

عنوان البحث

الأمن السيبراني ودوره في قرار استخدام الخدمات المصرفية عبر الإنترنت دراسة

ميدانية على مستخدمي الخدمات البنكية الرقمية

إعداد الطالب/

شروق المطيري

إشراف/

د. الفصيل عبد الحميد

د. فايز جراد

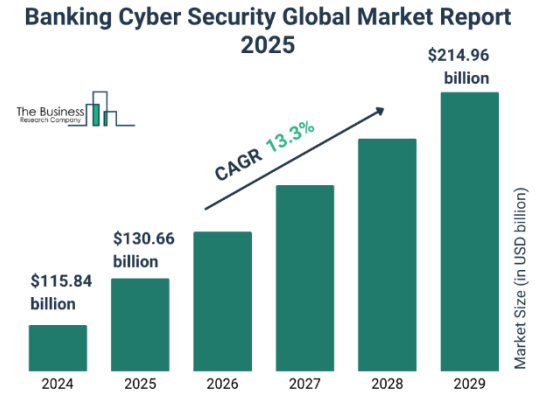
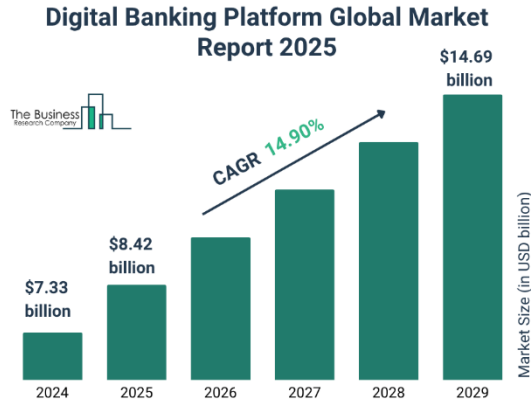
العام الدراسي:

2025

مقدمة:

أصبحت الخدمات المصرفية عبر الإنترنت جزءًا محوريًا من التحول الرقمي في القطاع المالي ، حيث تمكّن العملاء من تنفيذ معاملاتهم البنكية بسرعة وكفاءة دون الحاجة إلى زيارة الفروع التقليدية ، ومع توسع انتشار الهواتف الذكية والإنترنت عالي السرعة في الدول العربية ، وخاصة في المملكة العربية السعودية ، ازدادت معدلات الاعتماد على القنوات المصرفية الرقمية بشكل غير مسبوق ، وهو ما أكدته تقرير البنك الدولي الذي أوضح أن المنطقة العربية تشهد نموًا سريعًا في رقمنة المعاملات المالية نتيجة التغيرات السلوكية والثقة المتزايدة في البنية التحتية الرقمية . (البنك الدولي، 2023)

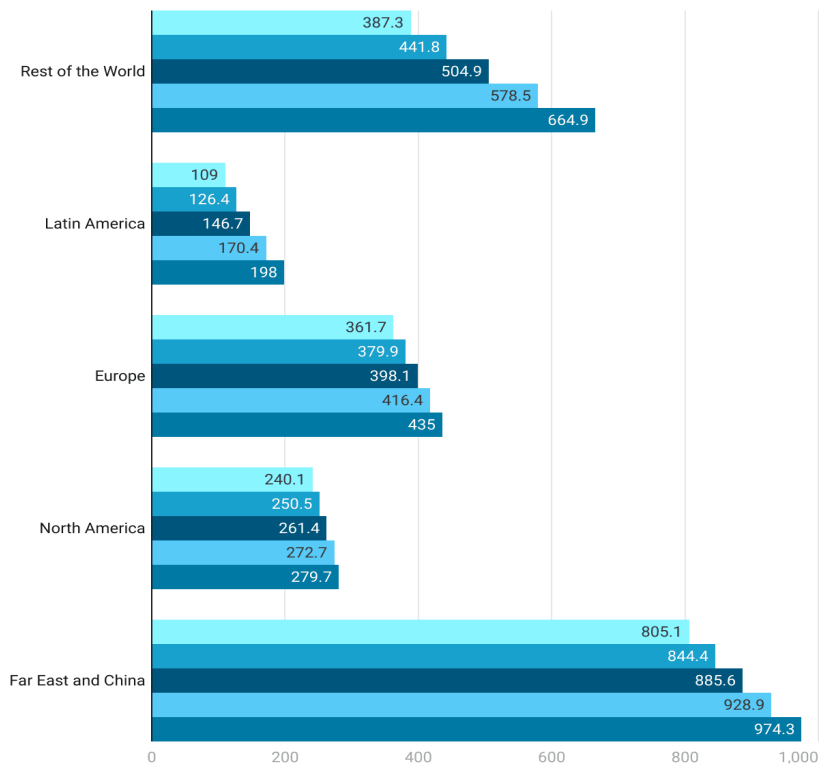
تشير الإحصائيات العالمية الحديثة إلى أن الاعتماد على الخدمات المصرفية الرقمية يشهد نموًا غير مسبوق، حيث أوضح تقرير **Bankrate (2025)** أن نحو 77٪ من المستهلكين يفضلون إدارة حساباتهم البنكية عبر التطبيقات الهاتفية أو المنصات الإلكترونية بدلاً من زيارة الفروع التقليدية وهو ما يعكس انتقالًا واضحًا نحو القنوات الرقمية باعتبارها الخيار الأول لإتمام العمليات المصرفية كما أشار تقرير **CoinLaw (2025)** إلى أن حجم المعاملات الرقمية عالميًا " بما في ذلك المحافظ الإلكترونية والتحويلات عبر الإنترنت " قد تجاوز 3.1 تريليون دولار خلال عام 2025 بزيادة تقدر بحوالي 24٪ مقارنة بالعام السابق وهي زيادة مدفوعة بتوسع الاعتماد على المصرفية الهاتفية وخدمات البنوك الإلكترونية مما يؤكد أن التحول نحو الخدمات المصرفية الرقمية لم يعد خيارًا تقنيًا بل أصبح اتجاهًا عالميًا متسارعًا تدعمه سلوكيات المستخدمين والابتكارات المالية الحديثة.



Online Banking Users Worldwide In 2020 With Forecasts To 2024,

Banking Users By Region (in million)

2020 2021 2022 2023 2024



Source: ElectroIQ

Electro IQ

ورغم هذا التوسع الكبير في الخدمات البنكية الرقمية ، إلا أن قرار المستخدم بالاعتماد على هذه الخدمات يظل مرتبطاً ارتباطاً وثيقاً بثقته في مستوى الأمن السيبراني الذي توفره المؤسسات المصرفية، إذ تشير الدراسات إلى أن المخاطر السيبرانية مثل الاحتيال المالي ، سرقة البيانات ، وانتحال الهوية الإلكترونية تشكل عائقاً رئيسياً أمام استخدام

الخدمات المصرفية عبر الإنترنت ، حيث أوضح الاتحاد العربي للاقتصاد الرقمي أن ضعف الوعي الأمني لدى المستخدمين يُعد من أبرز أسباب نجاح الهجمات الإلكترونية في المنطقة العربية . (الاتحاد العربي للاقتصاد الرقمي.

(2022)

وقد دفعت هذه التحديات المؤسسات المصرفية العربية إلى تبني معايير أمنية أكثر صرامة مثل المصادقة الثنائية -Two

Factor Authentication (2FA) ، التشفير المتقدم (AES) Advanced Encryption Standard او End-to-End

Encryption (E2EE) ، وأنظمة مراقبة المعاملات في الزمن الحقيقي Real-Time Transaction Monitoring

Systems ، وهي إجراءات أكدت أهمية الأمن السيبراني في حماية البيانات المالية وتعزيز ثقة العملاء ، كما قامت

مؤسسة النقد العربية السعودية "ساما SAMA" في إطار تطوير البيئة المالية الرقمية ، بإصدار عدد من الضوابط

الخاصة بالأمن السيبراني للمصارف لضمان أعلى درجات الحماية لمستخدمي الخدمات البنكية الإلكترونية (Saudi

Central Bank SAMA,2017)

تُجمع الأدبيات العربية الحديثة على أن القطاع المصرفي من أكثر القطاعات تعرّضًا للهجمات السيبرانية ، وأن تكلفة

هذه الهجمات على البنوك عالميًا تمثل نسبة كبيرة من إجمالي الخسائر الناتجة عن الجرائم الإلكترونية، وهو ما انعكس

على تشديد البنوك المركزية العربية لتعليماتها الرقابية في مجال أمن المعلومات ، وإلزام المصارف بوضع سياسات

وإجراءات شاملة لحماية التطبيقات البنكية الإلكترونية ، وتقييم المخاطر بصورة دورية، وتفعيل آليات الاستجابة

للحوادث السيبرانية، وتُشير دراسة Azura إلى أن الأمن السيبراني أصبح شرطًا أساسيًا لاستمرار الثقة في الخدمات

المصرفية الرقمية، وليس مجرد عنصر تقني مساعد إذ ربطت الدراسة بين فعالية الأطر التشريعية والرقابية وبين قدرة

البنوك على حماية بيانات العملاء واستمرار تعاملهم مع القنوات الإلكترونية . (Azura,2025)

قدّم صندوق النقد العربي عرضًا مقارنًا مهمًا للمعايير والتجارب الدولية والعربية في مجال الأمن السيبراني في القطاع المصرفي، مبيّنًا أن أغلب البنوك المركزية العربية اتجهت إلى إدماج مخاطر الأمن السيبراني ضمن إطار المخاطر التشغيلية ، مع إصدار تعليمات تفصيلية بشأن: حوكمة الأمن السيبراني Cybersecurity Governance، التي تُعد الإطار العام المنظم لإدارة المخاطر الرقمية داخل المؤسسات المصرفية ... وتشمل هذه المنظومات إلزام المصارف بإجراء اختبارات الاختراق (Penetration Testing (Pentest بشكل دوري لتقييم مستوى الحماية والكشف عن الثغرات قبل استغلالها من قبل المهاجمين ، إضافة إلى تطوير سياسات متقدمة لإدارة كلمات السر Password Management بما يشمل الحد الأدنى لطول كلمة المرور، وفترات تغييرها ، وآليات تخزينها وتشفيرها داخل الأنظمة المصرفية . (Saudi

Central Bank SAMA,2017)

كما تفرض هذه التعليمات وضع ضوابط لتحويل الأموال عبر القنوات الإلكترونية Electronic Funds Transfer Controls (EFT Controls) لتقليل احتمالية الاحتيال أو التلاعب بالمعاملات المالية وتضيف البنوك المركزية طبقات حماية أقوى عبر التحقق من هوية المستخدم من خلال المصادقة الثنائية Two-Factor Authentication – 2FA، والاعتماد على الرموز السرية لمرة واحدة One-Time Password – OTP كآلية أساسية للتأمين ضد محاولات الاختراق وانتحال الهوية الإلكترونية.

كما أبرزت الأدبيات السابقة أن المصارف العربية مُلزمة بتبني استراتيجيات واضحة للأمن السيبراني تُقرّها مجالس الإدارة ، مع وجود مسؤول مختص بأمن المعلومات (CISO) ، والتزام بتقييم دوري لنقاط الضعف في التطبيقات البنكية الإلكترونية ، وهو ما يوقّر خلفية معيارية تنظم المستوى الأدنى المقبول من الحماية الذي يبني عليه العميل قراره باستخدام الخدمات المصرفية عبر الإنترنت .

تُظهر الدراسات الميدانية في البيئة العربية أن الأمن والثقة يمثلان محورين أساسيين في قرار استخدام الخدمات المصرفية الإلكترونية، ففي دراسة محمد مفتاح الشيخ رحيل (2023) حول العوامل المؤثرة في الخدمات المصرفية الإلكترونية من وجهة نظر عملاء المصارف التجارية بالقطاع المصرفي الليبي (عينّة ٣٢٢ مستجيبًا)، توصّل الباحث إلى أن هناك نقصًا في ثقة العملاء بالخدمات المصرفية الإلكترونية ، وأن المخاطر المحتملة مثل فقدان البيانات الشخصية أو التعرّض للاختراق تُعدّ عائقًا واضحًا أمام تبني هذه الخدمات ، كما أظهرت الدراسة أن غياب التعليمات والشروحات الواضحة على المواقع الإلكترونية للبنوك يقلّل من سهولة الاستخدام، وأن انخفاض الفائدة المدركة (مثل عدم الإحساس بالراحة، أو عدم توفير تكلفة أو وقت حقيقي) يحدّ من الإقبال على الخدمات الرقمية، وبذلك تؤكد هذه الدراسة أن قرار الاستخدام يتشكّل عند تقاطع ثلاثة أبعاد: إدراك الأمان، وإدراك الفائدة، وإدراك سهولة الاستخدام، مع بروز الأمن السيبراني كعامل حاكم في البيئة العربية . (رحيل و الشيخ , 2023)

ومن هنا تأتي أهمية هذه الدراسة الميدانية التي تهدف إلى تحليل أثر الأمن السيبراني في قرار استخدام الخدمات المصرفية عبر الإنترنت ، من خلال فهم اتجاهات وسلوكيات مستخدمي الخدمات البنكية الرقمية في البيئة العربية ، ومحاولة رصد أهم العوامل المؤثرة في تبني الخدمات المالية الرقمية ، ومدى ارتباطها بإجراءات الأمن السيبراني المطبقة من قبل البنوك ، مما يساهم في تقديم توصيات عملية لرفع مستوى الثقة الرقمية وتحسين جودة الخدمات البنكية الإلكترونية .

مشكلة الدراسة:

تشهد المملكة العربية السعودية تحولاً رقمياً واسعاً في القطاع المصرفي ضمن مستهدفات رؤية 2030، حيث اتجهت البنوك السعودية إلى تطوير قنواتها الرقمية وتعزيز خدماتها المصرفية عبر الإنترنت استجابة لارتفاع مستوى استخدام الهواتف الذكية وانتشار خدمات الإنترنت، وقد أكدت مؤسسة النقد العربي السعودي " البنك المركزي السعودي (SAMA (2017) أن التحول الرقمي في القطاع المالي أصبح ركيزة أساسية لرفع جودة الخدمات ودعم الشمول المالي، إلا أن هذا التوسع صاحبه زيادة في حجم وتعقيد الهجمات السيبرانية التي تستهدف الأنظمة المصرفية ، وهو ما ظهر بوضوح في التقارير الصادرة عن المركز الوطني الإرشادي للأمن السيبراني (CERT-SA ، 2023) التي أشارت إلى ارتفاع محاولات الاختراق والاحتيال المالي الموجهة ضد المؤسسات المالية في السعودية، الأمر الذي أوجد تحدياً يتمثل في قدرة العملاء على الثقة في القنوات البنكية الإلكترونية ، خصوصاً في ظل وجود فجوة بين ما تنقذه البنوك من إجراءات أمنية وما يدركه المستخدم من مستوى الحماية المتاح له.

وتعود مشكلة الدراسة أيضاً إلى أن الأمن السيبراني لا يتحقق بمجرد تطبيق ضوابط تقنية، بل يرتبط بعدة أبعاد... منها البعد التقني الذي يشمل تطبيق نظم التشفير المتقدم *Advanced Encryption Standard (AES) أو End-to-End Encryption (E2EE)* وتفعيل المصادقة الثنائية *Two-Factor Authentication (2FA)* وأنظمة المراقبة الفورية للمعاملات *Real-Time Transaction Monitoring Systems*، إضافة إلى البعد الإداري المرتبط بحوكمة الأمن السيبراني *Cybersecurity Governance* والتي تؤكد عليها توجهات البنك المركزي السعودي (SAMA ، 2017) التي تلزم المصارف بإنشاء إدارات متخصصة للأمن السيبراني وتقييم المخاطر بصفة مستمرة ، والبعد السلوكي المتعلق

بمستوى وعي العملاء السعودي بطرق الاحتيال الإلكتروني وأساليب الهندسة الاجتماعية ، وهو ما أوضحته دراسة شرمهان التوني (2023) التي أكدت أن وعي العملاء عنصر مؤثر في فعالية الأمن السيبراني.

كما تُظهر الدراسات أن الثقة الرقمية أصبحت العامل الحاسم في قرار استخدام الخدمات البنكية الإلكترونية ؛ فدراسة صواق وآخرون (2023) تُبين أن إدراك الأمان هو المتغير الأكثر تأثيرًا في استعداد الأفراد لاستخدام الخدمات الرقمية، فيما تشير دراسات عربية أخرى إلى أن مخاوف العملاء من اختراق البيانات وسرقة الهوية وانتحال الحسابات البنكية تعد من أبرز العوائق التي تحد من استخدام القنوات المصرفية الإلكترونية رغم توافر البنية التكنولوجية ، وذلك يؤكد أن المشكلة لم تعد تقنية فحسب ، بل أصبحت سلوكية وإدراكية وإعلامية ، وأن نجاح البنوك السعودية في رفع معدل الاعتماد على الخدمات المصرفية الرقمية مرتبط بمدى قدرتها على تعزيز الثقة من خلال الوضوح في إجراءات الحماية، والإفصاح عن إدارة مخاطر الأمن السيبراني كما بينت دراسة كعموش (2024) التي أوضحت أهمية الإفصاح الشفاف في تعديل أحكام العملاء وقراراتهم.

وتُبرز الدراسات أن العملاء السعوديين يواجهون عدة مخاوف محددة ترتبط بالأمن السيبراني تشمل : الخوف من سرقة البيانات البنكية ، الخوف من اعتراض الرسائل النصية أو الرموز السرية OTP ، القلق من اختراق التطبيقات المصرفية ، ضعف معرفة البعض بطرق التحقق من الروابط المزيفة ، إضافة إلى الخوف من فشل النظام أثناء التحويلات المالية ، وهذه المخاوف " وفق ما أشار إليه المركز الوطني الإرشادي للأمن السيبراني (2023) " تؤثر بشكل مباشر في مستوى إقبال العملاء على استخدام الخدمات الرقمية مقارنة بالفروع التقليدية رغم توسع البنوك السعودية في تبني أعلى المعايير الأمنية . (المركز الوطني الإرشادي للأمن السيبراني CERT-SA , 2023)

وبناءً على ما تم ذكره تتبلور مشكلة الدراسة في وجود فجوة بين الإجراءات الأمنية الفعلية التي تطبقها المصارف السعودية وفق إطار الأمن السيبراني الصادر عن SAMA، وبين إدراك العملاء لمستوى الأمان الذي يحصلون عليه عند استخدام القنوات المصرفية الإلكترونية ، وهي فجوة تؤثر في قرار المستخدم السعودي وتحدُّ من تبني الخدمات المصرفية الرقمية بشكل كامل رغم جاهزية البنية التحتية السعودية وتقدّمها إقليمياً . (SAMA,2017)

ومما سبق ذكره نستطيع القول ان هذه الدراسة تهدف الى الإجابة على السؤال التالي " كيف يؤثر الأمن السيبراني بأبعاده التقنية والإدارية والسلوكية في قرار استخدام الخدمات المصرفية عبر الإنترنت لدى مستخدمي الخدمات البنكية الرقمية في المملكة العربية السعودية؟ "

أهمية الدراسة:

تنبع أهمية هذه الدراسة من كونها تتناول أحد أكثر التحديات تأثيراً في مستقبل القطاع المصرفي السعودي وهو عامل الأمن السيبراني الذي أصبح عنصراً حاسماً في بناء الثقة الرقمية وتعزيز استخدام الخدمات المصرفية عبر الإنترنت في ظل التحول الرقمي الذي تشهده المملكة ضمن مستهدفات رؤية 2030 حيث تشير تقارير البنك المركزي السعودي SAMA 2017 إلى أن توسع الخدمات البنكية الرقمية يعتمد بدرجة كبيرة على قدرة المؤسسات المالية على حماية البيانات الحساسة وضمان سرية المعاملات الإلكترونية كما تؤكد تقارير المركز الوطني الإرشادي للأمن السيبراني CERT SA 2023 أن المملكة من بين الدول الأكثر تعرضاً لمحاولات هجمات إلكترونية تستهدف القطاع المالي مما يجعل دراسة أثر الأمن السيبراني على قرار العميل السعودي ضرورة علمية وميدانية ملحة .

1. الأهمية النظرية للدراسة

تتمثل الأهمية النظرية لهذه الدراسة في كونها تسهم في تطوير المعرفة العلمية الخاصة بالأمن السيبراني في القطاع المصرفي السعودي من خلال معالجة فجوة واضحة في الأدبيات العربية التي غالبًا ما ركزت على الجانب التقني للأمن السيبراني دون دراسة تأثيره المباشر على قرار استخدام الخدمات المصرفية عبر الإنترنت حيث تؤكد تقارير البنك المركزي السعودي SAMA 2017 أن تطبيق الضوابط الأمنية وحده لا يكفي ما لم يقترن بإدراك المستخدم لمستوى الحماية كما ركزت دراسات عربية مثل التوني 2023 وصواق وآخرون 2023 على ارتباط الأمن السيبراني بسلوك المستهلك لكن دون دمج الأبعاد التقنية والإدارية والسلوكية معًا وهذا ما تمنحه الدراسة الحالية من قيمة علمية حيث تقدم إطارًا متكاملًا يربط بين الأمن السيبراني وإدراك الأمان والثقة الرقمية وقرار الاستخدام في السياق السعودي مما يثري الجانب النظري ويضيف بُعدًا تحليليًا جديدًا يُمكن الباحثين من بناء نماذج بحثية أكثر دقة في مجالات الأمن المعلوماتي والتحول الرقمي والتعاملات البنكية الإلكترونية.

2. الأهمية التطبيقية للدراسة

تنبع الأهمية التطبيقية لهذه الدراسة من قدرتها على تقديم نتائج وتوصيات مباشرة يمكن للمصارف السعودية تطبيقها لتعزيز مستوى الأمن المدرك لدى العملاء وبالتالي رفع معدلات استخدام الخدمات المصرفية الإلكترونية بما يتوافق مع مستهدفات التحول الرقمي لرؤية المملكة 2030 حيث تشير تقارير المركز الوطني الإرشادي للأمن السيبراني CERT SA 2023 إلى أن الهجمات الإلكترونية التي تستهدف القطاع المالي أصبحت أكثر تعقيدًا الأمر الذي يجعل معرفة العوامل المؤثرة في ثقة العملاء ضرورة عملية وملحة كما تُظهر دراسات مثل كعموش 2024 أن الإفصاح الواضح عن إدارة مخاطر الأمن السيبراني يغيّر أحكام العملاء ويزيد من قبولهم للتعاملات البنكية الإلكترونية ولذلك تتيح الدراسة الحالية للمؤسسات المصرفية إمكانية تصميم سياسات حماية أكثر ملاءمة وتطوير أنظمة التشفير

والمصادقة الثنائية وبرامج التوعية الأمنية للعملاء وتقديم خدمات رقمية أكثر أماناً وثقة وهو ما يدعم تحسين التجربة المصرفية الرقمية ويحد من الجرائم الإلكترونية ويرفع مستوى الاعتماد على القنوات البنكية الإلكترونية بوصفها بديلاً آمناً وفعالاً للفروع التقليدية.

أهداف الدراسة:

1. معرفة مستوى تطبيق الأمن السيبراني بأبعاده التقنية والإدارية والسلوكية في البنوك السعودية
2. معرفة مستوى الثقة الرقمية لدى مستخدمي الخدمات البنكية الإلكترونية في المملكة العربية السعودية
3. معرفة مستوى قرار استخدام الخدمات المصرفية عبر الإنترنت لدى عملاء البنوك السعودية
4. معرفة العلاقة بين تطبيق الأمن السيبراني في بُعدته التقني (التشفير المتقدم – المصادقة الثنائية – المراقبة الفورية للمعاملات) والثقة الرقمية لدى عملاء البنوك السعودية
5. معرفة العلاقة بين تطبيق الأمن السيبراني في بُعدته الإداري (حوكمة الأمن السيبراني – إدارة المخاطر – السياسات الأمنية – اختبارات الاختراق) والثقة الرقمية لدى عملاء البنوك السعودية
6. معرفة العلاقة بين تطبيق الأمن السيبراني في بُعدته السلوكي (الوعي الأمني – إدراك المخاطر – سلوكيات الحماية الشخصية) وقرار استخدام الخدمات المصرفية عبر الإنترنت
7. معرفة العلاقة بين الثقة الرقمية بأبعادها (الثقة في حماية البيانات – الثقة في سلامة العمليات – الثقة في موثوقية النظام) وقرار استخدام الخدمات البنكية الإلكترونية
8. معرفة العلاقة بين الأمن السيبراني بأبعاده الثلاثة وقرار استخدام الخدمات المصرفية عبر الإنترنت لدى العملاء.

تساؤلات الدراسة

السؤال الرئيسي

كيف يؤثر الأمن السيبراني بأبعاده التقنية والإدارية والسلوكية في قرار استخدام الخدمات المصرفية عبر الإنترنت لدى مستخدمي الخدمات البنكية الرقمية في المملكة العربية السعودية، وما الدور الذي تلعبه الثقة الرقمية في هذه العلاقة؟

التساؤلات الفرعية

- ما مستوى تطبيق الأمن السيبراني في البنوك السعودية بأبعاده التقنية والإدارية والسلوكية؟
- ما مستوى الثقة الرقمية لدى مستخدمي الخدمات البنكية الإلكترونية في المملكة العربية السعودية؟
- ما مستوى قرار استخدام الخدمات المصرفية عبر الإنترنت لدى عملاء البنوك السعودية؟
- ما العلاقة بين تطبيق الأمن السيبراني في أبعاده التقنية "التشفير المتقدم - المصادقة الثنائية - المراقبة الفورية للمعاملات" والثقة الرقمية من قبل العملاء؟
- ما العلاقة بين تطبيق الأمن السيبراني في أبعاده الإدارية "حوكمة الأمن السيبراني - إدارة المخاطر - سياسات الأمن - اختبارات الاختراق" والثقة الرقمية لدى عملاء البنوك السعودية؟
- ما العلاقة بين تطبيق الأمن السيبراني في أبعاده السلوكية "الوعي الأمني - إدراك المخاطر - سلوكيات الحماية الشخصية" وقرار استخدام الخدمات المصرفية عبر الإنترنت؟

▪ ما العلاقة بين الثقة الرقمية بأبعاده " الثقة في حماية البيانات – الثقة في سلامة العمليات – الثقة في موثوقية

النظام" وقرار استخدام الخدمات البنكية الإلكترونية في المملكة العربية السعودية؟

▪ ما العلاقة بين الأمن السيبراني بأبعاده الثلاثة وقرار استخدام الخدمات المصرفية عبر الإنترنت؟

▪ كيف تتوسط الثقة الرقمية العلاقة بين الأمن السيبراني "بأبعاده التقنية والإدارية والسلوكية" وقرار استخدام

الخدمات المصرفية عبر الإنترنت لدى العملاء في البنوك السعودية؟

فروض الدراسة:

الفرضية الرئيسة الاولى :

H1 : يوجد تأثير ذو دلالة إحصائية للأمن السيبراني بأبعاده التقنية والإدارية والسلوكية في قرار استخدام

الخدمات المصرفية عبر الإنترنت لدى عملاء البنوك السعودية

أولاً: فرضيات المتغير المستقل (الأمن السيبراني) وأبعاده

H1a : يوجد تأثير ذو دلالة إحصائية للبعد التقني للأمن السيبراني في قرار استخدام الخدمات المصرفية عبر

الإنترنت

H1b : يوجد تأثير ذو دلالة إحصائية للبعد الإداري / الحوكمة للأمن السيبراني في قرار استخدام الخدمات

المصرفية عبر الإنترنت

H1c: يوجد تأثير ذو دلالة إحصائية للبعد السلوكي / الوعي الأمني للأمن السيبراني في قرار استخدام الخدمات

المصرفية عبر الإنترنت

ثانيًا: فرضيات العلاقة بين الأمن السيبراني والثقة الرقمية

H1d: يوجد تأثير ذو دلالة إحصائية للأمن السيبراني بأبعاده التقنية والإدارية والسلوكية في الثقة الرقمية لدى

مستخدمي الخدمات البنكية الإلكترونية

ثالثًا: فرضيات المتغير الوسيط (الثقة الرقمية) و أبعاده

H1e: يوجد تأثير ذو دلالة إحصائية للثقة في حماية البيانات في قرار استخدام الخدمات المصرفية عبر الإنترنت

H1f: يوجد تأثير ذو دلالة إحصائية للثقة في سلامة العمليات البنكية الإلكترونية في قرار استخدام الخدمات

المصرفية عبر الإنترنت

H1g: يوجد تأثير ذو دلالة إحصائية للثقة في موثوقية النظام الإلكتروني للبنك في قرار استخدام الخدمات

المصرفية عبر الإنترنت

رابعًا: فرضية الوساطة

H1h: تتوسط الثقة الرقمية العلاقة بين الأمن السيبراني بأبعاده الثلاثة وقرار استخدام الخدمات المصرفية عبر

الإنترنت لدى عملاء البنوك السعودية

الدراسات السابقة:

تقدم دراسة Azura وزملائه (2025) إطاراً متكاملًا لإدارة مخاطر الأمن السيبراني في الأنظمة المصرفية عبر الإنترنت حيث توضح الدراسة أن انتشار الخدمات البنكية الرقمية أدى إلى ظهور تحديات متزايدة تتعلق بالخصوصية وحماية البيانات وأن النماذج الأمنية التقليدية لم تعد كافية لمواجهة الهجمات السيبرانية المعقدة التي تستهدف أنظمة البنوك وقد اقترح الباحثون إطاراً يعتمد على النمذجة المبنية على التهديدات والمخاطر ويشمل عمليات شاملة لإدارة المخاطر وتقييم الثغرات وتحليل سيناريوهات الهجوم بطريقة منظمة وسياقية كما يعمل الإطار المقترح على قياس المخاطر الرقمية وتحديد استراتيجيات التخفيف المناسبة مما يساعد في تطبيق سياسات حماية فعّالة في بيئات مصرفية حقيقية وقد أكدت نتائج التقييم أن الإطار قادر على معالجة مشكلات الأمن والخصوصية في البنوك الرقمية وأنه قابل للتطبيق والدمج مع البنية التكنولوجية والتنظيمية القائمة في الأنظمة المصرفية الحديثة

تُبرز دراسة أميرة هائف ودرغام العميدي وصفات بكاش (2024) أهمية القيادة الرقمية في تعزيز سلوك الأمن السيبراني لدى العاملين في المصارف الأهلية حيث تعاملت الدراسة مع القيادة الرقمية بوصفها متغيراً مستقلاً من خلال أبعاد تشمل الرؤية الرقمية والابتكار الرقمي والمعرفة الرقمية والمشاركة بينما تناولت سلوك الأمن السيبراني بوصفه متغيراً تابعاً مقاساً بأبعاد مثل تأمين الجهاز وإنشاء كلمة مرور قوية والوعي الاستباقي والتحديث المستمر وقد اعتمد الباحثون على استبانة طُبقت على عينة من العاملين في مصارف أهلية بمحافظة النجف الأشرف بلغ عددها 97 استبانة صالحة للتحليل باستخدام SPSS و SmartPLS وأظهرت النتائج وجود علاقة تأثير إيجابية واضحة بين القيادة الرقمية وسلوك الأمن السيبراني بما يشير إلى أن تطوير مهارات القادة في المجال الرقمي يعزز قدرة المؤسسات المصرفية على حماية بياناتها ورفع وعي العاملين لديها بالمخاطر السيبرانية

وتتناول دراسة شرف الدين بن قومار ونهاد دارم (2023) دور الذكاء الاصطناعي في تعزيز التكنولوجيا المالية وتحسين كفاءة الخدمات المالية في المؤسسات المصرفية الجزائرية حيث اعتمدت الدراسة على المنهج الوصفي والمقابلات مع مديري وكالات بنكية بولاية غرداية بهدف تحليل آراء الإدارة المصرفية حول مدى تبني تقنيات الذكاء الاصطناعي في تطوير الخدمات المالية وكشفت النتائج أن البنوك الجزائرية لا تتبنى الذكاء الاصطناعي أو التكنولوجيا المالية الذكية بسبب إدراكها أن استخدام هذه التقنيات يتطلب تغييرات جذرية في البنى التحتية المالية والمعلوماتية مما يحتاج إلى استثمارات كبيرة لا تستطيع البنوك تحملها في الوقت الحالي كما أظهرت الدراسة أن عدم الجاهزية الرقمية يمثل عائقاً رئيسياً أمام تطوير خدمات مالية رقمية متقدمة تعتمد على الذكاء الاصطناعي

يبرز إسماعيل 2019 في عرضه المقارن لمعايير الأمن السيبراني أن البنوك المركزية في الدول العربية اتجهت إلى دمج مخاطر الأمن السيبراني ضمن إطار إدارة المخاطر التشغيلية وكان ذلك من خلال تبني سياسات واضحة تشمل حوكمة الأمن السيبراني واختبارات الاختراق وإدارة كلمات المرور وضوابط تحويل الأموال الإلكترونية والتحقق من الهوية باستخدام المصادقة الثنائية والرموز السرية مرة واحدة كما يوضح أن المصارف العربية أصبحت مطالبة بإعداد استراتيجيات أمن سيبراني مُعتمدة من مجالس إدارتها مع ضرورة تعيين مسؤول مختص بأمن المعلومات CISO وتنفيذ تقييمات دورية لنقاط الضعف مما يوفر للعميل الحد الأدنى من الأمان الذي يبني عليه قراره باستخدام الخدمات البنكية عبر الإنترنت

صواق وبوداود وأولاد حيمودة (2023): جاهزية الأمن السيبراني وتأثيرها على استخدام الخدمات المصرفية الإلكترونية حيث تُظهر دراسة صواق وزملائه أن جاهزية البنية التكنولوجية والموارد البشرية للأمن السيبراني لها تأثير مباشر وغير مباشر على استخدام العملاء للخدمات المصرفية الإلكترونية إذ تكشف الدراسة أن تحسين البنية التحتية التقنية

والرفع من كفاءة الكوادر البشرية المتخصصة في أمن المعلومات يؤدي إلى خفض المخاطر المدركة لدى العملاء ومن ثم زيادة احتمالية استخدامهم للقنوات البنكية الإلكترونية وتبين النتائج أن قرار العميل لا يتأثر فقط بالضوابط التقنية الفعلية بل يتأثر بشكل أكبر بإحساسه بالطمأنينة واستشعاره لمستوى الأمن المتاح له أثناء استخدامه للخدمات المصرفية

تؤكد التوني 2023 أن وعي العملاء يمثل متغيرًا بالغ الأهمية في فعالية الأمن السيبراني داخل البنوك الحكومية حيث تبرز الدراسة دور الوعي الأمني في تعزيز قدرة العملاء على التعامل الآمن مع الخدمات البنكية الإلكترونية وذلك من خلال فهمهم لطرق الاحتيال والتصيد الإلكتروني والقدرة على التمييز بين الروابط المزيفة وتشير نتائج الدراسة إلى أن دور الأمن السيبراني في خفض الجرائم المالية لا يكتمل إلا عندما يقترن ببرامج توعية مستمرة مما يعني أن التكنولوجيا وحدها لا تكفي وأن سلوك العميل ووعيه يمثلان جزءًا أساسيًا في قرار استخدام الخدمات المصرفية عبر الإنترنت ويوضح رحيل 2023 أن قرار استخدام الخدمات المصرفية الإلكترونية يتحدد من خلال ثلاثة أبعاد رئيسية هي إدراك الأمان وإدراك الفائدة وإدراك سهولة الاستخدام وتكشف الدراسة عن وجود فجوة في الثقة لدى العملاء تجاه الخدمات المصرفية الإلكترونية حيث يرى الكثير من العملاء أن مخاطر فقدان البيانات الشخصية أو التعرض للاختراق تشكل عائقًا مباشرًا أمام تبنيهم لهذه الخدمات كما تبين الدراسة أن غياب الشروحات والتعليمات الواضحة في المواقع الإلكترونية للبنوك يقلل من سهولة الاستخدام ويؤثر في استعداد العملاء لاستخدام الخدمات الرقمية رغم توفر البنية التكنولوجية اللازمة

يُظهر البواعنة 2023 من خلال دراسته أن ارتفاع إدراك مخاطر الأمن السيبراني لدى العملاء يؤدي إلى انخفاض استخدامهم للبطاقات المصرفية خاصة في المعاملات الإلكترونية ويوضح أن المخاطر الأكثر تأثيرًا تشمل سرية البيانات

وسلامة العمليات واستمرارية تقديم الخدمات كما تشير الدراسة إلى أن حوكمة الأمن السيبراني أصبحت من محددات

الاشتمال المالي في البنوك الأردنية حيث تمثل سياسة الحماية وشفافية الإفصاح عن المخاطر عنصرين مهمين في اتخاذ

الأفراد قرارًا باستخدام الخدمات المالية الرقمية والانخراط في النظام المالي الرسمي

تُبين دراسة كعموش 2024 أن الإفصاح الواضح عن إدارة مخاطر الأمن السيبراني في البنوك له تأثير مباشر في قرارات

العملاء والمستثمرين وتوضح النتائج أن شكل الإفصاح ومكانه سواء في تقارير مجلس الإدارة أو في تقارير مستقلة يمكن

أن يعزز ثقة العملاء بالبنك أو يضعفها وتثبت الدراسة أن قرار استخدام الخدمات المصرفية عبر الإنترنت يرتبط ليس

فقط بمستوى الأمن الفعلي ولكن أيضًا بمدى شفافية البنك في عرض ممارسات الأمن السيبراني وشرح كيفية التعامل

مع التهديدات السيبرانية كما تشير إلى أن خصائص العملاء الديموغرافية مثل العمر والجنس قد تعدل من أثر

الإفصاح على قراراتهم

المنطلقات النظرية للدراسة:

تستند هذه الدراسة إلى مجموعة من الأسس النظرية التي تُشكّل الإطار العام لفهم العلاقة بين الأمن السيبراني وقرار استخدام الخدمات المصرفية عبر الإنترنت من خلال دمج المنظور التقني والتنظيمي والسلوكي الذي يفسر تفاعل العملاء مع القنوات البنكية الرقمية في البيئة السعودية حيث يقوم الإطار النظري على فرضية أن قرار استخدام الخدمات المصرفية الإلكترونية لا يتحدد فقط ببنية الأنظمة التقنية أو بجودة الخدمات الرقمية بل يرتكز بدرجة كبيرة على إدراك المستخدم لمستوى الأمان والثقة التي توفرها البنوك عبر منصاتها الإلكترونية وهو ما يتوافق مع الاتجاهات الحديثة في أدبيات التكنولوجيا المالية والتحول الرقمي. (Whitman & Mattord 2022)

ويعتمد هذا التوجه على أن الأمن السيبراني يمثل حجر الزاوية في نجاح الخدمات المصرفية عبر الإنترنت وأن أي قصور في الضوابط الأمنية أو آليات حماية البيانات ينعكس بشكل مباشر على انخفاض معدلات الاعتماد على القنوات البنكية الرقمية، إذ تُظهر الدراسات الدولية والعربية أن البيئة المصرفية الحديثة أصبحت أكثر عرضة للهجمات السيبرانية نتيجة تطور التهديدات وتنوعها بما يشمل هجمات الاختراق والتصيد والبرمجيات الخبيثة والهجمات الموجهة التي تستهدف تعطيل الأنظمة أو سرقة البيانات المالية الحساسة مما يجعل الأمن السيبراني عاملاً تفسيرياً رئيسياً لفهم سلوك العملاء واتخاذهم القرار باستخدام الخدمات الرقمية (Kim et al. 2009).

كما تستند الدراسة إلى الأساس النظري الذي يفترض أن الثقة الرقمية تُعد متغيراً وسيطاً بين الأمن السيبراني وقرار الاستخدام حيث تشير نظريات الثقة في الأنظمة التقنية إلى أن المستفيد لا يعتمد على الخدمات الرقمية إلا عندما يشعر بالاطمئنان تجاه قدرة النظام على حماية بياناته والحفاظ على سرية وسلامة المعاملات الإلكترونية وأن الثقة لا تُبنى فقط من خلال وجود الضوابط الأمنية بل من خلال إدراك المستخدم لاستقرار النظام وشفافية البنك في

الإفصاح عن سياساته الأمنية والاستجابة للحوادث السيبرانية وهو ما يجعل الثقة الرقمية جسراً يربط بين الأمن

المدرّك والاستخدام الفعلي للخدمات البنكية الإلكترونية. (Yousafzai et al. (2003

وترتكز الدراسة كذلك على منطلقات نماذج تبني التكنولوجيا مثل نموذج قبول التكنولوجيا Technology

Acceptance Model (TAM) الذي طرحه Davis (1989) ونموذج تكامل التكنولوجيا Unified Theory of

Acceptance and Use of Technology (UTAUT) الذي قدمه Venkatesh et al. (2003) حيث تفترض هذه النماذج

أن قرار استخدام الخدمات الإلكترونية يتشكل من خلال المتغيرات الإدراكية وبخاصة الأمان المدرّك والجدوى المدرّكة

وسهولة الاستخدام المدرّكة غير أن الدراسة الحالية تركز بصفة خاصة على الأمن السيبراني بوصفه المتغير الأكثر

تأثيراً في قرار الاستخدام في البيئة المصرفية العربية نظراً لحساسية البيانات المالية وارتفاع وتيرة الهجمات في

القطاعات البنكية العربية كما أوضحت تقارير ENISA (2021)

ويستند البحث أيضاً إلى الأساس النظري لاقتصاديات الثقة الذي يؤكد أن الثقة تمثل عنصراً حاكماً في التعاملات

المالية الرقمية وأن تراجعها يؤدي إلى اختلال العلاقة بين العميل والبنك وإلى تفضيل العملاء للقنوات التقليدية رغم

توفر البنية التكنولوجية الحديثة، كما تُبرز الأدبيات أن قرار الاستخدام يرتبط بدرجة كبيرة بالخطر المدرّك وأن

العملاء يميلون إلى تجنب الخدمات التي يشعرون بأنها غير آمنة حتى وإن كانت أسرع أو أكثر مرونة، مما يجعل الأمن

السيبراني عاملاً حاسماً في تشكيل القرار النهائي للعميل السعودي في اعتماد أو تجنب الخدمات المصرفية عبر

الإنترنت.

وانطلاقاً من هذه المنطلقات النظرية، فإن الدراسة تبني نموذجاً يدمج بين الأمن السيبراني بأبعاده التقنية والإدارية

والسلوكية والثقة الرقمية بأبعادها المتعلقة بحماية البيانات وسلامة العمليات وموثوقية النظام باعتبارها محددات

أساسية تؤثر في قرار استخدام الخدمات البنكية الإلكترونية كما يفترض النموذج أن الأبعاد الثلاثة للأمن السيبراني تشكل الأساس الذي يُؤدّد الثقة الرقمية لدى المستفيد والتي بدورها تُحوّل الإدراك الأمني إلى قرار استخدام فعلي وبذلك يستند البحث إلى إطار نظري متكامل يسمح بفهم العلاقة بين المتغيرات محل الدراسة وتفسير سلوك المستخدمين في البيئة المصرفية السعودية.

المنهجية وطرق البحث:

تعتمد هذه الدراسة على منهجية علمية تجمع بين المدخل الوصفي والتحليلي بهدف تحليل أثر الأمن السيبراني بأبعاده التقنية والإدارية والسلوكية في قرار استخدام الخدمات المصرفية عبر الإنترنت لدى عملاء البنوك السعودية، إضافة إلى تحليل الدور الوسيط للثقة الرقمية في هذه العلاقة، حيث يتناسب هذا الدمج المنهجي مع طبيعة الدراسة التي تتطلب توصيف الظاهرة كما يدركها العملاء من جهة، واختبار العلاقات بين المتغيرات من جهة أخرى، بما ينسجم مع التوجهات الحديثة في الدراسات المرتبطة بالتكنولوجيا المالية والأمن السيبراني.

ويُعدُّ المنهج الوصفي التحليلي الأنسب لهذه الدراسة نظرًا لقدرته على وصف مستوى تطبيق ضوابط الأمن السيبراني لدى البنوك السعودية، وقياس مستوى الثقة الرقمية، وتحديد درجة اعتماد العملاء على الخدمات البنكية الإلكترونية، كما يسمح هذا المنهج بتحليل المتغيرات واختبار الفرضيات الإحصائية باستخدام تقنيات التحليل الإحصائي المناسبة، الأمر الذي يضمن الوصول إلى نتائج دقيقة يمكن تعميمها على مجتمع الدراسة.

وقد اعتمدت الدراسة على أسلوب المسح الميداني باعتباره أسلوبًا ملائمًا لجمع بيانات كمية من عينة ممثلة لمستخدمي الخدمات المصرفية عبر الإنترنت في المملكة العربية السعودية، وقد تم هذا من خلال استخدام الاستبيان

بوصفه الأداة الرئيسة لجمع البيانات باعتباره الوسيلة الأكثر استخدامًا في الدراسات التي تتناول السلوك الرقمي والاتجاهات الإدراكية للعملاء تجاه الأنظمة الإلكترونية.

وتم تصميم أداة الدراسة بالاعتماد على الأدبيات العلمية والنماذج النظرية السابقة، حيث اشتملت الاستبانة على مجموعة من الفقرات التي تقيس المتغيرات الرئيسة للدراسة وهي الأمن السيبراني بأبعاده الثلاثة، والثقة الرقمية بأبعادها، وقرار الاستخدام بأبعاده السلوكية، وذلك باستخدام مقياس ليكرت الخماسي Lekert Scale الذي يتيح قياس اتجاهات المستجيبين بدقة عالية K كما خضعت الأداة للتحكيم العلمي من قبل مجموعة من المختصين في مجالات الأمن السيبراني وإدارة الأعمال بهدف التأكد من سلامة الصياغة ووضوح الفقرات ومدى ملاءمتها للأهداف البحثية، إضافة إلى إجراء اختبار أولي (Pilot Test) على عينة صغيرة للتحقق من صدق الاتساق الداخلي وموثوقية الأداة باستخدام معامل كرونباخ ألفا.

وتعتمد الدراسة في اختبار الفرضيات على مجموعة من الأساليب الإحصائية الملائمة لطبيعة المتغيرات مثل المتوسطات الحسابية والانحرافات المعيارية لقياس اتجاهات المستجيبين، ومعامل الارتباط بيرسون للكشف عن قوة واتجاه العلاقة بين المتغيرات، إضافة إلى تحليل الانحدار البسيط والمتعدد واختبار النمذجة الهيكلية (SEM) باستخدام برنامج SPSS للتحقق من أثر الأمن السيبراني في قرار الاستخدام ودور الثقة الرقمية كمتغير وسيط في هذه العلاقة، كما سيتم اختبار ملاءمة النموذج الإحصائي من خلال مؤشرات الصدق البنائي وملاءمة النموذج. وقد تم اختيار مجتمع الدراسة من مستخدمي الخدمات المصرفية عبر الإنترنت في البنوك السعودية، نظرًا لكونهم الفئة الأكثر قدرة على تقديم بيانات دقيقة تتعلق بتجربتهم الأمنية وثقتهم في التطبيقات البنكية، وتم اختيار العينة بأسلوب العينة العشوائية البسيطة لتمثيل شريحة واسعة من مستخدمي الخدمات البنكية الإلكترونية في المملكة

العربية السعودية، ويُتوقع أن تسهم هذه المنهجية المتكاملة في تقديم نتائج علمية موثوقة تدعم البنوك السعودية في

تطوير سياساتها الأمنية وتعزيز ثقة العملاء بالخدمات المصرفية الرقمية، وصولاً إلى رفع معدلات تبني القنوات

البنكية الإلكترونية في ظل التحول الرقمي المتسارع.

وقد تم توزيع رابط الاستبيان الإلكتروني على مستخدمي الخدمات المصرفية عبر الإنترنت من خلال وسائل التواصل

الاجتماعي والقوائم البريدية وقنوات الاتصال الرقمية المتاحة بهدف الوصول إلى أكبر عدد ممكن من أفراد المجتمع

المستهدف وبناءً على معادلة تحديد حجم العينة وفق جدول Morgan and Krejcie الذي يوضح أن العينة المناسبة

للمجتمعات الكبيرة يجب ألا تقل عن 250 مفردة لضمان تمثيل صحيح لأفراد المجتمع عند مستوى دلالة إحصائية

مقبول فقد حددت الدراسة الحد الأدنى اللازم لعدد أفراد العينة بـ 250 مستجيباً

أدوات الدراسة:

اعتمدت الدراسة على أداة بحثية رئيسية تمثلت في الاستبانة الإلكترونية التي تُعد من أكثر الأدوات ملائمة لقياس

المتغيرات السلوكية والإدراكية المتعلقة بالأمن السيبراني والثقة الرقمية وقرار استخدام الخدمات المصرفية عبر

الإنترنت وذلك نظراً لقدرتها على جمع بيانات كمية دقيقة من عينة واسعة من المستجيبين بطريقة سريعة ومنظمة كما

تتيح الاستبانة إمكانية قياس اتجاهات العملاء وتصوراتهم حول مستوى الأمان الرقمي المطبق في البنوك السعودية

ومدى تأثيره في قراراتهم باستخدام القنوات البنكية الإلكترونية

وقد جرى بناء الاستبانة وفق منهج علمي يعتمد على مراجعة شاملة للأدبيات العربية والأجنبية والدراسات السابقة

المرتبطة بموضوع الأمن السيبراني مثل أعمال Whitman و Mattord ودراسات الثقة الرقمية كما ورد لدى McKnight

و Kim وزملائه ودراسات تبني الخدمات البنكية الإلكترونية مثل Yousafzai و Pikkarainen إضافة إلى الأطر التنظيمية

الصادرة عن البنك المركزي السعودي SAMA والتي تمثل مرجعاً أساسياً في صياغة بنود البعد التقني والإداري للأمن السيبراني وقد صُممت فقرات الاستبانة بحيث تغطي أبعاد المتغيرات الثلاثة الرئيسة وهي الأمن السيبراني بأبعاده التقنية والإدارية والسلوكية والثقة الرقمية بأبعادها المتعلقة بحماية البيانات وسلامة العمليات وموثوقية النظام وقرار الاستخدام بأبعاده المتعلقة بالنية السلوكية والاستخدام الفعلي والاستمرارية

وقد تم استخدام مقياس ليكرت الخماسي لقياس إجابات المستجيبين حيث تراوحت درجات الاستجابة بين (1 = لا أوافق بشدة) و(5 = أوافق بشدة) بما يسمح بقياس مستوى الاتفاق وتحديد الاتجاهات بدقة .

ولغرض التحقق من ثبات أداة الدراسة فقد تم استخدام معامل الثبات كرونباخ ألفا لقياس مدى اتساق العبارات التي تقيس كل بُعد من أبعاد المتغيرات حيث إن قيمة معامل كرونباخ ألفا التي تتراوح بين 0.70 فأكثر تُعد مؤشراً قوياً على الثبات الداخلي للأداة كما تم استخدام تحليل الموثوقية Reliability Analysis من خلال برنامج SPSS للتحقق من ثبات كل محور وبناءً على النتائج التي سيتم الحصول عليها سيوضح البحث أن أداة الدراسة تمتلك مستوى مناسباً من الصدق والثبات بما يسمح بتطبيقها على عينة واسعة من مستخدمي الخدمات المصرفية الإلكترونية في المملكة العربية السعودية

وهكذا تمثل الاستبانة أداة الدراسة الأساسية التي سيتم من خلالها جمع البيانات وتحليلها بهدف اختبار فرضيات البحث والوصول إلى نتائج تمثل الواقع الفعلي لتأثير الأمن السيبراني في قرار استخدام الخدمات المصرفية عبر الإنترنت ودور الثقة الرقمية في تفسير هذه العلاقة بشكل علمي ودقيق

حدود الدراسة :

الحدود الزمنية

تغطي الحدود الزمنية لهذه الدراسة الفترة الممتدة ما بين يناير 2026 الى يونيو 2026

الحدود المكانية

تركز الحدود المكانية للدراسة على البنوك السعودية العاملة داخل المملكة العربية السعودية وتشمل فروعها المنتشرة

في المناطق الرئيسية مثل الرياض وجدة والدمام والمدينة المنورة ومكة المكرمة إضافة إلى المنصات الإلكترونية

والتطبيقات البنكية التي تقدمها هذه المصارف للعملاء عبر الإنترنت وتم اختيار هذا النطاق المكاني نظرًا لكون القطاع

المصرفي السعودي من أكثر القطاعات تقدمًا في التحول الرقمي والأكثر تعرضًا للهجمات السيبرانية وهو ما يجعل

دراسة تأثير الأمن السيبراني على قرار استخدام الخدمات المصرفية عبر الإنترنت داخل هذا الإطار المكاني ذات أهمية

علمية وعملية عالية خصوصًا في ظل التزام البنوك السعودية بإطار الأمن السيبراني الصادر عن SAMA وما يرتبط به

من ضوابط تشغيلية وتنظيمية

الحدود البشرية (عينة الدراسة)

تشمل الحدود البشرية لهذه الدراسة عملاء البنوك السعودية المستخدمين للخدمات المصرفية عبر الإنترنت سواء

من خلال التطبيقات البنكية أو المواقع الإلكترونية

الحدود الموضوعية

تقتصر الحدود الموضوعية للدراسة على تحليل أثر الأمن السيبراني بأبعاده التقنية والإدارية والسلوكية على قرار

استخدام الخدمات المصرفية عبر الإنترنت مع دراسة دور الثقة الرقمية كمتغير وسيط ولا تمتد الدراسة إلى تقييم

الأداء المالي للبنوك أو تحليل جودة البنية التحتية التقنية للدولة أو مقارنة دولية بين الأنظمة المصرفية وإنما تركز

على المتغيرات المرتبطة بسلوك العملاء واتجاهاتهم تجاه الأمان والثقة والاستخدام الفعلي للقنوات البنكية

الإلكترونية في البيئة السعودية

المراجع:

أولاً: المراجع العربية

1. البنك الدولي. (2023). الخدمات المالية الرقمية .
<https://www.albankaldawli.org/ar/topic/financialinclusion/brief/digital-financial-services>
2. الاتحاد العربي للاقتصاد الرقمي. (2022). تقارير ومبادرات الاقتصاد الرقمي في العالم العربي من
<https://arabfederationdigitaleconomy.org>
3. مؤسسة النقد العربي السعودي (سما). (2017). إطار الأمن السيبراني للمصارف العاملة في السعودية
<https://www.sama.gov.sa/ar-sa/finance/pages/cybersecurityframework.aspx>
4. المنظمة العربية لتكنولوجيا المعلومات. (2021). تقارير ودراسات التحول الرقمي في المنطقة العربية
<https://www.arabits.org>
5. المركز الوطني للإرشادي للأمن السيبراني. (2023). تقارير التوعية بالهجمات السيبرانية في السعودية
<https://cert.gov.sa>
6. جامعة الدول العربية. (2021). مبادرة التحول الرقمي العربي وتقارير تطوير البيئة الرقمية . من
<https://www.lasportal.org>
7. إسماعيل، محمد. (2019). الأمن السيبراني في القطاع المصرفي: عرض مقارن للمعايير والتجارب الدولية والعربية. صندوق النقد العربي.
<https://www.amf.org.ae/sites/default/files/publications/2022-01/cyber-security-december-15-2019.pdf>
8. صواق، عبد القادر، بوداود، بومدين، وأولاد حيمودة، عبد اللطيف. (2023). أثر جاهزية الأمن السيبراني على الخدمات المصرفية الإلكترونية. أبحاث اقتصادية معاصرة، 6(1)، 372-353.
<https://search.emarefa.net/detail/BIM-1474860>
9. التوني، شريهان مصطفى. (2023). أثر وعي العملاء بالقرصنة الإلكترونية كأداة لتحقيق الأمن السيبراني . مجلة التجارة والتمويل، 43(4)، 653-609.
https://caf.journals.ekb.eg/article_332810.html
10. رحيل، محمد مفتاح الشيخ. (2023). العوامل المؤثرة في الخدمات المصرفية الإلكترونية من وجهة نظر عملاء المصارف التجارية. مجلة البحوث الأكاديمية، 27، 113-93.
<https://lam-journal.ly/index.php/jar/article/view/489>
11. البواعنة، سهل محمد سودي. (2023). أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن. رسالة دكتوراه، جامعة العلوم الإسلامية العالمية.
<https://search.mandumah.com/Record/1461033>

12. كعموش، شريف علي خميس إبراهيم. (2024). أثر بدائل الإفصاح عن إدارة مخاطر الأمن السيبراني في القطاع المصرفي على أحكام المستفيدين. مجلة البحوث المحاسبية، 11(3)، 901–930.
https://abj.journals.ekb.eg/article_375936_84477bed41694ba0452e4edc039f42f1.pdf

ثانياً : المراجع الأجنبية

13. Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). *An integrated cyber security risk management framework for online banking systems*. Journal of Banking and Financial Technology. <https://doi.org/10.1007/s42786-025-00056-3>
14. Saudi Central Bank – SAMA. (2017). *Cybersecurity Framework*.
<https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Cyber%20Security%20Framework.pdf>
15. Hatif, A., Al-Ameedi, D., & Bakash, S. (2024). *Digital leadership and cybersecurity behaviour*. HNSJ, 5(1). <https://doi.org/10.53796/hnsj51/46>
16. Ben Goumar, C., & Darm, N. (2023). *AI and smart financial technology in Algerian banks*. University of Ghardaia. <https://dspace.univ-ghardaia.edu.dz/xmlui/handle/123456789/6269>
17. Davis, F. D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. MIS Quarterly, 13(3), 319–340.
<https://www.jstor.org/stable/249008>
18. ENISA. (2021). *ENISA Threat Landscape Report 2021*.
<https://www.enisa.europa.eu/publications>
19. Gefen, D. (2000). *E-commerce: The role of familiarity and trust*. Omega, 28(6), 725–737.
<https://www.sciencedirect.com/science/article/abs/pii/S0305048300000359>
20. Kim, D. J., Ferrin, D. L., & Rao, H. R. (2009). *Trust and satisfaction in online banking: An integrative perspective*. Decision Support Systems, 48(2), 343–356.
<https://www.sciencedirect.com/science/article/abs/pii/S0167923609000029>
21. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). *Developing and validating trust measures for e-commerce*. Information Systems Research, 13(3), 334–359.
<https://pubsonline.informs.org/doi/abs/10.1287/isre.13.3.334.81>
22. Whitman, M., & Mattord, H. (2022). *Principles of Information Security* (7th ed.). Cengage Learning.
23. Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2003). *A proposed model of e-trust for electronic banking*. Technovation, 23(11), 847–860.
<https://www.sciencedirect.com/science/article/abs/pii/S0160791X03000505>

