ خاتمة الفصل

تناول هذا الفصل الإطار النظري والدراسات السابقة المتعلقة بالمخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية. وتم توضيح مفهوم المخاطر السيبرانية وأنواعها ومصادرها وطرق إدارتها، بالإضافة إلى توضيح أهمية الإجراءات الأمنية والاستراتيجيات الوقائية في الحد من تأثير هذه المخاطر.

كما تم استعراض عدد من الدراسات السابقة التي أكدت أهمية الأمن السيبراني في القطاع المصرفي، وبينت وجود علاقة بين المخاطر السيبرانية واستمرارية الخدمات الإلكترونية. ومن خلال تحليل هذه الدراسات تم تحديد الفجوة البحثية التي تسعى الدراسة الحالية إلى معالجتها من خلال التطبيق على البيئة المصرفية السعودية.

الفصل الثالث:

منهجية الدراسة

٣.١ مقدمة:

يهدف هذا الفصل إلى توضيح المنهجية العلمية والإجراءات التي اتبعتها الدراسة لتحقيق أهدافها والإجابة عن تساؤلاتها واختبار فرضياتها. ويتناول الفصل منهج البحث المستخدم، وتصميم الدراسة، ومجتمع الدراسة وعينتها، وأداة جمع البيانات، وطريقة قياس متغيرات الدراسة، بالإضافة إلى إجراءات التحقق من صدق وثبات الأداة، وأساليب التحليل الإحصائي المستخدمة.

اعتمدت الدراسة على المنهج الوصفي التحليلي والمنهج الكمي، وذلك لملاءمتهما لطبيعة الدراسة التي تهدف إلى دراسة العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، وتحليل دور الإجراءات الأمنية والاستراتيجيات الوقائية في تعزيز استقرار الخدمات المصرفية الإلكترونية.

كما اعتمدت الدراسة على البيانات الأولية التي تم جمعها باستخدام الاستبانة، بالإضافة إلى الاستفادة من البيانات الثانوية المتمثلة في الكتب العلمية، والدراسات السابقة، والأبحاث المحكمة، والتقارير الرسمية ذات العلاقة بموضوع الأمن السيبراني والقطاع المصرفي.

٣.٢ منهج البحث:

اعتمدت الدراسة على المنهج الوصفي التحليلي، وهو أحد المناهج العلمية المستخدمة في دراسة الظواهر وتحليل العلاقات بين المتغيرات واختبار الفرضيات.

ويساعد هذا المنهج في وصف واقع المخاطر السيبرانية في البنوك السعودية، وتحليل تأثيرها على استقرار الخدمات المصرفية الإلكترونية، بالإضافة إلى دراسة العلاقة بين الإجراءات الأمنية والاستراتيجيات الوقائية ومستوى استقرار الخدمات الإلكترونية.

كما اعتمدت الدراسة على المنهج الكمي من خلال جمع البيانات باستخدام استبانة وتحليلها إحصائيًا بهدف الوصول إلى نتائج قابلة للقياس والتفسير.

وتعتمد الدراسة على نوعين من البيانات:

أولاً: البيانات الأولية

تم جمعها من خلال الاستبانة، وشملت قياس المتغيرات التالية:

- المخاطر السيبرانية (متغير مستقل).
- استقرار الخدمات المصرفية الإلكترونية (متغير تابع).
- الإجراءات الأمنية والاستراتيجيات الوقائية (متغير مستقل مفسر).

ثانيًا: البيانات الثانوية

تم الحصول عليها من الكتب، والدراسات السابقة، والمراجع العلمية، والتقارير الرسمية المتعلقة بالأمن السيبراني وإدارة المخاطر والقطاع المصرفي.

٣.٣ تصميم البحث:

يعتمد تصميم البحث الحالي على المنهج الوصفي التحليلي لدراسة العلاقة بين متغيرات الدراسة واختبار الفرضيات.

ويتكون نموذج الدراسة من ثلاث متغيرات رئيسية:

المتغير المستقل الأول:

المخاطر السيبرانية

وتشمل:

- الهجمات الإلكترونية.
- سرقة البيانات.
- الاحتيال الإلكتروني.
- اختراق الأنظمة.
- تعطل الخدمات الإلكترونية.

المتغير المستقل الثاني (المفسر):

الإجراءات الأمنية والاستراتيجيات الوقائية

وتشمل:

- سياسات الأمن السيبراني.
- تحديث الأنظمة الأمنية.
- التدريب الأمني.
- التشفير.
- أنظمة المراقبة والحماية.

المتغير التابع:

استقرار الخدمات المصرفية الإلكترونية

ويقاس من خلال:

- استمرارية الخدمات.
- حماية بيانات العملاء.
- كفاءة الأنظمة.
- سرعة الاستجابة للأعطال.
- ثقة العملاء.

٣.٤ مجتمع البحث:

يتكون مجتمع الدراسة من موظفي البنوك العاملة في المملكة العربية السعودية، وخاصة العاملين في الأقسام المرتبطة بالخدمات المصرفية الإلكترونية، وتقنية المعلومات، والأمن السيبراني، وإدارة المخاطر.

وتم اختيار هذا المجتمع لامتلاك أفراد المعرفة والخبرة المتعلقة بالمخاطر السيبرانية والإجراءات الأمنية المستخدمة في البيئة المصرفية.

٣.٥ عينة الدراسة:

تتكون عينة الدراسة من مجموعة من موظفي البنوك العاملة في المملكة العربية السعودية، ممن يعملون في الأقسام المرتبطة بالخدمات المصرفية الإلكترونية، وتقنية المعلومات، والأمن السيبراني، وإدارة المخاطر، وذلك لارتباط طبيعية عملهم المباشر بموضوع الدراسة.

وتم اختيار أفراد العينة باستخدام أسلوب العينة العشوائية البسيطة، بهدف منح أفراد مجتمع الدراسة فرصًا متساوية للمشاركة، مما يساعد على تعزيز موضوعية النتائج.

وقد روعي عند اختيار العينة أن تشمل أفرادًا من مختلف المستويات الوظيفية والمؤهلات العلمية وسنوات الخبرة، بما يحقق تنوعًا مناسبًا في آراء المشاركين.

وتم اختيار أفراد العينة بطريقة مناسبة لطبيعة الدراسة، مع مراعاة تنوع المشاركين من حيث:

الجنس.

العمر.

المؤهل العلمي.

سنوات الخبرة.

المجال الوظيفي.

ويعد حجم العينة مناسبًا لإجراء التحليلات الإحصائية اللازمة واختبار فرضيات الدراسة وبلغ حجم العينة النهائية (١٥٢) مفردة، وهو حجم مناسب لإجراء التحليلات الإحصائية المطلوبة واختبار فرضيات الدراسة بدرجة مناسبة من الدقة والموثوقية.

٣.٦ أداة الدراسة:

اعتمدت الدراسة الحالية على الاستبانة بوصفها الأداة الرئيسة لجمع البيانات الأولية من أفراد عينة الدراسة، وذلك لملاءمتها لطبيعة لدراسة وأهدافها، وقدرتها على جمع البيانات من عدد كبير من المشاركين خلال فترة زمنية مناسبة، بالإضافة إلى سهولة تحليل نتائجها باستخدام البرامج الإحصائية.

وقد تم إعداد الاستبانة بالاعتماد على الأدبيات العلمية والدراسات السابقة ذات الصلة بموضوع الدراسة، مع إجراء بعض التعديلات بما يتناسب مع أهداف الدراسة الحالية وطبيعية البيئة المصرفية السعودية.

وتكونت الاستبانة من أربعة أقسام رئيسة كما يأتي:

القسم الأول: البيانات الديموغرافية

وشمل المعلومات الآتية:

- الجنس
- العمر
- المؤهل العلمي
- سنوات الخبرة
- والمجال الوظيفي

القسم الثاني: المخاطر السيبرانية

وتضمن سبع فقرات التي تقيس مستوى المخاطر السيبرانية التي تواجه البنوك السعودية، وتشمل:

- الهجمات الإلكترونية
- الاحتيال الإلكتروني
- سرقة البيانات
- اختراق الأنظمة
- تعطل الخدمات الإلكترونية
- ضعف الوعي الأمني
- التهديدات السيبرانية

القسم الثالث: استقرار الخدمات المصرفية الإلكترونية

وتضمن سبع فقرات لقياس:

- خلال استمرارية الخدمات
- كفاءة الأنظمة
- استمرار الخدمة
- تأثر الخدمات بالمشكلات التقنية
- حماية البيانات العملاء
- سرعة الاستجابة للأعطال
- ثقة العملاء

القسم الرابع: الإجراءات الأمنية والاستراتيجيات الوقائية

وتضمن سبع فقرات التي لقياس:

- تحديث الأنظمة الأمنية
- التشفير
- تطبيق سياسات الأمن السيبراني
- التدريب المستمر
- إدارة المخاطر
- فعالية الإجراءات الأمنية
- أنظمة المراقبة

وقد استخدمت الدراسة مقياس ليكرت الخماسي لقياس استجابات أفراد العينة ذلك على النحو الآتي:

جدول (٣-١): قياس متغيرات الدراسة

جدول ٢ جدول (٣-١): قياس متغيرات الدراسة

الدرجة	درجة الموافقة
٥	أوافق بشدة
٤	أوافق
٣	محايد
٢	لا أوافق
١	لا أوافق بشدة

٣.٧ قياس متغيرات الدراسة

تم قياس متغيرات الدراسة من خلال فقرات الاستبانة كما هو موضح في الجدول التالي:

جدول (٣-٢): توزيع فقرات الاستبانة على متغيرات الدراسة

جدول ٣ جدول (٣-٢): توزيع فقرات الاستبانة على متغيرات الدراسة

المتغير	نوع المتغير	طريقة القياس
المخاطر السيبرانية	متغير مستقل	سبع فقرات
استقرار الخدمات المصرفية الإلكترونية	متغير تابع	سبع فقرات
الإجراءات الأمنية والاستراتيجيات الوقائية	متغير مستقل مفسر	سبع فقرات

٣.٨ فرضيات الدراسة

استناد إلى مشكلة الدراسة وأهدافها والإطار النظري والدراسات السابقة، تمت صياغة فرضيات الدراسة على النحو الآتي:

الفرضية الرئيسية

H0: لا توجد علاقة ذات دلالة إحصائية بين المخاطر السيبرانية و استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

ويتفرع عنها الفرضيات الفرعية الآتية:

H01: لا توجد علاقة ذات دلالة إحصائية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية

H02: لا توجد أثر علاقة ذات دلالة إحصائية بين الإجراءات الأمنية و الاستراتيجيات الوقائية و استقرار الخدمات المصرفية الإلكترونية

H03: لا توجد أثر علاقة ذات دلالة إحصائية بين المخاطر السيبرانية والإجراءات الأمنية والاستراتيجيات الوقائية

٣.٩ صدق وثبات أداة الدراسة

تم التحقق من صدق المحتوى بعرض الاستبانة على عدد من المحكمين والمتخصصين في مجالات إدارة المخاطر والأمن السيبراني والإدارة؛ للتأكد من وضوح الفقرات ومدى ملاءمتها لقياس متغيرات الدراسة.

كما تم التحقق من ثبات أداة الدراسة باستخدام معامل كرونباخ ألفا (Cronbach's Alpha) لقياس الاتساق الداخلي لفقرات الاستبانة، ويعد معامل الثبات مقبولا إذا بلغت قيمته (٠.٧٠) فأكثر، وهو ما يدل على تمتع الأداة بدرجة مناسبة من الثبات والاعتمادية.

٣.١٠ أساليب التحليل الإحصائي

تم تحليل البيانات باستخدام برنامج IBM SPSS Statistics، كما تم استخدام Microsoft Excel في إدخال البيانات وتنظيمها وإعداد الجداول والأشكال البيانية.

واستخدمت الدراسة الأساليب الإحصائية الآتية:

- التكرارات والنسب المئوية؛ لوصف الخصائص الديموغرافية لعينة الدراسة.
- المتوسطات الحسابية؛ لقياس مستوى استجابات أفراد العينة.
- الانحرافات المعيارية؛ لقياس تشتت الاستجابات.
- معامل ارتباط بيرسون (Pearson Correlation)؛ لدراسة العلاقة بين متغيرات الدراسة.
- معامل كرونباخ ألفا (Cronbach's Alpha)؛ للتحقق من ثبات أداة الدراسة.
- اعتماد مستوى الدلالة الإحصائية ($\alpha \leq 0.05$) عند اختبار الفرضيات

٣.١١ حدود الدراسة

أولاً: الحدود الموضوعية

تركز الدراسة على العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، مع دراسة الإجراءات الأمنية والاستراتيجيات الوقائية باعتبارها متغيراً مستقلاً مفسراً.

ثانيًا: الحدود المكانية

اقتصرت الدراسة على البنوك العاملة في المملكة العربية السعودية.

ثالثًا: الحدود البشرية

شملت الدراسة موظفي البنوك العاملين في أقسام الأمن السيبراني وتقنية المعلومات والخدمات المصرفية الإلكترونية وإدارة المخاطر.

رابعًا: الحدود الزمنية

تم تطبيق الدراسة خلال عام ٢٠٢٦م.

٣.١٢ خاتمة الفصل

تناول هذا الفصل منهجية الدراسة وإجراءاتها، من خلال توضيح منهج البحث، وتصميم الدراسة، ومجتمع الدراسة وعينتها، وأداة جمع البيانات، وطرق قياس متغيرات الدراسة، بالإضافة إلى إجراءات التحقق من صدق وثبات الأداة، والأساليب الإحصائية المستخدمة في تحليل البيانات واختبار فرضيات الدراسة.

وقد شكلت هذه الإجراءات الأساس العلمي الذي اعتمدت عليه الدراسة في تحليل البيانات والوصول إلى النتائج التي سيتم عرضها ومناقشتها في الفصل الرابع.

الفصل الرابع:

النتائج ومناقشتها

٤.١ مقدمة:

يهدف هذا الفصل إلى عرض وتحليل نتائج الدراسة الميدانية التي تم الحصول عليها من خلال الاستبانة الموزعة على أفراد عينة الدراسة، وذلك بهدف دراسة أثر المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

ويتناول هذا الفصل تحليل البيانات التي تم جمعها من أفراد العينة البالغ عددهم (١٥٢) مفردة، وذلك باستخدام الأساليب الإحصائية المناسبة، بهدف وصف خصائص العينة، وتحليل استجابات المشاركين حول متغيرات الدراسة، والتي تشمل المخاطر السيبرانية (المتغير المستقل)، واستقرار الخدمات المصرفية الإلكترونية (المتغير التابع)، والإجراءات الأمنية والاستراتيجيات الوقائية (المتغير المعدل).

كما يتضمن الفصل عرض النتائج المتعلقة بالبيانات الديموغرافية لأفراد العينة، وتحليل فقرات الاستبانة، واختبار فرضيات الدراسة، ومناقشة النتائج في ضوء الدراسات السابقة، بهدف الوصول إلى استنتاجات علمية تساعد في فهم العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البيئة المصرفية السعودية.

٤.٢ عرض وتحليل نتائج الدراسة

وصف خصائص عينة الدراسة

يهدف هذا الجزء إلى عرض وتحليل الخصائص الديموغرافية لأفراد عينة الدراسة، وذلك بهدف التعرف على طبيعة المشاركين ومدى تنوعهم من حيث الخصائص الشخصية والوظيفية. وقد تم تحليل البيانات الديموغرافية لأفراد العينة البالغ عددهم (١٥٢) مفردة، وتشمل هذه الخصائص: الجنس، العمر، المؤهل العلمي، سنوات الخبرة، والمجال الوظيفي.

توزيع أفراد عينة الدراسة حسب الجنس

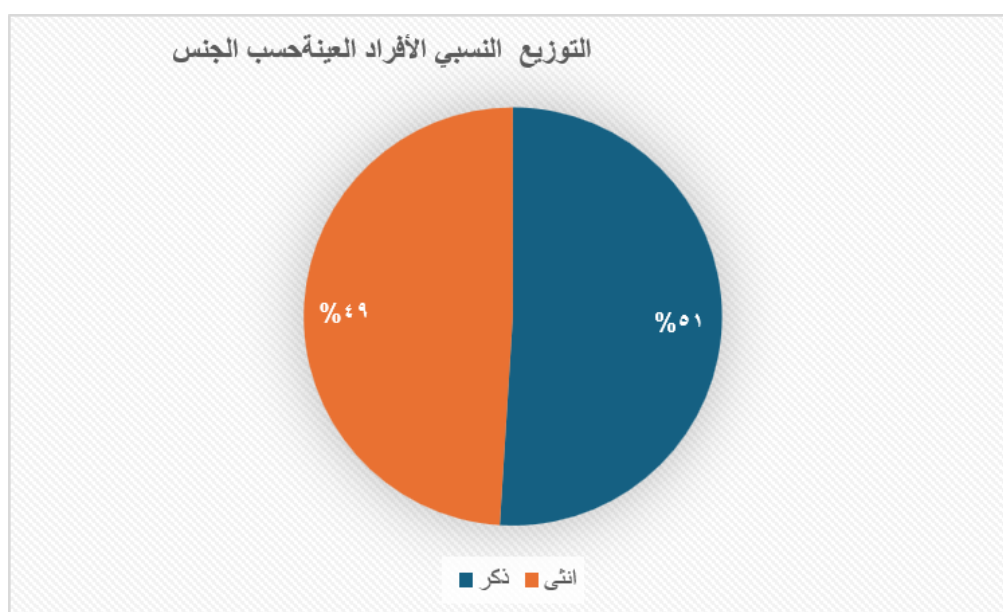
يوضح الجدول (١-٤): التالي توزيع أفراد عينة الدراسة حسب الجنس:

جدول ٤-١: توزيع أفراد عينة الدراسة حسب الجنس

الجنس	التكرار	النسبة المئوية
ذكر	٨٠	%٥٢.٦
أنثى	٧٢	%٤٧.٤
المجموع	١٥٢	%١٠٠

يوضح الجدول (١-٤) توزيع أفراد عينة الدراسة حسب الجنس، حيث يتضح أن نسبة الذكور بلغت (%٥٢.٦) بعدد (٨٠) مشاركاً، بينما بلغت نسبة الإناث (%٤٧.٤) بعدد (٧٢) مشاركة. وتشير هذه النتائج إلى وجود تقارب نسبي بين الذكور والإناث ضمن عينة الدراسة

شكل (١-٤) التوزيع النسبي لأفراد العينة حسب الجنس



رسم توضيحي ٢ (1-4) التوزيع النسبي لأفراد العينة حسب الجنس

توزيع أفراد لعينة الدراسة حسب العمر

يوضح الجدول (٤-٢): التالي توزيع أفراد عينة الدراسة حسب العمر

جدول ٥ جدول (٤-٢) توزيع أفراد عينة الدراسة حسب العمر

العمر	التكرار	النسبة المئوية
أقل من ٣٠ سنة	٤٢	٢٧.٦%
من ٣٠ إلى ٣٥ سنة	٧١	٤٦.٧%
من ٣٦ إلى ٤٠ سنة	٢٩	١٩.١%
من ٤٢ إلى ٤٦ سنة	٩	٥.٩%
٤٧ فأكثر	١	٠.٧%
المجموع	١٥٢	١٠٠%

يوضح الجدول (٤-٢) توزيع أفراد عينة الدراسة حسب العمر، حيث يتضح أن الفئة العمرية من (٣٠-٣٥ سنة) كانت الأكثر تمثيلاً في العينة بعدد (٧١) مشاركاً وبنسبة (٤٦.٧%)، تليها فئة أقل من ٣٠ سنة بعدد (٤٢) مشاركاً وبنسبة (٢٧.٦%). بينما كانت فئة (٤٧ سنة فأكثر) الأقل تمثيلاً بعدد (مشارك واحد) وبنسبة (٠.٧%)

توزيع أفراد عينة الدراسة حسب المؤهل العلمي

جدول (٤-٣): توضيح أفراد عينة الدراسة حسب المؤهل العلمي

جدول ٦ جدول (٤-٣): توضيح أفراد عينة الدراسة حسب المؤهل العلمي

المؤهل العلمي	التكرار	النسبة المئوية
دبلوم	٢٥	١٦.٤%
بكالوريوس	٩٢	٦٠.٥%
ماجستير	٣٢	٢١.١%
دكتوراه	٣	٢.٠%
المجموع	١٥٢	١٠٠%

وضح الجدول (٤-٣) توزيع أفراد عينة الدراسة حسب المؤهل العلمي، حيث يتضح أن حملة درجة البكالوريوس يمثلون النسبة الأكبر من أفراد العينة بعدد (٩٢) مشاركاً وبنسبة (٦٠.٥٪)، يليهم حملة درجة الماجستير بعدد (٣٢) مشاركاً وبنسبة (٢١.١٪). بينما بلغ عدد الحاصلين على الدبلوم (٢٥) مشاركاً بنسبة (١٦.٤٪)، في حين كانت نسبة حملة الدكتوراه الأقل بعدد (٣) مشاركين وبنسبة (٢.٠٪). وتشير هذه النتائج إلى أن غالبية أفراد العينة لديهم مؤهلات تعليمية جامعية

توزيع أفراد عينة الدراسة حسب سنوات الخبرة

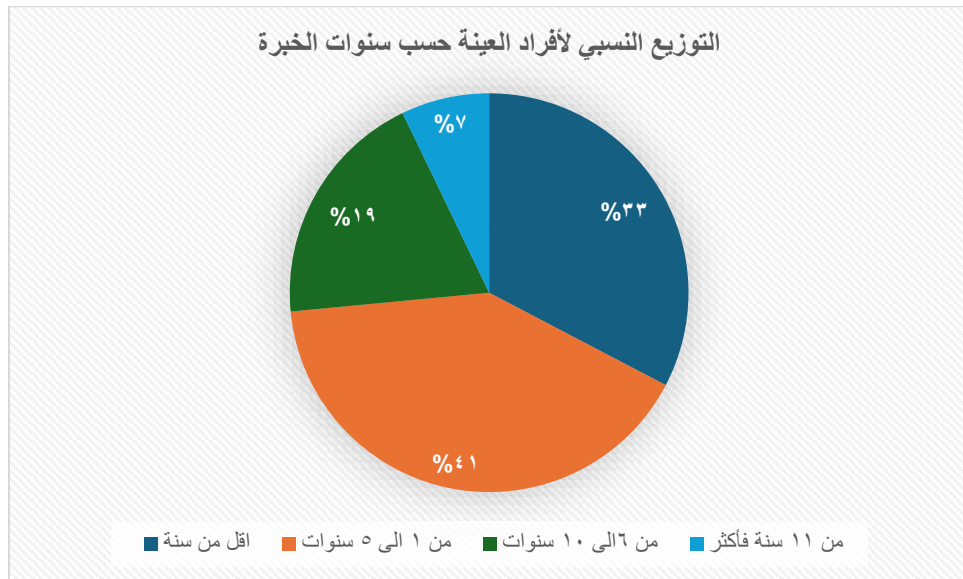
جدول (٤-٤): توزيع أفراد عينة الدراسة حسب سنوات الخبرة

جدول (4-4): توزيع أفراد عينة الدراسة حسب سنوات الخبرة

سنوات الخبرة	التكرار	النسبة المئوية
أقل من سنة	٥٠	٣٢.٩٪
من ١ الى ٥ سنوات	٦٢	٤٠.٨٪
من ٦ إلى ١٠ سنوات	٢٩	١٩.١٪
١١ سنة فأكثر	١١	٧.٢٪
المجموع	١٥٢	١٠٠٪

يوضح الجدول (٤-٤) توزيع أفراد عينة الدراسة حسب سنوات الخبرة، حيث يتضح أن الفئة الأكثر تمثيلاً هي فئة الخبرة من (١-٥ سنوات) بعدد (٦٢) مشاركاً وبنسبة (٤٠.٨٪)، تليها فئة أقل من سنة بعدد (٥٠) مشاركاً وبنسبة (٣٢.٩٪). بينما بلغت نسبة المشاركين الذين لديهم خبرة من (٦-١٠ سنوات) (١٩.١٪) بعدد (٢٩) مشاركاً، في حين كانت الفئة الأقل تمثيلاً هي فئة (١١ سنة فأكثر) بعدد (١١) مشاركاً وبنسبة (٧.٢٪). وتشير هذه النتائج إلى تنوع أفراد العينة من حيث مستوى الخبرة العملية

شكل (٢-٤): التوزيع النسبي لأفراد العينة حسب سنوات الخبرة



رسم توضيحي ٣ (٢-٤)

توزيع أفراد عينة الدراسة حسب المجال الوظيفي

جدول (٤-٥): توزيع أفراد عينة الدراسة حسب المجال الوظيفي

جدول ٨ (٤-٥) توزيع أفراد عينة الدراسة حسب المجال الوظيفي

النسبة المئوية	التكرار	المجال الوظيفي
١٨.٤%	٢٨	تقنية المعلومات
١٢.٥%	١٩	الأمن السيبراني
٢٩.٦%	٤٥	الخدمات المصرفية الإلكترونية
١٣.٢%	٢٠	إدارة المخاطر
٣.٣%	٥	المراجعة الداخلية/ التدقيق الداخلي
٢٣.٠%	٣٥	أخرى
١٠٠%	١٥٢	المجموع

يوضح الجدول (٤-٥) توزيع أفراد عينة الدراسة حسب مجال العمل، حيث يتضح أن العاملين في مجال الخدمات المصرفية الإلكترونية يمثلون النسبة الأكبر من أفراد العينة بعدد (٤٥) مشاركاً ونسبة (٢٩.٦٪)، يليهم أفراد الفئات الأخرى بعدد (٣٥) مشاركاً ونسبة (٢٣.٠٪). كما بلغت نسبة العاملين في مجال تقنية المعلومات (١٨.٤٪)، وإدارة المخاطر (١٣.٢٪)، والأمن السيبراني (١٢.٥٪). بينما كانت فئة المراجعة الداخلية/التدقيق الداخلي الأقل تمثيلاً بعدد (٥) مشاركين ونسبة (٣.٣٪). وتشير هذه النتائج إلى تنوع أفراد العينة من مختلف المجالات المرتبطة بموضوع الدراسة.

٤.٣ التحليل الوصفي لمحاور الدراسة

تم استخدام المتوسط الحسابي لتحليل استجابات أفراد عينة الدراسة حول محاور الاستبانة، وذلك بهدف التعرف على مستوى المخاطر السيبرانية، ومستوى استقرار الخدمات المصرفية الإلكترونية، ومدى تطبيق استراتيجيات وإجراءات الأمن السيبراني في البنوك السعودية.

جدول (٤-٦): المتوسطات الحسابية لمحاور الدراسة

جدول 9 (٤-٦) المتوسطات الحسابية لمحاور الدراسة

م	محور الدراسة	المتوسط الحسابي
١	المخاطر السيبرانية	٤.٦٩٦١
٢	استقرار الخدمات المصرفية الإلكترونية	٤.٢٨٣٨
٣	استراتيجيات وإجراءات الأمن السيبراني	٤.٦٨٨٩

يوضح الجدول (٤-٦) المتوسطات الحسابية لمحاور الدراسة، حيث أظهرت النتائج أن جميع محاور الدراسة حصلت على متوسطات حسابية مرتفعة.

حصل محور المخاطر السيبرانية على أعلى متوسط حسابي بلغ (٤.٦٩٦١)، مما يدل على ارتفاع مستوى إدراك أفراد العينة لأهمية المخاطر السيبرانية وتأثيرها على القطاع المصرفي.

كما حصل محور استراتيجيات وإجراءات الأمن السيبراني على متوسط حسابي بلغ (٤.٦٨٨٩)، مما يشير إلى ارتفاع مستوى تطبيق الإجراءات الأمنية داخل البنوك، مثل حماية البيانات، تحديث الأنظمة الأمنية، والتدريب المستمر على الأمن السيبراني.

بينما بلغ المتوسط الحسابي لمحور استقرار الخدمات المصرفية الإلكترونية (٤.٢٨٣٨)، مما يعكس وجود مستوى مرتفع من استقرار الخدمات المصرفية الإلكترونية من وجهة نظر أفراد العينة

٤.٤ اختبار فرضيات الدراسة

تم استخدام معامل ارتباط بيرسون (Pearson Correlation) لاختبار العلاقات بين متغيرات الدراسة، وذلك للتأكد من وجود علاقات ذات دلالة إحصائية بين محاور الدراسة.

الفرضية الأولى:

توجد علاقة ذات دلالة إحصائية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

لاختبار هذه الفرضية تم استخدام معامل ارتباط بيرسون لقياس العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية.

جدول (٧-٤): العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية

جدول 10 (٧-٤): العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية

المتغيرات	معامل الارتباط (r)	مستوى الدلالة (p-value)	النتيجة
المخاطر السيبرانية * استقرار الخدمات المصرفية الإلكترونية	٠.٠٦٨٩	9.71893E-23	قبول الفرضية

تشير نتائج الجدول (٧-٤) إلى وجود علاقة ذات دلالة إحصائية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، حيث بلغ معامل الارتباط ($r = 0.689$)، وكانت قيمة مستوى الدلالة أقل من (٠.٠٥). وهذا يدل على وجود علاقة معنوية بين المتغيرين، وبالتالي يتم قبول الفرضية الأولى

الفرضية الثانية:

توجد علاقة ذات دلالة إحصائية بين استراتيجيات وإجراءات الأمن السيبراني واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

جدول (٤-٨): العلاقة بين استراتيجيات الأمن السيبراني واستقرار الخدمات المصرفية الإلكترونية

جدول 11 (٤-٨): العلاقة بين استراتيجيات الأمن السيبراني واستقرار الخدمات المصرفية

المتغيرات	معامل الارتباط (r)	مستوى الدلالة (p-value)	النتيجة
الإجراءات الأمنية والاستراتيجيات الوقائية * استقرار الخدمات المصرفية الإلكترونية	٠.٠٦٥٠	1.32525E-19	قبول الفرضية

توضح نتائج الجدول (٤-٨) وجود علاقة موجبة ذات دلالة إحصائية بين استراتيجيات والإجراءات الأمنية والاستراتيجيات الوقائية واستقرار الخدمات المصرفية الإلكترونية، حيث بلغ معامل الارتباط ($r = 0.650$)، وكانت قيمة الدلالة أقل من (٠.٠٥). وتشير هذه النتيجة إلى أن زيادة تطبيق استراتيجيات الأمن السيبراني ترتبط بارتفاع مستوى استقرار الخدمات المصرفية الإلكترونية

الفرضية الثالثة:

توجد علاقة ذات دلالة إحصائية بين أنواع المخاطر السيبرانية ومستوى استجابة البنوك وإجراءاتها الأمنية.

جدول (٩-٤): اختبار العلاقة بين المخاطر السيبرانية والإجراءات الأمنية والاستراتيجيات الوقائية

جدول ١٢ (٩-٤): اختبار العلاقة بين المخاطر السيبرانية والإجراءات الأمنية والاستراتيجيات الوقائية

المتغيرات	معامل الارتباط (r)	مستوى الدلالة (p-value)	النتيجة
المخاطر السيبرانية * الإجراءات الأمنية والاستراتيجيات الوقائية	٠.٦٨٩	9.71893E-23	قبول الفرضية

أظهرت نتائج اختبار معامل ارتباط بيرسون وجود علاقة ذات دلالة إحصائية بين المخاطر السيبرانية والإجراءات الأمنية والاستراتيجيات الوقائية، حيث بلغ معامل الارتباط ($r = 0.689$)، وبلغ مستوى الدلالة ($p = 9.71893E-23$)، وهي قيمة أقل من (٠.٠٥). وتشير هذه النتيجة إلى وجود علاقة معنوية بين مستوى المخاطر السيبرانية والإجراءات الأمنية المتبعة في البنوك، وبناءً عليه يتم قبول الفرضية الثالثة

الفرضية الرابعة:

تؤدي زيادة الوعي الأمني لدى موظفي البنوك إلى تقليل الأثر السلبي للمخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية.

جدول (٤-١٠): اختبار العلاقة بين الوعي الأمني لدى الموظفين واستقرار الخدمات المصرفية الإلكترونية

جدول 13 (٤-١٠): اختبار العلاقة بين الوعي الأمني لدى الموظفين واستقرار الخدمات المصرفية الإلكترونية

المتغيرات	معامل الارتباط (r)	مستوى الدلالة (p-value)	النتيجة
الوعي الأمني لدى الموظفين * استقرار الخدمات المصرفية الإلكترونية	٠.٤٢٣	5.66869E-08	قبول الفرضية

أظهرت نتائج اختبار معامل ارتباط بيرسون وجود علاقة ذات دلالة إحصائية بين الوعي الأمني لدى موظفي البنوك واستقرار الخدمات المصرفية الإلكترونية، حيث بلغ معامل الارتباط ($r = 0.423$)، وبلغ مستوى الدلالة ($p = 5.66869E-08$)، وهي قيمة أقل من (٠.٠٥). وتشير هذه النتيجة إلى أن ارتفاع مستوى الوعي الأمني لدى الموظفين يرتبط بتحسين استقرار الخدمات المصرفية الإلكترونية وتقليل تأثير المخاطر السيبرانية، وبناءً عليه يتم قبول الفرضية الرابعة

٤.٥ ملخص نتائج الفصل الرابع

تناول هذا الفصل عرض وتحليل نتائج الدراسة الميدانية التي تم جمعها من أفراد عينة الدراسة البالغ عددهم (١٥٢) مشاركاً، حيث تم تحليل الخصائص الديموغرافية للعينة، بالإضافة إلى تحليل استجابات المشاركين حول محاور الدراسة واختبار فرضياتها.

أظهرت نتائج التحليل الوصفي ارتفاع مستوى إدراك أفراد العينة للمخاطر السيبرانية، حيث حصل محور المخاطر السيبرانية على متوسط حسابي بلغ (٤.٦٩٦١)، كما أظهر محور الإجراءات الأمنية والاستراتيجيات الوقائية مستوى مرتفعاً بمتوسط حسابي بلغ (٤.٦٨٨٩)، بينما بلغ متوسط محور استقرار الخدمات المصرفية الإلكترونية (٤.٢٨٣٨).

كما أظهرت نتائج اختبار الفرضيات وجود علاقات ذات دلالة إحصائية بين متغيرات الدراسة، حيث تم قبول جميع فرضيات الدراسة، وذلك على النحو التالي:

١. وجود علاقة ذات دلالة إحصائية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، حيث بلغ معامل الارتباط ($r = 0.689$).
 ٢. وجود علاقة ذات دلالة إحصائية بين الإجراءات الأمنية والاستراتيجيات الوقائية واستقرار الخدمات المصرفية الإلكترونية، حيث بلغ معامل الارتباط ($r = 0.650$).
 ٣. وجود علاقة ذات دلالة إحصائية بين المخاطر السيبرانية والإجراءات الأمنية والاستراتيجيات الوقائية، حيث بلغ معامل الارتباط ($r = 0.689$).
 ٤. وجود علاقة ذات دلالة إحصائية بين الوعي الأمني لدى الموظفين واستقرار الخدمات المصرفية الإلكترونية، حيث بلغ معامل الارتباط ($r = 0.423$).
- وبناءً على هذه النتائج، يتضح أن تعزيز الإجراءات الأمنية ورفع مستوى الوعي السيبراني لدى العاملين في القطاع المصرفي يساهم في دعم استقرار الخدمات المصرفية الإلكترونية والحد من آثار المخاطر السيبرانية

الفصل الخامس:

التوصيات والمقترحات الملاحق

١,٥ مقدمة:

يهدف هذا الفصل إلى مناقشة النتائج التي توصلت إليها الدراسة في ضوء أهدافها وفرضياتها، وربطها بما ورد في الدراسات السابقة والإطار النظري. كما يتناول الفصل الاستنتاجات الرئيسية التي تم التوصل إليها بناءً على نتائج التحليل الإحصائي، بالإضافة إلى تقديم مجموعة من التوصيات والمقترحات التي يمكن أن تسهم في تعزيز استقرار الخدمات المصرفية الإلكترونية والحد من تأثير المخاطر السيبرانية في البنوك السعودية.

٥.٢ مناقشة نتائج الدراسة

نبدأ بالفرضية الأولى:

• مناقشة نتيجة الفرضية الأولى

نص الفرضية:

توجد علاقة ذات دلالة إحصائية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

مناقشة النتيجة:

أظهرت نتائج الدراسة وجود علاقة ذات دلالة إحصائية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، حيث بلغ معامل الارتباط بين المتغيرين ($r = 0.689$)، وكانت قيمة الدلالة الإحصائية أقل من (0.05)، مما يشير إلى وجود علاقة معنوية بين مستوى المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية.

وتشير هذه النتيجة إلى أن ارتفاع مستوى المخاطر السيبرانية يمثل تحدياً مؤثراً على قدرة البنوك على المحافظة على استقرار خدماتها الإلكترونية، حيث إن الهجمات الإلكترونية، ومحاولات الاحتيال، وسرقة البيانات، واختراق الأنظمة قد تؤدي إلى اضطرابات تؤثر على جودة واستمرارية الخدمات المقدمة للعملاء.

كما تؤكد هذه النتيجة أهمية تعزيز أنظمة الحماية السيبرانية، وتطوير خطط الاستجابة للحوادث، ورفع جاهزية البنوك للتعامل مع التهديدات الإلكترونية بهدف المحافظة على استقرار الخدمات المصرفية الإلكترونية.

• مناقشة نتيجة الفرضية الثانية

نص الفرضية:

توجد علاقة ذات دلالة إحصائية بين الإجراءات الأمنية والاستراتيجيات الوقائية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

مناقشة النتيجة:

أظهرت نتائج الدراسة وجود علاقة ذات دلالة إحصائية بين الإجراءات الأمنية والاستراتيجيات الوقائية واستقرار الخدمات المصرفية الإلكترونية، حيث بلغ معامل الارتباط بين المتغيرين $r = 0.650$ ، وكانت قيمة الدلالة الإحصائية أقل من (0.05) ، مما يدل على وجود علاقة معنوية بين تطبيق الإجراءات الأمنية ومستوى استقرار الخدمات المصرفية الإلكترونية.

وتشير هذه النتيجة إلى أن البنوك التي تطبق استراتيجيات أمنية فعالة، مثل تحديث الأنظمة الأمنية بشكل مستمر، واستخدام تقنيات التشفير، وتطبيق سياسات واضحة لإدارة المخاطر السيبرانية، تكون أكثر قدرة على المحافظة على استمرارية الخدمات الإلكترونية وتقليل تأثير التهديدات السيبرانية.

كما تعكس هذه النتيجة أهمية الاستثمار في الحلول الأمنية المتقدمة، وتطوير إجراءات الوقاية والمراقبة المستمرة، بالإضافة إلى تدريب الموظفين على ممارسات الأمن السيبراني، مما يسهم في تعزيز الثقة بالخدمات المصرفية الإلكترونية وتحسين استقرارها.

• مناقشة نتيجة الفرضية الثالثة

نص الفرضية:

توجد علاقة ذات دلالة إحصائية بين المخاطر السيبرانية والإجراءات الأمنية والاستراتيجيات الوقائية في البنوك السعودية.

مناقشة النتيجة:

أظهرت نتائج الدراسة وجود علاقة ذات دلالة إحصائية بين المخاطر السيبرانية والإجراءات الأمنية والاستراتيجيات الوقائية، حيث بلغ معامل الارتباط بين المتغيرين ($r = 0.689$)، وكانت قيمة الدلالة الإحصائية أقل من (0.05)، مما يشير إلى وجود علاقة معنوية بين مستوى المخاطر السيبرانية والإجراءات الأمنية المتبعة في البنوك.

وتوضح هذه النتيجة أن زيادة إدراك البنوك للمخاطر السيبرانية المرتبطة بالهجمات الإلكترونية، والاحتيال الإلكتروني، وسرقة البيانات، يؤدي إلى زيادة الاهتمام بتطوير الإجراءات الأمنية والاستراتيجيات الوقائية لمواجهة هذه التهديدات.

كما تشير النتيجة إلى أن طبيعة المخاطر السيبرانية المتغيرة والمتطورة تتطلب من البنوك تحديث أنظمتها الأمنية بشكل مستمر، وتعزيز آليات المراقبة والاستجابة للحوادث، ووضع سياسات فعالة لإدارة المخاطر السيبرانية بما يضمن حماية البيانات واستمرارية الخدمات المصرفية الإلكترونية.

• مناقشة نتيجة الفرضية الرابعة

نص الفرضية:

تؤدي زيادة الوعي الأمني لدى موظفي البنوك إلى تقليل الأثر السلبي للمخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية.

مناقشة النتيجة:

أظهرت نتائج الدراسة وجود علاقة ذات دلالة إحصائية بين الوعي الأمني لدى الموظفين واستقرار الخدمات المصرفية الإلكترونية، حيث بلغ معامل الارتباط بين المتغيرين $r = 0.423$ ، وكانت قيمة الدلالة الإحصائية أقل من (0.005) ، مما يدل على وجود علاقة معنوية بين مستوى الوعي الأمني لدى الموظفين واستقرار الخدمات المصرفية الإلكترونية.

وتشير هذه النتيجة إلى أن رفع مستوى الوعي الأمني لدى العاملين في البنوك يساهم في تقليل احتمالية حدوث الأخطاء البشرية التي قد تؤدي إلى زيادة المخاطر السيبرانية، مثل التعامل غير الآمن مع البيانات، أو الوقوع في محاولات الاحتيال الإلكتروني، أو عدم الالتزام بالإجراءات الأمنية المعتمدة.

كما تؤكد هذه النتيجة أهمية استمرار برامج التدريب والتوعية الأمنية للموظفين، باعتبارهم أحد العناصر الأساسية في منظومة الأمن السيبراني، مما يساعد على تعزيز قدرة البنوك على حماية أنظمتها والمحافظة على استقرار الخدمات المصرفية الإلكترونية

٥.٣ استنتاجات الدراسة

بناءً على نتائج التحليل الإحصائي واختبار فرضيات الدراسة، توصلت الدراسة إلى مجموعة من الاستنتاجات، تتمثل فيما يلي:

أظهرت نتائج الدراسة أن أفراد العينة لديهم مستوى مرتفع من الإدراك بأهمية المخاطر السيبرانية التي تواجه البنوك السعودية، مما يعكس أهمية التعامل مع التهديدات الإلكترونية باعتبارها أحد التحديات الرئيسية في القطاع المصرفي.

بينت النتائج وجود علاقة ذات دلالة إحصائية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، مما يشير إلى أن التهديدات السيبرانية يمكن أن تؤثر على استمرارية وكفاءة الخدمات المصرفية الإلكترونية.

أظهرت الدراسة أن تطبيق الإجراءات الأمنية والاستراتيجيات الوقائية يرتبط بشكل إيجابي مع استقرار الخدمات المصرفية الإلكترونية، مما يؤكد أهمية تبني البنوك لأساليب حماية متقدمة لمواجهة المخاطر السيبرانية.

توصلت الدراسة إلى وجود علاقة ذات دلالة إحصائية بين المخاطر السيبرانية والإجراءات الأمنية والاستراتيجيات الوقائية، مما يشير إلى أن ارتفاع مستوى التهديدات يدفع البنوك إلى تعزيز وتطوير أنظمتها الأمنية.

أوضحت النتائج أهمية الوعي الأمني لدى الموظفين في دعم الأمن السيبراني، حيث يساهم تدريب الموظفين وزيادة معرفتهم بالممارسات الأمنية في تقليل احتمالية وقوع الحوادث السيبرانية.

أكدت الدراسة أن استقرار الخدمات المصرفية الإلكترونية يعتمد على تكامل عدة عوامل، تشمل قوة الأنظمة الأمنية، كفاءة الإجراءات الوقائية، ووعي الموظفين بالمخاطر السيبرانية.

٥.٤ توصيات الدراسة

بناءً على نتائج الدراسة والاستنتاجات التي تم التوصل إليها، تقدم الدراسة مجموعة من التوصيات التي يمكن أن تسهم في تعزيز استقرار الخدمات المصرفية الإلكترونية والحد من تأثير المخاطر السيبرانية في البنوك السعودية، كما يلي:

- تعزيز أنظمة الأمن السيبراني في البنوك السعودية من خلال الاستثمار المستمر في التقنيات الأمنية الحديثة، وتطوير أنظمة الحماية والمراقبة للكشف المبكر عن التهديدات الإلكترونية.
- تحديث الأنظمة الأمنية بشكل دوري لمواكبة التطورات المستمرة في أساليب الهجمات السيبرانية، وتقليل احتمالية تعرض الأنظمة المصرفية للاختراق أو التعطل.
- تطوير استراتيجيات شاملة لإدارة المخاطر السيبرانية تتضمن تحديد المخاطر المحتملة، ووضع خطط للاستجابة للحوادث، وضمان استمرارية الخدمات المصرفية الإلكترونية.
- رفع مستوى الوعي الأمني لدى موظفي البنوك من خلال تنفيذ برامج تدريبية دورية حول أساليب الحماية السيبرانية، وطرق التعامل مع محاولات الاختيال والهجمات الإلكترونية.
- تعزيز سياسات حماية البيانات وخصوصية العملاء من خلال تطبيق تقنيات التشفير، وتحسين إجراءات التحكم في الوصول إلى المعلومات الحساسة.
- زيادة أنظمة المراقبة والاستجابة للحوادث الأمنية لضمان اكتشاف التهديدات بسرعة وتقليل أثرها على استمرارية الخدمات المصرفية الإلكترونية.
- تعزيز ثقافة الأمن السيبراني داخل المؤسسات المصرفية بحيث تصبح مسؤولية مشتركة بين جميع العاملين وليس فقط فرق تقنية المعلومات والأمن السيبراني.

٥.٥ مقترحات الدراسات المستقبلية

في ضوء نتائج الدراسة الحالية، يمكن اقتراح مجموعة من الموضوعات للدراسات المستقبلية، كما يلي:

إجراء دراسات مستقبلية تتناول تأثير أنواع محددة من المخاطر السيبرانية، مثل هجمات التصيد الإلكتروني، وبرمجيات الفدية، وتسريب البيانات، على أداء واستمرارية الخدمات المصرفية الإلكترونية.

دراسة دور تقنيات الذكاء الاصطناعي في تعزيز قدرة البنوك على اكتشاف التهديدات السيبرانية والاستجابة لها بشكل أسرع.

إجراء دراسات مقارنة بين البنوك السعودية والبنوك في دول أخرى للتعرف على الاختلافات في استراتيجيات إدارة المخاطر السيبرانية ومستوى جاهزية الأمن السيبراني.

دراسة أثر ثقافة الأمن السيبراني لدى الموظفين والعملاء على تقليل الحوادث الأمنية وتعزيز الثقة في الخدمات المصرفية الإلكترونية.

دراسة العلاقة بين خطط استمرارية الأعمال وإدارة التعافي من الكوارث وبين قدرة البنوك على المحافظة على استقرار الخدمات المصرفية الإلكترونية أثناء حدوث الهجمات السيبرانية.

توسيع نطاق الدراسات المستقبلية لتشمل قطاعات أخرى تعتمد على الخدمات الإلكترونية، مثل شركات التأمين والجهات الحكومية والمؤسسات المالية.

المراجع:

أولاً: المراجع العربية

- البنك المركزي السعودي. (٢٠٢٢). إطار الأمن السيبراني للقطاع المالي. الرياض، المملكة العربية السعودية.
- إطار الأمن السيبراني للبنك المركزي السعودي
- البنك المركزي السعودي. (٢٠٢٣). التقرير السنوي للبنك المركزي السعودي. الرياض، المملكة العربية السعودية.
- الهيئة الوطنية للأمن السيبراني. (٢٠٢٢). الضوابط الأساسية للأمن السيبراني (ECC-1:2018).
- الهيئة الوطنية للأمن السيبراني. (٢٠٢٣). التقرير السنوي للهيئة الوطنية للأمن السيبراني.
- هيئة الاتصالات والفضاء والتقنية. (٢٠٢٣). تقرير حالة الإنترنت في المملكة العربية السعودية.

ثانياً: المراجع الإنجليزية

- Basel Committee on Banking Supervision. (2021). Principles for Operational Resilience.
- Basel Committee on Banking Supervision. (2023). Operational resilience and cyber risk management.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise Risk Management: Integrating with Strategy and Performance.
- International Organization for Standardization. (2018). ISO 31000:2018 Risk Management—Guidelines.
- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements.
- National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF) 2.0.
- World Bank. (2024). Digital Transformation and Cybersecurity Risks in the Financial Sector.

- Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security management and the role of human factors in organizations. *Information & Management*, 51(4), 438–449.
- Cebula, J. J., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks*. Carnegie Mellon University.
- Bouveret, A. (2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*. International Monetary Fund.
- European Banking Authority. (2021). *Guidelines on ICT and Security Risk Management*.
- Kopp, E., Kaffenberger, L., & Wilson, C. (2023). *Cyber Risk and Financial Stability: Implications for the Banking Sector*.
- Elsayed, A., et al. (2024). *Cybersecurity Disclosure, Corporate Governance, and Institutional Performance in Banking*.
- Alrawad, M. (2024). *Cyber Threats Facing Financial Institutions in the Era of Digital Transformation*.
- Sayari, A. (2024). *The Impact of Electronic Banking Services on the Performance of Saudi Banks*.

- Al Mohayya, A., & Makeen, M. (2025). The Impact of Social Engineering on Cybersecurity Risks in Saudi Banks.
- Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review .
- Tran, T. N. (2025). Systematic Review of Cybersecurity in Banking: Evolution from Pre–Industry 4.0 to Post–Industry 4.0 in Artificial Intelligence, Blockchain, Policies and Practice .
- Haruna, W., Aremu, T. A., & Modupe, Y. A. (2022). Defending against cybersecurity threats to the payments and banking system .
- Cumming, D., Nguyen, M., Pham, A. V., & Samarasinghe, A. (2025). Banking system stability: A global analysis of cybercrime laws .

الملاحق

استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

تقوم الباحثة بإجراء دراسة بعنوان: "تقييم المخاطر السيبرانية وأثرها على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية "

نظراً لما لديكم من معرفة وخبرة عملية في هذا المجال، يسعدنا دعوتكم للإسهام في هذه الدراسة من خلال الإجابة على أسئلة الاستبيان بدقة وموضوعية. ستساعد آراؤكم ومعلوماتكم القيمة في فهم طبيعة المخاطر السيبرانية وتأثيرها على الخدمات المصرفية الإلكترونية.

نؤكد لكم أن جميع البيانات التي سيتم جمعها ستعامل بسرية تامة، ولن تُستخدم إلا لأغراض البحث العلمي، مع احترام كامل للخصوصية.

نشكر لكم تعاونكم ومساهماتكم في إنجاح هذه الدراسة، ونسأل الله أن يجعل ذلك في موازين حسناتكم.

وتفضلوا بقبول فائق التقدير والاحترام،

القسم: البيانات الديموغرافية للمشاركة:

الجنس

- ذكر
- أنثى

العمر

- أقل من ٣٠ سنة
- من ٣٠ - ٣٥ سنة
- من ٣٦ - ٤١ سنة
- من ٤٢ - ٤٦ سنة
- من ٤٧ سنة فأكثر

المؤهل العلمي

- دبلوم
- بكالوريوس
- ماجستير
- دكتوراه

سنوات الخبرة

- أقل من سنة
- من ١ - ٥ سنوات
- من ٦ - ١٠ سنوات
- من ١١ سنة فأكثر

المجال الوظيفي

- تقنية المعلومات
- الأمن السيبراني
- الخدمات المصرفية الالكترونية
- إدارة المخاطر
- المراجعة الداخلية/ التدقيق الداخلي
- أخرى

القسم الثاني: المخاطر السيبرانية

١. تتعرض البنوك لمخاطر هجمات إلكترونية متكررة

- أوافق بشدة
- أوافق
- محايد
- لا أوافق
- لا أوافق بشدة

٢. توجد محاولات مستمرة للاحتيال الإلكتروني تستهدف العملاء

- أوافق بشدة
- أوافق
- محايد
- لا أوافق
- لا أوافق بشدة

٣. هناك تهديدات متزايدة تتعلق بسرقة البيانات المصرفية

- أوافق بشدة
- أوافق
- محايد
- لا أوافق
- لا أوافق بشدة

٤. تتعرض الأنظمة المصرفية لمحاولات اختراق بشكل دوري

- أوافق بشدة
- أوافق
- محايد
- لا أوافق
- لا أوافق بشدة

٥. يؤدي ضعف الوعي الأمني لدى بعض الموظفين إلى زيادة المخاطر السيبرانية

- أوافق بشدة
- أوافق
- محايد
- لا أوافق
- لا أوافق بشدة

٦. تواجه البنوك تهديدات تتعلق بتعطيل الأنظمة الالكترونية بشكل مفاجئ

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

٧. تعد الهجمات الالكترونية من أبرز التحديات التي تواجه القطاع المصرفي

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

القسم الثالث: استقرار الخدمات المصرفية الالكترونية

١. تعمل الخدمات المصرفية الالكترونية في البنك بشكل مستمر دون انقطاع

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

٢. يتمتع النظام المصرفي الالكتروني بدرجة عالية من الاستقرار والكفاءة

- أوافق بشدة
- أوافق
- محايد
- لا أوافق
- لا أوافق بشدة

٣. يتم حماية بيانات العملاء أثناء استخدام الخدمات المصرفية الالكترونية بشكل فعال

- أوافق بشدة
- أوافق
- محايد
- لا أوافق
- لا أوافق بشدة

٤. يتميز البنك بسرعة الاستجابة عند حدوث أعطال في الأنظمة الالكترونية

- أوافق بشدة
- أوافق
- محايد
- لا أوافق
- لا أوافق بشدة

٥. يحافظ البنك على استمرارية الخدمات المصرفية الالكترونية حتى في أوقات الضغط

العالي

○ أوافق بشدة

○ أوافق

○ محايد

○ لا أوافق

○ لا أوافق بشدة

٦. لا تتأثر الخدمات المصرفية الالكترونية بشكل كبير بالمشكلات التقنية او الأمنية

○ أوافق بشدة

○ أوافق

○ محايد

○ لا أوافق

○ لا أوافق بشدة

٧. يتمتع العملاء بمستوى عال من الثقة في الخدمات المصرفية الالكترونية المقدمة

○ أوافق بشدة

○ أوافق

○ محايد

○ لا أوافق

○ لا أوافق بشدة

القسم الرابع: الإجراءات الأمنية والاستراتيجيات الوقائية

١. يمتلك البنك أنظمة امن سيبراني متقدمة لحماية البيانات والأنظمة

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشد

٢. يتم تحديث الأنظمة الأمنية بشكل دوري لمواكبة التهديدات الحديثة

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

٣. توجد سياسات واضحة ومعتمدة لإدارة المخاطر السيبرانية داخل البنك

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

٤. يتم تدريب الموظفين بشكل مستمر على أساليب الامن السيبراني

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

٥. يستخدم البنك تقنيات التشفير لحماية البيانات والمعاملات الالكترونية

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

٦. توجد أنظمة مراقبة مستمرة لرصد أي تهديدات او اختراقات محتملة

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

٧. تسهم الإجراءات الأمنية المتبعة في تقليل أثر المخاطر السيبرانية على خدمات

المصرفية

○ أوافق بشدة

○ أوافق

○ محايد

○ لا أوافق

○ لا أوافق بشدة

Midocean University
College of Management
Department of Master of Risk



Assessing Cybersecurity Risks and Their Impact on the Stability of Electronic Banking Services in Saudi Banks

:Prepared by

Abrar Duayj Alrajeh

:Supervised by

Dr. / Faisal Abdul Hamad Muhammad

Dr. / Fayez Ali Jarad

Year:2026