

أثر الأمن السيبراني على ثقة العملاء في المعاملات البنكية الإلكترونية

دراسة ميدانية على المصارف السعودية

إعداد الطالبة/دلال ضويحي مبارك القحطاني

الرقم الجامعي /252200066

إشراف/

د. الفیصل عبد الحمید محمد حسن

د.فايز جراد

العام الدراسي: 2025

3	مقدمة:
3	مشكلة الدراسة
4	أهمية الدراسة:
5	أهداف الدراسة:
6	تساؤلات الدراسة
7	فروض الدراسة:
7	الدراسات السابقة:
17	الفجوة البحثية:
19	المنطلقات النظرية للدراسة:
22	المنهجية وطرق البحث:
22	ثانياً: مجتمع الدراسة
22	ثالثاً: عينة الدراسة
23	رابعاً: أداة الدراسة
25	حدود الدراسة:
26	المراجع

مقدمة:

يشكل الأمن السيبراني في العصر الرقمي محوراً استراتيجياً لضمان استدامة الثقة بين البنوك وعملائها، لاسيما مع التحول الواسع نحو المعاملات البنكية الإلكترونية التي أصبحت العمود الفقري للقطاع المالي في المملكة العربية السعودية. فقد أدى توسع استخدام التكنولوجيا المالية والخدمات الرقمية إلى زيادة تعرض المؤسسات المصرفية لمخاطر الجرائم السيبرانية، مما جعل حماية البيانات والمعلومات أمراً جوهرياً للحفاظ على سمعة المصارف وثقة العملاء بها. فالأمن السيبراني لا يُعد فقط أداة تقنية، بل هو عنصر حاكم في بناء المصداقية والاستقرار في البيئة المصرفية الرقمية (قلاع الضروس، 2022؛ جربوعه وبوطمين، 2023).

تؤكد الدراسات أن فعالية الأمن السيبراني تعتمد على تكامل أبعاده التقنية والقانونية والتنظيمية والبشرية في منظومة واحدة متماسكة. إذ أظهرت دراسة (محارب، 2023) أن تقنيات الذكاء الاصطناعي أسهمت في تحسين سرعة اكتشاف الهجمات الرقمية والتعامل معها، بينما كشفت دراسة (عباس وآخرون، 2023) أن غياب التشريعات الشاملة وضعف التنسيق المؤسسي يشكلان أبرز التحديات أمام تأمين الفضاء السيبراني. كما أوضحت دراسة (البدوي، 2024) أن الأمن السيبراني لم يعد شأنًا تقنياً فحسب، بل أصبح قضية سيادية تتطلب تكاملاً بين الجوانب السياسية والتقنية والقانونية لتحقيق الردع الفعال ضد التهديدات الرقمية.

من ناحية أخرى، أثبتت الدراسات في القطاع المصرفي العربي أن رفع مستوى الأمان السيبراني يسهم مباشرة في تعزيز ثقة العملاء، وهو ما أكدته دراسة (فتوح، 2021) التي بيّنت أن الأمان والسرية في المعاملات الإلكترونية يمثلان ركيزةً لتعزيز كفاءة النظام المصرفي العربي. وخلصت دراسة (Hira et al., 2025) إلى وجود علاقة طردية قوية بين إدراك العملاء للأمن السيبراني ومستوى ثقتهم بالخدمات المصرفية الإلكترونية، في حين أكدت دراسة (Khoiriah et al., 2024) أن ضعف الحماية من الهجمات السيبرانية يؤدي إلى تراجع الأداء المالي والسمعة المؤسسية للمصارف.

وعليه، تسعى هذه الدراسة إلى تحليل أثر الأمن السيبراني بأبعاده المختلفة على مستوى ثقة العملاء في المعاملات البنكية الإلكترونية بالمصارف السعودية، بهدف تقديم تصور متكامل يساهم في تعزيز بيئة مصرفية رقمية آمنة وموثوقة، تدعم مستهدفات رؤية المملكة 2030 في التحول الرقمي والابتكار المالي.

مشكلة الدراسة

يشهد القطاع المصرفي السعودي تحولاً رقمياً متسارعاً في إطار رؤية المملكة 2030، حيث أصبحت المعاملات البنكية الإلكترونية جزءاً أساسياً من المنظومة المالية الحديثة. ومع هذا التحول، برزت التحديات الأمنية المرتبطة بالجرائم السيبرانية التي تهدد سرية البيانات وسلامة المعاملات الإلكترونية، مما أثر بشكل مباشر على مستوى ثقة العملاء في التعامل مع القنوات المصرفية الرقمية (قلاع الضروس، 2022؛ جربوعه وبوطمين، 2023). فالهجمات الإلكترونية لم تعد تستهدف الأنظمة التقنية فقط، بل تمسّ العلاقة الجوهرية بين العميل والمؤسسة المالية، وهو ما ينعكس على سلوك العملاء واتجاهاتهم نحو الخدمات المصرفية الإلكترونية.

تؤكد الدراسات الحديثة أن الأمن السيبراني يمثل أحد أهم العوامل المؤثرة في استدامة ثقة العملاء، إذ بيّنت دراسة (Hira et al., 2025) أن ارتفاع مستوى الوعي بالأمان الرقمي ووضوح إجراءات الحماية يعززان ثقة العملاء في المعاملات البنكية الإلكترونية. في المقابل، أظهرت دراسة (Khoiriah et al., 2024) أن ضعف البنية التحتية للأمن السيبراني يؤدي إلى تراجع الأداء المالي والسمعة المؤسسية، مما يقلل من درجة الثقة المتبادلة بين البنك وعملائه. وهذا يوضح أن الأمن السيبراني لا يُعد مجرد وسيلة تقنية، بل هو عامل نفسي وسلوكي مرتبط بتصور العملاء لموثوقية البنك.

كما أشار (فتوح، 2021) إلى أن ضعف نظم الحماية في المصارف العربية يشكل عائقاً أمام تحقيق الشمول المالي، وأن تعزيز الأمان والسرية يمثلان حجر الزاوية في بناء الثقة الرقمية بين العملاء والبنوك. وأكدت دراسة (محارب، 2023) أن الاعتماد على تقنيات الذكاء الاصطناعي في كشف التهديدات وتحليل البيانات الأمنية يساهم في رفع جاهزية الأنظمة المصرفية ضد الهجمات الإلكترونية، إلا أن غياب التكامل بين الجانب التقني والتنظيمي يضعف من فعالية تلك الجهود.

ومن جهة أخرى، بيّنت دراسة (عبدالفتاح، 2022) أن بعض العملاء ما زالوا يترددون في استخدام الخدمات البنكية الرقمية بسبب مخاوف تتعلق بضعف الأمان السيبراني، ونقص الوعي بآليات الحماية، مما يعكس فجوة بين التطور التقني ومستوى الثقة الفعلي لدى المستخدمين. كما أكدت دراسة (لحمر، 2022) أن الثقة عبر الإنترنت تعدّ عاملاً حاسماً في تعزيز الولاء الإلكتروني، وأن أي تهديد أمني يُضعف الرضا والالتزام لدى العملاء في البيئة المصرفية الرقمية.

بناءً على ما سبق، تتحدد مشكلة الدراسة في أن التوسع في الخدمات البنكية الإلكترونية بالمملكة العربية السعودية ترافق مع تصاعد التهديدات السيبرانية التي قد تؤثر على مستوى ثقة العملاء في التعاملات المصرفية الرقمية. ومن هنا ينبثق التساؤل الرئيس الآتي:

ما أثر الأمن السيبراني بأبعاده المختلفة على ثقة العملاء في المعاملات البنكية الإلكترونية بالمصارف السعودية؟

أهمية الدراسة:

تعتمد أهمية هذه الدراسة على إسهاماتها النظرية والتطبيقية فيما يلي:

أولاً: الأهمية العلمية

- تُسهم الدراسة في إثراء المعرفة الأكاديمية في مجال الأمن السيبراني وعلاقته بثقة العملاء في الخدمات البنكية الإلكترونية، من خلال تقديم إطار نظري يدمج بين المفاهيم التقنية والسلوكية.
- توضح العلاقة بين أبعاد الأمن السيبراني (السرية، السلامة، الخصوصية، الموثوقية) وسلوك العملاء تجاه الخدمات المصرفية الرقمية، مما يعزز من فهم التفاعل بين التكنولوجيا والسلوك المالي.
- تقدم نموذجاً علمياً يمكن الاستفادة منه في الدراسات المستقبلية التي تتناول الأمن السيبراني في القطاعات المالية، وتفتح المجال لإجراء مقارنات بين بيانات مصرفية مختلفة.
- ترصد حقل الدراسات المصرفية برؤية تحليلية تستند إلى الواقع السعودي، في ظل التحول الرقمي السريع ضمن رؤية المملكة 2030، مما يجعلها مرجعاً محلياً يمكن البناء عليه في الدراسات اللاحقة.

- تساعد في تطوير أدوات قياس علمية دقيقة لقياس إدراك العملاء للأمن السيبراني ومستوى الثقة في الخدمات الإلكترونية البنكية.

ثانياً: الأهمية العملية

- تمكّن إدارات البنوك السعودية من تحديد الأبعاد الأكثر تأثيراً في ثقة العملاء، مما يساهم في تطوير سياسات حماية فعالة وأنظمة أمنية متكاملة.
- تقدم نتائج الدراسة مؤشرات تساعد صناع القرار في القطاع المالي على تحسين البنية التحتية للأمن السيبراني وتعزيز الإجراءات الوقائية ضد الهجمات الإلكترونية.
- تساهم في رفع مستوى وعي العملاء والموظفين بالمخاطر الرقمية وكيفية التعامل معها، مما يعزز ثقافة الأمان الرقمي في البيئة المصرفية.
- تدعم جهود البنوك في بناء علاقة ثقة مستدامة مع العملاء من خلال تبني استراتيجيات شفافة في حماية البيانات وضمان الخصوصية.
- يمكن الاستفادة من نتائجها في تطوير برامج تدريبية وتوعوية تستهدف تعزيز السلوك الأمني لدى العاملين في البنوك والمؤسسات المالية.
- تساعد الجهات التنظيمية والرقابية في صياغة سياسات وتشريعات تدعم الأمن السيبراني وتحد من الجرائم الإلكترونية في النظام المصرفي.

أهداف الدراسة:

الهدف الرئيسى: التعرف على أثر الأمن السيبراني بأبعاده المختلفة (سرية المعلومات، سلامة النظام، الموثوقية، الخصوصية) على ثقة العملاء في المعاملات البنكية الإلكترونية في المصارف السعودية.

الأهداف الفرعية:

- تحليل أثر سرية المعلومات على ثقة العملاء في المعاملات البنكية الإلكترونية.
- دراسة أثر سلامة النظام على إدراك العملاء لأمان المعاملات الإلكترونية المصرفية.
- التعرف على أثر الموثوقية في بناء واستدامة ثقة العملاء في القنوات الرقمية البنكية.

- تحديد أثر الخصوصية على شعور العملاء بالأمان والثقة أثناء تنفيذ معاملاتهم البنكية عبر الإنترنت.

تساؤلات الدراسة

سؤال الدراسة الرئيس:

ما أثر الأمن السيبراني بأبعاده المختلفة (سرية المعلومات، سلامة النظام، الموثوقية، الخصوصية) على ثقة العملاء في المعاملات البنكية الإلكترونية في المصارف السعودية؟

الأسئلة الفرعية:

- ما أثر سرية المعلومات على ثقة العملاء في التعاملات البنكية الإلكترونية؟
- كيف تؤثر سلامة النظام على إدراك العملاء لأمان المعاملات المصرفية الإلكترونية؟
- ما دور الموثوقية في بناء واستدامة ثقة العملاء في القنوات البنكية الرقمية؟
- ما أثر الخصوصية على شعور العملاء بالأمان والثقة أثناء تنفيذ المعاملات البنكية عبر الإنترنت؟

فروض الدراسة:

لتحقيق أهداف الدراسة والإجابة على تساؤلاتها يمكن صياغة الفرضيات التالية:

الفرض الرئيس:

- هناك أثر ذو دلالة إحصائية للأمن السيبراني بأبعاده المختلفة (سرية المعلومات، سلامة النظام، الموثوقية، الخصوصية) على ثقة العملاء في المعاملات البنكية الإلكترونية في المصارف السعودية.

الفرضيات الفرعية:

1. الفرض الأول: هناك أثر ذو دلالة إحصائية لسرية المعلومات على ثقة العملاء في التعاملات البنكية الإلكترونية.
2. الفرض الثاني: هناك أثر ذو دلالة إحصائية لسلامة النظام على إدراك العملاء لأمان المعاملات البنكية الإلكترونية.
3. الفرض الثالث: هناك أثر ذو دلالة إحصائية للموثوقية في بناء واستدامة ثقة العملاء في القنوات الرقمية البنكية.
4. الفرض الرابع: هناك أثر ذو دلالة إحصائية للخصوصية على شعور العملاء بالأمان والثقة أثناء تنفيذ المعاملات البنكية عبر الإنترنت.

الدراسات السابقة:

دراسة (قلاع الضروس، 2022)

هدفت الدراسة إلى التعرف على أهمية الأمن السيبراني والجريمة الإلكترونية بأبعادهما (البعد الأمني، البعد التقني، البعد القانوني، والبعد الاستراتيجي) على تعزيز الأمن السيبراني الوطني في الجزائر، من خلال تحليل التحديات والتهديدات التي تواجه الفضاء السيبراني الجزائري، واستعراض الاستراتيجيات الأمنية والتقنية المتبعة لمواجهة الجريمة الإلكترونية.

اعتمدت الدراسة على المنهج الوصفي التحليلي، من خلال تحليل الأدبيات والنصوص القانونية والتقارير الرسمية ذات الصلة بالأمن السيبراني، مع محاولة إسقاط المفاهيم النظرية على الواقع الجزائري.

توصلت الدراسة إلى أن الأمن السيبراني يمثل أحد الركائز الحيوية في حماية سيادة الدولة وأمنها الوطني، وأن التحديات الرئيسية تتمثل في ضعف التنسيق بين الهيئات الأمنية والتقنية، ونقص الكفاءات المتخصصة، وتطور أساليب الهجمات الإلكترونية. كما أوصت الدراسة بضرورة تطوير استراتيجية وطنية متكاملة للأمن السيبراني، وتعزيز التعاون بين المؤسسات الأمنية والتقنية، وتكثيف برامج التوعية والتدريب، وتحديث الإطار التشريعي لمكافحة الجريمة الإلكترونية بما يتماشى مع المعايير الدولية. دراسة (محارب، 2023)

هدفت الدراسة إلى التعرف على أثر الذكاء الاصطناعي بأبعاده (القدرة على التعلم، الاستنتاج، التفاعل مع المواقف غير المبرمجة، وتحليل البيانات الضخمة) على تعزيز الأمن السيبراني في المؤسسات التقنية، من خلال استعراض دور تقنيات الذكاء الاصطناعي في كشف الهجمات الرقمية وتحليل البيانات الأمنية وتحسين سرعة الاستجابة للتهديدات.

استخدمت الدراسة المنهج الوصفي التحليلي بالاعتماد على تحليل الأدبيات والنماذج التطبيقية الحديثة التي توضح العلاقة بين الذكاء الاصطناعي والأمن السيبراني.

أظهرت النتائج أن توظيف تقنيات الذكاء الاصطناعي يسهم في رفع كفاءة أنظمة الأمن السيبراني من خلال التنبؤ بالهجمات، وتحليل الأنماط، واكتشاف الثغرات بسرعة أكبر من الأساليب التقليدية، في حين تبقى هناك تحديات تتعلق بمخاطر الخصوصية، والاعتماد المفرط على الخوارزميات، واحتمالية إساءة استخدام التقنية.

وأوصت الدراسة بضرورة تعزيز التكامل بين الذكاء الاصطناعي والأمن السيبراني عبر تطوير خوارزميات أكثر شفافية، وتدريب الكوادر التقنية على التعامل مع أنظمة الذكاء الاصطناعي، وتحديث الأطر التشريعية لضمان حماية البيانات وحقوق الأفراد في البيئة الرقمية.

دراسة (عباس وآخرون، 2023)

هدفت الدراسة إلى التعرف على أمن الفضاء السيبراني بأبعاده (البعد القانوني، البعد التقني، البعد التنظيمي، والبعد التشريعي) على تعزيز حماية الفضاء السيبراني والخدمات الإلكترونية في العراق، وذلك من خلال تحليل طبيعة هذا الفضاء وتحديد أهم المخاطر والتحديات التي تواجهه في ظل التطور المتسارع لتقنيات الاتصالات والمعلومات.

استخدمت الدراسة المنهج الوصفي التحليلي من خلال استعراض الأدبيات القانونية والتقنية ذات الصلة، وتحليل التجارب الدولية في تنظيم وتأمين الفضاء السيبراني.

توصلت النتائج إلى أن غياب إطار تشريعي متكامل وضعف التنسيق بين المؤسسات التقنية والقانونية يشكلان أبرز معوقات حماية الفضاء السيبراني في العراق، وأن تطوير تشريعات متخصصة وتفعيل آليات المراقبة والاستجابة السريعة يمثلان ضرورة ملحة.

وأوصت الدراسة بضرورة إصدار قانون وطني شامل للأمن السيبراني، وتأسيس هيئة مستقلة تعنى بحماية الفضاء السيبراني، وتبني معايير دولية للأمن المعلوماتي، وتعزيز الوعي المجتمعي بأهمية حماية البيانات والخصوصية في البيئة الرقمية.

دراسة (جربوعه وبوطمين، 2023)

هدفت الدراسة إلى التعرف على أثر الأمن السيبراني بأبعاده (البعد التقني، البعد البشري، البعد القانوني، والبعد التنظيمي) على حماية البيانات والمعلومات في الفضاء الرقمي، في ظل التوسع الكبير في استخدام تكنولوجيا المعلومات والاتصالات وما يصاحبه من مخاطر متزايدة تتمثل في الجرائم الإلكترونية والاختراقات الأمنية.

استخدمت الدراسة المنهج الوصفي التحليلي من خلال تحليل الظاهرة السيبرانية ومخاطرها، واستعراض الجهود الوطنية والدولية المبذولة لتعزيز الأمن السيبراني وحماية البيانات.

توصلت النتائج إلى أن تحقيق أمن سيبراني فعال يتطلب تكاملاً بين الجوانب التقنية والتشريعية والبشرية والتنظيمية، وأن ضعف الوعي الأمني، ونقص الكفاءات المتخصصة، وغياب التشريعات الرادعة تشكل أبرز التحديات التي تواجه حماية الفضاء الرقمي.

وأوصت الدراسة بضرورة تعزيز القدرات الوطنية في مجال الأمن السيبراني، وتطوير التشريعات الخاصة بالجرائم الإلكترونية، وتكثيف برامج التوعية الرقمية، وتبني استراتيجيات وطنية شاملة تدمج بين التكنولوجيا والقانون لضمان حماية فعالة للبيانات والمعلومات.

دراسة (البدوي، 2024)

هدفت الدراسة إلى التعرف على أثر الحرب السيبرانية بأبعادها (البعد التقني، البعد العسكري، البعد القانوني، والبعد السياسي) على تعزيز الأمن السيبراني العالمي، من خلال تحليل مظاهر الحرب الرقمية وتحديد الاستراتيجيات الفعالة لمواجهتها والحد من آثارها على الدول والمؤسسات والأفراد.

استخدمت الدراسة المنهج الوصفي التحليلي، بالاعتماد على تحليل البيانات والمصادر العلمية الموثوقة، ودراسة الحالات الواقعية للهجمات السيبرانية، إضافةً إلى تحليل الاستجابات الحكومية والدولية والإجراءات القانونية والتعاونية بين الدول والقطاع الخاص.

أظهرت النتائج أن الحرب السيبرانية تمثل تهديداً استراتيجياً متنامياً للأمن الوطني والدولي، وأن فعالية الأمن السيبراني تعتمد على التنسيق بين الأبعاد التقنية والسياسية والقانونية، وعلى بناء قدرات وطنية قوية في مجال الدفاع الرقمي والاستجابة السريعة للهجمات. كما تبين أن ضعف التعاون الدولي وتباين الأطر التشريعية بين الدول يشكلان تحدياً أساسياً في مكافحة الحرب السيبرانية.

وأوصت الدراسة بضرورة تطوير سياسات واستراتيجيات دفاع سيبراني وطنية متكاملة، وتعزيز الشراكات الدولية لتبادل المعلومات، وتوحيد الأطر القانونية لمكافحة الهجمات الإلكترونية، إضافة إلى الاستثمار في الذكاء الاصطناعي وتحليل البيانات للكشف المبكر عن التهديدات، ونشر ثقافة الوعي الأمني الرقمي بين الأفراد والمؤسسات.

دراسة (جعفر، 2024)

هدفت الدراسة إلى التعرف على أثر الأمن السيبراني بأبعاده (البعد التشريعي، البعد التقني، البعد التنظيمي، والبعد الإداري) على تعزيز التحول الرقمي في المنظومة العدلية في جمهورية مصر العربية، وذلك في ظل التحولات الجذرية التي شهدتها قطاع العدالة عقب جائحة كورونا واعتماد مشاريع العدالة الرقمية والتقاضي الإلكتروني.

استخدمت الدراسة المنهج الوصفي التحليلي من خلال استعراض الإطار القانوني والتقني لمشروعات التحول الرقمي في المحاكم المصرية، وتحليل القوانين ذات الصلة مثل قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، وقانون حماية البيانات الشخصية رقم 151 لسنة 2020، بالإضافة إلى دراسة البنية المؤسسية للأمن السيبراني في القطاع العدلي.

أظهرت النتائج أن نجاح التحول الرقمي في المجال القضائي يعتمد على فاعلية منظومة الأمن السيبراني، ومدى تكامل التشريعات مع البنية التقنية والتنظيمية للجهات العدلية، كما تبين أن ضعف التنسيق المؤسسي وغياب الوعي الأمني لدى بعض العاملين يشكلان تحدياً أمام تحقيق منظومة عدالة إلكترونية آمنة ومستدامة.

وأوصت الدراسة بضرورة تعزيز الإطار التشريعي والتنظيمي للأمن السيبراني في القطاع العدلي، وتكثيف برامج التدريب والتوعية للعاملين، وإنشاء مراكز سيبرانية متخصصة لحماية الأنظمة القضائية، وتطوير

آليات المراقبة والاستجابة السريعة للهجمات الرقمية، مع الاستمرار في دعم القيادة السياسية لمشروعات العدالة الرقمية لتحقيق العدالة الناجزة والمؤمنة إلكترونياً.

دراسة (فتوح، 2021)

هدفت الدراسة إلى التعرف على أثر الأمن السيبراني بأبعاده (البعد التقني، البعد التنظيمي، البعد القانوني، والبعد التوعوي) على تعزيز كفاءة النظام المصرفي العربي، وذلك من خلال تحليل واقع الأمن السيبراني في المصارف والمؤسسات المالية بالمنطقة العربية ومدى التزامها بالمعايير العالمية لحماية البنى التحتية للمعلومات.

استخدمت الدراسة المنهج الوصفي التحليلي، من خلال استعراض الجهود الإقليمية والدولية لتطوير السياسات والإجراءات الخاصة بالأمن السيبراني، ودراسة مبادرات المصارف العربية في تبني نظم الحماية والتأمين الرقمي.

أظهرت النتائج أن تعزيز الأمن السيبراني يعد شرطاً أساسياً لتحقيق الشمول المالي والتنمية الاقتصادية والاجتماعية المستدامة، وأن تطوير الأطر القانونية والتشريعية، وتبادل الخبرات بين الدول العربية، وتكثيف الوعي المؤسسي بالأمن الرقمي من العوامل الحاسمة في حماية الأنظمة المصرفية من المخاطر السيبرانية.

وأوصت الدراسة بضرورة تبني استراتيجيات عربية موحدة للأمن السيبراني في القطاع المصرفي، وإنشاء مراكز إقليمية لمراقبة التهديدات الإلكترونية، وتحديث التشريعات الخاصة بمؤسسات الدفع الإلكتروني، وتعزيز التدريب المستمر للعاملين في المصارف لضمان جاهزيتهم في مواجهة الهجمات السيبرانية.

دراسة (الشورة، 2024)

هدفت الدراسة إلى التعرف على درجة وعي المعلمين بالأمن السيبراني بأبعاده (الإدراك المفاهيمي، ودور الإدارة المدرسية في نشر ثقافة الأمن السيبراني، والمعوقات التي تحد من نشر الثقافة السيبرانية) في المدارس الأردنية من وجهة نظر المعلمين.

استخدمت الدراسة المنهج الوصفي التحليلي، من خلال توزيع استبانة مكونة من (28) فقرة على عينة بلغت (809) معلماً ومعلمة تم اختيارهم بطريقة عشوائية طبقية من مدارس مديرية تربية لواء القويسمة خلال الفصل الدراسي الأول من العام الدراسي 2021/2022.

أظهرت النتائج أن درجة إدراك المعلمين بمفاهيم الأمن السيبراني كانت مرتفعة، في حين جاء دور الإدارة المدرسية في نشر ثقافة الأمن السيبراني بدرجة متوسطة، كما تبين وجود عدة معوقات تحد من نشر هذه الثقافة في المدارس الأردنية. كما لم تظهر فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) في درجة الوعي بالأمن السيبراني تُعزى لمتغيرات الجنس، أو التخصص الأكاديمي، أو عدد سنوات الخبرة. وأوصت الدراسة بصياغة خطط مدرسية لنشر الوعي بالأمن السيبراني، واستمرار التحذير من المخاطر والتهديدات السيبرانية، وتنفيذ برامج تدريبية منتظمة للمعلمين والطلبة لرفع مستوى الوعي والإجراءات الوقائية ضد الانتهاكات السيبرانية.

دراسة (الحمر، 2022)

هدفت الدراسة إلى التعرف على أثر جودة العلاقة مع العميل عبر الإنترنت بأبعادها (الثقة عبر الإنترنت، الالتزام عبر الإنترنت، الرضا عبر الإنترنت) على الولاء الإلكتروني في الخدمات البنكية عبر الإنترنت. استخدمت الدراسة المنهج الوصفي التحليلي لقياس طبيعة العلاقة بين المتغيرات.

وتوصلت النتائج إلى وجود تأثير دال إحصائياً لجودة العلاقة مع العميل عبر الإنترنت بأبعادها مجتمعة على الولاء الإلكتروني، كما تبين أن أبعاد الرضا والالتزام عبر الإنترنت كانا الأكثر تأثيراً في تعزيز الولاء الإلكتروني للعملاء في الخدمات البنكية الإلكترونية.

وأوصت الدراسة بضرورة تعزيز مستوى الرضا والالتزام والثقة عبر الإنترنت من خلال تحسين تجربة العميل الرقمية، وتبني سياسات شفافة وتفاعلية لزيادة الثقة، وضمان استمرارية العلاقة الإيجابية بين البنوك وعملائها عبر المنصات الإلكترونية.

دراسة (عبدالفتاح، 2022)

هدفت الدراسة إلى التعرف على الفعالية الاجتماعية لرقمنة الخدمات المصرفية بأبعادها (سهولة الوصول إلى الخدمات، سرعة إنجاز المعاملات، الأمان والسرية، ورضا العملاء) وانعكاساتها على المستفيدين في البنوك الحكومية المصرية، وبخاصة البنك الأهلي وبنك مصر.

استخدمت الدراسة المنهج الوصفي التحليلي معتمدةً على المقابلات المتعمقة وأداة الملاحظة لجمع البيانات من عينة من العملاء في محافظتي القاهرة والجيزة.

أظهرت النتائج أن رقمنة الخدمات المصرفية أسهمت في تحسين جودة الخدمة، وتوفير الوقت والجهد، وزيادة القدرة التنافسية للبنوك الحكومية، كما عززت من الاستثمار الرقمي والمدخرات نتيجة سهولة السحب والإيداع وإدارة الحسابات إلكترونياً. ومع ذلك، كشفت الدراسة عن تحديات رئيسية تمثلت في ضعف البنية التحتية ونقص الوعي التكنولوجي لدى بعض العملاء.

وأوصت الدراسة بضرورة تعزيز الثقة الرقمية بين البنوك والعملاء، وتكثيف برامج التوعية والتدريب، وتطوير آليات مراقبة أداء الخدمات الرقمية، وتحديث أنظمة الأمان السيبراني، والاعتماد على تقنيات التسويق الرقمي لتعزيز العلاقة مع العملاء وتحسين تجربتهم المصرفية الإلكترونية

دراسة (فؤاد و عراقات ،2021)

هدفت الدراسة إلى التعرف على الفعالية الاجتماعية لرقمنة الخدمات المصرفية بأبعادها (سهولة الوصول إلى الخدمات المصرفية، سرعة إنجاز المعاملات البنكية، الأمان والسرية المعلوماتية، ورضا العملاء) وانعكاساتها على المستفيدين في البنوك الحكومية المصرية، وبخاصة البنك الأهلي المصري وبنك مصر.

استخدمت الدراسة المنهج الوصفي التحليلي معتمدةً على المقابلات المتعمقة وأداة الملاحظة لجمع البيانات من عينة من العملاء في محافظتي القاهرة والجيزة.

وتوصلت النتائج إلى أن رقمنة الخدمات المصرفية أسهمت في تعزيز كفاءة العمل المصرفي، وتيسير الوصول إلى الحسابات، وتوفير الوقت والجهد، وزيادة القدرة التنافسية للبنوك الحكومية، كما أدت إلى ارتفاع مستوى الاستثمار الرقمي والمدخرات نتيجة سهولة السحب والإيداع إلكترونياً. ومع ذلك، كشفت الدراسة عن وجود تحديات تتعلق بضعف البنية التحتية التقنية ونقص الوعي التكنولوجي لدى بعض العملاء.

وأوصت الدراسة بضرورة تعزيز الثقة بين البنوك والعملاء عبر تحسين سرعة الاستجابة للخدمات الرقمية، وتدريب وتأهيل الكوادر البشرية، وتطوير أنظمة الأمان السيبراني، وتنفيذ حملات توعية لرفع الثقافة المصرفية الإلكترونية، إلى جانب الاستفادة من تقنيات التسويق الرقمي لتعزيز العلاقة مع العملاء وتحقيق رضاهم.

دراسة (Sebihi et al., 2024)

هدفت الدراسة إلى التعرف على العوامل المؤثرة في سلوك المستهلك المصري تجاه استخدام المحافظ الإلكترونية بأبعادها (الثقة والأمان، جودة الخدمة، سهولة الاستخدام، الوعي المالي، والدعم التقني)، والتعرف على أسباب مقاومة انتشار خدمات الدفع الإلكتروني في المجتمع المصري رغم التوجه العالمي نحو تقليل الاعتماد على النقد.

اعتمدت الدراسة على المنهج الوصفي التحليلي، واستخدمت المقابلات الشخصية والمكالمات الهاتفية لجمع البيانات من عينة مكونة من 48 مديراً تنفيذياً وقادة فرق في البنوك الحكومية والخاصة، و62 فرداً من فئات عمرية مختلفة.

أظهرت النتائج أن الثقة والأمان وجودة الخدمة يمثلان العاملين الأكثر تأثيراً في قبول العملاء للمحافظ الإلكترونية، وأن الفئة العمرية من 20 إلى 40 عاماً هي الأكثر استخداماً لخدمات الدفع الإلكتروني. كما تبين أن الخوف من الأخطاء في المعاملات، وصعوبة استرداد الأموال، وضعف تغطية شبكات الهاتف، ونقص الوعي التكنولوجي تعد من أبرز معوقات انتشار المحافظ الإلكترونية.

وأوصت الدراسة بضرورة تنفيذ حملات توعية منظمة لتعزيز الثقة بخدمات الدفع الإلكتروني، وتبسيط تطبيقات المحافظ الإلكترونية لتناسب جميع الفئات، وتدريب موظفي الدعم الفني في البنوك على حل مشكلات العملاء بسرعة، إضافة إلى إطلاق برامج تحفيزية وبرامج ولاء لزيادة الإقبال على استخدام المحافظ الإلكترونية في المجتمع المصري.

دراسة (Hira et al., 2025)

هدفت الدراسة إلى التعرف على أثر الأمن السيبراني بأبعاده (سرية المعلومات، سلامة النظام، الموثوقية، والخصوصية) على ثقة العملاء في الخدمات المصرفية الإلكترونية في قطاع البنوك بدولة الإمارات العربية المتحدة.

استخدمت الدراسة المنهج الوصفي التحليلي من خلال استبانة ميدانية وبيانات تم جمعها من موظفين في مصرفين رئيسيين بهدف تحليل العوامل المؤثرة في إدراك العملاء لمستوى الأمن السيبراني وعلاقته بثقتهم في المعاملات البنكية عبر الإنترنت.

وتوصلت النتائج إلى وجود علاقة طردية قوية ومعنوية بين إدراك الأمن السيبراني ومستوى ثقة العملاء في الخدمات المصرفية الإلكترونية، مما يؤكد أن تحسين إجراءات الأمان والخصوصية يساهم في تعزيز ثقة العملاء واستدامة تعاملهم مع القنوات الرقمية.

وأوصت الدراسة بضرورة تعزيز البنية التحتية للأمن السيبراني في المصارف الإماراتية، وتطوير استراتيجيات استباقية لمواجهة التهديدات الإلكترونية، وتكثيف برامج التوعية الرقمية، وتبني أفضل الممارسات العالمية في أمن المعلومات بما يعزز الثقة المتبادلة بين المصارف والعملاء، ويدعم تنافسية القطاع المالي محلياً وعالمياً.

دراسة (Khoiriah et al., 2024)

هدفت الدراسة إلى التعرف على أثر مخاطر الأمن السيبراني بأبعاده (الأداء المالي، السمعة المؤسسية، وثقة العملاء) على أداء البنوك في القطاع المصرفي الخاص بمدينة فيصل آباد - باكستان، إضافة إلى تحديد أبرز المخاطر السيبرانية التي تواجه البنوك في ظل التحول الرقمي.

استخدمت الدراسة المنهج الكمي التحليلي بالاعتماد على استبيان موجه إلى عينة مكونة من (121) مستخدماً للبنوك الخاصة، مع تطبيق تحليل الارتباط والانحدار لقياس أثر المخاطر واستراتيجيات التخفيف منها.

وتوصلت النتائج إلى أن مخاطر الأمن السيبراني تؤثر سلباً على الأداء المالي والسمعة المؤسسية للبنوك، لكنها في الوقت ذاته تدفع نحو تبني استراتيجيات فعالة للتخفيف من هذه المخاطر، مثل استخدام تقنيات التشفير وجدران الحماية وأنظمة كشف التسلل والمصادقة الثنائية، إلى جانب تدريب الموظفين وإجراء تقييمات دورية لنقاط الضعف. كما تبين أن تطبيق استراتيجيات التخفيف يساهم إيجاباً في تحسين الأداء المالي وزيادة ثقة العملاء، خصوصاً لدى الفئات الشابة الأكثر وعياً بالتقنيات.

وأوصت الدراسة بضرورة تعزيز التعاون بين البنوك وشركات التكنولوجيا المالية والجهات التنظيمية لوضع استجابات تكاملية ضد التهديدات السيبرانية، وتبني أطر حماية مرنة تراعي التحديات التقنية والديموغرافية في الاقتصادات النامية.

دراسة (Waliullah et al., 2025)

هدفت الدراسة إلى التعرف على أثر التهديدات السيبرانية بأبعادها (التصيد الإلكتروني، البرمجيات الخبيثة، برامج الفدية، اختراق البيانات، والوصول غير المصرح به) على أمن الخدمات المصرفية الرقمية وتبنيها والامتثال التنظيمي لها، وذلك في ضوء التحول الرقمي المتسارع في القطاع المصرفي العالمي خلال الفترة (2015-2024م).

استخدمت الدراسة المنهج الوصفي التحليلي مع تطبيق أسلوب المراجعة المنهجية وفق نموذج PRISMA لتحليل (78) دراسة أكاديمية محكمة تناولت العلاقة بين التهديدات السيبرانية وأمن المعاملات المصرفية الرقمية.

وتوصلت النتائج إلى أن هجمات التصيد والبرمجيات الخبيثة تُعدّ أكثر التهديدات شيوعاً وتؤدي إلى خسائر مالية كبيرة وتراجع ثقة العملاء، في حين أن استخدام التحقق المتعدد العوامل (MFA) وأنظمة الأمان البيومترية أسهما في الحد من الوصول غير المصرح به. كما أظهرت الدراسة أن تقنيات الذكاء الاصطناعي للكشف عن الاحتيال وتقنية البلوك تشين تمثل حلولاً واعدة لتعزيز أمن المعاملات. وأشارت النتائج إلى أن تكامل تطبيقات التكنولوجيا المالية (FinTech) يرفع مستوى المخاطر الأمنية، مما يتطلب رقابة تنظيمية أكثر صرامة وتحديثاً مستمراً للبنية التحتية للأمن السيبراني. كما بينت أن الامتثال للوائح الدولية مثل (GDPR)، PSD2، (GLBA) يعزز أمن المصارف الرقمية من خلال تطبيق إجراءات مصادقة مشددة وبروتوكولات تشفير ورقابة لحظية لعمليات الاحتيال. وأوصت الدراسة بضرورة تبني استراتيجية أمنية متعددة المستويات تشمل التشفير المتقدم، والذكاء الاصطناعي في رصد الاحتيال، وتأمين المعاملات عبر البلوك تشين، إلى جانب أطر تنظيمية قوية تضمن استدامة الثقة والأمان في البيئة المصرفية الرقمية.

الفجوة البحثية:

تشير مراجعة الدراسات السابقة إلى اتفاق واسع حول أهمية الأمن السيبراني كعامل رئيسي في تعزيز الثقة في البيئة الرقمية، حيث أكدت أغلب الدراسات مثل (Hira et al., 2025) و(جربوعه وبوطمين، 2023) أن سرية المعلومات وسلامة النظام والخصوصية تشكل الأساس في بناء ثقة العملاء في الخدمات البنكية الإلكترونية. ومع ذلك، ركزت تلك الدراسات على بيئات مصرفية خارج السعودية مثل الإمارات والعراق والجزائر، ما يبرز الحاجة إلى دراسة ميدانية في السياق السعودي الذي يتميز ببيئة مصرفية رقمية متقدمة وتوسع متسارع في الخدمات الإلكترونية ضمن رؤية المملكة 2030.

كما اتفقت الدراسات السابقة على أن الأمن السيبراني لا يُعد قضية تقنية فحسب، بل له أبعاد تنظيمية وبشرية وتشريعية تؤثر في ثقة العملاء، وهو ما أشار إليه (فتوح، 2021) و(عباس وآخرون، 2023). غير أن تلك الدراسات لم تتناول بعمق الجانب السلوكي والنفسي المرتبط بإدراك العملاء لمستوى الأمان الرقمي، ولم تقم بقياس العلاقة التجريبية بين الأمان السيبراني والثقة باستخدام أدوات كمية ميدانية في القطاع المصرفي السعودي.

ركزت بعض الدراسات مثل (Khoiriah et al., 2024) و(Waliullah et al., 2025) على المخاطر السيبرانية وتأثيرها على الأداء المالي والسمعة المؤسسية، دون تحليل مباشر لتأثيرها على ثقة العملاء كعنصر نفسي وسلوكي يحدد استمرارية تعاملهم مع الخدمات البنكية الإلكترونية. وهذا ما يجعل الدراسة الحالية أكثر تخصصاً في استكشاف أثر الأمن السيبراني بأبعاده المتعددة على ثقة العملاء تحديداً، وليس على الجوانب التشغيلية أو الإدارية للبنوك.

تختلف الدراسة الحالية أيضاً عن الدراسات السابقة في نطاقها الجغرافي والميداني؛ إذ تُجرى على المصارف السعودية التي تتبنى سياسات أمنية رقمية متقدمة مقارنة بالعديد من الدول العربية الأخرى، مما يمنحها قيمة تطبيقية واقعية يمكن أن تسهم في صياغة سياسات محلية قائمة على الأدلة والبيانات. كما تمتاز باستخدامها للمنهج الكمي التحليلي القائم على الاستبيان الميداني الذي يقيس إدراك العملاء الفعلي لمستوى الأمان السيبراني وتأثيره على ثقتهم.

بناءً على ذلك، تتبع الفجوة البحثية من غياب دراسات ميدانية سعودية متخصصة تربط بين أبعاد الأمن السيبراني الأربعة (السرية، سلامة النظام، الموثوقية، الخصوصية) ومستوى ثقة العملاء في المعاملات البنكية الإلكترونية بشكل مباشر، باستخدام نموذج إحصائي تحليلي يختبر الأثر الحقيقي للعوامل التقنية على الثقة الرقمية في البيئة المصرفية السعودية.

المنطلقات النظرية للدراسة:

يُعد الأمن السيبراني من أهم الركائز في البيئة المصرفية الحديثة، إذ يُمثل الإطار الذي يحمي المعلومات البنكية وبيانات العملاء من المخاطر الإلكترونية، بما في ذلك محاولات الاختراق أو التلاعب بالمعاملات الرقمية. ومع التحول المتسارع نحو الخدمات البنكية الإلكترونية في المملكة العربية السعودية، أصبح الحفاظ على أمن المعلومات ليس مجرد مسألة تقنية، بل عاملاً أساسياً لبناء الثقة بين المصارف والعملاء. وقد أكدت دراسات عديدة أن المؤسسات التي تستثمر في البنية التحتية للأمن السيبراني تحقق مستويات أعلى من الثقة والولاء من قبل العملاء، مما ينعكس إيجاباً على استدامة الخدمات الإلكترونية (الشمري، 2020).

يمثل الأمن السيبراني في السياق البنكي نظاماً متكاملًا من السياسات والتقنيات والإجراءات التي تهدف إلى حماية سرية وسلامة وتوافر المعلومات المالية. ويتضمن ذلك جوانب متعددة مثل سياسات الحماية الإلكترونية، والتدريب والتوعية الأمنية، ومراقبة التهديدات والاستجابة للحوادث، والتقييم المستمر للمخاطر. وتشير الدراسات إلى أن تكامل هذه الأبعاد يُعد مؤشراً رئيسياً على فعالية النظام الأمني المصرفي، وأن ضعف أي بُعد منها يؤدي إلى انخفاض مستوى الثقة لدى العملاء (الأنصاري، 2021).

تُظهر الأدبيات الحديثة أن **الثقة الرقمية (Digital Trust)** أصبحت عاملاً استراتيجياً في نجاح القنوات البنكية الإلكترونية، إذ يتوقف تبني العملاء لها على مدى إحساسهم بالأمان أثناء تنفيذ المعاملات المالية. فكلما شعر العميل أن بياناته ومعلوماته المصرفية محمية، ازدادت رغبته في استخدام الخدمات الإلكترونية. وأكدت دراسة **Safa et al. (2019)** أن وجود سياسات أمنية واضحة وتدابير استجابة فعالة للحوادث الإلكترونية يساهم في رفع مستوى الثقة الرقمية في المؤسسات المالية.

كما تبين أن سياسات الحماية الإلكترونية تمثل خط الدفاع الأول ضد التهديدات السيبرانية، وتشمل أنظمة التشفير والمصادقة والتحقق الثنائي وإدارة كلمات المرور، وغيرها من الممارسات التقنية التي تضمن أمان العمليات البنكية عبر الإنترنت. وأكدت دراسة (Alharthi (2022 أن تطبيق مثل هذه السياسات في المصارف السعودية يعزز الثقة المؤسسية ويقلل من خوف العملاء من تسرب بياناتهم المالية، خاصة في ظل تزايد حجم الهجمات الإلكترونية في القطاع المصرفي المحلي.

إلى جانب ذلك، فإن التدريب والتوعية الأمنية يمثلان بعداً بشرياً مكملاً للبنية التقنية، حيث أظهرت دراسات متعددة أن العامل البشري هو الحلقة الأضعف في منظومة الأمن السيبراني إذا لم يتم تأهيله. وأوضحت دراسة (Safa et al. (2019 أن تدريب الموظفين والعاملين على أساليب كشف الاحتيال والاستجابة الفورية للمخاطر يزيد من فعالية الحماية ويعزز ثقة العملاء الذين يشعرون بأن البنك يمتلك قدرات بشرية مؤهلة لمواجهة التهديدات. كما أن توعية العملاء أنفسهم بمخاطر الاحتيال الإلكتروني ترفع من مستوى الأمن العام وتدعم شعورهم بالثقة في التعاملات البنكية الرقمية (الأنصاري، 2021).

أما مراقبة التهديدات والاستجابة للحوادث فهي عملية مستمرة تهدف إلى الكشف المبكر عن محاولات الاختراق والتعامل معها فوراً قبل أن تؤثر على الأنظمة المصرفية. وأشارت دراسة (Alqahtani & Kavakli (2021 إلى أن المؤسسات التي تمتلك مراكز مراقبة إلكترونية تعمل على مدار الساعة وتصدر تقارير استجابة فورية، تحافظ على مستويات عالية من الثقة حتى في حال وقوع الهجمات، لأن العملاء يدركون أن المؤسسة قادرة على السيطرة السريعة واستعادة النظام دون خسائر.

كذلك، فإن التقييم المستمر للمخاطر يمثل بعداً وقائياً يضمن للمصارف تقييم جاهزيتها الأمنية بشكل دوري وتحليل الثغرات المحتملة قبل أن تُستغل من قبل المهاجمين. وقد بينت دراسة (Alghamdi (2020 أن المؤسسات التي تتبنى آليات تقييم دورية لمخاطر الأمن السيبراني تكون أكثر قدرة على تعزيز ثقة عملائها، إذ يشعر المستخدم بأن المصرف يتعامل استباقياً مع التهديدات قبل وقوعها.

من جهة أخرى، ترتبط ثقة العملاء في الخدمات البنكية الإلكترونية بعدة أبعاد رئيسية هي: المصادقية، والأمان المدرك، وسرية البيانات، والاستجابة السريعة. وقد أوضحت دراسة (Gefen et al. (2003 أن الأمان المدرك يمثل المحرك الأساسي لتكوين الثقة الرقمية، وأن وجود نظام أمني موثوق يرفع من نية العميل للاستمرار في استخدام القنوات البنكية الإلكترونية. كما أظهرت دراسة (Alotaibi (2021

أن الثقة الرقمية هي حلقة الوصل بين جودة البنية التحتية للأمن السيبراني ورضا العملاء في البيئة المصرفية السعودية.

ويشير عدد من الدراسات إلى أن الشفافية المؤسسية في إدارة الحوادث الأمنية تلعب دوراً مهماً في استعادة ثقة العملاء عند تعرض البنك لأي اختراق. فالمؤسسات التي تتعامل بصراحة وتصدر بيانات توضيحية لعملائها تكسب احترامهم وثقتهم على المدى الطويل، في حين أن التعتيم الإعلامي يؤدي إلى نتائج عكسية. وقد دعمت نتائج (Alqahtani & Kavakli, 2021) هذا الاتجاه موضحة أن سرعة التواصل مع العملاء بعد أي حادث أمني تقلل من تأثير الأزمة على الثقة المؤسسية.

وفي السياق السعودي، تُظهر بيانات البنك المركزي السعودي (SAMA, 2023) أن البنوك المحلية تتعرض لمحاولات اختراق متزايدة سنوياً، إلا أن التطور في أنظمة الدفاع السيبراني والتزام المصارف بمعايير الأمن العالمية مثل ISO 27001 ساهم في الحفاظ على استقرار الثقة العامة بالنظام المصرفي الإلكتروني. ويؤكد التقرير أن بناء الثقة الرقمية لم يعد وظيفة العلاقات العامة فقط، بل أصبح مؤشراً رئيسياً في تقييم كفاءة الأمن السيبراني لدى المؤسسات المالية. (SAMA, 2023)

وتؤكد الأدبيات الحديثة أن العلاقة بين الأمن السيبراني وثقة العملاء ليست مباشرة فقط، بل تتأثر بعوامل وسيطة مثل جودة الخدمة الإلكترونية والسمعة الرقمية للمؤسسة. فحتى لو كان النظام مؤمناً تقنياً، فإن تجربة المستخدم السيئة أو بطء الاستجابة قد تضعف الثقة. وفي المقابل، يمكن لخدمة إلكترونية سلسة وشفافة أن تزيد ثقة العملاء حتى في وجود تهديدات محدودة. وقد أثبتت دراسة Alshammari & Alghamdi (2022) أن جودة التجربة الرقمية تشكل الوسيط الأقوى بين الأمن السيبراني والثقة في الخدمات البنكية عبر الإنترنت.

ختاماً، يمكن القول إن الأمن السيبراني لم يعد مجرد أداة تقنية لحماية الأنظمة البنكية، بل أصبح عنصراً استراتيجياً في بناء الثقة المؤسسية واستدامة العلاقات مع العملاء. ويتطلب هذا التكامل بين الأبعاد التقنية (مثل التشفير والمراقبة والتقييم) والأبعاد البشرية والتنظيمية (مثل التدريب والشفافية والثقافة الأمنية). لذا، تهدف هذه الدراسة إلى تحليل الأثر الفعلي لممارسات الأمن السيبراني بأبعادها المختلفة على مستوى ثقة العملاء في المعاملات البنكية الإلكترونية في المصارف السعودية، استناداً إلى الأدلة النظرية والتطبيقية الحديثة في المجال (الشمري، 2020؛ Safa et al., 2019؛ Alharthi, 2022؛ Alqahtani & Kavakli, 2021).

المنهجية وطرق البحث:

اعتمدت الدراسة على المنهج الوصفي التحليلي بوصفه الأنسب لطبيعة البحث الذي يهدف إلى تحليل أثر ممارسات الأمن السيبراني بأبعادها المختلفة على ثقة العملاء في المعاملات البنكية الإلكترونية. يقوم هذا المنهج على جمع البيانات من واقع الميدان وتحليلها إحصائيًا بهدف وصف الظاهرة المدروسة وتفسير العلاقة بين متغيراتها، بما يسمح باستخلاص النتائج العلمية الدقيقة وتعميمها على مجتمع الدراسة (الخالدي، 2020).

يتيح المنهج الوصفي التحليلي للباحث إمكانية تحديد درجة ممارسة البنوك السعودية لمتغيرات الأمن السيبراني من جهة، ومستوى ثقة العملاء من جهة أخرى، ثم دراسة العلاقة السببية بينهما باستخدام أدوات التحليل الإحصائي المناسبة، وبذلك يجمع بين الوصف الكمي والتحليل التفسيري (العبيدي، 2019).

ثانياً: مجتمع الدراسة

سيكوّن مجتمع الدراسة من جميع عملاء المصارف السعودية الذين سيستخدمون الخدمات البنكية الإلكترونية عبر المواقع الرسمية أو تطبيقات الهاتف المحمول. ووفقاً لتقارير البنك المركزي السعودي (SAMA, 2024)، من المتوقع أن يتجاوز عدد عملاء الخدمات البنكية الإلكترونية 22.4 مليون عميل نشط، أي ما يعادل أكثر من 85% من إجمالي العملاء في النظام المصرفي السعودي. وسيمثل هذا المجتمع محور الدراسة نظراً لارتباطه المباشر بموضوع الأمن السيبراني والثقة في المعاملات البنكية الإلكترونية، إذ سيُعد العملاء المستخدمون فعلياً للخدمات الرقمية الفئة الأكثر تأثراً بمستوى الحماية الإلكترونية وفعالية الإجراءات الأمنية المتبعة في المصارف السعودية.

ثالثاً: عينة الدراسة

سيتم اختيار عينة عشوائية بسيطة من عملاء المصارف السعودية بهدف تمثيل المجتمع تمثيلاً علمياً دقيقاً. ومن المتوقع أن يبلغ حجم العينة 176 مفردة، وهو حجم مناسب من الناحية الإحصائية وفقاً لمعادلة Krejcie & Morgan (1970) لتحديد العينات من المجتمعات الكبيرة، مما يضمن مستوى ثقة يبلغ 95% وهامش خطأ $\pm 5\%$. وسيتم توزيع الاستبانة إلكترونياً على عملاء عدد من البنوك السعودية الكبرى مثل الراجحي، الأهلي السعودي، الإنماء، الرياض، والبلاد، لضمان تنوع المشاركين واختلاف مستويات تعاملهم مع الأنظمة البنكية الإلكترونية. كما يُتوقع أن تتنوع خصائص أفراد العينة من حيث الجنس، العمر، ومستوى التعليم، بما يعكس واقع العملاء المستخدمين للخدمات البنكية الرقمية في المملكة، ويُسهّم في الوصول إلى نتائج دقيقة حول أثر الأمن السيبراني على ثقة العملاء في المعاملات البنكية الإلكترونية..

رابعاً: أداة الدراسة

ستعتمد الدراسة على الاستبانة كأداة رئيسة لجمع البيانات من أفراد العينة، وذلك لملاءمتها لطبيعة الدراسة التي تهدف إلى قياس أثر الأمن السيبراني بأبعاده المختلفة على ثقة العملاء في المعاملات البنكية الإلكترونية.

سيتم إعداد الاستبانة استناداً إلى الإطارين النظري والميداني، وإلى ما ورد في الدراسات السابقة ذات الصلة بموضوع الأمن السيبراني والثقة الرقمية في البيئة المصرفية. وستتكون الاستبانة من جزأين رئيسيين: الجزء الأول: يتضمن البيانات العامة للمبحوثين مثل الجنس، العمر، المستوى التعليمي، مدة التعامل مع الخدمات البنكية الإلكترونية، ونوع البنك الذي يتعامل معه العميل.

الجزء الثاني: يضم فقرات قياس متغيرات الدراسة، حيث سيُقسم إلى محورين أساسيين:

المتغير المستقل (الأمن السيبراني) بأبعاده:

- سياسات الحماية الإلكترونية.

- التدريب والتوعية الأمنية.
 - مراقبة التهديدات والاستجابة للحوادث.
 - التقييم المستمر للمخاطر.
- ويُتوقع أن يحتوي كل بُعد على أربع فقرات تُقاس باستخدام مقياس ليكرت الخماسي (من 1 = لا أوافق بشدة إلى 5 = أوافق بشدة).

المتغير التابع (ثقة العملاء في المعاملات البنكية الإلكترونية) بأبعاده:

- الأمان المدرك.
 - المصداقية والشفافية.
 - سلامة العمليات البنكية الإلكترونية.
 - الرضا والثقة المؤسسية.
- وسيُخصص لكل بُعد مجموعة من الفقرات التي تُعبّر عن مدى إدراك العميل لمستوى الثقة في الخدمات البنكية الإلكترونية المقدمة له.

وسيتّم عرض الاستبانة على مجموعة من المحكمين الأكاديميين والمتخصصين في مجالي الإدارة والمصارف للتأكد من صدقها الظاهري ومناسبتها لأهداف الدراسة. وبعد اعتمادها، ستُجرى دراسة استطلاعية أولية على عينة محدودة (تقدّر بـ 25 مفردة) للتحقق من وضوح العبارات وصدق البناء الداخلي للأداة، ثم سيتم حساب معامل الثبات باستخدام معامل كرونباخ ألفا (Cronbach's Alpha)، حيث ستُعد القيمة المقبولة إحصائيًا عند (0.70) فأعلى مؤشرًا على الاتساق الداخلي الجيد لفقرات الأداة.

الأساليب الإحصائية المستخدمة

سيتم تحليل بيانات الدراسة باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS)، لما يتميز به من دقة وكفاءة في إجراء التحليلات الإحصائية المتقدمة. وستُستخدم مجموعة من الأساليب الإحصائية الوصفية والاستدلالية بما يتناسب مع أهداف الدراسة وطبيعة فرضياتها، وذلك على النحو الآتي:

الأساليب الإحصائية الوصفية:

حساب التكرارات والنسب المئوية لوصف الخصائص الديموغرافية لأفراد العينة.

حساب المتوسطات الحسابية والانحرافات المعيارية لتحديد مستوى استجابات المشاركين لكل فقرة من فقرات الاستبانة، وتحليل اتجاهاتهم نحو متغيرات الدراسة (الأمن السيبراني وثقة العملاء).

الأساليب الإحصائية الاستدلالية:

- اختبار معامل الثبات (كرونباخ ألفا Cronbach's Alpha) للتحقق من درجة الاتساق الداخلي لفقرات الاستبانة.
- معامل الارتباط البسيط (Pearson Correlation) لقياس قوة واتجاه العلاقة بين أبعاد الأمن السيبراني وثقة العملاء في المعاملات البنكية الإلكترونية.
- تحليل الانحدار الخطي المتعدد (Multiple Linear Regression) لاختبار الفرضية الرئيسية المتعلقة بأثر مجمل أبعاد الأمن السيبراني على ثقة العملاء.
- تحليل الانحدار الخطي البسيط (Simple Linear Regression) لاختبار الفرضيات الفرعية الخاصة بكل بعد من أبعاد الأمن السيبراني على حدة.

حدود الدراسة:

- حدود موضوعية: ستتناول الدراسة أثر الأمن السيبراني بأبعاده الأربعة (سياسات الحماية الإلكترونية، التدريب والتوعية الأمنية، مراقبة التهديدات والاستجابة للحوادث، التقييم المستمر للمخاطر) على ثقة العملاء في المعاملات البنكية الإلكترونية بأبعادها.
- حدود مكانية: ستجرى الدراسة ميدانياً في المصارف السعودية التي تقدم خدمات بنكية إلكترونية لعملائها، مثل بنك الراجحي، البنك الأهلي السعودي، بنك الإنماء، بنك الرياض، وبنك البلاد.
- حدود زمانية: سيجري تنفيذ الدراسة خلال العام الأكاديمي 2025م.
- حدود بشرية: ستركز الدراسة على عملاء المصارف السعودية المستخدمين فعلياً للخدمات البنكية الإلكترونية.

المراجع

- البدوي، حبيب. (2024). الحرب الرقمية والأمن السيبراني: خطر التهديدات يقابله تعزيز الدفاعات. مجلة بحوث الإعلام الرقمي، ع3 ، 154 - 180. مسترجع من <http://search.mandumah.com/Record/1497116>
- جربوعة، عادل، و بوطمين، عبد الجبار. (2023). الفضاء الرقمي والأمن السيبراني. مجلة العلوم الإنسانية، مج34، ع3 ، 453 - 464. مسترجع من <http://search.mandumah.com/Record/1418616>
- جعفر، حاتم. (2024). التقاضي الإلكتروني والأمن السيبراني: تحديات وآفاق: دراسة حالة للمحاكم المصرية. مجلة البحوث القانونية والاقتصادية، عدد خاص ، 1372 - 1422. مسترجع من <http://search.mandumah.com/Record/1524267>
- الشورة، خالد سليمان سمحان. (2024). درجة وعي المعلمين بالأمن السيبراني: دراسة ميدانية من وجهة نظر معلمي المدارس الأردنية. مجلة اتحاد الجامعات العربية للبحوث في التعليم العالي، مج44، ع2 ، 415 - 436. مسترجع من <http://search.mandumah.com/Record/1468123>
- عباس، محمد خزعل، و المخزومي، وليد مرزة حمزة. (2023). أمن الفضاء السيبراني: قراءة في المفهوم القانوني. مجلة العلوم القانونية، مج37، عدد خاص ، 1 - 25. مسترجع من <http://search.mandumah.com/Record/1417676>
- عبدالفتاح، نورا سعيد. (2022). رقمنة الخدمات المصرفية وفعاليتها الاجتماعية: دراسة ميدانية. حوليات آداب عين شمس، مج50 ، 231 - 283. مسترجع من <http://search.mandumah.com/Record/1335565>
- فتوح، وسام حسن. (2021). الأمن السيبراني في المنطقة العربية: توعية المصارف والمؤسسات المالية لإتباع المعايير العالمية. مجلة اتحاد المصارف العربية، ع490 ، 5. مسترجع من <http://search.mandumah.com/Record/1312821>
- فؤاد، كريم علاء الدين أحمد، و عراقات، آلاء طارق. (2021). Assessing Resistance to Accept Electronic Wallets in Egypt. مجلة العلوم الاقتصادية والإدارية والقانونية،

مج5، ع18 ، 204 - 224. مسترجع من

<http://search.mandumah.com/Record/1237269>

- قلاع الضروس، سمير. (2022). الأمن السيبراني الوطني: قراءة في أهم الاستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر. مجلة الرواق للدراسات الاجتماعية والإنسانية،

مج8، ع2 ، 249 - 267. مسترجع من

<http://search.mandumah.com/Record/1345992>

- لحمر، حكيمة. (2022). تأثير أبعاد جودة العلاقة عبر الإنترنت على الولاء الإلكتروني للعملاء في الخدمات البنكية: دراسة عينة من عملاء البنوك التجارية في ولاية سكيكدة. دفاتر بوادكس السياسة الصناعية وتنمية المبادلات الخارجية، مج11، ع2 ، 253 - 272. مسترجع من

<http://search.mandumah.com/Record/1349188>

- محارب، عبدالعزيز قاسم. (2023). الذكاء الاصطناعي والأمن السيبراني. مجلة المال والتجارة،

ع653 ، 4 - 23. مسترجع من

<http://search.mandumah.com/Record/1415707>

- Sebihi, A., Naveed, O., Alnaqbi, R., & Banu, S. R. (2024). Empowering Trust: Evaluating Cyber-Security Standards in UAE's Online Banking and Education to Strengthen Consumer Confidence. 1–5. <https://doi.org/10.1109/odicon62106.2024.10797560>
- Hira, M., Hafeez, K., & Yaseen, M. N. J. M. (2025). Impact of Cybersecurity Risks and Mitigation Strategies on Banking Industry. NICE Research Journal, 18(1). <https://doi.org/10.51239/nrjss.v18i1.497>
- Khoiriah, Z., Harahap, M. I., & Yanti, N. (2024). Cybersecurity Impact of Cybercrime in Strengthening Trust In BSI Kc Rantau Prapat. Kontigensi: Jurnal Ilmiah Manajemen, 12(1), 320–331. <https://doi.org/10.56457/jimk.v12i1.559>

- Pengaruh cyber crime terhadap tingkat kepercayaan masyarakat dalam bertransaksi di bank syariah kota pekanbaru. (2024). Jurnal Islamika, 7(01), 75–90. <https://doi.org/10.37859/jsi.v7i01.7713>
- Waliullah, Md., George, M. J., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. 01(01), 226–257. <https://doi.org/10.63125/fh49az18>

Mid Ocean University

College of Management

Master of business administration



**The Impact of Total Quality Management on Operational
Performance:
A Field Study on Food Manufacturing Plants in the Riyadh
Region**

Prepared by:

Supervision:

Dr. Al-Faisal Abdelhamid Mohamed Hassan

Dr. Fayez Jarad

1447-2025